accenture

Global Incident Report: Russia-Ukraine Crisis March 25

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.

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 an update and continuation of the Global Incident Report dated March 17 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 covers US, United Kingdom and Ukrainian warnings about Russian cyberespionage and probing activity that could facilitate future attacks; hacktivist activity against Russian entities and against companies doing business in Russia; disruptive incidents involving Russia-based threat actors; updates on Russia's internet isolation; and updates to the lists of threat actors and mitigations.

MITIGATIONS are available at the end of this report.

Analysis

Cyber-related Events Involving Ukraine, Russia and Belarus

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

[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

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.[2]

- 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.[3] 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.[4]

- On 10 March, CyberScoop detailed how criminals are posing as fundraisers for Ukraine to steal cryptocurrency.[5]

- 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".[6]

- 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.[7]

- 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[8], which is also tracked as TA471, SaintBear, and Lorec53.[9]

- 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.[10]

- 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

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

Signal" to learn of Russian troop movements.[11]

- 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.[12]

- 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".[13]

- 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.[14]

- 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.[15]

- 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.[16]

- 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.[17]

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

- 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 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.[18]

- In a 16 March briefing, Ukrainian cybersecurity official Viktor Zhora claimed that "enemy hackers" had conducted over 3,000 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.[19]

- 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.[20]

- 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.[21]

- 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.[22]

- 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).[23] 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

[18] 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
[19] https://24tv.ua/ru/za-misjac-ukrainski-servisi-zaznali-ponad-3-tisjach-ddos-atak_n1908711
[20] https://cert.gov.ua/article/37815
[21] https://twitter.com/dsszzi/status/1504899939322765314
[22] https://www.nytimes.com/2022/03/17/briefing/russia-ukraine-war-kharkiv.html
[23] https://cert.gov.ua/article/37829

connectivity" associated with power outages, according to NetBlocks.[24] In Kherson, the power cuts come amid protests against Russia's occupation.[25]

- 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.[26]

- 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.[27]

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 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, published on 12 March, which @Cyberknow20 published on 20 March, listed 51 pro-Ukrainian and 25 pro-Russian groups.[28]

- 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.[29]

- 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.[30]

- 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.[31] On 1 March, NB65 had also claimed it would leak data from Roscosmos,

[24] https://twitter.com/netblocks/status/1505308560477073409
[25] https://twitter.com/netblocks/status/1505550245912006659
[26] https://cert.gov.ua/article/38088
[27] https://cert.gov.ua/article/38097
[28] https://twitter.com/Cyberknow20/status/1505526132481097728
[29] 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
[30] https://twitter.com/S0ufi4n3/status/1501851883882921987
[31] http://web.archive.org/web/20220313070149/

the Russian state space agency.[32]

- 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".[33]

- 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.[34]

- 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.[35]

- 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.[36]

- On 13 March, #LeakTheAnalyst claimed it would release sensitive US military research data from research organization SRI International.[37] On 14 March, the same entity announced it was leaking information of job candidates for the UK Defense Ministry on its victim list.[38] The veracity of this claim is unclear.

- 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".[39]

- 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[40], had sent over 20 million messages.[41]

- 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.[42]

[32] https://twitter.com/YourAnonTV/status/1498792639877074945
[33] 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/
[34] https://www.reuters.com/article/ukraine-crisis-russia-hack-idCNL5N2VE4EU
[35] hxxps://www.securitylab[.]ru/news/530582.php
[36] https://www.bbc.com/news/technology-60697261
[37] https://twitter.com/S0ufi4n3/status/1503057681506095105/photo/1
[38] https://twitter.com/darktracer_int/status/1503378378555940864
[39] https://www.spiegel.de/netzwelt/web/bundeskriminalamt-ermittelt-hackerangriff-auf-rosneft-deutschland-a-74e3a53a-e747-4500-8198-ea6780a7d79a
[40] https://twitter.com/AnonymousVideo/status/1503484842809438208
[41] https://twitter.com/squad3o3/status/1503428370306113536
[42] https://twitter.com/IAmMrGrey2/status/1503396245477502980

