accenture

Global Incident Report: Russia-Ukraine Crisis | April 21

Key Findings

- The Russian military action that began 24 February 2022 against Ukraine has cyber and information-warfare components.
- Residents in Ukraine, Belarus, and Russia have experienced disruptions of essential business and government services, including electricity, transportation, and payments services, and more disruptions will likely occur.
- Hacktivists sympathetic to Ukraine have targeted Russian entities.
- Russian ransomware operators have threatened to attack Western critical infrastructure and leak sensitive stolen data in retribution for perceived attacks on Russia.
- Entities in North Atlantic Treaty Organization (NATO) countries should expect potential disruptive activity and information operations with the goal of eroding popular sentiment and political will aligning with support for Ukraine. Such activity could include criminal ransomware, hacktivist or other disruptive attacks against government or critical infrastructure in NATO countries by threat actors aligning themselves with one side of the conflict or the other.
- Economic sanctions that countries have imposed against Russia could trigger retaliatory cyber threat activities by actors aligning themselves with Russian state interests. The United States (US) White House has warned that increased Russian scanning of US and allied countries' critical infrastructure indicates Russia's government is "exploring the options" for retaliatory attacks.
- Numerous ransomware and distributed denial of service (DDoS) attacks have occurred after countries imposed sanctions on Russia; however, in some cases, only circumstantial evidence ties these to the Russia-Ukraine conflict.
- Publicly known Russian state cyber threat activity in the first weeks of the invasion has been less intense than expected, likely for a variety of reasons ACTI explores below, including the resilience of Ukrainian defenses. However, organizations worldwide should remain vigilant for renewed Russian activity designed for maximum service disruption and psychological impact.

Copyright © 2022 Accenture. All Rights Reserved.

Revelations of a sophisticated 8 April operation intended to cripple the Ukrainian energy grid have led some analysts to assess that a cyberwar has begun.

Summary

After a several-month military buildup on Ukraine's borders, on 24 February 2022, Russian President Vladimir Putin sent Russian troops into Ukraine.[1] The offensive's cyber component has affected parties in multiple locations, including Russia, Ukraine, Belarus, NATO countries, and their allies, and has included familiar patterns of Russian state-sponsored activity, including espionage, disruption, and information operations. However, unpredictable new elements have emerged.

Both sides have recruited volunteer hacktivists to help them, and cyber criminals are increasingly taking one side or the other. The lines among state-sponsored threat actors, hacktivists, and criminals are blurring, leading to a chaotic situation with the potential for dangerous, unintended consequences. Each side seeks to control the information space, both via limiting Internet connectivity and information flows to each other and via cyber-enabled information operations.

Some ransomware, data leaks, and other disruptive activity affecting entities in other countries has occurred, with circumstantial evidence pointing to possible connections to the Russia-Ukraine conflict. In the first weeks of the war, known Russian state cyber threat activity has not reached the level many have expected; however, the potential remains for dramatic cyber attacks intended to demoralize Ukraine or countries supporting Ukraine.

This Global Incident Report is a continuation of the Global Incident Report dated April 14 which provided ongoing updates of cyber threat activity and connectivity-related issues affecting Ukraine and Russia as well as those affecting other countries along with information on pro-Ukrainian and pro-Russian hacktivist activity.

The updated report contains: additional information on the Industroyer2 (CRASHOVERRIDE) malware; the industrial control system (ICS)-focused malware suite PIPEDREAM; wormable malware (here "wormable" refers to malware that can potentially spread in an automatic, self-sustaining way[2]); the apparent return of the REvil ransomware group; and other incidents that appear related to the Russia-Ukraine war, particularly those involving energy and transportation.

MITIGATIONS are available at the end of this report.

Analysis

Cyber-related Events Involving Ukraine, Russia and Belarus

[1] https://www.nytimes.com/2022/02/23/world/europe/putin-announces-a-military-operation-in-ukraine-as-the-un-security-council-pleads-with-him-to-pull-back.html
[2] https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

Copyright © 2022 Accenture. All Rights Reserved.

Residents in Ukraine, Russia and Belarus have experienced communications disruptions that have at times affected other business and government services. These disruptions include likely state-sponsored disruptive and espionage activity, connectivity disruptions related to kinetic military activity, and ordinary criminal activity exploiting the crisis through phishing campaigns and other schemes.

- On 9 March, Cisco Talos warned that threat actors were disguising credential-stealing malware as tools for pro-Ukrainian hacktivism.[3]

- On 9 March, major Ukrainian provider Triolan, based in embattled Kharkiv, suffered a cyber attack when threat actors "reset the settings to the factory level," as one source told Forbes. Another source said Triolan had also undergone a cyber attack on 24 February, the day Russia invaded Ukraine.[4] On 15 March, Triolan reported that it was slowly restoring nodes in affected cities. For example, it had restored nodes in most neighborhoods of Kyiv and restored 629 out of 2,971 nodes in Kharkiv.[5]

- On 10 March, CyberScoop detailed how criminals are posing as fundraisers for Ukraine to steal cryptocurrency.[6]

- On 10 March, Doug Madory of connectivity research firm Kentik reported: "I was told by someone knowledgeable that there was a fiber cut between Kyiv and Fastiv at about 10:00 UTC today degrading a lot of service in/out of the country".[7]

- On 10-12 March, embattled Ukrainian cities, such as Sumy and Chernihiv, experienced periods of Internet outages. Internet Outage Detection and Analysis signals from the United States (US)-based Center for Applied Internet Data Analysis showed Ukraine-wide degradation of Internet access to about 70 percent.[8]

- On 11-12 March, Ukraine's Computer Emergency Response Team (CERT-UA) reported on a phishing campaign with emails that purported to come from Ukrainian government sources and to contain cybersecurity information. However, the lure document links to a malicious website, forkscenter[.]fr, that downloads Cobalt Strike Beacon and the GrimPlant and GraphSteel backdoors. CERT-UA attributes this to a group it calls UAC-0056,[9] which is also tracked as TA471, SaintBear, and Lorec53.[10]

- On 11 March, Quad9, a provider that blocks domain name system lookups to known malicious sites, saw a tenfold increase in Ukrainian systems reaching out to malware command-and-control sites on 9 March.[11]

- On 11 March, Data Center Knowledge described how Ukrainian communications technicians brave dangerous conditions to repair damaged equipment and run Internet cables to underground bomb shelters. Ukrainian intelligence services were relying on "chatbot, email, and secure messaging through WhatsApp, Telegram, and

[3] https://blog.talosintelligence.com/2022/03/threat-advisory-cybercriminals.html
[4] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=58cf1f516573
[5] hxxps://mediasat[.]info/2022/03/15/triolan-prodolzhaet-vosstanavlivat-set-posle-kiberataki-gde-uzhe-dostupen-internet/
[6] https://www.cyberscoop.com/cybercriminals-are-posing-as-ukraine-fundraisers-to-steal-cryptocurrency/
[7] https://twitter.com/DougMadory/status/1502038861584740357
[8] https://twitter.com/OliverLinow/status/1502589239053238272
[9] hxxps://cert.gov[.]ua/article/37704
[10] https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/
[11] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/

Copyright © 2022 Accenture. All Rights Reserved.

Signal" to learn of Russian troop movements.[12]

- On 12 March, Ukrainian cybersecurity officials said they had developed a website, defenseua[.]com, containing resource information for Russian and Belarusian military who refuse to participate in the war.[13]

- On 13 March, NetBlocks reported on a "major Internet disruption" at a network in the Vinnytsia region in Ukraine, with a network staff member reporting a "massive cyber attack with elements of sabotage and theft" and that "a lot of expensive equipment was stolen".[14]

- On 14 March, ESET reported the deployment of a new wiper called CaddyWiper on Ukrainian systems: "Similarly to HermeticWiper deployments, we observed CaddyWiper being deployed via GPO [Group Policy Object], indicating the attackers had prior control of the target's network beforehand." The malware avoids destroying data on domain controllers, probably to retain access.[15]

- On 14 March, CNN reported that Ukrainian Railways executives are relying on Soviet-era closed-circuit phone systems, as they coordinate efforts to keep the trains running. They use the Starlink satellite system that businessman Elon Musk provided, but only briefly because "the satellites make it easier for the enemy to pinpoint their location," according to CNN.[16]

- On 15 March, the Security Service of Ukraine said it had detained an individual who was routing phone calls to facilitate mobile communications among the Russian forces in Ukraine. This suggests there are weaknesses in Russia's secure military communications and might help explain why Russia has not destroyed Ukrainian communications infrastructure more thoroughly. The suspect also allegedly sent text messages to Ukrainian government employees, calling on them to side with Russia.[17]

- On 16 March, SentinelOne provided additional information on a campaign that CERT-UA reported earlier in which emails purporting to come from Ukrainian government sources and to contain cybersecurity information actually link to a malicious website, forkscenter[.]fr, that downloads Cobalt Strike Beacon and the GrimPlant and GraphSteel backdoors. SentinelOne discovered the group using a Python-compiled binary masquerading as a Ukrainian-language translation software, the launching of which leads to GrimPlant and GraphSteel infections. The group behind this, UAC-0056 (a.k.a. SaintBear, UNC2589, TA471), is "believed to be behind the WhisperGate activity in early January 2022," SentinelOne said, although other analysts attribute the WhisperGate activity to a separate group, DEV-0586.[18]

- On 16 March, threat actors published on a Ukrainian tabloid website what media described as an artificial intelligence (AI)-generated "deepfake" video purporting to show Ukrainian President Volodymyr Zelensky encouraging Ukrainians to surrender. On the same day, threat actors breached a Ukrainian TV news broadcast and showed

[12] https://www.datacenterknowledge.com/networks/battle-intensifies-keep-ukraine-online
[13] https://twitter.com/dsszzi/status/1502683855639171083
[14] https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K
[15] https://twitter.com/ESETresearch/status/1503436423818534915
[16] https://www.cnn.com/2022/03/14/europe/ukrainian-railways-war-intl-cmd/index.html
[17] https://www.vice.com/en/article/v7djda/ukraine-arrests-hacker-routing-calls-for-russian-troops
[18] https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/, https://cert.gov.ua/article/37704

Copyright © 2022 Accenture. All Rights Reserved.

similar demoralizing messages on the program's news ticker. Ukrainian officials had warned two weeks ago that pro-Russian actors would likely attempt to create such false messaging.[19]

- In a 16 March briefing, Ukrainian cybersecurity official Viktor Zhora claimed that "enemy hackers" had conducted over 3,000 distributed denial of service (DDoS) attacks against Ukraine in the past month, with the one-day record being 275 and the most powerful exceeding 100 Gbps. Finance, government, and telecommunications organizations were the most-targeted sectors. Nevertheless, Ukrainian communications providers were coping with the attacks and providing services. Zhora also noted that mobile operators had introduced national roaming, which would allow Ukrainians a means of communication even if their own operators' services were temporarily disrupted.[20]

- On 17 March, CERT-UA reported on a phishing campaign using "supply"-themed emails sent to Ukrainian government agencies and infecting victims' computers with the modular malware SPECTR. CERT-UA attributes the campaign to the group UAC-0020 (a.k.a. Vermin), associated with (translated) "so-called security agencies of the so called LNR [the separatist Luhansk 'republic']," according to CERT-UA.[21]

- On 17 March, Ukrainian cybersecurity officials warned users of a spam campaign involving text messages that claimed (translated): "You are credited with PB24 6500 cash assistance" and could infect a user's phone if users clicked the provided link.[22]

- On 17 March, citing two US military officials, the New York Times reported that on one occasion, Ukrainians killed a Russian general after geolocating him based on a conversation he had on an unsecured phone.[23]

- On 17 March, CERT-UA discovered lure documents in the form of ZIP archives with titles purportedly warning about a dangerous virus. When activated, the malware runs the wiper program DoubleZero. CERT-UA tracks the group behind these ZIP files as UAC-0088.[24]
  - On 24 March, Cisco Talos provided additional DoubleZero details and IOCs.[25]

- On 18 March, CERT-UA reported a phishing campaign involving a lure document with a ZIP file containing an LNK shortcut file with VBSCript code that downloads the LoadEdge malware. CERT-UA associates this with the group UAC-0035 (a.k.a. InvisiMole).[26] ACTI assesses this group works closely with hacker group WINTERFLOUNDER (a.k.a. Gamaredon).

- On 19 and 20 March, internet provider Skyline in embattled Kharkiv, Ukraine and provider Volia in Russian-occupied Kherson, Ukraine experienced a "collapse of

[19] https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/, https://www.dailydot.com/debug/hackers-zelensky-deepfake-surrender-ukraine-war
[20] https://24tv.ua/ru/za-misjac-ukrainski-servisi-zaznali-ponad-3-tisjach-ddos-atak_n1908711
[21] https://cert.gov.ua/article/37815
[22] https://twitter.com/dsszzi/status/1504899939322765314
[23] https://www.nytimes.com/2022/03/17/briefing/russia-ukraine-war-kharkiv.html
[24] https://cert.gov.ua/article/38088
[25] https://blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html
[26] https://cert.gov.ua/article/37829

Copyright © 2022 Accenture. All Rights Reserved.

connectivity" associated with power outages, according to NetBlocks.[27] In Kherson, the power cuts come amid protests against Russia's occupation.[28]

- On 22 March, CERT-UA reported on a RAR file purportedly related to documenting Russia's "criminal actions." The file contains an executable file that results in a HeaderTip infection. CERT-UA attributed it to a group they call UAC-0026.[29]

- On 23 March, Russian meat producer Miratorg Agribusiness Holding reported a sabotage attack, which malicious actors carried out using BitLocker to encrypt the company's files. This likely resulted from a supply-chain compromise of the veterinary information system VetIS, which tens of thousands of software systems inside and outside of Russia use. The company said the attack would not affect its meat supplies.[30]

- In a 23 March briefing, Victor Zhora, deputy chief of Ukraine's State Service of Special Communications and Information Protection (SSCIP), made several points about cyber threat activity targeting Ukraine in the week of 15-22 March:
  - CERT-UA had detected 60 cyber attacks against local governments, the financial and energy sectors, security and defense entities, commercial organizations, telecommunications and software companies, and other entities, and that most of the attacks were less serious than attacks earlier in the year and that most had failed to affect critical infrastructure[31];
  - CERT-UA detected 14 malware families or groups attacking Ukrainian systems between 15 and 22 March. Prior versions of this Global Incident Report have covered most of these malware families, including: four types of wipers (HermeticWiper, IsaacWiper, CaddyWiper and Double Zero); HeaderTip, SunSeed, GrimPlant, and GraphSteel; LoadEdge; and MicroBackdoor. The report also mentions APT28 (which ACTI tracks as SNAKEMACKEREL), XDSpy, an Eastern Europe-oriented group, and the threat group TA416;
  - Some of the groups CERT-UA detected have been targeting not just Ukraine but also EU organizations that help refugees.[32] To do so, the hackers "try to obtain data on contacts, bank accounts, goods that are purchased for helping Ukrainians";[33]
  - Some Russian cyber criminals "are refusing offers to attack Ukraine, which is a very important sign"[34]
  - The State Special Communications Service does not coordinate anti-Russian hacktivist activity, which Zhora said was "carried out by volunteers - ordinary Ukrainians who have the appropriate skills".[35]

- On 23 March, Twitter account Shadow Chaser reported a phishing campaign apparently targeting entities in Russia. A screenshot showed an email purportedly sent from a US-sanctioned Russian electronics firm to an employee of the Kaluga

[27] https://twitter.com/netblocks/status/1505308560477073409
[28] https://twitter.com/netblocks/status/1505550245912006659
[29] https://cert.gov.ua/article/38097
[30] https://www.itworldcanada.com/post/top-russian-meat-producer-suffers-cyberattack
[31] https://cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya
[32] https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya
[33] https://cip.gov.ua/en/news/russian-hackers-attack-charity-and-volunteer-organizations
[34] https://cip.gov.ua/en/news/cyberattacks-against-ukraine-are-carried-out-by-russian-military-hackers
[35] https://cip.gov.ua/ua/news/derzhspeczv-yazku-otrimuye-chisleni-propoziciyi-shodo-dopomogi-vid-uryadiv-ta-organizacii-vid-usogo-svitu

Copyright © 2022 Accenture. All Rights Reserved.

Research Institute of Radio Engineering (–ö–ù–Ò–†–¢–Ò) with an attached lure document titled "List of Persons at the Ekran Research Institute Under US Sanctions for Ukraine Invasion"[36]. Once opened, the document supposedly implants cyber espionage software, according to espionage news source The Spy Collection.[37]A 24 March Financial Times article provided more information on cyber threat activity preceding and accompanying the 24 February Russian invasion. The report noted that Ukrenergo, the Ukrainian government-owned power transmission company, noticed a threefold increase in failed attempts to break into its networks in February 2022, compared with the previous February. "One particularly audacious attempt involved a compromised local employee trying to sneak malicious code on to company premises," the article stated. In addition, on February 24, not only did hackers target Viasat, but"some 100 highly skilled hackers from nearly a dozen groups with ties to Russia and Belarus" carried out attacks on IT infrastructure throughout Ukraine, according to National Security and Defense Council deputy secretary Serhii Demediuk, a former Ukrainian cyber police chief. Threat actors also targeted a Ukrainian financial institution on invasion day, and then targeted the same entity with wiper malware on 14 March, the article stated.[38]

- On 24 March, SecurityWeek reported that a security researcher had published a proof of concept for exploiting vulnerabilities in a building control system widely in wide used in Russia for elevators and other building systems. The researcher said threat actors could use default credentials to gain administrator privileges and could also use LUA script plug-ins to take complete control of the more than 100 Internet-connected the Tekon controllers throughout Russia at once. The researcher did not mention the fact that many hacktivists have been carrying out disruptive attacks on Russian targets throughout the war, SecurityWeek noted.[39]

- On 25 March, the Irish Mirror reported that cloud-based cybersecurity company Cyren had identified more than 100,000 fake donation emails originating from all over the globe and purporting to come from Ukraine. They also found fake charity scams on Twitter, Facebook, and YouTube. Most of these scams ask for cryptocurrency donations, according to the Irish Mirror.[40]

- On 28 March, the Ukrainian Security Service announced that since the start of the war, it had shut down five bot farms that had been using over 100,000 inauthentic social media accounts to distribute demoralizing information to Ukrainians. The Service claimed Russian intelligence agencies instigated the operation.[41]

- On 28 March, CERT-UA reported on a phishing campaign involving a lure document purportedly about military losses in Ukraine, the Pseudosteel malware, and the exfiltration of files to an FTP server.[42]

---

[36] https://twitter.com/ShadowChasing1/status/1506596042636083206
[37] https://medium.com/@thespycollection/spy-news-2022-week-12-a94a1d1531d1
[38] https://www.ft.com/content/20544951-2c98-4d47-842d-b34a246a564f
[39] https://www.securityweek.com/over-100-building-controllers-russia-vulnerable-remote-hacker-attacks
[40] https://www.irishmirror.ie/news/what-look-out-cyber-experts-26556320
[41] https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv
[42] https://www.bleepingcomputer.com/news/security/ukraine-dismantles-5-disinformation-bot-farms-seizes-10-000-sim-cards/

Copyright © 2022 Accenture. All Rights Reserved.

- On 28 March, Ukraine's largest fixed-line communications operator, the privately owned Ukrtelecom, reported its services were down nationwide due to a "powerful cyber attack of the enemy." Ukrtelecom's internet service, Facebook and Ukrtelecom's contact center faced disruptions, with connectivity "collapsing to 13% of pre-war levels." The director of NetBlocks told Forbes that the "gradual loss of connectivity" showed the incident was not the result of a physical cable cut or loss of electricity.[43] Within five hours, SSSCIP reported it had "neutralized" the attack and that Ukrtelecom was temporarily restricting services to most private users to free up space for military use. Within 15 hours, Ukrtelecom was restoring connectivity to most users.[44]

- On 29 March, the head of the SSSCIP, Yurii Shchyhol, claimed it was not possible to cut off Ukraine's internet connectivity by cutting fiber optic cables, as the country had worked to build backup fiber-optic networks, although Shchyhol provided few further details.[45]

- On 30 March, CERT-UA warned of a phishing campaign targeting Ukrainian government employees with a lure document purportedly about wage arrears. A macro in the document runs the file "Base-Update.exe," which downloads a bootloader that runs GraphSteel and GrimPlant malware.[46]

- On 30 March, CERT-UA also warned of a phishing campaign targeting Ukrainians with a lure document purportedly from the Education Ministry, with an archived attachment that downloads MarsStealer, a program written in C/ASM and widely available on underground forums, which CERT-UA described as an alternative to Raccoon Stealer. The developers claim the code will not function in former-Soviet countries, but users can easily circumvent this restriction, thus enabling its use against Ukrainian targets, CERT-UA reported.[47]

- On 30 March, Malwarebytes reported on a spearphishing campaign targeting entities in Russia who use virtual private networks (VPNs) and social media platforms that Russian authorities have banned. The Russian-language lure documents in use in the campaign exploit the so-called MSHTML remote-code execution vulnerability (CVE-2021-40444), using a variant exploit called CABLESS and an RTF file instead of a Word document.

    - Researchers have found similarities between the lures the Carbon Spider threat group users.[48] ACTI tracks Carbon Spider as Fin7 and has been exploring its links with the REvil ransomware family. Also, Fin7 has targeted the US defense industry using malicious USB devices in the so-called BadUSB campaign, which is the subject of a US Federal Bureau of Investigation (FBI) warning.[49]

[43] https://forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom
[44] https://venturebeat.com/2022/03/28/ukraine-says-major-cyberattack-against-telecom-has-been-neutralized/
[45] https://cip.gov.ua/ua/news/yurii-shigol-zv-yazok-v-ukrayini-nemozhlivo-vidklyuchiti-perebivshi-kabel
[46] https://cip.gov.ua/ua/news/sproba-vorozhikh-khakeriv-zavdati-podviinogo-udaru
[47] https://cert.gov.ua/article/38606
[48] https://threatpost.com/mshtml-flaw-exploited-to-attack-russian-dissidents/179150/
[49] https://www.cybereason.com/blog/fbi-warns-us-companies-to-avoid-malicious-usb-devices

Copyright © 2022 Accenture. All Rights Reserved.

- On 30 March, DefenseOne reported on a volunteer Ukrainian hacker group called CyberPan Ukraine that work with the Ukrainian military and allegedly receive funding from Israel and the US. They have disrupted GLONASS navigation system signals for Russian field units and are now attempting to disrupt the precision guidance systems of Russian rockets, DefenseOne reported.[50]

- On 29 March, Newlines magazine reported that "Ukraine's IT warriors" and telecom specialists are using hacked telephone databases to track Russian soldiers and conduct psychological operations through WhatsApp messages and audio recordings to dissuade the invaders from staying and fighting.[51]

- On 5 April, CERT-UA reported that threat actors were seeking to obtain user credentials for Telegram accounts, using false error messages claiming that someone had attempted an unauthorized login and sending the user to the malicious domain ohsxy[.]com to "confirm" their credentials. CERT-UA associates this activity with the group UAC-0094.[52]

- On 5 April, Ukrainian cybersecurity official Viktor Zhora and the director of Ukrtelekom gave a briefing on cyber threats, claiming that there had been thrice the number of cyber attacks this year in 2022 with respect to the same period last year. Over half of these attacks were focused on stealing information and spreading malware. In one case, attackers exploited a vulnerability in a document management server to gain access to mailboxes containing the passport details of Ukrtelekom employees. As for the serious Ukrtelecom disruption of 28 March (described elsewhere in this Incident Report), with help from Cisco and Microsoft, the company has restored 95 percent of the damage in less than a day. The speakers said that in some cases, the hackers had loudly announced their activity as "the greatest cyberattack in the whole war," according to dev.ua.[53]

- On 6 April, Cybernews reported a claim that the Main Directorate of Intelligence at the Ministry of Defense of Ukraine (GURMO) had attacked operational technology (OT) in the Russian energy sector.[54] The article claimed GURMO had compromised pipeline pressurization controls at natural gas supplier Gazprom and caused the pipeline to rupture and burst into flame. Cybernews cited several recent pipeline fires or explosions in Russia, implying without proof that Ukrainian cyber threat actors had caused them. Given that this report cites a single source and provides no clear evidence, ACTI urges treating this report with caution until further information emerges.

- Also on 6 April, another incident affecting Gazprom occurred and it too deserves skepticism. On that day, the website of Gazprom oil subsidiary Gazprom Neft showed a statement, purportedly from Gazprom chief Aleksey Miller, criticizing Russia's war effort. Then the site stopped working. A Gazprom Neft statement claimed that the anti-war statement "is not true and cannot be regarded as an official statement of the company's representatives or shareholders," according to a Reuters

[50] https://www.defenseone.com/technology/2022/03/ukrainian-hackers-take-aim-russian-artillery-navigation-signals/363854/
[51] https://newlinesmag.com/reportage/inside-ukraines-psyops-on-russian-and-belarusian-soldiers/
[52] https://cert.gov.ua/article/39253
[53] https://dev.ua/ru/news/recent-cyber-attacks-on-ukraine
[54] https://cybernews.com/cyber-war/ukrainian-hackers-attacked-gazprom-says-expert/

Copyright © 2022 Accenture. All Rights Reserved.

report on the incident.[55] This resembles a similar 2 April 2022 incident this report covered in which the United Aircraft Corporation website briefly showed a statement ostensibly from the company's director, announcing his resignation in protest against Russia's war in Ukraine. On the same day, Russian media reported the director denied resigning and said the false message resulted from a hack. These reports raise the following questions:

- Did Ukrainian hacktivists and/or state hackers breach the company websites and deface them with anti-war messages?
- Did the company chiefs really speak out against the war, making the website shutdowns and publishing of distracting information mere damage-control efforts?

At a time when major Russian company executives are cautiously criticizing the war,[56] various interpretations are possible.

- On 7 April, Microsoft reported on measures it has taken to disrupt operations of the Strontium (a.k.a. SNAKEMACKEREL, APT28) group targeting Ukrainian media and other organizations, as well as US and European foreign-policy-oriented government agencies and think tanks. Microsoft obtained a court order to take down seven domains Strontiumused. Microsoft assessed that Strontium was attempting to "establish long-term access to the systems of its targets, provide tactical support for the physical invasion and exfiltrate sensitive information."[57]

- On 7 April 2022, Facebook's parent company Meta released its quarterly Adversarial Threat Report. It announced it had blocked numerous inauthentic social media accounts targeting Ukrainians, including the following:

  - A Ghostwriter cyber espionage and disinformation campaign that used compromised Ukrainian military personnel accounts to urge Ukraine's army to surrender
  - Accounts associated with the Internet Research Agency, the famous Russian troll farm that posed as a human-rights non-governmental organization (NGO) and published about police violence in the West but subsequently switched to blaming the West and NATO for Russia's attack on Ukraine
  - A network in Russia that falsely accused people in Russia and Ukraine of hate speech in an attempt to force Facebook to disable the accused's accounts
  - A coordinated network of false Ukrainian social media accounts, complete with deepfake profile pictures, that published claims about Ukraine being a failed state
  - A coordinated network of accounts, with deepfake profile pictures, in use to solicit Arabic-speaking journalists and African media outlets to release pro-

[55] https://www.reuters.com/business/energy/russian-oil-company-gazprom-nefts-website-appears-have-been-hacked-2022-04-06/
[56] https://www.ft.com/content/edd298ef-7e19-4bb4-a2d0-76f4295c3240
[57] https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/

Copyright © 2022 Accenture. All Rights Reserved.

Russian stories about Middle Eastern and African politics.[58] Such an operation is consistent with Russian efforts to sway public opinion in Africa, Latin America, India, and other countries outside the West[59] and is likely intended to garner support for Russia at international forums, such as the United Nations General Assembly (UNGA); potential evidence of this was 58 non-Western countries having abstained from voting at a 7 April UNGA vote on suspending Russia from the Human Rights Council.

- On 7 April, CERT-UA announced a new Gamaredon (a.k.a. Armageddon, WINTERFLOUNDER) phishing campaign in which a lure document purportedly referred to Russian murders and the persecution of Ukrainian prosecutors in occupied territories.[60]

- On 7 April, several pro-Ukrainian social media accounts tweeted, referring to the massacres during the Russian occupation of the Kyiv suburb of Bucha: "In #Bucha, russians worked according to pre-prepared lists. They were looking for veterans of ATO, law enforcement agencies, owners of hunting weapons. The order was to liquidate when found. Where did they get all the lists with names and addresses - this is a question!".[61] A possible answer appears in a report the UK's Royal United Services Institute (RUSI) wrote before the invasion. Citing Ukrainian military and intelligence officers, the report said that the 9th Directorate of the Russian FSB planned and rehearsed special operations to establish control after a planned takeover of Ukraine. The 9th Directorate identified likely supporters and resisters with help from a car registration database that Russian cyber threat actors had stolen during the January 2022 WhisperGate campaign.[62]

- On 12 April, ESET and CERT-UA reported that Russian military hacker group Sandworm (which ACTI tracks as SANDFISH) had targeted a Ukrainian energy entity using a new version of the Industroyer (a.k.a. CRASHOVERRIDE) malware, which the group used to cause a blackout in Ukraine in December 2016.[63] According to the report, the threat actors breached the target in February 2022, compiled the Industroyer2 executable attack on 23 March, and intended to launch it on 8 April. "The attack used ICS-capable malware and regular disk wipers for Windows, Linux, and Solaris operating systems," ESET reported. Industroyer2, the new version of the malware, uses the IEC-104 protocol to communicate with protection relays and other industrial equipment in electrical substations. Sandworm also used the recently discovered CaddyWiper malware, likely to slow recovery and wipe evidence of Industroyer use. The threat actors additionally used malware that ESET identified as ORCSHRED, AWFULSHRED, and SOLOSHRED.[64] Analyst Joe Slowik noted the Sandworm threat actors' use of Impacket for Industroyer2 overlaps with HermeticWiper activity this SITREP covered earlier.[65] Slowik also found a filename in the Industroyer2 code that overlaps with the 2015 Ukrainian blackout the SANDFISH

[58] https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf
[59] https://www.aspistrategist.org.au/russia-may-be-winning-the-ukraine-information-war-outside-the-west/
[60] https://cert.gov.ua/article/39386
[61] https://twitter.com/EuromaidanPR/status/1512011047644938240
[62] https://static.rusi.org/special-report-202202-ukraine-web.pdf
[63] https://cert.gov.ua/article/39518
[64] https://welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/; https://cert.gov.ua/article/39518
[65] https://twitter.com/jfslowik/status/1514029219117891584

Copyright © 2022 Accenture. All Rights Reserved.

group allegedly carried out.[66]

- If it had been successful, the Industroyer2 attack could have cut power to the over two million people the utility serves, a Ukrainian official said.[67] However, Ukrainian cyber security official Victor Zhora the threat actors intended "to shut down a number of high-voltage electrical substations, destroy the computers running WindowsOS, destroy the workstation infrastructure and Linux-operated servers, [and] infect network equipment" and that they partially succeeded: "a part of the IT infrastructure had already been affected by the time we intervened," according to his agency's 13 April Twitter thread.[68] Zhora's public statement may have disguised the true extent of damage. The MIT Technology Review cited what it described as a private report that the CERT-UA "shared with international partners in recent weeks." That document describes "at least two successful attack attempts," with one of those attempts having begun on March 19, a few days after Ukraine tried to end its dependence on Russia by joining Europe's power grid. The document also said Russian hackers had successfully disabled nine electric substations, at least temporarily.[69]

- Faced with evidence of sustained and repeated use of wipers and other malware targeting operational technology in key areas, such as the energy sector, some analysts who previously avoided applying the term "cyberwar" to Russian activity have begun to do so.[70]

- Of particular note in ESET's report on the Industroyer2 malware it found on the network of the target company is the presence of a worm coupled with a wiper designed for systems running Linux and Solaris.[71] The worm, called sc.sh and written in Bash, adds a scheduled task (cron job) to launch the wiper component at a certain time. The script looks for secure shell (SSH) servers on TCP ports 22, 2468, 24687, and 522, then tries to log in using credentials from a list hardcoded in the malware. Many industrial systems use default credentials. If a hardcoded list includes widely used default credentials, the sc.sh worm could spread widely within an organization. Depending on what networks the compromised systems belong to, this worm could potentially spread beyond the utility for which it was customized. This SITREP has noted that if threat actors used wormable malware, even in a targeted way, it could cause enormous collateral damage, as WannaCry and Not Petya did in 2017.

On 14 April, CERT-UA warned of cyberattacks on Ukrainian state agencies using the IcedID malware. They said Ukrainian citizens were receiving Excel spreadsheets with the filename "Mobilization Register.xls". These contain a malicious macro that, if activated, downloads an EXE file that decrypts and runs the GzipLoader malware, which turn delivers IcedID, a banking Trojan that can steal authentication data.[72]

---

[66] https://twitter.com/jfslowik/status/1513896501625327617
[67] https://arstechnica.com/information-technology/2022/04/russias-sandworm-hackers-attempted-a-third-blackout-in-ukraine/
[68] https://twitter.com/dsszzi/status/1514202610068246534
[69] https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/
[70] https://twitter.com/ILDannyMoore/status/1513842172679933952?cxt=HHwWgMC-ye7bn4IqAAAA
[71] https://welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
[72] https://cert.gov.ua/article/39609

Copyright © 2022 Accenture. All Rights Reserved.

- On 14 April, CERT-UA warned of attacks on Ukrainian state agencies exploiting the cross-site scripting vulnerability in the Zimbra Collaboration Suite (CVE-2018-6882). Lure emails with a subject line about medals for Ukrainian soldiers contained JavaScript code that forwards the victim's emails to a third party.[73]

- On 14 April, Group-IB reported that a Russian mining company was among the victims of a ransomware attack by the OldGremlin group, which includes at least some members who write fluently in Russian. The threat actors used lure documents about sanctions and Visa and Mastercard bans. Their tools include a backdoor called TinyFluff, which is a variant of TinyNode.[74]

- On 17 April, Belarus-based cryptocurrency exchange currency.com announced it had repelled a DDoS attack on 12 April, the same day it announced it was ceasing operations for Russian residents.[75] On 17 April, a user on the cryptocurrency discussion forum bitcointalk denounced cryptocurrency exchanges, such as currency.com, that were putting restrictions on Russian users.[76]

- On 18 April, CERT-UA warned that cyber criminals were distributing phishing emails with lures regarding Ukraine's defense of the Azovstal factory in Mariyupol. The email subject lines read 'Urgent! Unblocking Azovstal Terminovo! Unblocking Azovstal' and the attached document contains a macro-enabled XLS document that, when activated, installs Cobalt Strike Beacon.[77]

- On 19 April, Malwarebytes analyst Hossein Jazi reported on a malicious document that claims to advertise a job at Saudi Aramco but instead delivers a Trojan. Jazi notes the Russian-language lure document "seems it's a targeted attack against Russian speaking people"[78], but the perpetrators and motive remain unclear.

- On 20 April, Symantec released a report summarizing trends in Gamaredon (a.k.a. WINTERFLOUNDER) activity against Ukrainian targets, noting that threat actors use multiple variants of the same malware (backdoor.Pterodo), each communicating with a different C2 server, apparently as a way of persisting in victim computers.[79]

Pro-Ukrainian and Pro-Russian Hacktivist Activities

The Ukrainian government has welcomed help from cyber volunteers and supported several initiatives: the "IT Army of Ukraine" to help protect Ukrainian systems and disable Russian websites; the "Cyber Front," to share information on vulnerabilities in Russian cyber defenses; and the "Internet Forces of Ukraine" to get realistic information to Russian citizens who are blocked from receiving it. These and other pro-Ukrainian hacktivist groups, posting on social media in association with the amorphous hacktivist

[73] https://cert.gov.ua/article/39606
[74] https://www.bleepingcomputer.com/news/security/oldgremlin-ransomware-deploys-new-malware-on-russian-mining-org/
[75] https://finance.yahoo.com/news/currency-com-evades-russian-ddos-103535200.html
[76] https://bitcointalk.org/index.php?topic=5394956.0
[77] https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-na-derzhavni-organizaciyi-ukrayini-kiberzlovmisniki-vikoristovuyut-temu-mariupolskoyi-azovstali
[78] https://twitter.com/h2jazi/status/1516443236264521740
[79] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine

Copyright © 2022 Accenture. All Rights Reserved.

collective Anonymous, have claimed to have breached numerous Russian websites and cyber assets.

Pro-Russian hacktivist groups have also claimed attacks on Ukrainian systems. The Twitter account @Cyberknow20 keeps a regularly updated chart of cyber threat groups on both sides. The latest edition, which @Cyberknow20 published on 11 April, listed 50 pro-Ukrainian groups and 20 pro-Russian ones.[80]

- On 10 March, transparency website DDoSecrets published 340,000 files of data that a hacker claimed to have stolen from a regional office of Russia's Internet watchdog, Roskomnadzor, as an act of information warfare.[81]

- On 10 March, pro-Ukrainian hacktivist group Network Battalion 65 (NB65) leaked what it claimed was source code from Russian-owned Kaspersky Lab; however, many commentators pointed out that the data was easily available and not the result of a breach.[82]

- On 11 March, NB65 acknowledged that its Kaspersky Lab leak had been merely a "troll" and promised they "will only be sharing legit drops from here on out." The group then offered leaked emails from a regional institute of the Russian Academy of Sciences.[83] On 1 March, NB65 had also claimed it would leak data from Roscosmos, the Russian state space agency.[84]

- On 11 March, Russian defense firm Rostec (Russian Technologies) shut down its website briefly after what it described as a DDoS attack by "Ukrainian extremists".[85]

- On 11 March, Russian telecom company Rostelecom's cybersecurity arm reported that between 1 and 10 March malicious actors had attacked Russian sites, having launched 1,100 DDoS attacks, primarily targeting the sites of government entities and secondarily targeting those of financial services providers and other businesses that Western countries have sanctioned, according to Reuters.[86]

- On 11 March, Russia's National Coordination Centre for Computer Incidents (NKTsKI) warned of mass cyber attacks on web apps in Russia, including via JavaScript libraries, CSS frameworks, and plug-ins.[87]

- On 12 March, the BBC reported that a Norwegian citizen had set up a spam website to send 22 million emails condemning the war to Russian email addresses.[88]

- On 13 March, #LeakTheAnalyst claimed it would release sensitive US military research data from research organization SRI International.[89] On 14 March, the same entity announced it was leaking information of job candidates for the UK Defense Ministry on its victim list.[90] The veracity of this claim is unclear.

---

[80] https://twitter.com/Cyberknow20/status/1513499727328804865
[81] https://www.forbes.com/sites/thomasbrewster/2022/03/10/dddosecrets-in-the-russia-ukraine-information-war-promises-a-huge-leak-of-data-stolen-from-the-kremlins-internet-censor
[82] https://twitter.com/S0ufi4n3/status/1501851883882921987
[83] http://web.archive.org/web/20220313070149/
[84] https://twitter.com/YourAnonTV/status/1498792639877074945
[85] https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/ and https://www.hackread.com/anonymous-hacks-roskomnadzor-russia-agency/
[86] https://www.reuters.com/article/ukraine-crisis-russia-hack-idCNL5N2VE4EU
[87] hxxps://www.securitylab[.]ru/news/530582.php
[88] https://www.bbc.com/news/technology-60697261
[89] https://twitter.com/S0ufi4n3/status/1503057681506095105/photo/1
[90] https://twitter.com/darktracer_int/status/1503783785555940864

Copyright © 2022 Accenture. All Rights Reserved.

- As of late March 2022, LeakTheAnalyst remains highly active and continues to leak sensitive data. This entity has targeted Western and Ukrainian entities and does not feature any Russian organizations on its leak site; this suggests the entity is aligned with Russia, despite not stating a political motive.

- On 13 March, German officials reported that Anonymous-linked hackers had claimed to have stolen 20 terabytes of data from the German branch of Russian state oil company Rosneft. The company reportedly took its systems offline temporarily but Der Spiegel published that (translated): "this should not restrict the operation of the pipelines and refineries".[91]

- On 14 March, Polish programming group @squad3o3 announced that its website, which it designed as a "voice of freedom" to allow anyone to spam random Russian entities with phone messages and emails[92], had sent over 20 million messages.[93]

- On 14 March, Twitter account @IAmMrGrey2 claimed to have stolen records from "the hospital exclusively treating Putin" and called on others to explore the stolen data for Putin's medical records.[94]

- On 14 March, Ukrainian media reported that Ukraine's amateur "IT Army" had reached 300,000 members.[95]

- On 15 March, the pro-Russian Xaknet team tweeted it would use "the most sophisticated methods" to target critical information infrastructure in Ukraine until they ceased hacker attacks against Russia: "we call on the fascists to accept their defeat in cyber warfare".[96]

- On 15 March, cloud-focused cybersecurity company Aqua reported on its research on cloud-based how-to guides and tool repositories for hacktivist attacks. About 40 percent of hacktivist packages in use related to DDoS attacks, while other hacktivist packages focused on blocking user networks from the conflict area. The researchers also saw defacement banners and sources connected with doxing (i.e., releasing personal information about a victim). Analyzing lists of suggested targets, they found 84 percent of the targets were associated with Russia-based IP addresses and only 16 percent with Ukraine-based addresses, suggesting that pro-Ukrainian, anti-Russian hacktivists were more active on these cloud repositories than pro-Russian ones.[97]

- On 15 March, the developer of the node-ipc networking tool released a "protestware" module called "peacenotwar" that came bundled with some versions of node-ipc and that overwrote Russia- and Belarus-based computer files with a heart emoji. Some GitHub users reacted negatively to the module release. According to Vice News: one wrote "You're a stain on the FOSS [free and open source software] community"; another one wrote: "You just destroyed your work, career and probably your online

[91] https://www.spiegel.de/netzwelt/web/bundeskriminalamt-ermittelt-hackerangriff-auf-rosneft-deutschland-a-74e3a53a-e747-4500-8198-ea6780a7d79a
[92] https://twitter.com/AnonymousVideo/status/1503484842809438208
[93] https://twitter.com/squad3o3/status/1503428370306113536
[94] https://twitter.com/IAmMrGrey2/status/1503396245477502980
[95] hxxps://tech.segodnya[.]ua/tech/v-ukrainskoy-kiberarmii-uzhe-300-tysyach-chelovek-kak-tuda-popast-i-chem-oni-zanimayutsya-1608837.html
[96] https://twitter.com/Cyberknow20/status/1503699552989167617
[97] https://blog.aquasec.com/cloud-native-attacks-russia-ukraine

Copyright © 2022 Accenture. All Rights Reserved.

life".[98]

- To guard Russian users against such "protestware," Sberbank urged Russians to turn off automatic software updates, according to Russian cybersecurity company Positive Technologies.[99]

- On 16 March, cybersecurity researcher Jeremiah Fowler reported that pro-Ukrainian hacktivist groups identifying with Anonymous have "proven to be a very capable group that has penetrated some high value targets, records and databases in the Russian Federation." Analyzing non-password-protected cloud-based datasets hosted on IP addresses in Russia, Fowler found the following:[100]

  - In many cases, hacktivists had deleted files and then defaced databases with phrases like "Glory to Ukraine" or "putin stop this war."

  - They have used a script similar to the MeowBot wiper. They claimed to have disrupted targets including state oil company Gazprom, multiple state media outlets, and the control center of the Russian Space Agency.

  - The hacktivists have accessed numerous databases containing sensitive personal data and secret keys. Depending on what the hacktivists do with this information, threat actors could use it in further cyber threat activity.