- On 14 March, Ukrainian media reported that Ukraine's amateur "IT Army" had reached 300,000 members.[43]

- 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".[44]

- 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.[45]

- 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 life".[46]

    - To guard Russian users against such "protestware," Sberbank urged Russians to turn off automatic software updates, according to Russian cybersecurity company Positive Technologies.[47]

- 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:[48]

    - 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

[43] hxxps://tech.segodnya[.]ua/tech/v-ukrainskoy-kiberarmii-uzhe-300-tysyach-chelovek-kak-tuda-popast-i-chem-oni-zanimayutsya-1608837.html
[44] https://twitter.com/Cyberknow20/status/1503699552989167617
[45] https://blog.aquasec.com/cloud-native-attacks-russia-ukraine
[46] https://www.vice.com/en/article/dypeek/open-source-sabotage-node-ipc-wipe-russia-belraus-computers
[47] https://twitter.com/iiyonite/status/1505122185886810114
[48] https://www.websiteplanet.com/blog/cyberwarfare-ukraine-anonymous/

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[49] and the Kremlin.[50] Leak victims include Russian state pipeline company Transneft.[51]

- From 19 to 21 March, pro-Ukrainian hacktivists claimed to have disrupted access to the city of Grodno, Belarus[52] and to Russian government targets, including:
  - The Ministry of Foreign Affairs[53]
  - The backend of the Foreign Intelligence Service's secure drop site on the TOR anonymity service[54]
  - The government of the Voronezh region[55]
  - The Vologda Research Center of the Russian Academy of Sciences[56]
  - The Joint Institute of Nuclear Research[57]
  - Russian weather agency Roshydromet[58]
  - A Russian defense contractor[59]

- 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".[60]

- 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,[61] which has faced criticism for continuing to do business in Russia.[62]

- 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!".[63]

---

[49] hxxps://www.kommersant[.]ru/doc/5259896
[50] https://twitter.com/YourAnonNews/status/1504104835242725379
[51] https://twitter.com/MikaelThalen/status/1504317329550704643
[52] https://twitter.com/_Blue_hornet/status/1505460977550118913
[53] https://twitter.com/BeeHiveCyberSec/status/1505264447106867201
[54] https://twitter.com/_Blue_hornet/status/1505162369223307264
[55] https://twitter.com/_Blue_hornet/status/1505173866469117955
[56] https://twitter.com/_Blue_hornet/status/1505616461582188544
[57] https://twitter.com/_Blue_hornet/status/1505183938544914433
[58] https://twitter.com/S0ufi4n3/status/1505945517557231620
[59] https://twitter.com/AlvieriD/status/1505569186457669633
[60] https://web.archive.org/web/20220320132156/https://twitter.com/_Blue_hornet/status/1505534912044179457
[61] https://twitter.com/_Blue_hornet/status/1505641356026429442
[62] https://fortune.com/2022/03/18/nestle-russia-boycott-denys-shmyhal-tweet-mark-schneider/
[63] https://twitter.com/YourAnonTV/status/1505679705797713927

- 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".[64] 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 look it all over - I think the coordinates may be quite helpful to them".[65] The #DoomSec activists have also leaked what they claim is information on Russian military communications.[66]

- 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".[67] 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.

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).

[64] https://twitter.com/nexta_tv/status/1505613701436559366
[65] https://twitter.com/DeepNetAnon/status/1505815819611123712
[66] https://twitter.com/hashtag/DoomSec
[67] https://www.ibtimes.com.au/anonymous-strikes-russia-printer-attack-disrupts-kremlins-propaganda-1802456

- 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.