- As of 17 March, Russian websites that had experienced disruptions included the Ministry for Emergency Situations[101] and the Kremlin.[102] Leak victims include Russian state pipeline company Transneft.[103]

- From 19 to 21 March, pro-Ukrainian hacktivists claimed to have disrupted access to the city of Grodno, Belarus[104] and to Russian government targets, including:

  - The Ministry of Foreign Affairs[105]
  - The backend of the Foreign Intelligence Service's secure drop site on the TOR anonymity service[106]
  - The government of the Voronezh region[107]
  - The Vologda Research Center of the Russian Academy of Sciences[108]
  - The Joint Institute of Nuclear Research[109]
  - Russian weather agency Roshydromet[110]
  - A Russian defense contractor[111]

[98] https://www.vice.com/en/article/dypeek/open-source-sabotage-node-ipc-wipe-russia-belraus-computers
[99] https://twitter.com/iiyonite/status/1505122185886810114
[100] https://www.websiteplanet.com/blog/cyberwarfare-ukraine-anonymous/
[101] hxxps://www.kommersant[.]ru/doc/5259896
[102] https://twitter.com/YourAnonNews/status/1504104835242725379
[103] https://twitter.com/MikaelThalen/status/1504317329550704643
[104] https://twitter.com/_Blue_hornet/status/1505460977550118913
[105] https://twitter.com/BeeHiveCyberSec/status/1505264447106867201
[106] https://twitter.com/_Blue_hornet/status/1505162369223307264
[107] https://twitter.com/_Blue_hornet/status/1505173866469117955
[108] https://twitter.com/_Blue_hornet/status/1505616461582188544
[109] https://twitter.com/_Blue_hornet/status/1505183938544914433
[110] https://twitter.com/S0ufi4n3/status/1505945517557231620
[111] https://twitter.com/AlvieriD/status/1505569186457669633

Copyright © 2022 Accenture. All Rights Reserved.

- On 20 March, the BlueHornet | AgainstTheWest group (@Blue_hornet), referring to the expected Russian blockage of YouTube, announced: “Our team will be working on an open-source software to bypass this block for regular citizens to use”.[112]

- On 20 March, the BlueHornet | AgainstTheWest group also said it would leak a short list of high-ranking officers—"Plant managers, contracting officers, Program Managers etc.”—of the Nestlé company,[113] which has faced criticism for continuing to do business in Russia.[114]

  - On 23 March, Nestlé said the data Anonymous leaked online was not secret information but rather some test data that Nestlé itself had accidentally leaked earlier. Nestlé also said it would stop selling certain products in Russia.[115]
  - On 30 March, the BlueHornet | AgainstTheWest group tweeted: "Starbucks has been breached yet again. Until Nestlé fully leave Russia, this will continue. P.S - Alibaba Cloud and it's [sic] customer data is being sorted out and will be posted on http://breached.co in due time. #FreeUkraine".[116]

- On 20 March, Anonymous tweeted: “We call on all companies that continue to operate in Russia by paying taxes to the budget of the Kremlin's criminal regime: Pull out of Russia! We give you 48 hours to reflect and withdraw from Russia or else you will be under our target!”.[117]
  - On 24 March, Anonymous-affiliated groups claimed to have taken down the following websites of companies that continue to operate in Russia: auchan[.]ru, leroymerlin[.]ru, and decathlon[.]ru.[118] Both pro-Ukrainian and pro-Russian groups choose targets based on the so-called "Yale list" (so named because a Yale professor created it[119] of companies that have either pulled out of Russia or stayed in the country.

- On 20 March, Belarusian opposition media source Nexta tweeted that someone had breached the official group page of VK (VKontakte), a social media outlet popular in Russia, on the VKontakte platform, and published a manifesto denouncing Russia’s invasion of Ukraine. It also warned that (translated) “VKontakte is breached. All personal data, posts, and communications of users have been downloaded and transferred to competent agencies. Any message you write expressing support of the Russian occupiers, or with the letter “Z” in your avatar, will be interpreted as a crime without a statute of limitations. Then you will be declared wanted by Interpol and arrested in any country of the world”.[120] The Russian-language text was full of misspellings as well as diacritical marks vaguely resembling those of the Czech language. The document might be a satire, spoof, or false-flag incident.

- On 21 March, someone allegedly affiliated with Anonymous tweeted: “#DoomSec will be leaking some very juicy intel. I want to allow the Ukrainian military a chance to

[112] https://web.archive.org/web/20220320132156/https://twitter.com/_Blue_hornet/status/1505534912044179457
[113] https://twitter.com/_Blue_hornet/status/1505641356026429442
[114] https://fortune.com/2022/03/18/nestle-russia-boycott-denys-shmyhal-tweet-mark-schneider/
[115] https://www.theregister.com/2022/03/23/nestle_russia_anonymous/
[116] https://twitter.com/_Blue_hornet/status/1509023279209721861
[117] https://twitter.com/YourAnonTV/status/1505679705797713927
[118] https://twitter.com/YourAnonTV/status/1506776596157370369?cxt=HHwWgsConZfVkukpAAAA
[119] https://www.cnbc.com/2022/03/09/ukraine-war-news-us-companies-on-yale-list-suspend-russia-business.html
[120] https://twitter.com/nexta_tv/status/1505613701436559366

Copyright © 2022 Accenture. All Rights Reserved.

look it all over - I think the coordinates may be quite helpful to them".[121] The #DoomSec activists have also leaked what they claim is information on Russian military communications.[122]

- On 21 March, International Business Times in Australia reported that an Anonymous-affiliated group said it had hijacked printers in Russia to print over 100,000 copies of "anti-propaganda and tor installation instructions".[123] Based on a screenshot of the Russian-language manifesto, ACTI assesses the authors are not native Russian speakers, though the writing errors are not as obvious as those in the alleged VKontakte defacement described above.

- On 23 March, Balkan Insight reported that hackers breached the website of Croatian daily Slobodna Dalmacija and replaced its older articles with pro-Russian propaganda.[124]

- On 24 March, Anonymous-affiliated hackers claimed to have breached the Central Bank of Russia and claimed it would release 35,000 stolen documents containing "secret agreements" within 48 hours of the breach.[125]

    - On 25 March, Anonymous-linked hackers published 28 GB of data they allegedly stole from the Central Bank of Russia; this data included internal data on bank agreements, correspondence, money transfers, overseas agents, and trading partners. The transparency activist group DDoSecrets also posted the data.[126] DDoSecrets' co-founder tweeted, "Russian speakers should organize (while taking proper steps for OPSEC and anonymity, when needed!) to help sort and translate all the leaked material coming out".[127] However, Russian state media agency RIA Novosti said it analyzed the "leaked" data and found it all predated 2018 and was publicly available on the Central Bank's site.[128]

- On 25 March, pro-Ukrainian hacktivist group Network Battalion 65 claimed to have breached the All-Russian State Television and Radio Broadcasting Company (VGTRK) and that it would release 870 GB of data.[129]

- On 26 March, the pro-Russian Killnet group reportedly threatened cyber attacks on the Polish government if Poland were to introduce peacekeepers into Ukraine. Killnet claimed to have carried out a warning attack on the National Bank of Poland.[130] In early March, Killnet had launched a "KillNet Botnet DDoS" service.[131]

- On 27 March, Anonymous-affiliated Twitter account @DepaixPorteur tweeted, "We have created a new site to host our upcoming leaks + future Anonymous leaks. We also hacked Rostproekt emails as a treat to celebrate the new site & to hold you over

[121] https://twitter.com/DeepNetAnon/status/1505815819611123712
[122] https://twitter.com/hashtag/DoomSec
[123] https://www.ibtimes.com.au/anonymous-strikes-russia-printer-attack-disrupts-kremlins-propaganda-1802456
[124] https://balkaninsight.com/2022/03/23/hackers-attack-croatian-daily-post-kremlin-propaganda/
[125] https://twitter.com/YourAnonTV/status/1506769001040551937
[126] https://twitter.com/YourAnonTV/status/1507427538745896966
[127] https://twitter.com/NatSecGeek/status/1508122259927539713
[128] hxxps://ria[.]ru/20220328/khakery-1780504316.html
[129] https://twitter.com/xxNB65/status/1507456443385266179
[130] hxxps://newizv[.]ru/news/society/26-03-2022/hakery-killnet-predupredili-polshu-o-posledstviyah-vvoda-mirotvortsev-v-ukrainu
[131] https://blog.checkpoint.com/2022/03/03/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/

Copyright © 2022 Accenture. All Rights Reserved.

while waiting for the upcoming dump(s)," according to Security Affairs.[132] A screenshot showed the name of the new leak site: anonymousleaks[.]xyz. Another screenshot showed that data from Rostproekt, a Russian construction company, had also appeared on the DDoSecrets transparency website. Security Affairs also reported, DDoSecrets additionally published data that Anonymous-affiliated hacktivists claimed to have stolen from Mashoil, a Russian petroleum services company. International Business Times reporters said they had conversed with Anonymous actors, who had "hinted that 'one guy did say he might've found malware sent to FSB [Federal Security Service of the Russian Federation] agents'".[133]

- On 28 March, Ukraine's main military investigative service published a list titled "FSB Employees Participating in Criminal Activity of the Aggressor Country in Europe" and subtitled "List of FSB Employees Registered at the address ul. Bolshaya Lubyanka, Moscow" (hxxps://gur.gov[.]ua/content/sotrudnyky-fsb-rossyy-uchastvuiushchye-v-prestupnoi-deiatelnosty-stranyahressora-na-terrytoryy-evropy.html). It is unclear whether the list of 620 people came from proprietary sources or publicly available address books. The title appears to align with the theme of a recent Financial Times article about a rise in Russian spying activity in Europe.[134] Hacktivists or law enforcement agencies in various countries could potentially use the published personal information to target these FSB employees.

- On 28 March, Bleeping Computer reported that pro-Russian actors are inserting malware into secretly compromised WordPress sites, which then causes the browsers of site visitors to conduct DDoS attacks against pro-Ukrainian websites. Conversely, at least one pro-Ukrainian site is openly using visitors' browsers to conduct DDoS attacks against Russian websites.[135]

- According to a 29 March article by Russian state news agency RIA Novosti, Russia's Foreign Ministry described the hacktivist activities against Russia as a "cyberwar" that the US and its allies initiated, complete with "cyber-mercenaries" whose activities "often border on open terrorism."[136] The article claimed that US- and NATO-trained Ukrainian special cyber forces are attacking Russia, as are "anonymous hackers and provocateurs, acting on orders from the Western overseers of the Kyiv regime."

- On 29 March, a denial of service attack took down the website of Bradley International Airport in the US state of Connecticut; however, the incident did not affect airport operations, according to media reports. The reports cited the service CyberKnow, which provides situational awareness notices, as attributing the attack to the Killnet group and said the hackers had left behind a message saying (translated): "when the supply of weapons to Ukraine stops, attacks on the information structure of your country will instantly stop....America, no one is afraid of you".[137]

[132] https://securityaffairs.co/wordpress/129576/hacktivism/anonymous-huge-data-dump.html
[133] https://www.ibtimes.com/anonymous-starts-huge-data-dump-will-blow-russia-away-leaks-rostproekt-emails-3452789
[134] https://www.ft.com/content/bd74a542-3ce3-44de-a93a-36dc5929912b
[135] https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/
[136] hxxps://ria[.]ru/20220329/kiberoperatsiya-1780638325.html
[137] https://www.newsweek.com/us-airport-hit-cyberattack-over-ukraine-no-one-afraid-you-1692903

Copyright © 2022 Accenture. All Rights Reserved.

- On 30 March, Le Monde published an investigation of massive troll farms that spread pro-Russian propaganda and disinformation to French-speaking audiences.[138]

- On 30 March, a subdomain of a Facebook page for the Democratic Party of the US displayed the defacement message "Hacked by TurkishHacktivist RootAyyldiz" and a message criticizing US and Turkish involvement in "provoking Russia" by supporting Ukraine.[139] The group name, a variant of the more-famous RootAyyildiz, raises the possibility that this operation is a spoof or false flag.

- On 31 March, CyberKnow20 reported that the pro-Russian Xaknet team declared its support for Russia and referred to Ukrainians as "fascists" and "Nazis". Xaknet claimed to have begun leaking documents from the Ukrainian Foreign Ministry.[140] A screenshot on the anti-malware[.]ru site shows a document from a Ukrainian agricultural agency, rather than from the Foreign Ministry.[141] On 1 April, cybersecurity researcher Catalin Cimpanu noted that various threat actors using the name Xaknet had been active for years, selling malware and other services, and that someone claiming to represent Xaknet had also posted a retirement message, thus calling into question who Xaknet is and what kind of threat they represent.[142]

- On 30 March, pro-Russian group Killnet posted the following on its Telegram channel[143]:

  - "Weather forecast for the next three days in United States of America [sic].
    - DDoS ATTACK MEDIA
    - CORPORATE NETWORK HACKING
    - PRINTERS BEGIN TO OBEY KILLNET"

- On 1 April 2022, investigations group Bellingcat cited a leak of registration data from the food-delivery site for Yandex Food; Bellingcat said the leaked data could provide insight into the identities and whereabouts of Russian military and security personnel.[144]

- On 1 April, the prolific hacktivist BlueHornet | AgainstTheWest (ATW), calling themselves APT49 tweeted: "Oh boy. Can't wait to drop all of these at once, included with the APT28 and APT38 documents. We'll call it the APT FILES." They then showed a screenshot of numerous global groups the US FBI has indicted over the years.[145] On 2 April, ATW released a document about APT28 (a.k.a. Fancy Bear), with a screenshot showing contact information for Dmitriy Badin, one of the Russian military hackers the US indicted in 2018. ATW wrote, apparently referring to the FBI: "They needed information, so we supplied it".[146] It is unclear how much of this is genuine, especially because the first post appeared on April Fools' Day. On 3 April, ATW claimed: "KILLNET, the Russian 'hacker' group, has been ruined. Document involving one of

[138] https://www.lemonde.fr/les-decodeurs/article/2022/03/30/guerre-en-ukraine-sur-les-reseaux-sociaux-ces-comptes-en-francais-qui-relaient-la-propagande-du-kremlin_6119724_4355770.html
[139] https://web.archive.org/web/20220330130147/https://twitter.com/Cyberknow20/status/1509153701952327680
[140] https://twitter.com/Cyberknow20/status/1509448590413860866
[141] hxxps://www.anti-malware[.]ru/news/2022-03-31-114534/38437
[142] https://twitter.com/campuscodi/status/1509828246204039176
[143] https://t.me/killnet_channel/146
[144] https://www.bellingcat.com/news/rest-of-world/2022/04/01/food-delivery-leak-unmasks-russian-security-agents/
[145] https://twitter.com/_Blue_hornet/status/1509872408701853696
[146] http://twitter.com/_Blue_hornet/status/1510378147040083972

Copyright © 2022 Accenture. All Rights Reserved.

it's [sic] key members has been released in the DoomSec telegram".[147]

- On 1 April, transparency organization DDoSecrets published three sets of leaked documents from the following incidents[148]:
  - Network Battalion 65's (NB65's) hack on Russian state-owned Mosekspertiza, which provides services to Russian businesses; this document set includes 150,000 "emails" (unclear whether this indicates email addresses and/or email messages), 8,200 files, and several hundred gigabytes of databases.
  - Anonymous's hack on Russian law firm Capital Legal Services; this document set includes 200,000 "emails" (unclear whether this indicates email addresses and/or email messages).
  - Anonymous's hack on Russian Orthodox Church; this document set includes 57,500 "emails" (unclear whether this indicates email addresses and/or email messages).
- On 2 April, the website of the United Aircraft Corporation group (a.k.a. Sukhoi) showed a statement ostensibly by the company's director, announcing his resignation in protest against Russia's war in Ukraine. On the same day, Russian media reported that this resignation message is false and that someone had hacked the Sukhoi site to show the message.[149]
- On 3 April, pro-Ukrainian hacktivist group NB65 claimed to have breached Russian pipeline supplier Gazregion. The group claimed to have adapted Conti ransomware to destroy the victim company's files and delete backups. NB65 concluded with a note to the Russian government: "This will stop as soon as you cease all activity in Ukraine".[150]
  - On 9 April, more information emerged on NB65's breach of Gazregion on 3 April 2022; the group claimed to have adapted the Conti ransomware to destroy a victim company's files and delete backups. NB65 concluded with a note to the Russian government: "This will stop as soon as you cease all activity in Ukraine." Bleeping Computer analyzed a sample of the NB65 group's modified Conti code and communicated with NB65, which said the group modifies each sample so existing decryptors will not work. NB65 told Bleeping Computer that none of the victims had yet communicated with NB65. NB65 also said that if it did receive any ransom payments, it would donate the funds to Ukraine, Bleeping Computer reported.[151]
- On 5 April, pro-Ukrainian hacktivist group NB65 claimed to have compromised its first civilian-operated business, Continent Express, the largest travel management

[147] http://twitter.com/_Blue_hornet/status/1510470877548322816
[148] https://twitter.com/NatSecGeek/status/1509920756716740630
[149] https://twitter.com/cyber_etc/status/1510234525678321666
[150] https://twitter.com/xxNB65/status/1510484074070224896
[151] https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

Copyright © 2022 Accenture. All Rights Reserved.

company in Russia.[152]

- On 7 April, the IT Army of Ukraine claimed to have breached and leaked user data from a beta version of Rossgram, the Russian substitute for Instagram.[153]

- On 6 April, pro-Russian Twitter account @RUH4X0R tweeted: "Considering other countries, states etc are getting involved with the hacking against #Russia and have been for a while, we're going to expand to attacking #Ukraine #Poland #Brazil Poland will be effective for a few reasons, Brazil because we have inside members in the Military".[154] In another tweet, the account user added: "Also we're seeing that the US is helping Ukraine as @elonmusk has given internet etc. In this case, we could attack America with Ransomware but we think that's extreme, we'll do some public scares. Let us prep, we've already tested this".[155] In the second tweet, @RUH4X0R posted photos that appeared to come from closed-circuit cameras and to depict police officers and vehicles. @RUH4X0R's intentions and capabilities are unclear.

- On 6 April, YourAnonTV tweeted that hacker group TheBlackRabbitWorld had gained access to a closed-circuit TV (CCTV) system inside the Kremlin. The tweet quoted TheBlackRabbitWorld as saying "We won't stop until we reveal all of your secrets." YourAnonTV's tweet included images that resemble CCTV footage, but the veracity of the claims is unclear.[156]

  - Similarly, on 7 April, the group NB65 claimed to have obtained security camera access.[157]

- On 7 April, transparency group DDoSecrets announced it had posted new documents from hacktivist breaches of Russian entities, including: Petrovsky Fort, a Saint Petersburg office building; Forest, a logging firm; and Aerogas, "an engineering company which specializes in the oil and gas industry".[158]

- On 7 April, pro-Ukrainian hacker group AgainstTheWest claimed to have breached Russian federal employment-related site Rabotut, a Chinese bank, and a China-based Cross-Border Interbank Payment System that presumably could have facilitated Russian sanctions evasions and served as an alternative to SWIFT.

  - On 9 April, AgainstTheWest claimed via Twitter (tweet subsequently deleted) to have breached the main ATM software source code for the People's Bank of China.[159] On 10 April, the group also claimed via Twitter (tweet subsequently deleted) claimed to have breached the China branch of UBS Securities.[160]

- On 10 April, pro-Ukrainian group BanderaHackers claimed to have breached the website of the Russian "Committee for Protection Against Defamation, Discrimination and Harassment on the Internet" (CADDPI); the group posted screenshots purporting

[152] https://twitter.com/xxNB65/status/1511472012925050880
[153] https://twitter.com/iiyonite/status/1512001395255357443
[154] https://twitter.com/RUH4X0R/status/1511664928666624003
[155] https://twitter.com/RUH4X0R/status/1511666561148493824
[156] https://twitter.com/YourAnonTV/status/1511656225687154688
[157] https://twitter.com/xxNB65/status/1512264261594140718
[158] https://ddosecrets.substack.com/p/releases-petrovsky-fort-aerogas-and?s=r
[159] https://web.archive.org/web/20220409183648/https://twitter.com/_Blue_hornet/status/1512862017899667459
[160] http://web.archive.org/web/20220410115606/https://twitter.com/_Blue_hornet/status/1513122336828014595

Copyright © 2022 Accenture. All Rights Reserved.

to show that website defaced with real news of Russian atrocities in Ukraine.[161]

- On 11 April, DDoSecrets posted 446 GB of data from Russia's Ministry of Culture.[162]
- On 18 April, Russian media outlet lenta[.]ru reported that the pro-Russian hacktivist group KillNet had paralyzed the websites of eight Polish airports with DDoS attacks. However, the Twitter account @cyber_etc commented, "for the moment, no disruption has been reported on the sites of these airports".[163]
- On 19 April, transparency site DDoSecrets posted 87,500 emails (107 GB) that Anonymous-affiliated hacktivists had stolen from Russian engineering firm Neocom Geoservice, which provides exploration and drilling support to customers like Gazprom.[164] DDoSecrets also announced a leak of documents from a Russian Defense Ministry-linked construction firm.[165]
- On 20 April, a post on the VK.com social media page of Russia's Ministry of Emergency Situations (MChS) claimed the agency's website had been defaced with tips on how to survive a "a retaliatory nuclear strike" that NATO countries supposedly planned for 24 April (Eastern Orthodox Christian Easter), according to media reports and a cached version of the page.[166] Hackers previously defaced the same agency's website with a message urging Russian soldiers to defect from the army.[167]

Cyber-related Events in Other Countries

Numerous disruptive attacks have occurred in countries outside Russia, Ukraine, and Belarus in the weeks after the invasion and after countries imposed sanctions on Russia. In many of these cases, circumstantial evidence suggests, but does not prove, a possible link to the Russia-Ukraine conflict.

ACTI's database of ransomware incidents—based largely on postings from ransomware actors' data leak sites and insights gained from Accenture Security's CIFR team — showed 105 ransomware incidents between 16 February and 15 March. About these incidents, ACTI notes that:

- The top three attacker groups were Conti (with 39 incidents), LockBit 2.0 (31 incidents), and AlphV (14 incidents).
- The top three industries threat groups have targeted were manufacturing (23 incidents), financial services (12 incidents), and wholesale (11 incidents).
- The top four countries threat actors have targeted were the US (42 incidents), Germany (7 incidents), the UK (6 incidents), and Canada (6 incidents).

The totals represent a decrease from the period of 15 January-15 February, which saw 143 incidents, dominated by LockBit 2.0, which was responsible for 50 incidents.

[161] https://twitter.com/BanderaHackers/status/1513092391301001218
[162] https://twitter.com/NatSecGeek/status/1513594910397669386
[163] https://twitter.com/cyber_etc/status/1516118620857851909/photo/1
[164] https://ddosecrets.com/wiki/Neocom_Geoservice
[165] https://twitter.com/NatSecGeek/status/1516341878450491394
[166] http://securitylab.ru/news/531218.php
[167] https://www.washingtonpost.com/world/2022/03/17/russia-government-hacking-wave-unprecedented/

Copyright © 2022 Accenture. All Rights Reserved.

The business sectors in which the targets reside generally align with those of past financially motivated ransomware activity; most of the named victims do not relate to the Russia-Ukraine conflict in an obvious way, despite some ransomware actors' declarations of support for one side or another.[168]

Specific cyber-related events in countries other than Ukraine, Russia, and Belarus include the following:

- During 6-10 March, Finnish aircraft reported increased GPS jamming near the Russian border.[169] In January, Israeli pilots reported GPS spoofing from the Russian airbase at Khmeimim in Syria.[170]

- On 7 March, Spain's National Intelligence Center (CNI) reported that the Spanish government had intercepted Russian plans to carry out a cyberattack on Spain's State Employment Service (SEPE). The CNI said Russia counted Spain among its main enemies because of Spain's prominence in the NATO presence protecting the Baltic states. SEPE had suffered two cyberattacks in 2021, in which Spanish intelligence suspected Russia. In previous days, the Spanish government had put numerous agencies and sites, including embassies, the Social Security administration, and the Nuclear Security Council on high alert in anticipation of cyber attacks. The Spanish government also ordered public employees to shut down and disconnect devices as a security measure. Other recommendations included shutting down remote computers daily, performing security updates at night, issuing new passwords, exercising caution with emails, minimizing connections to the internet, using secure passwords, and updating all systems.[171]

- As the Global Incident Report published on March 10 mentioned, on 8 March, Germany's Federal Office for Information Security (BSI) intelligence service had warned of the threat of an imminent cyber attack[172] on high-value German targets such as military or energy-related entities.

- On 9 March, the US Cybersecurity and Infrastructure Security Agency (CISA) updated its Conti ransomware alert with indicators of compromise (IOCs) consisting of close to 100 malicious domain names the group uses.[173]

- The Lapsus$ (a.k.a. Lapsus and Lapsu$) extortion gang's Telegram channel, which is also its leak site, features numerous dramatic postings from the second week of March 2022.
  - These postings include the following:

[168] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[169] https://www.gpsworld.com/finnish-airline-finds-gps-interference-near-russian-border/
[170] https://www.middleeastmonitor.com/20220201-russia-refuses-israeli-demand-to-stop-jamming-gps-of-flights-into-tel-aviv/
[171] https://www.abc.es/economia/abci-administracion-pone-alerta-funcionarios-riesgo-ciberataque-202202281200_noticia.html and https://www.elconfidencialdigital.com/articulo/seguridad/alerta-gobierno-indicios-ciberataque-rusia-que-espana-pueda-pagar-millones-parados/20220303135135359167.html
[172] https://www.spiegel.de/netzwelt/warnung-der-bundesregierung-cyberangriff-auf-deutsche-hochwertziele-koennte-schon-bald-starten-a-3d80a9a1-7558-4fd4-873b-070fd6ceec0f
[173] https://www.bleepingcomputer.com/news/security/cisa-updates-conti- ransomware-alert-with-nearly-100-domain-names/

Copyright © 2022 Accenture. All Rights Reserved.

- A 10 March posting seeking to recruit insiders at telecommunications and video game companies.[174]

- An 11 March posting ACTI observed on Lapsus$'s insider chat, in which someone claiming to be a former telecommunications call center employee stated that the company had bad security.

- An 11 March posting seemingly claiming responsibility for the breach of French video game company Ubisoft. The company admitted an incident had temporarily disrupted some games, systems, and services but had apparently not resulted in unauthorized access to players' personal information.[175]

- A 14 March posting that ACTI observed, announcing the winner of a "poll" the Lapsus$ gang had held to choose the next leak victim. The group wrote: "What should we leak next? Vodafone winner. We work to ready the data to leak." They then posted a link to a Telegram channel called "t[.]me/saudechat."

- Additionally, on 8 March, the Lapsus$ group posted on Twitter, seemingly taking credit for that day's disruptions at Spotify and Discord, but deleted the tweet almost immediately, according to researcher Soufiane Tahiri.[176]

- As previously reported, Lapsus$ had leaked Samsung data on 7 March and had breached US-based graphic processor company Nvidia on 28 February. Besides Samsung and Nvidia, Lapsus$ has also breached Brazilian and Portuguese government and media entities, raising questions about the group's origin and motives.[177]

- According to a dox (i.e., a release of personal information) from March 7,[178] at least one Lapsus$ member is a UK-based teenager.

On 10 March, the German corporate network of Japan-based Denso, a supplier of power train systems, hybrid vehicle components, and fuel injectors for multiple automotive companies, detected an unauthorized access.

- On 13 March, extortion group "Pandora" posted a threat to leak 1.4 terabytes worth of data on 16 March. Bleeping Computer reported seeing a sample of leaked Denso data, including purchase orders, emails, and technical schematics (https://www.bleepingcomputer.com/news/security/automotive-giant-denso-hit-by-new-pandora- ransomware-gang/). The Pandora malware is derived from Babuk malware code, which the Pandora developers may have obtained via a September 2021 source code leak.[179]

[174] https://twitter.com/S0ufi4n3/status/1502032449643192325
[175] https://www.msn.com/en-us/entertainment/gaming/ubisoft-says-it-experienced-a-e2-80-98cyber-security-incident-e2-80-99/ar-AAUWMgW
[176] https://twitter.com/S0ufi4n3/status/1501269430025826311
[177] https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/
[178] hxxps://doxbin[.]com/upload/white
[179] https://twitter.com/BleepinComputer/status/1503388889007939586

Copyright © 2022 Accenture. All Rights Reserved.

- Previous attacks on Toyota and Volvo had led to suspicions of connections between the attacks and Japan's and Sweden's support for Ukraine[180].

On 11 March, Ireland's National Cyber Security Center informed the Kerry County Council it had observed "suspicious activity / potential for cyber-attack on our email / IT system arising from traffic from Russian IP Addresses and certain domains / sub-domains," according to The Kerryman.[181]

On 11 March, Bridgestone Americas confirmed it had suffered a ransomware attack. The LockBit ransomware group has indeed leaked data belonging to Bridgestone.[182] LockBit actors had previously vowed to leak data from anti-Russian countries and entities.[183]

On 11 March, Reuters published new information on the crippling of KA-SAT, a European subsidiary of satellite Internet provider Viasat, on 24 February, the day Russia invaded Ukraine.[184] According to Reuters, analysts for the US National Security Agency (NSA), the French government cybersecurity organization Agence nationale de la sécurité des systèmes d'information (ANSSI), and Ukrainian intelligence services are assessing whether Russian- state-backed hackers carried out the attack in an attempt to sever communications on the eve of the invasion. KA-SAT provides connectivity to Ukrainian military and police units, and parent company Viasat acts as a defense contractor for the US and several of its allies. A Viasat official has cited a "misconfiguration in the 'management section'" of KA-SAT's network that threat actors abused to gain remote access to modems.

- Spanish security researcher Ruben Santamarta hypothesized that Viasat's words about a misconfigured "management section" means "the attackers likely managed to compromise/spoof a Ground Station…specifically the 'Element Management' section…to issue a command by abusing a legitimate control protocol (probably TR-069) that deployed a malicious firmware update to the terminals…this could have been performed using well-known attacks involving VLANs".[185]

- On 15 March, NetBlocks reported that KA-SAT's network "remains heavily impacted," 18 days after the 24 February cyber attack.[186] On 15 March a Ukrainian official admitted for the first time that the Viasat breach caused a "huge loss" to Ukrainian communications. German wind operator Enercon, one of the first KA-SAT customers to report the outage, noted on 15 March that "85% of its modems

[180] https://www.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html, Global Incident Report March 10
[181] https://www.independent.ie/regionals/kerryman/news/kerry-county-council-on-cyber-attack-alert- over-suspicious-russian-online-activity-41439254.html
[182] https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware- attack-lockbit-leaks-data/
[183] https://acn-marketing-blog.accenture.com/wp- content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog- 14MARCH22.pdf
[184] https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
[185] https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html
[186] https://twitter.com/netblocks/status/1503791987161505801

Copyright © 2022 Accenture. All Rights Reserved.

were still offline" and that it would take weeks to recover.[187]

- On 12 March, the French School of Civil Aviation fell victim to Hive ransomware.[188] The threat actors using the ransomware initially demanded US$1.2 million in bitcoin; then, on 20 March, they raised the demand to US$2 million. Other Hive victims during the Ukraine crisis include the Romanian petrol company mentioned in an earlier version of this report (published on 10 March).

- On 14 March, Russian Deputy Foreign Minister Oleg Syromolotov said in an interview that the stalled Russian-US dialogue on cybersecurity could resume, provided that the US observe conditions Putin set in a September 2020 speech.[189] Putin's September 2020 speech had demanded that the US not "intervene" in Russian affairs.[190] Russian officials interpret "interference" broadly to include any criticism of the country.[191]
  - Syromolotov noted that high-level cybersecurity talks had already brought tangible results, such as the 14 January 2022 arrest of REvil ransomware operators who had targeted US critical infrastructure.
  - Some analysts interpreted Syromolotov's comment as a veiled threat from Russia to unleash criminals REvil actors.[192] The criminals whom Russia arrested on 14 January, including a person the US suspects of carrying out the May 2021 DarkSide ransomware attack on Colonial Pipeline[193], were scheduled to be eligible for release on bail on 13 March.[194]

- On 15 March the head of CERT Latvia said that the quantity of cyber attacks against the country had grown by 25 percent since the beginning of the war. This activity was mostly "quite primitive," involving mass credential phishing attacks and DDoS attacks.[195]

- On 15 March, Germany's Federal Office for Information Security (BSI) advised against using Kaspersky anti-virus products. They warned (translated): "A Russian IT manufacturer can carry out offensive operations itself, be forced to attack target systems against its will, or be spied on without its knowledge as a victim of a cyber operation, or be misused as a tool for attacks against its own customers".[196]

- On 15 March, the US CISA and the US Federal Bureau of Investigation issued Alert AA22-074A, "Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multi-Factor Authentication Protocols and "PrintNightmare" Vulnerability".[197] They wrote: "As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA [multi- factor authentication] protocols at a non-governmental organization (NGO), allowing them

[187] https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/
[188] https://www.lemagit.fr/actualites/252514685/LEcole-Nationale-de-lAviation-Civile-paralysee-par-une-cyberattaque
[189] hxxps://tass[.]ru/politika/14063755
[190] https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html
[191] https://www.dw.com/en/world-leaders-condemn-navalny-sentence-russia-denounces-interference/a-56436335
[192] https://twitter.com/C_C_Krebs/status/1503395668387377155
[193] https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest/index.html
[194] https://twitter.com/Zilla57826895/status/1482064786770776066
[195] https://rus.lsm.lv/statja/novosti/obschestvo/v-latvii-uchastilis-sluchai-kiberatak.a448086/
[196] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html
[197] https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

Copyright © 2022 Accenture. All Rights Reserved.

to enroll a new device for MFA and access the victim network." Then the actors exploited the "PrintNightmare" vulnerability, CVE-2021-34527, to gain system privileges. The alert urges that organizations enforce MFA, review configuration policies, disable inactive accounts, and patch for known exploited vulnerabilities.

- On 16 March, News 5 (Cleveland) reported that the US FBI had warned businesses in northeast Ohio of increased cyber threats, which News 5 reported the FBI suspects may be Russian retaliation for sanctions. "We're seeing just about everybody having something. It doesn't mean they've been hacked, but the attempts are there...from health care to financial services — even more supply chain," said an Ohio cybersecurity vendor News 5 quoted.[198]

- On 16 March, GovInfoSecurity noted several cyber incidents affecting the healthcare industry; these incidents include the disruption of some patient services at the East Tennessee Children's Hospital and patient information breaches in Missouri and Colorado.[199] It is unclear whether these incidents relate to Russian threat groups.

- On 16 March, cybersecurity research group vx-underground tweeted, "ALPHV, also labeled BlackCat ransomware group, is a suspected rebrand of DarkSide & BlackMatter ransomware group Today, ALPHV unveiled ALPHV MORPH. A polymorphic ransomware variant written in Rust and discovered today by @pancak3lullz." [200]

- On 16 March, Microsoft detailed how the TrickBot malware uses Internet of Things (IoT) devices, particularly MikroTik routers, in C2 infrastructure. Microsoft provides a forensic tool to test whether its IoT devices are vulnerable to these attacks.[201] This is relevant to the Russia-Ukraine conflict, given the leaked correspondence of some actors using TrickBot or Conti shows these actors have taken targeting guidance from JACKMACKEREL (a.k.a. Cozy Bear) a threat group operating out of Russia.[202]

- On 16 March, Dragos, an industrial control systems (ICS)-focused cybersecurity company, observed network communications among "numerous auto manufacturing companies" in North America and Japan and Emotet malware C2 servers that the Conti ransomware group appears to control.[203] It is unclear whether this Conti activity is part of the group's ordinary criminal activity or is related to its declared support for Russia.

- On 17 March, Trend Micro published an update on the Cyclops Blink malware, which is associated with the hacker group Sandworm and which recruits IoT devices for a botnet. Whereas previous reporting had focused on Cyclops Blink recruiting Watchguard firewalls, the new report details a strain that targets Asus routers. The

[198] https://www.news5cleveland.com/news/local-news/exclusive-fbi-warns-of-increased-cyber-threats-against-northeast-ohio-businesses
[199] https://www.govinfosecurity.com/tennessee-pediatric-hospital-responding-to-cyber-incident-a-18730
[200] https://twitter.com/vxunderground/status/1504238897194221570
[201] https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
[202] https://www.wired.com/story/trickbot-malware-group-internal-messages/, https://www.wired.com/story/conti-ransomware-russia/
[203] https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/

Copyright © 2022 Accenture. All Rights Reserved.

new report also lists over 150 current and historical C2 servers.[204]

- On 17 March, a technical fault disrupted Polish rail service for most of the day. This railroad has been transporting thousands of Ukrainian refugees to safety. The transport minister said traffic control systems that Alstom makes had experienced identical faults in India, Singapore, and possibly Pakistan. Alstom as not indicated any suspicions of malicious activity, saying a time-formatting error was responsible and said that the incident had not affected safety.[205] An Alstom software glitch also disrupted a signaling system on Spanish rail operator Renfe on 21 March.[206] Although the cause may be merely technical, the timing is of concern, as Spanish authorities have identified their country as a top target for Russian retaliatory cyber attacks (see above).

- On 17 March, the European Union Aviation Safety Agency warned of spoofing and jamming incidents affecting Global Navigation Satellite Systems in the areas of Kaliningrad, Eastern Finland, the Black Sea, and the Eastern Mediterranean since the 24 February Russian invasion of Ukraine. Finnish authorities had reported this previously; other reports say Poland, Lithuania, and Latvia also felt the effects. Israel also reported GPS interference coming from Russia's Khmeimim airbase in Syria. During military exercises in 2017 and 2018, NATO and Norway faced GPS disruption problems, which Norway blamed on Russia.[207] Interested parties can read ACTI's January 2022 blog highlighting GPS-related threats to transportation.[208]

- On 17 March, the ALPHV ransomware group claimed to have exfiltrated data from Noble Oil, a North Carolina-based used oil services recycling company.[209] ALPHV is the same group that has breached petrochemical industry-related logistics and port companies in Europe.[210]

    - A 17 March Talos report reaffirms a relationship ACTI previously identified between BlackMatter ransomware, a spinoff of the DarkSide malware used in the Colonial Pipeline attack, and the BlackCat (a.k.a. ALPHV) ransomware used in the European petrochemical industry-related logistics and port attacks mentioned above.[211] This suggests that the perpetrators of those European attacks may be acquainted with those responsible for the Colonial Pipeline attack.

- On 17 March, the US CISA and FBI issued an alert about "possible threats to U.S. and international satellite communication (SATCOM) networks." They wrote: "Given the current geopolitical situation, CISA's Shields Up[212] initiative requests that all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity".[213] The alert followed the Viasat/KA-SAT hack of 24 February. The alert directed readers to the February 2022 "Annual Threat Assessment of the U.S. Intelligence Community." This document explicitly named Russia's

[204] https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html
[205] https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/
[206] https://www.reuters.com/world/europe/madrids-suburban-trains-disrupted-after-alstom-software-glitch-2022-03-21/
[207] https://www.bleepingcomputer.com/news/security/europe-warns-of-aircraft-gps-outages-tied-to-russian-invasion
[208] https://www.accenture.com/us-en/blogs/cyber-defense/overreliance-gps-risk
[209] https://twitter.com/S0ufi4n3/status/1504542952110108677
[210] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say/
[211] https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
[212] https://www.cisa.gov/shields-up
[213] https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

Copyright © 2022 Accenture. All Rights Reserved.

development of "nondestructive and destructive counterspace weapons—including jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities and ground-based ASAT capabilities—to target U.S. and allied satellites."[214]

- On 17 March, a joint US cybersecurity advisory warned readers about AvosLocker, a ransomware-as-a-service group that has targeted potential victims in US financial services, critical manufacturing, and government facilities.[215] The advisory notes that the likely intrusion vectors included Microsoft Exchange Server vulnerabilities CVE-2021-31207, CVE-2021-34523, CVE-2021-34473, and CVE-2021-26855. AvosLocker advertises on the pro-Russian ransomware-oriented RAMP forum[216] and the group's name contains the Russian word "Avos" (meaning "perhaps"), suggesting AvosLocker may be a Russian group.

- On 17 March, researcher Brett Callow reported that the number of ransomware attacks on US local governments had decreased since the invasion of Ukraine.[217] This aligns with ACTI's own figures based on data-leak sites, listed above.

- On 20 March, the Lapsus$ extortion group posted an image that appeared to represent Microsoft's internal DevOps platform, but soon deleted the posting. Microsoft said it was investigating the claims, Vice News reported.[218]

- On 20 March, the Twitter account @ContiLeaks released version 3 of the Conti ransomware source code, which includes a compiled locker and decryptor.[219] The leaker's primary intention behind releasing this code may be to hurt the Conti developers, but the act also increases the cyber threat level for everyone, as it allows other threat actors to adapt and use the Conti source code.[220]

- On 20 March, the media reported that the British Army, citing "significant security concerns," prohibited military personnel from using the WhatsApp messaging service for professional work. According to the Daily Mail, Russian cruise missile operators have used phone metadata to target a training camp for foreign fighters in Ukraine.[221]

- On 20 March a threat actor on the underground forum Breached[.]co, the successor to Raidforums, offered to pay US$50,000 for working credentials for vpn1.colpipe.com (Colonial Pipeline). The threat actor, "Charles Carmakal," is associated with the Caishen2844 ransom collective. This "Charles Carmakal" actor likely chose this nickname as a taunt at the real Charles Carmakal, Senior Vice President and Chief Technology Officer at cybersecurity firm Mandiant, who consulted on the Colonial Pipeline response in 2021.

---

[214] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf
[215] https://www.ic3.gov/Media/News/2022/220318.pdf
[216] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[217] https://twitter.com/BrettCallow/status/1504504599239045120
[218] https://www.vice.com/en/article/y3vk9x/microsoft-hacked-lapsus-extortion-investigating
[219] https://twitter.com/vxunderground/status/1505555084452798469
[220] https://www.bleepingcomputer.com/news/security/more-conti-ransomware-source-code-leaked-on-twitter-out-of-revenge/
[221] https://www.dailymail.co.uk/news/article-10633873/British-soldiers-ordered-WhatsApp-hacking-fears.html

Copyright © 2022 Accenture. All Rights Reserved.

- On 21 March, ACTI observed online actor "pl0uton" advertising personal information about Ukrainian Security Service members. Actor "Charles Carmakal" responded, somewhat jokingly, "give info free I kill them" [sic]..

On 20 March, Israel's National Cyber Directorate and the Knesset [Parliament] information security unit said they had thwarted multiple cyber attacks aimed at disrupting Ukrainian President Zelensky's video address to Israeli lawmakers.[222]

On 20 March, German media, citing "Berlin security circles," reported that the Russian military intelligence service GRU has reconnoitered possible German targets for sabotage. One possible target is the Federal Network Agency, which is the regulatory office for electricity, gas, telecommunications, post, and railway markets.[223]

On 21 March, US President Joseph Biden issued an urgent statement warning that, in response to US and allied countries' sanctions, Russia could retaliate with cyber threat activity: "Today, my Administration is reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks." The statement called on private-sector critical infrastructure operators to "harden [their] cyber defenses immediately."[224]

- White House cybersecurity advisor Anne Neuberger explained that the US government had not seen evidence of specific cyber attacks but had seen "preparatory activity"—a term that could include scanning websites or hunting for vulnerabilities. She warned that threat actors continued to exploit unpatched vulnerabilities to compromise American companies.[225]

- On 22 March, CBS News wrote that the "evolving intelligence" from Biden's announcement on 21 March might refer to a non-public 18 March FBI warning to the US energy sector of increased network-scanning activities from Russian IP addresses. Of the 140 overlapping IP addresses the FBI has identified, the bureau discovered "abnormal scanning" for at least 18 US companies in the defense industrial base, financial services, and information technology industries, and at least five US energy companies.[226]

- Some details of this FBI warning resemble details of the reporting from 7 March on Russian probing of companies that produce liquefied natural gas[227] (see March 10 report). That reporting cited five US companies and implied that the Russian probing affected at least 15 energy companies in other countries.