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.[68] 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.[69] In January, Israeli pilots reported GPS spoofing from the Russian airbase at Khmeimim in Syria.[70]

- 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.[71]

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

    - A 10 March posting seeking to recruit insiders at telecommunications and video game companies.[72]

    - 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.[73]

[68] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[69] https://www.gpsworld.com/finnish-airline-finds-gps-interference-near-russian-border/
[70] https://www.middleeastmonitor.com/20220201-russia-refuses-israeli-demand-to-stop-jamming-gps-of-flights-into-tel-aviv/
[71] https://www.bleepingcomputer.com/news/security/cisa-updates-conti- ransomware-alert-with-nearly-100-domain-names/
[72] https://twitter.com/S0ufi4n3/status/1502032449643192325
[73] https://www.msn.com/en-us/entertainment/gaming/ubisoft-says-it-experienced-a-e2-80-98cyber-security-incident-e2-80-99/ar-AAUWMgW

- 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.[74]

- 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.[75]

- According to a dox (i.e., a release of personal information) from March 7[76], 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.[77]

- Previous attacks on Toyota and Volvo had led to suspicions of connections between the attacks and Japan's and Sweden's support for Ukraine[78].

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.[79]

[74] https://twitter.com/S0ufi4n3/status/1501269430025826311
[75] https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/
[76] hxxps://doxbin[.]com/upload/white
[77] https://twitter.com/BleepinComputer/status/1503388889007939586
[78] https://www.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html, SITREP version 8.1
[79] https://www.independent.ie/regionals/kerryman/news/kerry-county-council-on-cyber-attack-alert- over-suspicious-russian-online-activity-41439254.html

- On 11 March, Bridgestone Americas confirmed it had suffered a ransomware attack. The LockBit ransomware group has indeed leaked data belonging to Bridgestone.[80] LockBit actors had previously vowed to leak data from anti-Russian countries and entities.[81]

- 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.[82] 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".[83]

    - On 15 March, NetBlocks reported that KA-SAT's network "remains heavily impacted," 18 days after the 24 February cyber attack.[84] 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 were still offline" and that it would take weeks to recover.[85]

- On 12 March, the French School of Civil Aviation fell victim to Hive ransomware.[86] 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).

---

[80] https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware- attack-lockbit-leaks-data/
[81] https://acn-marketing-blog.accenture.com/wp- content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog- 14MARCH22.pdf
[82] https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
[83] https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html
[84] https://twitter.com/netblocks/status/1503791987161505801
[85] https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/
[86] https://www.lemagit.fr/actualites/252514685/LEcole-Nationale-de-lAviation-Civile-paralysee-par-une-cyberattaque

- 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.[87] Putin's September 2020 speech had demanded that the US not "intervene" in Russian affairs.[88] Russian officials interpret "interference" broadly to include any criticism of the country.[89]
  - 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.[90] 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[91], were scheduled to be eligible for release on bail on 13 March.[92]

- 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.[93]

- 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".[94]

- 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".[95] 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 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.

[87] hxxps://tass[.]ru/politika/14063755
[88] https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html
[89] https://www.dw.com/en/world-leaders-condemn-navalny-sentence-russia-denounces-interference/a-56436335
[90] https://twitter.com/C_C_Krebs/status/1503395668387377155
[91] https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest/index.html
[92] https://twitter.com/Zilla57826895/status/1482064786770776066
[93] https://rus.lsm.lv/statja/novosti/obschestvo/v-latvii-uchastilis-sluchai-kiberatak.a448086/
[94] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html
[95] https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

- 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.[96]

- 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.[97] 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.” [98]

- 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.[99] 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.[100]

- 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.[101] 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 new report also lists over 150 current and historical C2 servers.[102]

---

[96] https://www.news5cleveland.com/news/local-news/exclusive-fbi-warns-of-increased-cyber-threats-against-northeast-ohio-businesses
[97] https://www.govinfosecurity.com/tennessee-pediatric-hospital-responding-to-cyber-incident-a-18730
[98] https://twitter.com/vxunderground/status/1504238897194221570
[99] https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
[100] https://www.wired.com/story/trickbot-malware-group-internal-messages/, https://www.wired.com/story/conti-ransomware-russia/
[101] https://www.dragos.com/blog/industry-news/suspected-conti-ransomware-activity-in-the-auto-manufacturing-sector/
[102] https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

- 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.[103] An Alstom software glitch also disrupted a signaling system on Spanish rail operator Renfe on 21 March.[104]