- In a 26 March interview on CNN, US CISA director Jen Easterly further explained Biden's warning. She said that all critical infrastructure operators "need to assume" that Russian threat actors are preparing and exploring options for

[222] https://www.jpost.com/breaking-news/article-701828
[223] https://www.merkur.de/politik/konflikt-russland-militaergeheimdienst-deutschland-spionage-angriffsziele-bundesnetzagentur-verfassungsschutz-ukraine-krieg-zr-91419216.html
[224] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/
[225] https://nypost.com/2022/03/21/white-house-warns-intelligence-points-to-russian-cyberattacks/
[226] https://www.cbsnews.com/news/russia-cyberattacks-us-energy-fbi-warning/
[227] https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine

Copyright © 2022 Accenture. All Rights Reserved.

disruptive cyber activity. Easterly also stated: "it's not about panic. It's about preparation".[228]

- On 21 March, Canada's National Research Council (NRC) said a "cyber incident" forced it to take parts of its Internet presence offline. "NRC staff were not immediately able to say whether this cyber attack came from Russia or individuals and organizations associated with the Russian government," the Globe and Mail reported.[229] However, previous cyber incidents disrupted the foreign ministries of both Canada and the UK in early 2022 after both countries threatened to sanction Russia if it were to invade Ukraine.

- On 21 March, the Scottish Association for Mental Health said a "sophisticated and criminal" cyber attack on 17 March had affected "emails" and phone lines.[230] In a tweet without citation, BBC reporter Joe Tidy said Emsisoft had said the RansomExx crew carried out the attack.[231] RansomEXX (a.k.a. Defray777) has targeted North American local government agencies—particularly transportation departments—as well as electronics firms in the past. A possible connection with the Ukraine crisis is that Scotland has demonstratively welcomed Ukrainian refugees.[232]

- On 22 March, extortion group Lapsus$ said it was going to leak data from customers of the Okta authentication service. Okta said its initial review of the sample screenshots showed the data came from a January 2022 breach at a sub-processor and that "there is no evidence of ongoing malicious activity beyond the activity [Okta] detected in January".[233] Lapsus$ has recently focused on attacking telecommunications and gaming companies and has sought insiders to help breach those companies. WIRED, citing cybersecurity executive Dan Tentler, reported that "the screenshots suggest Lapsus$ compromised the access of an Okta site reliability engineer, a role that would potentially have extensive system privileges," and that the Okta compromise may have led to cascading compromises of Okta's many customers, putting it on a par with the SolarWinds supply-chain espionage operation.[234] ACTI has published a separate report about the Okta compromise.

    - On 22 March, Microsoft reported that Lapsus$ (which it tracks as DEV-0537) gains access and elevated privileges at target organizations through extensive social engineering and the purchase of stolen credentials and session tokens. The social engineering includes targeting employees' personal email accounts. Microsoft also acknowledged that Lapsus had breached it.[235]

    - On 23 March, ACTI observed the Lapsus$ Telegram account announcing a brief hiatus. The message read: "A few of our members has a vacation until 30/3/2022. We might be quiet for some times."

[228] https://www.cnn.com/2022/03/26/politics/jen-easterly-interview-russia-cnntv/index.html
[229] https://www.theglobeandmail.com/canada/article-canadas-national-research-council-hit-by-cyber-incident/
[230] https://www.bbc.com/news/uk-scotland-60826263
[231] https://twitter.com/joetidy/status/1505928374790893569
[232] https://www.bbc.com/news/uk-scotland-scotland-politics-60800831
[233] https://www.zdnet.com/article/okta-says-breach-evidence-shared-by-lapsus-ransomware-group-linked-to-january-hack-attempt/
[234] https://www.wired.com/story/okta-hack-microsoft-bing-code-leak-lapsus/
[235] https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Copyright © 2022 Accenture. All Rights Reserved.

- On 24 March, British police announced they had arrested seven people aged 16-21 "in connection with an investigation into a hacking group" and released them pending the investigation. They did not name the arrestees for privacy reasons.[236]

- On 30 March, the Lapsus$ group's Telegram channel announced, "We are officially back from a vacation" and posting what Lapsus$ claimedwas data stolen from Globant, a Luxembourg- and Argentina-based software development company. Globant acknowledged that someone had accessed some of its code but said it had no evidence of any effects on client data.[237]

- Also on 30 March, as a backup measure in case Telegram deleted Lapsus$'s Telegram chats, the Lapsus$ Telegram channel created and announced the creation of a chat group on the encrypted messaging platform Element. In addition, the Lapsus$ account wrote: "F**k AgainstTheWest".[238] The roots of this hostility, and whether it relates to the Russia-Ukraine conflict, are unclear. It is also unclear who now controls the Lapsus$ Telegram channel after the arrest of the UK teens (see bullet point above).

- On 1 April, a UK court presented formal charges against two of the teenagers in connection with the Lapsus$ activity but released them on bail.[239]

- On 7 April, the US Department of Health and Human Services warned of the Lapsus$ group's focus on compromising healthcare organizations and managed service providers in many areas of the globe and then stealing data for extortion.[240] Although authorities have arrested the UK teenagers believed to be associated with Lapsus$, the arrests will not stop other members dispersed globally or separate groups from conducting activity under the Lapsus$ banner.

- A 13 April tweet by vx-underground said a ransomware entity called NWGEN, which is currently or formerly associated with Lapsus$, had targeted a hospital in Chile and planned to leak data from the East Tennessee Children's Hospital (ETCH).[241] (This global incident report previously reported on the initial ETCH compromise in March). In an 8 April report, DataBreaches.net said it found NWGEN had posted on a Russian-language forum, showing purported samples of personal data from ETCH. NWGEN warned that if the hospital did not pay additional ransom money, the threat group would leak the rest of the data. Despite NWGEN's threat, DataBreaches.net said it did not find postings of additional ETCH data on any underground forums afterward.[242]

- On 19 April, Okta reported the results of its investigation of the January 2022 compromise. It said the impact was "significantly less" than initially estimated. During the 25 minutes a threat actor controlled a workstation with access to Okta, "the threat actor accessed two active customer tenants within the SuperUser application" but "was unable to successfully perform any configuration changes, MFA or password resets, or customer support 'impersonation' events"; they were

[236] https://www.bbc.com/news/technology-60864283
[237] https://www.reuters.com/technology/globant-says-its-code-repository-was-breached-2022-03-30/
[238] https://twitter.com/vxunderground/status/1509260154184904709
[239] https://bbc.com/news/technology-60953527
[240] https://www.hhs.gov/sites/default/files/lapsus-okta-health-sector-tlpwhite.pdf
[241] https://twitter.com/vxunderground/status/1514350335304814595
[242] https://www.databreaches.net/east-tennessee-childrens-hospital-updates-information-on-ransomware-incident/

Copyright © 2022 Accenture. All Rights Reserved.

also unable to log into any Okta accounts, according to the report.[243]

- Media reports say tens of thousands of tech specialists are leaving Russia in search of better professional and political prospects.[244] However, on 22 March, Vasiliy Shpak, a Russian deputy trade minister, proposed the creation of cyber troops in Russia. According to Russian state news agency ria[.]ru, Shpak said such an idea would make Russian software developers "think ten times before leaving their homeland in pursuit of a long ruble in foreign companies".[245] Shpak's implication that Russia currently has no cyber troops contradicts various media reports over the years, which have identified one or another organization within the Russian military as "cyber troops."

    - On 22 March, Russian publication Fontanka reported on a more informal type of "cyber troops" who provide pro-Russian social media messaging to counter "the Ukrainian propaganda machine".[246]

    - On 22 March, Ilya Sachkov, a prominent Russian IT specialist and founder of the cybersecurity company Group-IB, asked for release from pre-trial detention, stating that "Russia needs me now more than ever".[247] Authorities are holding him until 28 May while awaiting his trial for treason charges.

- On 23 March, Italy's state rail company halted some ticket sales after a cryptolocker attack. Unnamed security sources initially suspected a Russian nation-state attack but, on 24 March, analysts tentatively attributed the incident to the Hive ransomware group, which has affiliates in Russia and Bulgaria, according to Wired.[248] Citing reported screenshots and allegedly leaked messages from the negotiation chat, Wired says the Hive actors initially demanded 5 million euros in bitcoin, but then raised the demand to 10 million euros.[249] Hive actors had previously breached the French School of Civil Aviation and a Romanian petrol company, as this Global Incident Report reported.

- On 24 March, Lab52, a threat intelligence division of international cybersecurity company S2 Grupo, identified a cyber espionage campaign that used English-language lure documents referring to the Russia-Ukraine conflict and dropped Quasar RAT, which is an open-source remote access tool.[250]

- On 24 March, Twitter user @cyberwar_15 claimed that North Korean cyber threat actors had carried out a "massive cyber attack" using phishing emails supposedly from a South Korean think tank, with the emails including an attachment purporting to be a document on Russian-North Korean relations.[251] @cyberwar_15 describes themself as a South Korean who hunts North Korean cyber groups. The veracity of this report is unclear. As of 30 March, only two vendors on VirusTotal had labeled the

[243] https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/
[244] https://www.intellinews.com/putin-s-war-triggers-russian-tech-brain-drain-237348/
[245] hxxps://ria[.]ru/20220322/kibervoyska-1779400881.html
[246] https://www.newsweek.com/russia-cyber-warriors-cyber-attack-invasion-sanction-joe-biden-telegram-1690429
[247] hxxps://ria[.]ru/20220322/group-ib-1779505012.html
[248] https://www.wired.it/article/ferrovie-attacco-ransomware/
[249] http://web.archive.org/web/20220323211722/ and https://www.reuters.com/world/us/italys-state-railway-may-have-been-target-cyber-attack-2022-03-23/
[250] https://lab52.io/blog/another-cyber-espionage-campaign-in-the-russia-ukrainian-ongoing-cyber-attacks/
[251] https://twitter.com/cyberwar_15/status/1506926863176040448

Copyright © 2022 Accenture. All Rights Reserved.

alleged lure document as suspicious or malicious.[252]

On 24 March, the US Department of Justice unsealed two indictments charging four employees of the Russian government military or intelligence service with targeting the global energy sector between 2012 and 2018.[253] ACTI identified these groups early on as having the potential to carry out disruptive activity in operational technology systems. These suspects are not in US custody, but the indictment has signaled US awareness of them.

- The suspects include employees of:
  - The Central Research Institute of Chemistry and Mechanics (TsNIIKhM, which is under the Russian Defense Ministry), who allegedly caused the Triton attack that disabled safety-instrumented systems at a petrochemical plant in Saudi Arabia in 2017. ACTI tracks this group as ZANDER.
  - Russia's Federal Security Service, Center 16 (the Center for Radioelectronic Communications Intelligence), who allegedly installed malware backdoors in computers at hundreds of entities related to the energy sector worldwide in 2012-2018, laying the groundwork for potential disruption or damage. ACTI refers to this activity as that of threat group BLACK GHOST KNIFEFISH (a.k.a. Dragonfly, Havex).

- On 24 March, the UK government echoed the US attribution of Dragonfly activity to FSB's Center 16. The UK's Foreign Secretary also sanctioned the TsNIIKhM for the Triton attack and cited the FSB's "long raft of malign cyber activity," including the targeting of UK energy companies and probing of the US aviation sector.[254]

- On 24 March, the US CISA also published a list of TTPs the BLACK GHOST KNIFEFISH and ZANDER threat actors have used. The US CISA also listed mitigations for enterprise accounts (e.g., implementing privileged account management, enforcing password policies, conducting audits, checking operating system configurations, using multi-factor authentication, filtering network traffic, segmenting networks, limiting access to file shares and remote access, and blocking code execution) as well as particular mitigations for ICS environments (e.g., segmenting networks and following other ICS best practices).[255] However, ICS security expert Robert M. Lee warned in a tweet that some of the mitigation advice for ICS is "not practical & in some cases dangerous".[256] As examples, he said: data diodes are not always practical; alarms for all unusual traffic will create multiple false alerts; updating all software and replacing out-of-date hardware and software are not always feasible; and not allowing vendors to connect their devices to ICS is impractical.

- Also on 24 March, the FBI issued a Private Industry Notification warning that TRITON malware remains a threat to industrial control systems worldwide, as TsNIIKhM “continues to conduct activity targeting the global energy sector.” Specifically, TRITON modified Triconex Tricon safety controllers. The FBI did not

[252] https://www.virustotal.com/gui/domain/naver-bigfile.sec.irish
[253] https://justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
[254] https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents
[255] https://www.cisa.gov/uscert/ncas/alerts/aa22-083a
[256] https://twitter.com/RobertMLee/status/1507114690366697481

Copyright © 2022 Accenture. All Rights Reserved.

elaborate on post-2017 activity but noted that any versions of the Tricon control that predate version 11.3, which Schneider Electric issued in June 2018, remain vulnerable to Triton-style attacks.[257]

- On 24 March, the Washington Post, citing unnamed US officials, said US intelligence analysts assessed hackers from Russia's GRU had carried out the 24 February attack on Viasat. The US government has not formerly attributed the attack, however. Ukrainian cybersecurity official Victor Zhora said "we have obvious evidence that it was organized by Russian hackers".[258]

    - On 30 March, Viasat released an incident report on the 24 February KA-SAT attack. The report stated that malicious actors used several SurfBeam modems in Ukraine to carry out DDoS attacks against other modems, then gradually disappeared from the network. An investigation revealed “a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network.” The attacker then executed “legitimate, targeted management commands” that “overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable.” The report concluded, “To date, Viasat has no evidence that standard modem software or firmware distribution or update processes involved in normal network operations were used or compromised in the attack”.[259]

    - Juan Andres Guerrero-Saade at SentinelOne finds Viasat’s conclusions “difficult to reconcile.” He discovered a wiper, AcidRain, that he hypothesizes is responsible for the Viasat satellite modem hack. He wrote that AcidRain, an ELF MIPS malware, referring to malware using the Microprocessor without Interlocked Pipeline Stages architecture and the Executable and Linkable Format (ELF), is designed to wipe modems and routers. He found what he called “developmental similarities” between AcidRain and a plug-in for the VPNFilter malware that US and UK governments have attributed to the Russian military hacker group Sandworm (a.k.a. SANDFISH).[260]

    - On 1 April, Viasat confirmed that Guerrero-Saade's analysis is consistent with the company’s own findings: "SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described".[261]

- On 25 March, the US Federal Communications Commission (FCC) added Russia-based security firm AO Kaspersky Lab ("Kaspersky") to its list of companies "deemed to pose an unacceptable risk to the national security of the United States," making Kaspersky the first Russian company on the FCC's covered list, which the FCC had previously limited to Chinese firms.[262] Entities on the list may not buy components

[257] https://www.ic3.gov/Media/News/2022/220325.pdf
[258] https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/
[259] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/
[260] https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[261] https://www.zdnet.com/article/modem-wiping-malware-was-behind-viasat-cyberattack
[262] https://www.fcc.gov/supplychain/coveredlist

Copyright © 2022 Accenture. All Rights Reserved.

from US companies without US government approval.[263]

- On 25 March, Raytheon chief executive Gregory Hayes said in an interview that the company, which provides Ukraine with Stinger and Javelin missiles, "faces two million attempts to penetrate its network per week," but that "So far the damage has been minimal".[264]

- On 26 March, Russia's Federal Air Transport Agency, Rosaviatsiya, allegedly suffered a cyber attack that led to data loss and forced the organization to go back to using pen and paper. The compromise of a supplier, probably IT provider InfAvia, reportedly enabled the attack. As part of the attack, malicious actors supposedly destroyed 65 terabytes of data, including 18 months of emails; Rosaviatsiya lacks backups, according to Russian business media reports.[265]

    - On 30 March, International Business Times and other media outlets reported that Anonymous actors denied breaching Rosaviatsiya, saying Anonymous would never endanger civilians).[266] For its part, Rosaviatsiya issued a statement blaming the necessity to use pen and paper rather than computers on (translated) “temporary lack of access to Internet and malfunction of the electronic document flow system [sic]”.[267] The Rosaviatsiya statement said: "Information exchange will be carried out via AFTN channel (for urgent short message) and postal mail”.[268]

- On 27 March, Bleeping Computer reported that Hive ransomware operators revised their VMware ESXi Linux encryptor to the Rust programming language and borrowed a feature from BlackCat (a.k.a. ALPHV-ng) ransomware: removing the URL of the negotiation site from their code, making it harder for researchers to access the victim's Tor negotiation page based on samples those researchers find in VirusTotal. The move to the Rust programming language also mirrors BlackCat's tactics.[269] Both groups have targeted important transportation and supply facilities in: Central Europe (BlackCat); and Italy, France, and Romania (Hive).

- On 28 March, Trellix, a cybersecurity firm merging McAfee Enterprise and FireEye, and the US think tank Center for Strategic and International Studies published a report on organizations' perceptions of targeting by nation-states. Citing their own survey of 800 IT security decision makers from seven countries in November and December 2021, the report said 86 percent of respondents thought it likely that "a criminal organization acting on behalf of a nation-state" had targeted them.[270] Among other statements, the report referred to the Colonial Pipeline and Solar Winds incidents as examples of nation-state attacks.

- On 28 March, a border gateway protocol (BGP) incident occurred in which some internet traffic to Twitter was rerouted through Russian Internet provider RTComm for about 45 minutes. Doug Madory of network analytics company Kentik

[263] https://www.zdnet.com/article/kaspersky-blacklisted-by-fcc-alongside-china-telecom-and-china-mobile/#ftag=RSSbaffb68
[264] https://www.bostonglobe.com/2022/03/25/business/raytheon-fending-off-millions-cyberattacks-week/
[265] hxxps://www.kommersant[.]ru/doc/5281896
[266] https://www.ibtimes.com/anonymous-denies-hacking-russian-civil-aviation-authority-rosaviatsia-3455247
[267] https://avherald.com/h?article=4f6a8fd6&opt=0
[268] https://www.ibtimes.com/anonymous-denies-hacking-russian-civil-aviation-authority-rosaviatsia-3455247
[269] https://www.bleepingcomputer.com/news/security/hive-ransomware-ports-its-linux-vmware-esxi-encryptor-to-rust/
[270] https://www.trellix.com/en-us/assets/docs/trellix-csis-organizations-and-nation-state-cyber-threats-report.pdf

Copyright © 2022 Accenture. All Rights Reserved.

hypothesizes that the Russian government may have ordered ISPs to block Russians from visiting Twitter, and that RTComm may have used BGP to cause this blockage and may have accidentally "made those changes apply to the Internet as a whole".[271] Most internet providers ignored the incorrect BGP routing because Twitter had signed a Route Origin Authorization to identify the correct path.[272] BGPStream detected the BGP rerouting beginning at 12:06 UTC[273] and Russian state news agency RIA Novosti claimed Twitter outages were occurring in a variety of countries beginning at 14:48 Moscow time (11:48 UTC).[274] If Russian authorities were seeking to throttle Twitter traffic at that time, a state media report of a global disruption could allay domestic consumers' suspicions that their own government was throttling it.

- On 29 March, Finnish Security and Intelligence Service Supo said Russia "may attempt to influence the public and political debate around Finland's potential membership in NATO." Supo said it had not observed significant new Russian activity targeting Finland but that the situation could change very quickly.[275]

- On 29 March, UK National Cyber Security Centre (NCSC) Technical Director Ian Levy provided guidance for users of Russian technology products and services. Levy acknowledged that "we've not seen - and don't expect to see - the massive, global cyber attacks that some had predicted." However, Russia had carried out attacks "against UK interests," including attacks via the software supply chain. The UK had already advised national-security-related government entities to avoid using Russian products such as the Kaspersky anti-virus software in 2017. Given current uncertainties, Levy advised that organizations at higher risk-such as government entities, organizations "providing services to Ukraine," or organizations with high profiles or a perceived anti-Russian stance-reconsider the risks involved in using Russian-nexus products and services. Such products and services include cloud-enabled anti-virus products and development or support services. For their part, home users of Kaspersky products likely do not face particular risks unless Kaspersky becomes subject to sanctions and ceases to provide updates. Levy advised enterprises to follow NCSC guidelines for developing resiliency and formulating recovery plans.[276]

- On 29 March, Estonia's public broadcasting service, Eesti Rahvusringh√§√§ling (ERR), citing the Deputy Director General of the Department of State Information Systems of Estonia, said that malicious Russian cyber activity against Estonia and the other Baltic countries had increased. He cited a 21 March DDoS attack that briefly disrupted the ERR news portal as well as phishing attacks from Russia-based criminals.[277]

- On 29 March, the US CISA and the US Department of Energy issued a “CISA Insights” document on threats to uninterruptible power supply (UPS) devices.[278] The alert said threat actors had gained access to internet-connected UPS devices through default

[271] https://arstechnica.com/information-technology/2022/03/absence-of-malice-russian-isps-hijacking-of-twitter-ips-appears-to-be-a-goof/
[272] https://twitter.com/CloudflareRadar/status/1508450831338721281
[273] https://bgpstream.com/event/288327
[274] hxxps://ria[.]ru/20220328/twitter-1780504770.html
[275] https://yle.fi/news/3-12380786
[276] https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine
[277] https://rus.err.ee/1608548011/departament-gosudarstvennoj-infosistemy-uroven-kiberugroz-vyros-v-svjazi-s-ukrainskoj-vojnoj
[278] https://www.cisa.gov/sites/default/files/publications/CISA-DOE_Insights-Mitigating_Vulnerabilities_Affecting_Uninterruptible_Power_Supply_Devices_Mar_29.pdf

Copyright © 2022 Accenture. All Rights Reserved.

usernames and passwords. The alert recommended that organizations enumerate existing UPS devices, remove them from the internet or protect those devices' credentials with MFA and VPNs, and replace any default credentials with robust, new credentials. ACTI reported on UPS vulnerabilities in the Global Incident Report dated March 10, citing vulnerabilities CVE-2022-22806, CVE-2022-22805, and CVE-2022-0715 in particular.

- On 29 March, Hungarian periodical Direct36 reported that Russian hackers had "full access to Hungary's foreign ministry networks" from at least mid-2021 through at least January 2022 at the same time as the NATO and EU crisis summits and the invasion of Ukraine.[279] This may have given Russian intelligence services insight into Hungarian decision-making.[280]

- On 30 March, Google's Threat Analysis Group (TAG) issued a report on cyber threat activity related to the war in Ukraine. It reported numerous financially and politically motivated threat actors using war-related lures, including humanitarian appeals, in phishing, malware, and extortion campaigns. The Russian group that Google's TAG calls COLDRIVER (a.k.a. Gamaredon), which ACTI tracks as WINTERFLOUNDER, has carried out credential phishing campaigns targeting US NGOs and think tanks, a Ukraine-based defense contractor, and military personnel in many Eastern European countries. Google's TAG has also observed Ghostwriter actors using a new "Browser in the Browser" phishing technique,[281] whereby a browser window simulates a browser to display a trusted URL.[282]

    - In a 4 April posting, CERT-UA provided further details on the WINTERFLOUNDER (a.k.a. Gamaredon) activity. Some of the activity used Ukrainian-language lures reading "Information on war criminals of the Russian Federation." Once the file executes, it runs the PowerShell script "get.php" (GammaLoad.PS1) and obtains remote access to the victim's computer.[283] CERT-UA also provided details on an English-language email sent the Latvian government received; it included a lure document purporting to deal with humanitarian assistance to Ukraine.[284]

    - Beginning 30 March, ACTI has been observing this WINTERFLOUNDER activity. ACTI is analyzing several malicious LNK files with English-language titles about providing military humanitarian assistance to Ukraine, as well as the Ukrainian-language lure document. The use of an English-language lure breaks with this group's usual focus on Ukrainian targets. The malware calls back to several URLs, including the domain military-ukraine[.]site.

- On 30 March, the Financial Times reported that Russian search engine Yandex collects user data from Apple and Android mobile apps and sends the information to servers in Russia.[285]

---

[279] https://www.direkt36.hu/en/putyin-hekkerei-is-latjak-a-magyar-kulugy-titkait-az-orban-kormany-evek-ota-nem-birja-elharitani-oket/
[280] https://apnews.com/article/russia-ukraine-viktor-orban-europe-nato-budapest-e29b5d42a86086bb65b413e2b6d1c2bc
[281] https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/
[282] https://mrd0x.com/browser-in-the-browser-phishing-attack/
[283] https://cert.gov.ua/article/39138
[284] https://cert.gov.ua/article/39086
[285] https://www.ft.com/content/c02083b5-8a0a-48e5-b850-831a3e6406bb

Copyright © 2022 Accenture. All Rights Reserved.

- On 30 March, Texas-based cybersecurity provider Inquest reported on a malicious campaign impersonating the US Security and Exchange Commission (SEC) asking recipients for data on their Russian clients. Once malicious Microsoft documents execute as part of this campaign, a payload beacons to a remote server. Inquest attributes this activity to cyberespionage group Cloud Atlas (a.k.a Inception), which targets government and aerospace clients[286] and which analysts assess to be based in Ukraine. ACTI tracks this group as THORNSTURGEON.

- On 30 March, the US FBI published a TLP:White Private Industry Notification to warn US local government entities of ransomware threats. Citing a "State of Ransomware in Government 2021" survey of 30 countries, as well as media reports, the FBI alert said: "underfunded public sector organizations' understaffed and outdated systems often put them in the position to pay ransoms simply to get the data back".[287] As ACTI has noted, criminal ransomware attacks on government and other critical infrastructure in a country can align with an adversary state's strategic interest in undermining that country.

- On 31 March, the US Department of the Treasury sanctioned major Russian chipmaker Mikron plus other tech companies, as well as anyone working in the aerospace, marine, and electronics sectors of Russia's economy.[288]

- On 31 March, CISA released two advisories on vulnerabilities in Rockwell Automation products that are widely used throughout the world: CVE-2022-1161 and CVE-2022-1159, affecting firmware in Rockwell Logix programmable logic controllers. CISA cites a report by Claroty, which said attackers could cause physical damage and safety hazards to manufacturing assembly lines and affect the reliability of robotic devices. Threat actors could disguise malicious activity to go undetected by "hiding code inside ladder logic that gets loaded into the PLCs," as a report in The Record explained.[289] This alert is of particular interest considering government warnings about potential Russian threats to critical infrastructure in adversary countries.

- On 31 March, Euro Weekly News reported on a breach at a subsidiary of Spanish electricity company Iberdrola in which threat actors obtained access to contact information, but not financial data, for 1.3 million customers.[290] The article reports: "The company relates it [the incident] to a campaign of cyberattacks that affected other companies and Spanish and European public institutions, such as the Congress of Deputies." That statement likely refers to a DDoS attack that briefly affected the Spanish Congress of Deputies on 24 March.[291] Iberdrola, which claims to be one of the top renewable energy companies in the US, said that after the Ukraine invasion, the US government had warned the company it could face Russian cyber attacks.[292] As Russia relies heavily on fossil fuel revenues, it may have an incentive to delay the development of renewable energy.

[286] https://inquest.net/blog/2022/03/30/cloud-atlas-maldoc
[287] https://www.ic3.gov/Media/News/2022/220330.pdf
[288] https://home.treasury.gov/news/press-releases/jy0692
[289] https://therecord.media/cisa-claroty-warn-of-two-vulnerabilities-affecting-industrial-rockwell-products/
[290] https://euroweeklynews.com/2022/03/31/iberdrola-cyberattack
[291] https://epe.es/es/politica/20220324/ciberataque-tumba-durante-horas-pagina-13424025
[292] https://www.elmundo.es/economia/2022/03/31/6245c7dce4d4d8b12d8b457f.html

Copyright © 2022 Accenture. All Rights Reserved.

- On 31 March, Robert M. Lee, CEO of operational technology (OT)-focused cybersecurity firm Dragos, told Texas media his firm has seen energy-related facilities in Texas incur an increase in the volume of probing by Russian hackers since the Russian invasion of Ukraine. Texas has key export facilities for LNG; a major disruption at one of those sites would mean "you don't get fuel exports out to certain countries," Lee said.[293]

- On 31 March, German wind turbine maker Nordex shut down IT systems after detecting a "cybersecurity incident." Its telephone lines, email systems, and website were unusable over the weekend[294], but there is no indication that the incident has affected OT systems. Although Nordex provided little information publicly, the GovInfoSecurity website cited a Danish tech correspondent as hypothesizing the incident was likely a ransomware case and asking whether the frequent incidents affecting renewable energy companies were mere coincidence.[295]
  - Examples of incidents affecting such companies include: one in which actors launched the LockBit ransomware on Danish wind turbine maker Vestas in November 2021; German wind farm operator Enercon facing disruptions connected to the Viasat hack; and the 31 March data breach of Spanish renewable energy company Iberdrola.

  - On 11 April, Conti ransomware operators claimed responsibility for the attack on Nordex.[296] Conti operators have made political statements pledging to attack any country that attacks Russia.[297]

- On 31 March, ACTI observed a post on the RAMP forum from the moniker "Jordan Conti," who is associated with the Conti ransomware group. The author claims that the group is thriving, despite the disclosure of Conti source code and other materials in February 2022.[298] In the 31 March post, Jordan Conti boasts that Conti is as resilient as the Ukrainian capital of Kyiv, which Russian strategists had allegedly predicted would fall within two days of the invasion.[299] Jordan Conti's mocking of Russia's military effort appears to contrast with the Conti group's vow of support for Russia. Furthermore, the threat actor could risk jail time for questioning official Russian messaging on the Ukraine war.[300] This suggests Jordan Conti is not physically in Russia or that someone else is using the Jordan Conti account.

- On 5 April, in further Conti activity, the ransomware's leak site featured data from Panasonic Canada, according to Twitter user and information security enthusiast Soufiane Tahiri (@S0ufi4n3).[301] It is unclear whether this choice of target was at all related to Canada's involvement in anti-Russian sanctions.

[293] https://www.brownwoodnews.com/2022/03/31/texas-power-grid-energy-sectors-facing-elevated-russian-cyber-threats-during-war-in-ukraine/
[294] https://www.erneuerbareenergien.de/windenergie/it-sicherheit-nordex-am-freitag-kein-anschluss-unter-dieser-url
[295] https://www.govinfosecurity.com/hackers-target-wind-turbine-manufacturer-nordex-a-18833
[296] https://twitter.com/BrettCallow/status/1514715780377575427
[297] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[298] https://www.securityweek.com/ukrainian-security-researcher-leaks-newer-conti-ransomware-source-code
[299] https://www.npr.org/2022/03/08/1085155440/cia-director-putin-is-angry-and-frustrated-likely-to-double-down
[300] https://abcnews.go.com/US/wireStory/journalists-impeded-muzzled-russian-reporting-rules-83817340
[301] https://twitter.com/S0ufi4n3/status/1511272698130976768

Copyright © 2022 Accenture. All Rights Reserved.

- On 3 April, Australia passed cybersecurity legislation for critical infrastructure. It empowers the government to impose enhanced obligations on "systems of national significance," including requiring critical infrastructure operators to "install software that reports system information back to the Australian Signals Directorate".[302]

- On 4 April, social media accounts posted screenshots in which the Stormous ransomware group issued an implied warning to French President Emmanuel Macron on the eve of France's 9 April presidential election. Stormous wrote: "A French president interferes in the affairs of the state and does not interfere in the affairs of his country!!" Stormous then warned they "may include France in our very goals...," implying the group might unleash cyber attacks on France.[303] As ACTI noted in the March 10 Global Incident Report, Stormous, an Arabic-speaking group, had declared support for Russia and claimed support for breaches against Ukrainian entities and a US military contractor.

- On 4 April, the largest Ford dealer in the UK, TrustFord, acknowledged having incurred a Conti-related "cyber incident" possibly dating back to 28 March.[304] Whether this targeting is related to the UK's anti-Russian sanctions is unclear.

- On 5 April, the Conti leak site featured data from Panasonic Canada.[305] Whether this targeting is related to Canada's anti-Russian sanctions is unclear.

- On 5 April, the US Justice Department and German federal police announced they had jointly seized servers and cryptocurrency wallets belonging to the underground marketplace Hydra. They also charged a Hydra administrator[306] and imposed sanctions on Hydra and on virtual currency exchange Garantex.[307]

    - In another criminal takedown, on 12 April, European and US law enforcement announced the seizure of infrastructure from the RaidForums underground marketplace.[308] The US also unsealed criminal charges against the alleged RaidForums founder, 21-year-old Diogo Santos Coelho of Portugal, whom UK officials arrested on 31 January.[309] These marketplaces facilitated cyber criminals' resale of stolen data.

    - On 14 April, Russian state media announced the arrest of Dmitriy Pavlov, the alleged founder of the Hydra Darknet market, on drug trafficking charges[310] Russian cybersecurity officials have recently been claiming they tried to cooperate with the US on cybersecurity efforts but that the US broke off the cooperation. The arrest is possibly a bargaining chip of some kind.

[302] https://www.iothub.com.au/news/second-critical-infrastructure-cyber-security-bill-passes-parliament-578253
[303] https://twitter.com/S0ufi4n3/status/1511044720469889026
[304] https://thestack.technology/trustford-cyber-attack-conti/
[305] https://twitter.com/S0ufi4n3/status/1511272698130976768
[306] https://www.zdnet.com/article/us-justice-department-shuts-down-russian-dark-web-marketplace-hydra/
[307] https://home.treasury.gov/news/press-releases/jy0701
[308] https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down
[309] https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator
[310] hxxps://ria[.]ru/20220414/arest-1783623004.html

Copyright © 2022 Accenture. All Rights Reserved.

- In a 5 April tweet, Blue Hornet | AgainstTheWest announced plans to target Stormous. The tweet read, "For reference, this is the list we're going down in order" and included a screenshot with a list in the following order: APT29; Killnet Owner; Salisbury Novichok GRU; Stormous; Conti.[311] The only non-cyber entity on the list is the penultimate one; it refers to the Russian military intelligence agents who attempted to assassinate a former Russian intelligence agent in Salisbury, England, using the poison Novichok.

- On 5 April, a report by industrial cybersecurity company Dragos assessed threats to European industrial infrastructure. Dragos reported that criminals or other adversaries motivated by regional tensions could carry out operations affecting industrial operations. "Particularly of concern are geographically dispersed industrial operations such as renewable electric generation, electric transmission, upstream and midstream oil and gas, water and wastewater management, etc." The report noted that ransomware also remained a threat, particularly to small- and medium-sized manufacturing entities. Nevertheless, "Dragos assesses with moderate confidence Europe is at low risk for widespread industrial infrastructure-targeted destruction and disruption campaigns.... due to the deterrence posed by potential political and economic impact." Despite this overall moderate assessment of risks, Dragos did point out that "key regasification plants such as those located in Rotterdam, present a target for adversaries looking to disrupt the flow of Oil & Natural Gas (ONG) energy into Europe".[312] This aligns with Dragos' previous warning about Russian probing of Texas LNG exporters who are helping global customers reduce reliance on Russian energy supplies (as noted earlier in this report). At least six oil terminals in the Amsterdam-Rotterdam-Antwerp refining hub experienced difficulty in cargo loading and unloading after an ALPHV (a.k.a. BlackCat) ransomware attack at the end of January 2022.[313]

- On 6 April, the US DOJ announced it had disrupted the global botnet that the Russian military threat group SANDFISH controlled. The DOJ said it had copied and removed Cyclops Blink malware from the botnet's command-and-control devices. The DOJ warned owners of infected WatchGuard and Asus devices that had made up the botnet that they "may remain vulnerable to Sandworm" and should still take the detection and remediation steps WatchGuard and Asus had recommended.[314]

    - On 6 April, Ars Technica reported that WatchGuard had failed to disclose CVE-2022-23176, the critical authentication bypass vulnerability that Russian hackers exploited.[315]

    - On 11 April, the US added the critical Watchguard Firebox and XTM Privilege Escalation vulnerability (CVE-2022-23176) to CISA's Known Exploited Vulnerabilities catalog.[316] CISA also added two Microsoft Active Directory privilege escalation vulnerabilities to the list. Conti actors exploited these

[311] https://twitter.com/_Blue_hornet/status/1511437228102275074
[312] https://www.dragos.com/blog/industry-news/assessing-threats-to-european-industrial-infrastructure/
[313] https://www.argusmedia.com/en/news/2297896-cyberattack-causing-problems-at-ara-storage-terminals
[314] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation
[315] https://arstechnica.com/information-technology/2022/04/watchguard-failed-to-disclose-critical-flaw-exploited-by-russian-hackers
[316] https://www.cisa.gov/uscert/ncas/current-activity/2022/04/11/cisa-adds-eight-known-exploited-vulnerabilities-catalog

Copyright © 2022 Accenture. All Rights Reserved.

vulnerabilities in 2021.[317] CISA is mandating that federal agencies address the new vulnerabilities by 2 May 2022.

- On 7 April, ACTI observed an actor on the Exploit underground forum advertising corporate network access to German-based used oil recycling company Avista oil. As this SITREP has reported previously, on 17 March, the ALPHV ransomware group claimed to have exfiltrated data from US oil recycling company Noble Oil.[318] ALPHV operators also allegedly carried out attacks on petrochemical services companies and ports in central Europe in January 2022.[319] The easy availability of breached credentials and data from organizations throughout oil and gas supply chains could facilitate the kinds of Russian critical infrastructure attacks that US President Biden and other Western leaders have warned about.

- On 7 April, the North American Electric Reliability Corporation (NERC) released the results of GridExVI, an exercise it carried out on 18 November. Simulating a nationwide wave of coordinated cyber and physical attacks against industrial control systems, generators, pipelines, and liquefied natural gas production facilities, NERC found that "telecommunications disruptions impair power system restoration activities and complicate coordination with government".[320]

- On 8 April, DDoS attacks briefly disabled the websites of Finland's Defense Department and Foreign Ministry, forcing those agencies to communicate with the public via Twitter.[321] A Russian state aircraft violated Finnish airspace on the same day, Finland's Defense Ministry said. These incidents occurred on the day that Ukrainian President Zelensky addressed the Finnish parliament and at a time when Finland is considering joining NATO. On 11 April, Russian officials warned Sweden and Finland against joining the alliance.[322] Finnish officials have warned of possible Russian cyber threat activity designed to discourage Sweden and Finland's NATO membership.

- A 7 April Avast report identified a new Traffic Direction System (TDS), which Avast calls Parrot TDS, that has infected web servers and their hosted websites with FakeUpdate (a.k.a. SocGholish) malware. Avast says that in the first nine days of March 2022 alone, Avast "protected more than 600,000 unique users from around the globe from visiting these infected sites".[323] SocGholish is associated with the Russia-based EvilCorp threat group[324]; the US Treasury Department has sanctioned the leader of that group for working with Russia's FSB.[325]

- On 7 April, the Everest ransomware gang announced access to systems of the "United States of America GOV, servers with administrative privileges".[326] On 29 November 2021, ACTI observed the group offering access to the US judicial system, with passports, tax documents, and court cases—a set of sources that aligns with the

[317] https://thedfirreport.com/2022/04/04/stolen-images-campaign-ends-in-conti-ransomware/
[318] https://twitter.com/S0ufi4n3/status/1504542952110108677
[319] https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/
[320] https://www.hstoday.us/featured/gridexvi-finds-communications-challenges-that-could-cripple-response-to-attacks-on-power-grid/
[321] https://www.infosecurity-magazine.com/news/finland-government-sites-offline/
[322] https://www.newsweek.com/russia-peskov-warns-sweden-finland-joining-nato-1696947
[323] https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/
[324] sentinelone.com/labs/sanctions-be-damned-from-dridex-to-macaw-the-evolution-of-evil-corp/
[325] https://home.treasury.gov/news/press-releases/sm845
[326] https://twitter.com/darktracer_int/status/1511868022784335878

Copyright © 2022 Accenture. All Rights Reserved.

agencies that the Russian state hackers reportedly breached in the SolarWinds case.[327]

- On 25 March, the Everest ransomware gang offered to sell access to an organization "directly related to the country's economy. UK GOV," according to Indian cybersecurity vendor Kulkarni Defence. The tweet thread, which cited Everest's post, continued, "State-owned company for generating, transmitting, and distributing electricity. Root access to many servers. Databases, backups, employee access to the administration of POS terminals, and much more. Multiple settings and developments. You can become the king of electricity in the whole country. The largest defense electronic equipment company appears in files and accesses".[328] The reliability of this posting is unclear.

On 11 April, media outlets, citing the Funke media group, reported that Germany's domestic intelligence agency (the BfV) had warned Bundestag members of possible Russian cyber targeting. The BfV urged members to take extra care when opening emails—even those appearing to come from familiar addresses, as the Ghostwriter threat group sometimes uses the domain name email.eu in its phishing campaigns, for example.[329]

On 12 April, Sophos reported that threat actors who deployed the LockBit ransomware in a regional US government agency network had for at least five months dwelt within the agency's systems before launching the ransomware. The threat actors installed commercial remote-access tools as well as custom scripts. They also disabled endpoint protection on the servers and some desktops, taking advantage of a lapse by maintenance personnel at the agency who failed to enable a protective feature. Sophos assessed that two different sets of threat actors operated: first, less-sophisticated threat actors breached the victim network, exploiting open Remote Desktop Protocol ports in a public-facing firewall; later, more-sophisticated groups took over and eventually deployed the ransomware and a LockBit 2.0 ransomware note that encourages readers to act as malicious insiders by stealing valuable data and launching malware.[330]

On 12 April, Indian government-owned Oil India Limited shut down its IT systems after discovering a breach that had occurred on 10 April.[331] A spokesperson predicted the incident "will take months to resolve".[332] The breach occurred just before Indian president Narendra Modi held a video call with US President Biden, who urged Modi not to purchase Russian oil.[333] On 12 April, a different Indian oil company, Indian Oil, removed Russian oil from its latest tender.[334] On 19 April, a new leak site for REvil, a Russian ransomware group whose past targeting has sometimes aligned

[327] https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/
[328] https://twitter.com/IscsBalakrishna/status/1507368768657563658
[329] https://www.dw.com/ru/vedomstvo-po-okhrane-konstitucii-predupredilo-chlenov-bundestaga-ob-atakakh-rossijskikh-khakerov/a-61441676
[330] https://news.sophos.com/en-us/2022/04/12/attackers-linger-on-government-agency-computers-before-deploying-lockbit-ransomware/
[331] https://www.business-standard.com/article/companies/oil-india-suffers-cyber-attack-receives-rs-57-crore-ransom-demand-122041301002_1.html
[332] https://www.northeasttoday.in/2022/04/12/assam-cyberattack-on-duliajan-based-oil-india-limited-oil-office-it-systems-shut-down/
[333] https://www.reuters.com/world/indian-pm-modi-suggests-direct-talks-between-putin-zelenskiy-2022-04-11/
[334] https://www.reuters.com/world/india/indian-oil-removes-russian-urals-latest-tender-sources-say-2022-04-12/

Copyright © 2022 Accenture. All Rights Reserved.

with Russian strategic interests, claimed to have carried out the breach, according to screenshots that cybersecurity researchers have posted.