- 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.[105] Interested parties can read ACTI's January 2022 blog highlighting GPS-related threats to transportation.[106]

- On 17 March, the ALPHV ransomware group claimed to have exfiltrated data from Noble Oil, a North Carolina-based used oil services recycling company.[107] ALPHV is the same group that has breached petrochemical industry-related logistics and port companies in Europe.[108]

    - 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.[109] 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[110] initiative requests that all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity".[111] 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 development of "nondestructive and destructive counterspace weapons—including

[103] https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/
[104] https://www.reuters.com/world/europe/madrids-suburban-trains-disrupted-after-alstom-software-glitch-2022-03-21/
[105] https://www.bleepingcomputer.com/news/security/europe-warns-of-aircraft-gps-outages-tied-to-russian-invasion
[106] https://www.accenture.com/us-en/blogs/cyber-defense/overreliance-gps-risk
[107] https://twitter.com/S0ufi4n3/status/1504542952110108677
[108] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say/
[109] https://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html
[110] https://www.cisa.gov/shields-up
[111] https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities and ground-based ASAT capabilities—to target U.S. and allied satellites."[112]

- 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.[113] 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[114] 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.[115] 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.[116]

- On 20 March, the Twitter account @ContiLeaks released version 3 of the Conti ransomware source code, which includes a compiled locker and decryptor.[117] 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.[118]

- 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.[119]

- 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.

- 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

---

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

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."[120]

- 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.[121]

- 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.[122]

- Some details of this FBI warning resemble details of the reporting from 7 March on Russian probing of companies that produce liquefied natural gas[123] (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.

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.[124] 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.[125] In a tweet without citation, BBC reporter Joe Tidy said Emsisoft had said the RansomExx crew carried out the attack.[126] 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

[120] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/
[121] https://nypost.com/2022/03/21/white-house-warns-intelligence-points-to-russian-cyberattacks/
[122] https://www.cbsnews.com/news/russia-cyberattacks-us-energy-fbi-warning/
[123] https:/www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine
[124] https://www.theglobeandmail.com/canada/article-canadas-national-research-council-hit-by-cyber-incident/
[125] https://www.bbc.com/news/uk-scotland-60826263
[126] https://twitter.com/joetidy/status/1505928374790893569

that Scotland has demonstratively welcomed Ukrainian refugees.[127]

- 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".[128] 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.[129] 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. Microsoft also acknowledged that Lapsus had breached it.[130]

    - 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."

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.[131] 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.[132]

[127] https://www.bbc.com/news/uk-scotland-scotland-politics-60800831
[128] https://www.zdnet.com/article/okta-says-breach-evidence-shared-by-lapsus-ransomware-group-linked-to-january-hack-attempt/
[129] https://www.wired.com/story/okta-hack-microsoft-bing-code-leak-lapsus/
[130] https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
[131] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[132] https://www.zdnet.com/article/icann-rejects-ukraines-request-to-block-russia-from-the-internet/#ftag=RSSbaffb68

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.[133] 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.[134] This is consistent with the measures required to implement the Sovereign Russian Internet program described elsewhere in this SITREP. This situation may change since LINX's announcement on 11 March that it would stop routing for Rostelecom and MegaFon.[135]

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.[136] Back on March 11, Brian Krebs cited Kentik connectivity researcher Doug Madory as saying "If the other major European exchanges 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.[137]

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.[138]

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".[139] This

[133] https://intelgraph.idefense.com/#/node/intelligence_alert/view/821210b8-16f1-47a3-8c75-1013c8329bd9
[134] https://www.thousandeyes.com/blog/russia-global-internet
[135] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[136] https://www.datacenterdynamics.com/en/news/london-internet-exchange-disconnects-megafon-and-rostelecom/
[137] https://securityboulevard.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[138] https://www.bleepingcomputer.com/news/technology/russia-faces-it-crisis-with-just-two-months-of-data-storage-left/
[139] https://twitter.com/Ilirik1985/status/1504394220576161792

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.[140]