- On 13 April, the Honolulu Star-Advertiser reported that officials from the DHS Homeland Security Investigations (HSI) unit had disrupted a cyber incident targeting an undersea cable that connects Hawaii with the Pacific region. Citing an HSI news release, the news report said an international cyber threat group had breached servers at a private company that manages the undersea cable. HSI agents blocked the threat actors' access and worked with international partners to arrest a suspect, the report said.[335] The report does not identify the hackers' background. US intelligence officials previously warned of Russian interest in disrupting undersea cable traffic[336], and the Russian-language Snatch ransomware team claimed on 7 March to have breached Xtera, a US-based undersea fiber optic cable manufacturer.[337] Subsea cable traffic contributed US$649 billion to the US economy in 2019, according to an estimate that the Center for Strategic and International Studies, a US think tank, cited.[338]

- On 13 April, CISA, the FBI, the US National Security Agency, and the US Department of Energy issued a joint advisory warning of cyber espionage actors who have developed custom tools for targeting ICS and supervisory control and data acquisition (SCADA) devices including Schneider Electric programmable logic controllers (PLCs), OMRON Sysmac NEX PLCs, and Open Platform Communications Unified Architecture (OPC UA) servers.[339]

  - Dragos, an OT-focused cybersecurity firm, reported on 13 April that it had discovered a highly motivated, skilled, and well-funded group it calls CHERNOVITE developing a malware suite Dragos calls PIPEDREAM that targets the abovementioned and other ICS and SCADA technologies. The company said it had discovered the malware before threat actors had a chance to deploy it.[340] Dragos has not attributed CHERNOVITE to a particular country as of 20 April 2022. Dragos noted malicious actors most likely created the malware to target LNG and electric power environments.[341] This aligns with earlier Dragos warnings that Russian threat actors could target crucial LNG export facilities in US states like Texas[342] and gasification plants such as those in Rotterdam.[343] Also, it was employees of LNG facilities whose credentials Russian threat actors allegedly tried to harvest.[344] Disruption of LNG facilities could hinder Europe's efforts to reduce itsdependence on Russian gas and oil.[345]

  - On 16 April, Dragos analyst Jimmy Wylie noted that PIPEDREAM combines the breadth of CRASHOVERRIDE with the depth of the Triton (a.k.a. Trisis) malware,

[335] https://staradvertiser.com/2022/04/12/breaking-news/cyberattack-on-hawaii-undersea-communications-cable-thwarted-by-homeland-security/
[336] https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf
[337] https://twitter.com/S0ufi4n3/status/1500934560627970058
[338] https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options
[339] https://cisa.gov/uscert/ncas/alerts/aa22-103a
[340] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf
[341] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf
[342] https://www.brownwoodnews.com/2022/03/31/texas-power-grid-energy-sectors-facing-elevated-russian-cyber-threats-during-war-in-ukraine/
[343] https://www.dragos.com/blog/industry-news/assessing-threats-to-european-industrial-infrastructure/
[344] https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine
[345] https://www.washingtonpost.com/technology/2022/04/13/pipedream-malware-russia-lng/

Copyright © 2022 Accenture. All Rights Reserved.

including “custom-written CODESYS libraries, interactive tools for manipulating devices over OPC-UA, and FINS [Factory Interface Network Service], as well as basic recon using Modbus,” Wylie continued, “The adversary has evolved from having a dumb hammer to a swiss army knife that will help them both research and recon targets and achieve impacts”.[346]

- On 13 April, Mandiant reported on the same malware, which it calls INCONTROLLER. The company noted, “the activity is consistent with Russia's historical interest in ICS. While our evidence connecting INCONTROLLER to Russia is largely circumstantial, we note it given Russia's history of destructive cyber attacks, its current invasion of Ukraine, and related threats against Europe and North America".[347]

On 13 April, Microsoft announced it had disrupted the Zloader botnet. It obtained a US court order to sinkhole 65 domains and take control of newly generated domains. Microsoft identified Denis Malikov, a resident of Russian-occupied Crimea, as the creator of a malware component. Zloader operators used the botnet to steal money and rented it out to operators of ransomware families such as Ryuk.[348] Analysts view Ryuk as the predecessor of the Conti ransomware.[349]

On 13 April, CISA urged organizations[350] to review a 12 April Microsoft security update about CVE-2022-26809, a remote procedure call runtime remote code execution vulnerability affecting systems running Windows.[351] According to Microsoft, an attacker could exploit this vulnerability via a remote procedure call, and it urged organizations to block TCP port 445 at the enterprise perimeter firewall and to secure Server Message Block (SMB) traffic.

- According to research company Censys, at least 824,011 hosts with Windows-based operating systems are running the SMB protocol; some 366,000 of these are in the US. Even if organizations block external access to port 445, a threat actor with access to even one victim's machine could spread the malware to all machines in a local network, experts told The Record.[352]

- Other vulnerabilities that Microsoft reported in April 2022, such as CVE-2022-24491 and CVE-2022-24497 in Windows Network File System and CVE-2022-24500 in Windows SMB, are wormable.[353] Russian and North Korean state threat actors exploited SMB vulnerabilities to massively spread the WannaCry and NotPetya malware in 2017. This SITREP has noted that use of wormable malware, even in a targeted way, could cause enormous collateral damage, as WannaCry and Not Petya did in 2017.

On 13 April, Ukraine’s Minister of Digital Transformation claimed that, after the Russian invasion, his organization and Ukraine’s “mobilized...cyber-society” had

[346] https://twitter.com/mayahustle/status/1515448505837535241
[347] https://mandiant.com/resources/incontroller-state-sponsored-ics-tool
[348] https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
[349] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti
[350] https://www.cisa.gov/uscert/ncas/current-activity/2022/04/13/microsoft-releases-advisory-address-critical-remote-code-execution
[351] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26809
[352] https://therecord.media/experts-warn-of-concerns-around-microsoft-rpc-bug/
[353] https://krebsonsecurity.com/2022/04/microsoft-patch-tuesday-april-2022-edition/

Copyright © 2022 Accenture. All Rights Reserved.

conducted offensive cyber operations against Russia, including leaking personal data and disrupting Russian telecommunications and database infrastructure.[354]

- On 14 April, DDoSecrets announced it had uploaded stolen documents from Gazprom Linde Engineering, a Russian engineering company that designs gas and petrochemical processing facilities and oil refineries.[355]

- On 14 April, German media reported that German wind farm maintenance company Deutsche Windtechnik AG had experienced an attack on the company's IT systems. The attack did not affect the wind turbines themselves but hampered communications with them.[356]

- On 16 April, pro-Russian group KillNet claimed to have breached US-based Devon Energy Corporation, according to a post reproduced in a tweet by Cyberknow20 that reads, "The attack is dedicated to the Russian hacker group REvil…".[357] This cryptic statement appears to show KillNet has an affinity for REvil.

    - Since the war began, several Russian cybersecurity authorities have publicly commented on Russia's arrest of REvil suspects in January 2022. The officials claimed that Russia made good-faith efforts to cooperate with the US against cyber crime by detaining REvil suspects and the Colonial Pipeline hacker on the US' request, but that the US had unilaterally pulled out of the anti-cybercrime cooperation process.[358] The commentaries by Deputy Foreign Minister Oleg Syromolotov on 14 March and by cybersecurity negotiator Andrey Krutskikh on 14 April (summarized elsewhere in this SITREP) could be veiled threats that Russia could encourage further cyber criminal activity against the US and its allies.

    - On 19 April, a new underground leak site for the REvil group briefly reappeared and claimed to have breached Oil India, as this SITREP described above.[359]

- On 18 April, after the Easter holiday weekend, local media in Germany reported on cyber attacks affecting computer equipment maker Reitzner, a small-town energy utility, and another small town's municipal IT systems.[360] In the US, Kansas City, Kansas, and its surrounding county government also reported a cyber attack on its data centers.[361]

- On 20 April, the National Cyber and Information Security Agency of the Czech Republic warned that hackers had recently been conducting DDoS attacks on the websites of Czech railways and airports, likely in connection with the Ukraine

[354] https://www.ukrinform.ru/rubric-technology/3456507-ukraina-nacala-soversat-kiberataki-na-resursy-rf-s-24-fevrala-fedorov.html
[355] https://twitter.com/NatSecGeek/status/1514518629324398592
[356] https://www.butenunbinnen.de/nachrichten/cyberangriff-auf-deutsche-windtechnik-ag-bremen-102.html
[357] https://twitter.com/Cyberknow20/status/1515474245882507266
[358] hxxps://mid[.]ru/ru/press_servic/1809317/?msclkid=95f247eebc2211ec8f5f530d2df3cf1c
hxxps://rg[.]ru/2022/04/07/sovbez-rf-soedinennye-shtaty-v-ocherednoj-raz-dokazali-chto-im-verit-nelzia.html
[359] https://twitter.com/campuscodi/status/1516739066674483207/photo/1
[360] https://www.augsburger-allgemeine.de/dillingen/dillingen-lauingen-cyberangriff-auf-die-donau-stadtwerke-dsdl-id62406836.html, https://www.rnz.de/nachrichten/bergstrasse_artikel,-schriesheim-cyber-attacke-nichts-geht-mehr-im-rathaus-_arid,871081.html
[361] https://www.wycokck.org/Engage-With-Us/News-articles/UG-Cybersecurity-Attack

Copyright © 2022 Accenture. All Rights Reserved.

conflict.[362]

Analytical Notes

Russian Internet Isolation

The aftermath of the invasion has seen an abrupt move toward the isolation of Russian cyberspace. This has originated partly from the outside: several countries have banned Russia from the SWIFT international payments messaging network; tech platforms have discontinued service to Russia; Internet backbone providers Cogent and Lumen withdrew from Russia; and the London Internet Exchange (LINX) announced it would stop routing for Russia's largest digital services provider Rostelecom and Russian mobile provider MegaFon.[363] However, on 3 March, the Internet Corporation for Assigned Names and Numbers (ICANN) rejected Ukraine's request to revoke Russia's top-level domains and Secure Sockets Layer (SSL) certifications, a move that would have effectively blocked Russia from the Internet.[364]

The Russian government has itself enacted policies at home that increase Russia's isolation from global information providers, imposing strict censorship policies and accelerating portions of Russia's years-long program to build a self-sufficient Russian Internet segment that can operate in isolation from the global Internet. The ACTI report "Russian Internet Isolation Scenarios Accelerate" explores this further.[365] Still, Russian Internet isolation is less than expected so far, despite the withdrawal of Internet backbones Cogent and Lumen from Russia. On 11 March, Cisco's Thousand Eyes reported: "Despite reports of Russia's possible disconnection from the global Internet, connectivity continues as it has historically, with global transit providers exchanging traffic with major Russian internet service providers (ISPs) at locations outside of Russia." However, Russian websites belonging to government and critical infrastructure entities have experienced "erratic" network conditions. This is likely due to ISPs blackholing traffic to combat DDoS attacks, and in some cases due to filtering of traffic coming from outside Russia.[366] This is consistent with the measures required to implement the Sovereign Russian Internet program described elsewhere in this report. This situation may change since LINX's announcement on 11 March that it would stop routing for Rostelecom and MegaFon.[367]

However, on 14 March, Rostelecom claimed the Russian Internet "has reserves and alternative routes for traffic exchange with foreign sites," according to a DataCenterDynamics article. The report added: "Mobile phone operator MegaFon said that traffic going through LINX had already decreased significantly over the last few years, adding that it 'already planned to end our cooperation with this organization in 2022 and began a systematic redistribution of traffic.'" ACTI is unaware of any independent verification of this claim.[368] Back on March 11, Brian Krebs cited Kentik connectivity researcher Doug Madory as saying "If the other major European exchanges

[362] https://aroundprague.cz/news/kriminal/po-dannyim-nukib-xakeryi-atakuyut-nekotoryie-cheshskie-sajtyi
[363] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[364] https://www.zdnet.com/article/icann-rejects-ukraines-request-to-block-russia-from-the-internet/#ftag=RSSbaffb68
[365] https://intelgraph.idefense.com/#/node/intelligence_alert/view/821210b8-16f1-47a3-8c75-1013c8329bd9
[366] https://www.thousandeyes.com/blog/russia-global-internet
[367] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[368] https://www.datacenterdynamics.com/en/news/london-internet-exchange-disconnects-megafon-and-rostelecom/

Copyright © 2022 Accenture. All Rights Reserved.

followed suit, it could be really problematic for Russian connectivity," suggesting that the LINX cutoff on its own might not be a devastating blow unless it starts a trend.[369]

Russia's isolation has led to a concession on one aspect of the country's political crackdown. On 15 March, media reported that the exodus of Western cloud providers from Russia has left that country with only two months' worth of data storage left. To ease this impending issue, Russia's Digital Ministry reportedly suspended a quota for storage capacity that telecommunications operators must set aside for surveillance purposes.[370]

Illustrating the increasingly authoritarian political environment and the challenges Russia faces in developing its own systems to replace international financial infrastructure is the story of the plastic credit card shortage. On 16 March, Russia-based Tinkoff Bank fielded many customer questions on Twitter about how to obtain an MIR, a Russian national payment card. Tinkoff tweeted: "We are not currently issuing plastic MIR cards, because we ran out of plastic." However, on 17 March, they corrected themselves: "Sorry, we were mistaken in our response. We issued, issue, and will issue MIR plastic cards; we have enough resources to provide cards for everyone who wants one".[371] This wording is a subtle political comment likening current events to the repressive Soviet era; the wording resembles a famous Soviet slogan: "Lenin lived; Lenin lives; Lenin will live." Sberbank has also cited reports of a plastic shortage, calling them "fake," but has acknowledged likely delays in the delivery of the plastic cards.[372]

On 17 March, Russia's Digital Ministry announced it would help banks filter traffic from abroad to mitigate a recent wave of DDoS attacks.[373] Like the TLS certificates the Russian government has offered for free to organizations, ACTI assesses this filtering will provide the Russian government opportunities for greater surveillance and control of internet traffic in Russia, along the lines of the country's "sovereign internet" efforts. On 18 March, ZDNet pointed out that only Russia's Yandex browser and Atom products trust the TLS certificates the Russian government is providing.[374]

On 17 March, the Internet Protection Society, a Russian internet-freedom advocacy group, posted a video on what to do in case Russia's government shuts down the country's internet from within.[375] Group-IB tweeted that if Russian providers enact the deep packet inspection that the 2019 sovereign internet law mandated, they will be able to block the internet protocols that VPNs use. Users can circumvent the blockages but will experience slow and unstable service by doing so.[376]

On 18 March, data-storage-focused news source Blocks&Files analyzed the Russian cloud storage shortage.[377] Citing a report on Russian newspaper Kommersant, Blocks&Files points out that: a computing power shortage could hinder Russian government operations; Chinese suppliers have put deliveries on hold due to sanctions; and the Russian Ministry of Digital Transformation was exploring emergency solutions such as taking over IT assets of companies that had left Russia. The report notes that Russia had a mere 170 datacenters, eight network fabrics (sets of interconnected network devices), and 267 communications providers. Blocks&Files noted that Chinese

[369] https://securityboulevard.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[370] https://www.bleepingcomputer.com/news/technology/russia-faces-it-crisis-with-just-two-months-of-data-storage-left/
[371] https://twitter.com/llirik1985/status/1504394220576161792
[372] hxxps://ria[.]ru/20220317/mir-1778662806.html
[373] hxxps://securitylab[.]ru\news\530627.php
[374] https://www.zdnet.com/article/russia-remains-connected-to-the-internet/
[375] https://www.youtube.com/watch?v=O2CfRMTl6QU
[376] https://twitter.com/GroupIB/status/1504414698690822148
[377] https://blocksandfiles.com/2022/03/18/russia-cloud-gap-western-tech/

Copyright © 2022 Accenture. All Rights Reserved.

provider Alibaba cloud, Amazon Web Services, Google, and Azure do not have Russia-based data centers, although the latter three might provide some services to legacy customers. The options for resolving this shortage that the Russian government has explored, such as confiscations of foreign assets, may not fully satisfy Russia's data storage needs.

On 19 March, the Head of the Russian Space Agency said the US might try to cut Russia off from the GPS but noted that Russia's GLONASS navigation system, which smartphones are equipped to run, could take up the slack.[378]

On 28 March, Bleeping Computer reported that a Russian business association had warned that sanctions-induced shortages of telecommunications equipment could cause internet service outages as early as the summer of 2022. The association also warned that the high-tech industry could lose up to 30 percent of IT specialists in the coming months.[379]

On 5 April, US chipmaker Intel said it was shutting down all business operations in Russia.[380]

On 8 April 2022, the US Treasury Department announced exemptions on sanctions on Russia relating to telecommunications and internet-based communications.[381] The move likely aims to ease Russian people's isolation and facilitate their access to global news sources and social media platforms.[382]

Low Levels of Sophisticated Russian State Threat Activity Explained

ACTI and other analysts have admitted surprise at the relatively low level of disruptive and destructive cyber activity that Russian state and criminal threat actors have unleashed, as of 15 March 2022, as part of the invasion of Ukraine and following the imposition of sanctions on Russia.[383]

Likely hypothesis analysts have identified for this shortfall include the following:

- Strategic restraint, as Russian planners may have refrained from destroying communications infrastructure they want to use and take over.
- Defense improvements and resilience in both Ukraine and other countries that could be cyber targets in this crisis.
- Russian operations that have not yet become public.
- Russian preparations laying the groundwork for new operations.

[378] hxxps://ria[.]ru/20220319/gps-1778998824.html
[379] https://www.bleepingcomputer.com/news/technology/russia-facing-internet-outages-due-to-equipment-shortage/
[380] https://www.bleepingcomputer.com/news/technology/intel-shuts-down-all-business-operations-in-russia/
[381] https://home.treasury.gov/system/files/126/russia_gl25.pdf
[382] https://www.bleepingcomputer.com/news/technology/us-eases-sanctions-that-may-lead-to-russias-internet-isolation/#.YlBIH3x1Ab0.twitter
[383] https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/ https://www.lawfareblog.com/cyber-realism-time-war, https://twitter.com/thegrugq/status/1499311771642830851, https://twitter.com/DAlperovitch/status/1497021630220218371, https://twitter.com/johnhultquist/status/1499112887767511048 and https://www.nytimes.com/2022/02/18/technology/kazakhstan-internet-russia-ukraine.html

Copyright © 2022 Accenture. All Rights Reserved.

- Turmoil in cyber criminal circles (ACTI has observed Russian and Ukrainian underground community members facing off against each other on ideological grounds).

Officials' explanations for the low levels of sophisticated Russian-state threat activity cite improved Ukrainian preparation; these explanations follow:

- **US Official's Assessment:** On 8 March, at the US House of Representatives' Intelligence Committee's annual hearing on worldwide threats, National Security Agency director Paul Nakasone told the committee that the US has observed "three or four" Russian cyber attacks on Ukraine. Asked why the world has not seen more attacks, Nakasone cited "I think that's obviously some of the work that the Ukrainians have done, some of the challenges that the Russians have encountered and some of the work that others have been able to prevent their actions."[384]

    - On 9 March, the Financial Times enumerated US government efforts since October 2021 to harden Ukrainian cyber networks against an expected Russian offensive. For example, US experts reportedly found wiperware on the networks of Ukrainian Railways and were able to remediate it, allowing Ukrainians to escape to safety via rail. Similar malware had remained undetected in the networks of Ukraine's border police, likely contributing to computer failures at one border crossing in early March. The US government has also called on private companies to help: following the 23 February DDoS attacks against Ukrainian government entities, US officials rapidly approved and funded the installation of Fortinet software on Ukrainian police servers.[385]

- **Ukrainian Official's Assessment:** On 16 March, Viktor Zhora, head of Ukraine's cybersecurity service, said that since the start of Russia's invasion there have not been "sophisticated cyberattacks against Ukraine's vital information infrastructure".[386] He noted there have been no attacks similar to WhisperGate or previous cyber attacks on Ukraine's energy grid, or similar to NotPetya attacks.[387] He attributed this to three factors:

    - Russian hackers previously spent a lot of time preparing for such attacks; now they lack the time to do so.

    - Russia does not need to use cyber attacks for this purpose as it is already engaged in open war with Ukraine and can therefore use other means of attack, presumably referring to kinetic weapons.

    - The potential of Russia's hackers has probably been "somewhat overestimated" and that, while risks still exist, Ukraine has "become much stronger lately."

Other assessments about this low-level activity include the following:

- **24 February Disruption More Severe Than Initially Known:** As of 15 March, information is coming to light about the extent of disruptive operations against Ukrainian communications that occurred on 24 February, the day of the Russian

[384] https://therecord.media/intel-chiefs-lawmakers-wait-for-other-shoe-to-drop-on-russian-cyberattacks-against-ukraine/
[385] https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471
[386] hxxps://cip.gov[.]ua/en/news/viktor-zhora-potencial-rosiiskikh-khakeriv-imovirno-pereocinenii
[387] https://t.me/dsszzi_official/2386

Copyright © 2022 Accenture. All Rights Reserved.

invasion. The disruption of the KA-SAT satellite Internet provider, as mentioned above, caused a "huge loss" to Ukrainian communications and disrupted Internet service for tens of thousands of European customers for weeks at least. Furthermore, major Ukrainian telecommunications provider Triolan admitted that it too had experienced a disruption on 24 February.[388] If additional incidents from 24 February come to light and are attributed to Russia, analysts may revise their view of a relative lack of Russian cyber threat activity.

- **Cyber Threat Activity for Psychological Effect:** Despite the relatively low level of disruptive cyber threat activity, much more central to the crisis has been cyber-enabled information operations to "hack minds" and control the information space by demoralizing enemy fighters and populations, hindering communications among political and military leaders, and influencing adversary decision-making. This psychological emphasis helps explain the different intensities and types of attacks that occurred at different stages:

  - **Deterrence:** In the weeks before the invasion, a suspected Russian state-backed attack disrupted Canada's foreign ministry,[389] and Russian-origin criminal ransomware paralyzed fuel distribution and port infrastructure in Germany, Belgium, and the Netherlands.[390] ACTI assesses that both had the effect of illustrating the vulnerability of NATO's infrastructure and the likely consequences of harsh sanctions against Russia. However, they have failed to prevent countries from unifying behind harsh anti-Russian sanctions.

  - **Justification:** In the days before the invasion, as the US government predicted, the Russian government used cyber-enabled disinformation to create a pretext for the invasion and justify it in the eyes of domestic Russian and global opinion.[391] They have succeeded in convincing the Russian population but have not influenced global public opinion.[392]

  - **Communications Disruption:** On the day of the invasion, the Viasat outage likely pursued the goal of disabling the Ukrainian military assets that use its satellite communications. ACTI is unaware of evidence indicating whether the Viasat attack has hindered Ukrainian military communications.

  - **Demoralization:** After the attack began, some of the most immediate threat activities have included using stolen identities and personal information to craft disinformation campaigns that demoralize Ukrainians, Poles, and others in the region and reduce their will to fight Russia.

  - **Degradation Operation:** The current conflict also leads to another form of psychological damage resembling a "degradation operation" to frustrate

[388] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/
[389] https://globalnews.ca/news/8533835/global-affairs-hit-with-significant- multi-day-disruption-to-it-networks-sources/
[390] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not- coordinated-officials-say/
[391] https://www.janes.com/defence-news/news-detail/behind-the-veil-information-warfare-in-ukraine-paves-a-shadowy-path-to-war
[392] https://www.bbc.com/news/world-europe-60600487

Copyright © 2022 Accenture. All Rights Reserved.

defenders, with "discord, confusion, and fatigue" amounting to what researcher Alex Orleans has called "death by a thousand cuts".[393]

On 12 April, after reports of likely Russian attempts to cripple a Ukrainian utility with a new version of the Industroyer (CRASHOVERRIDE) malware and evidence of sustained and repeated use of wipers and other malware targeting OT in key areas, such as the energy sector, some analysts who previously avoided applying the term "cyberwar" to Russian activity have conceded that this activity looks like cyber warfare.[394]

- On 12 April, analyst JD Work of the US National Defense University tweeted (using the Twitter account @HostileSpectrum), "Count of major cyber engagements in Ukraine stands at least a dozen different fires [sic] types across government defense, transportation, telecom, energy. Operational targeting with intended strategic effects. Reporting lag remains same or worse. Yes, this war is also a cyberwar." Work added, "One notes these fires have included worms, with variable execution guardrails. Keep in mind always that we still almost certainly have not seen war reserve capabilities deployed, that are held in reserve for strategic fires under conditions of regional war or large scale war".[395]

- On 14 April, the Russian Foreign Ministry website posted a commentary by Andrey Krutskikh, a veteran Russian cyber negotiator, dismissing Western countries' warnings about Russian cyber attacks. Citing international hacktivist attacks against Russia, Krutskikh said, "The US government and their allies are more and more frequently accusing Russia of 'preparing for a cyber-war' with the West…they claim we intend to retaliate for sanctions. In that way, apparently, they are trying to justify to their own domestic audience the massive cyber-aggression that is already being carried out against our country and also justify new measures for pressuring Russia." He also complained that the US refuses to accept Russia's proposals for international agreements on information security. He concluded, "We warn Western functionaries against flirting with the hacker community. Don't sink to the Machiavellian logic 'against the enemy, all means are good'".[396] A Russian Foreign Ministry tweet about Krutskikh's essay shows a banner headline: "Who sows the cyber-wind will reap the cyber-whirlwind".[397] This headline appears to blame the pro-Ukrainian hacktivism on the US and to threaten the US with reprisals in the cyber sphere.

What To Expect

If state-dominated actors and pro-Russian cyber criminal actors recover from initial setbacks and turmoil and reckon with the changed landscape of the conflict, and complete the prepositioning campaigns currently underway, they will likely take advantage of the defender community's burnout and will renew attacks when these will have the greatest psychological effect. In ACTI's assessment, events and circumstances that could trigger renewed Russian state-associated cyber threat activity could include the following:

- Moments of decision such as elections, sanctions discussions, and court cases

[393] https://www.youtube.com/watch?v=4XTTYr5rrrw&t=883s
[394] https://twitter.com/ILDannyMoore/status/1513842172679933952?cxt=HHwWgMC-ye7bn4IqAAAA
[395] https://twitter.com/HostileSpectrum/status/1513842907240968193
[396] hxxps://mid[.]ru/ru/press_service/1809317/?msclkid=95f247eebc2211ec8f5f530d2df3cf1c
[397] https://twitter.com/MID_RF/status/1514639078876143620

Copyright © 2022 Accenture. All Rights Reserved.

- High-profile events from which countries have excluded Russia, such as the World Cup qualifying matches through 24 March and the World Figure Skating Championships, scheduled for 21 to 27 March in France.
- Advances in the development of alternative energy or other moves that could reduce Russia's fossil fuel revenue. Symbolic dates, such as the anniversary of victory over Germany in World War II. Russia celebrates this holiday on 9 May.

This assessment may evolve as ACTI continues to analyze ongoing developments.

Dates to Watch

Dates and timeframes that Russian strategists might choose for psychological impact include:

- **24 April:** This marks the second round of presidential elections in France, pitting incumbent president Emmanuel Macron against Marine LePen. Russia has supported LePen in the past; the "Macron Leaks" cyber-enabled information leak targeted Macron's candidacy in 2017 to assist LePen.[398]
- **9 May:** This marks the anniversary of the victory over Germany in World War II. Putin draws on the memory of WWII for legitimacy and popular support. Putin will likely want something he can show as a victory by this date. Victory could include a face-saving reduction in hostilities or some kind of humiliating blow to one of Russia's adversary countries. Russia reportedly plans to hold a "referendum" in the Russian-occupied Ukrainian city of Kherson between 1 and 10 May 2022. Analyst Samuel Ramani of the UK's Royal United Services Institutes notes that if Russia can engineer a positive vote for Kherson to join Russia, Putin could present that as a victory on 9 May.[399]
- **May – June:** Analysts expect that Finland and possibly Sweden will apply to join NATO after years of neutrality. A NATO meeting scheduled for 29-30 June is one date analysts are watching in relation to this.[400]

Related Threat Groups and Capabilities

Several threat groups aligned with Russian interests are active against Ukraine and Eastern European targets. Notably, some groups do carry out destructive attacks, primarily against Eastern Europe critical infrastructure. Although these groups are highly regimented in their missions and target sets, the spillover from these events could affect organizations outside of their traditional target sets, as seen with the NotPetya attacks in 2017, the fallout of which was partly due to the potency of ShadowBroker exploits that facilitated an extremely wormable wiper campaign. Russia-sympathetic cyber crime operators and the presence of cyber crime operations in Ukraine present additional opportunities for criminal actors to be involved in threat activity.

[398] https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf
[399] https://twitter.com/SamRamani2/status/1515642316622553097
[400] https://www.dw.com/en/finland-sweden-expect-rapid-domestic-debate-on-nato-membership/a-61458860

Copyright © 2022 Accenture. All Rights Reserved.

Primary Russian-based Threat Groups

Accenture Cyber Threat Intelligence (ACTI) assesses the following groups are most active within Ukraine and Eastern Europe:

- **SANDFISH (a.k.a. Sandworm, TeleBots, Quedagh, BlackEnergy, Voodoo Bear, TEMP.Noble, GreyEnergy):** This threat group has carried out a wide variety of attacks, targeting political entities, the press, and critical infrastructure. These attacks include the 2015 and 2016 blackouts in Ukraine and the June 2017 NotPetya pseudo-ransomware campaign.
- **WINTERFLOUNDER (a.k.a. Gamaredon Group, Calisto Group, Dancing Salome)**: ACTI has traced this group's activity back to 2013 when the group's social engineering campaigns targeted the Ukrainian government, military, and law enforcement agencies. These campaigns continued through 2014 and 2015, reaching peaks during the heaviest fighting between Ukrainian national forces and pro-Russian separatists. In fact, many decoy documents dropped by WINTERFLOUNDER campaigns leveraged related topics, such as Ukraine and Russia casualty reports, troop movements, etc. More-recent targeting by WINTERFLOUNDER suggests Ukrainian collection is still a priority. However, ACTI has also observed additional targeting to include other nations in Eastern Europe, suggesting WINTERFLOUNDER's scope may widen as tensions increase.
- **WALLEYE (a.k.a. Zebrocy, Earworm):** Based on its victims since as early as 2018, WALLEYE's traditional intelligence mission focuses on gathering intelligence against state institutions, security bodies, and military industries in Eastern Europe, the Middle East, and South and Central Asia. While WALLEYE may sometimes share infrastructure with other Russia-based groups, WALLEYE's toolset and targeting remains distinct. In fact, unlike other Russia-based groups, there is little known WALLEYE targeting of Western European or North American countries, which is likely due to WALLEYE's mission, which appears to be aligned with that of a different part of a military and security establishment than, for example, SNAKEMACKEREL's (a.k.a. APT28, Swallowtail, Sofacy, Fancy Bear) mission.

Ukrainian authorities have attributed activity described in this report to the following groups:

- UAC-0056 (a.k.a. TA471, UNC2589, SaintBear, Lorec53)
- DEV-0586, the group that carried out the WhisperGate attacks in January
- UAC-0020 (a.k.a. Vermin), associated with the "so-called security agencies of the so called LNR [the separatist Luhansk 'republic']," according to CERT-UA (https://cert.gov.ua/article/37815)
- InvisiMole (https://cert.gov.ua/article/37829), which ACTI assesses is linked with hacker group WINTERFLOUNDER (a.k.a. Gamaredon)
- UNC1151, the Belarusian/Russian group behind the Ghostwriter campaigns
- UAC-0088 (https://cert.gov.ua/article/38088).
- UAC-0026, which researchers have linked with a Chinese-speaking group called Scarab.

Copyright © 2022 Accenture. All Rights Reserved.

ACTI assesses the following groups are most active in targeting critical infrastructure:

- **BLACK GHOST KNIFEFISH (a.k.a. Dragonfly, Berserk Bear, Energetic Bear):** This group, which the US government has linked to the Russian government, is known for targeting energy entities in multiple countries.[401] In March 2018, the US Department of Homeland Security's (DHS') CISA wrote that "Russian government cyber actors" had "gained remote access into energy sector networks" and accessed a human machine interface.[402] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[403] targeting of network infrastructure devices (such as routers, switches, firewalls, and network intrusion detection systems) enabled with the generic routing encapsulation protocol, Cisco Smart Install feature, or simple network management protocol. The threat actors conducted man-in-the-middle attacks for espionage, to steal intellectual property, and potentially to prepare for future disruptive or destructive activity.

  Signs of cooperation exist between BLACK GHOST KNIFEFISH and BELUGASTURGEON (a.k.a. Turla), according to US and UK officials. BELUGASTURGEON's targets are mostly political entities but have included the Armenian natural resources ministry.[404] UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors.[405]

- **ZANDER:** This group carried out the August 2017 Triton malware attack on the operational technology (OT) systems of a refinery in Saudi Arabia, which, if it had been successful, could have endangered human lives.[406] The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics (TsNIIKhM) under Russia's Defense Ministry.[407] ZANDER has also searched for remote login portals and vulnerabilities in the networks of at least 20 targets in electricity generation, transmission, and distribution systems in the US and elsewhere.

- **Pseudo- and Hybrid Ransomware:** The WhisperGate campaign this report describes below appears to be pseudo-ransomware its developers created with purely disruptive rather than money-making intentions. ACTI assesses that some ransomware criminals may choose targets and timing that align with Russian state priorities due to patriotic motives, law enforcement pressure to cooperate, or hope to avoid punishment through patriotic gestures. The US Department of the Treasury has stated that HighRollers (a.k.a. Evil Corp) boss Maksim Yakubets has worked for the FSB.[408] WIRED, citing leaked private chats, alleged that TrickBot and Conti ransomware operators have at times received targeting guidance from members of JACKMACKEREL (a.k.a. Cozy Bear), a group the US has linked to Russia's Foreign Intelligence Service.[409] Additionally, a half-dozen suspected REvil ransomware operators and at least one suspect in the Colonial Pipeline attack have been in Russian custody since mid-January, according to reports.[410] ACTI assesses that

[401] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[402] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[403] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
[404] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[405] https://www.ncsc.gov.uk/news/turla-group-behind-cyber-attack and https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims
[406] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments
[407] https://home.treasury.gov/news/press-releases/sm1162
[408] https://home.treasury.gov/news/press-releases/sm845
[409] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a
[410] https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/

Copyright © 2022 Accenture. All Rights Reserved.

Russian law enforcement has sometimes used the threat of law enforcement action to compel criminals to cooperate in state-directed threat activity in the past.[411]

Mitigations

To mitigate the risk of potential cyber threats stemming from Russia's invasion of Ukraine, Accenture's Cyber Investigation and Forensics Response (CIFR) team suggests the following high-priority tactical mitigations and secondary strategic mitigations. Following these are suggested urgent measures organizations can take in the case of a crisis:

High-priority Tactical Mitigations

Patching externally facing infrastructure (virtual private network appliances, firewalls, web servers, load balancers, etc.) to the latest supported vendor releases, as threat actors often exploit vulnerabilities in externally facing infrastructure to gain initial access to an environment.

- Auditing domain controllers to log successful Kerberos TGS (ticket-granting service) requests and monitoring such events for anomalous activity.
- Having an adequate incidence response (IR) retainer in place to provide necessary surge support and domain-level IR expertise in the event of an incident.
- Treating malware detections for Cobalt Strike and webshells with high priority, as an attacker could use them for lateral movement and persistence.
- Testing and conducting backup procedures on a frequent, regular basis and isolating backups from network connections that could enable malware spreading.

Secondary Strategic Mitigations

To mitigate the threat of cyber threats stemming from hostilities between Russia and Ukraine, CIFR treating the following mitigation suggestions with a strategic mindset:

- Monitoring service accounts and administrator accounts for signs of credential misuse and abuse, especially for accounts that should not have interactive logon rights.
- Monitoring installation of file transfer tools such as FileZilla and rclone as well as the processes associated with compression or archival tools.
- Creating, maintaining, and periodically exercising a cyber incident response and continuity of operations plan.
- Identifying a resilience plan that addresses how to operate, given a loss of access to or control of an information technology (IT) and/or operational technology (OT) environment.

[411] https://buzzfeednews.com/article/sheerafrenkel/inside-the-hunt-for-russias-hackers

Copyright © 2022 Accenture. All Rights Reserved.

- Implementing network segmentation between IT and OT networks, where appropriate.
- Implementing effective credential and password policies, rejecting weak passwords, or enforcing strong password rules.
- Implementing strong encryption procedures to prevent threat actors from accessing sensitive data.
- Implementing email anomaly detection systems to detect spear-phishing links.

Government- and Vendor-provided Mitigations

In addition to CIFR's secondary strategic mitigations, ACTI suggests that organizations consult relevant government alerts for guidance; for the US, these include the following:

- "Understanding and Mitigating Russian State-Sponsored Cyber Threats to US Critical Infrastructure" 11 January 2022 (https://www.cisa.gov/uscert/ncas/alerts/aa22-011a).
- "Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure" (https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf).
- Patching the vulnerabilities that Cisco Talos has assessed as most likely for threat actors to exploit (https://blog.talosintelligence.com/2022/03/ukraine-update.html).

ACTI suggests that organizations consider the mitigations that CISA and the FBI recommended in a 22 March 2022 stakeholder phone call. CISA and the FBI provided some of these with the US specifically in mind, but they are applicable to organizations in other countries as well; they are:

- Actively hunt for any indications of Russian state-sponsored tactics, techniques, and procedures (TTPs), using the abovementioned 11 January 2022 CISA document for reference.
- Know your network and any connectivity you have in Russia and surrounding territories.
- Mitigate public-facing vulnerabilities, particularly actively exploited ones, referring to CISA's Known Exploited Vulnerabilities catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) for guidance.
- Secure credentials.
- For organizations with OT or ICS, take note of any unexpected behavior such as reboots.
- Refer to the US alert on SatCom threats (https://www.cisa.gov/uscert/ncas/alerts/aa22-076a) if satellite communication networks are in use.
- Take steps possible to maximize resilience.
- Dust off and exercise incident response plans, designate a crisis response team, ensure key personnel, test backups, test manual controls. Make sure your plans

Copyright © 2022 Accenture. All Rights Reserved.

include contact information for the FBI and CISA and that you know in advance whom you would hire for incident response and legal services.

- Call the FBI field office quickly if you see social media posts indicating disinformation.
- Report to CISA or local FBI offices any anomalous activity even if it appears to be mundane or routine scanning.

Crisis Recommendations for Cybersecurity Leadership

Immediate

CIFR suggests that immediately after an incident, cybersecurity leadership:

- Review all escalation lists, contact information, and plans, and distribute hard copies of those plans to critical delivery teams.
- Review plans and playbooks for disruptive/destructive attacks.
- Ensure that an out-of-band communications capability is in place and practiced, especially for clients of cloud-delivered mail and domain services.
- Communicate workforce safety measures.
- Communicate the need for heightened awareness and vigilance for new attacks and inbound threats, including phishing campaigns and attacks against potential external vulnerabilities. Scrutinize events and infrastructure, including administrative actions, and search for:
  - Known bad indicator (e.g., an attack will most likely not originate from a Russian or even foreign IP address).
  - Anomalous behavior (e.g., hosts acting out of the norm but not necessarily demonstrating malicious and/or odd administrative activity).
  - Suspicious activity (e.g., with respect to users or administrators).
- Identify critical supply chain vendors.

Week One

CIFR suggests that within the first week after an incident, cybersecurity leadership:

- Communicate to cybersecurity delivery leads the need to review current telemetry (hunt) for potentially missed IOCs related to Russian threat actors.
- Build a critical threats watchlist for known tactics, techniques, and procedures (TTPs) and ATT&CK model vectors.
- Review and prioritize BC/DR critical-asset lists to support potential response efforts.
- Review IT/OT cybersecurity vision completeness.
- Review availability of current staffing and delivery team to ensure capacity for major disruptions. Maintain IR teams with relevant IT and/or OT capabilities. In the event of suspicious activity or an attack, it is crucial to have the following types of third parties on standby:

Copyright © 2022 Accenture. All Rights Reserved.

- One or more threat intelligence partners to receive bulletins and updates and validate findings.
- One or more IR partner(s) to handle surge capacity in the event of an attack or to validate security operations center findings.

- Communicate workforce safety measures.
- Contact critical supply chain vendors to ensure both awareness and review of "ideal versus actual" process efficacy (e.g., use of multi-factor authentication and VPNs, and insider threat mitigations).

Long-term
In the long-term after an incident, CIFR suggests that to better mitigate future incidents, cybersecurity leadership practice recovery plans for all areas of the business, ensuring:

- Administrators have secured immutable backups offline.
- Restoration bandwidth can support domain-wide impacts.
- Awareness of potential physical impacts.
- Review of IT/OT response plans for currency and completeness and ensure that staffing and controls are sufficient to address known Russian TTPs and relevant industry threats.
- The right parties have access to multiple threat intelligence sources and relevant leadership and technical ingestion capabilities exist.
- Close monitoring of social media, news outlets, and threat intelligence partner bulletins for advance warnings of attacks.

Crisis Recommendations for Cybersecurity Operations and Delivery Teams

Immediate
CIFR suggests that immediately after an incident, cybersecurity operations and delivery teams:

- Print and distribute IR planning and contact information.
- Review delivery team staffing and availability.
- Ensure retro-hunting of all published IOCs-or, at minimum, six months back-to help determine that there are no active threats.
- Increase escalation points of contact to ensure timely and comprehensive understanding of suspected or detected malicious events.
- Validate knowledge, labeling, and cataloging of the enterprise's high-value assets for heightened monitoring.
- Communicate preparedness plans upward to C-suite and other executives.

Copyright © 2022 Accenture. All Rights Reserved.

Week One
CIFR suggests that within the first week after an incident, cybersecurity operations and delivery teams:

- Review published TTPs and validate that existing controls can detect them.
- Initiate critical resource backups and configuration preservation, if not current, and ensure critical systems are ready for restoration.
- Review/renew peer and law enforcement intelligence and notification relationships to support information sharing.

Long-term
In the long-term after an incident, CIFR suggests that to better mitigate future incidents, cybersecurity operations and delivery teams practice recovery plans for all areas of the business, ensuring:

- Close identification of detection gaps.
- Alignment of security controls and content development to proactive threat intelligence sources.
- Completely offline storage of critical information and contacts (email addresses and phone numbers) necessary to use in a crisis, as threat actors could target these contacts to complicate response efforts if such contact information is accessible online.
- Practice of two scenarios—internet down and destructive attacks—that would involve changing or wiping out critical data.
- Close partnerships with physical security teams.

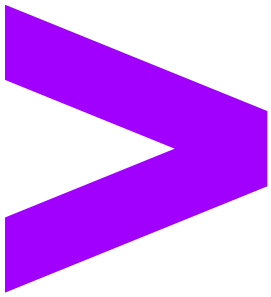
About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.

Accenture Cyber Threat Intelligence, part of Accenture Security, has been creating relevant, timely and actionable threat intelligence for more than 20 years. Our cyber threat intelligence and incident response team is continually investigating numerous cases of financially motivated targeting and suspected cyber espionage. We have over 150 dedicated intelligence professionals spanning 11 countries, including those with backgrounds in the Intelligence Community and Law Enforcement. Accenture analysts are subject matter experts in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats.

Copyright © 2022 Accenture. All Rights Reserved.



LEGAL NOTICE & DISCLAIMER: © 2022 Accenture. All rights reserved. Accenture, the Accenture logo, Accenture Cyber Threat Intelligence (ACTI) and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from ACTI. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change.

ACCENTURE PROVIDES THE INFORMATION ON AN “AS-IS” BASIS WITHOUT REPRESENTATION OR WARRANTY AND ACCEPTS NO LIABILITY FOR ANY ACTION OR FAILURE TO ACT TAKEN IN RESPONSE TO THE INFORMATION CONTAINED OR REFERENCED IN THIS ALERT.

Copyright © 2022 Accenture. All Rights Reserved.