On 17 March, Russia's Digital Ministry announced it would help banks filter traffic from abroad to mitigate a recent wave of DDoS attacks.[141] 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.[142]

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.[143] 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.[144]

On 18 March, data-storage-focused news source Blocks&Files analyzed the Russian cloud storage shortage.[145] 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 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.[146]

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

[140] hxxps://ria[.]ru/20220317/mir-1778662806.html
[141] hxxps://securitylab[.]ru\news\530627.php
[142] https://www.zdnet.com/article/russia-remains-connected-to-the-internet/
[143] https://www.youtube.com/watch?v=O2CfRMTI6QU
[144] https://twitter.com/GroupIB/status/1504414698690822148
[145] https://blocksandfiles.com/2022/03/18/russia-cloud-gap-western-tech/
[146] hxxps://ria[.]ru/20220319/gps-1778998824.html

unleashed, as of 15 March 2022, as part of the invasion of Ukraine and following the imposition of sanctions on Russia.[147]

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.
- 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."[148]
    - 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.[149]

[147] 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
[148] https://therecord.media/intel-chiefs-lawmakers-wait-for-other-shoe-to-drop-on-russian-cyberattacks-against-ukraine/
[149] https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471

- **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".[150] He noted there have been no attacks similar to WhisperGate or previous cyber attacks on Ukraine's energy grid, or similar to NotPetya attacks.[151] 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 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.[152] 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,[153] and Russian-origin criminal ransomware paralyzed fuel distribution and port infrastructure in Germany, Belgium,

[150] hxxps://cip.gov[.]ua/en/news/viktor-zhora-potencial-rosiiskikh-khakeriv-imovirno-pereocinenii
[151] https://t.me/dsszzi_official/2386
[152] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/
[153] https://globalnews.ca/news/8533835/global-affairs-hit-with-significant- multi-day-disruption-to-it-networks-sources/

and the Netherlands.[154] 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.[155] They have succeeded in convincing the Russian population but have not influenced global public opinion.[156]

- **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 defenders, with "discord, confusion, and fatigue" amounting to what researcher Alex Orleans has called "death by a thousand cuts".[157]

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

- 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.

[154] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not- coordinated-officials-say/
[155] https://www.janes.com/defence-news/news-detail/behind-the-veil-information-warfare-in-ukraine-paves-a-shadowy-path-to-war
[156] https://www.bbc.com/news/world-europe-60600487
[157] https://www.youtube.com/watch?v=4XTTYr5rrrw&t=883s

- 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.

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. (Here "wormable" refers to malware that can potentially spread in an automatic, self-sustaining way.[158]) 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.

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

[158] https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

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).

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.[159] 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.[160] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[161] 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

[159] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[160] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[161] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A

Armenian natural resources ministry.[162] UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors.[163]

- **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.[164] The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics (TsNIIKhM) under Russia's Defense Ministry.[165] 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.[166] 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.[167] 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.[168] ACTI assesses that 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.[169]

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)

[162] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[163] 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
[164] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments
[165] https://home.treasury.gov/news/press-releases/sm1162
[166] https://home.treasury.gov/news/press-releases/sm845
[167] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a
[168] https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/
[169] https://buzzfeednews.com/article/sheerafrenkel/inside-the-hunt-for-russias-hackers

- UNC1151, the Belarusian/Russian group behind the Ghostwriter campaigns
- UAC-0088 (https://cert.gov.ua/article/38088).

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.[170] 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.[171] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[172] 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.[173] UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors.[174]

- **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.[175] The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics (TsNIIKhM) under Russia's Defense Ministry.[176] 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.[177] WIRED, citing leaked private chats, alleged that TrickBot and Conti ransomware operators have at times received targeting guidance from members of

[170] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[171] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[172] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
[173] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[174] 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
[175] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments
[176] https://home.treasury.gov/news/press-releases/sm1162
[177] https://home.treasury.gov/news/press-releases/sm845

JACKMACKEREL (a.k.a. Cozy Bear), a group the US has linked to Russia's Foreign Intelligence Service.[178] 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.[179] ACTI assesses that 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.[180]

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.

[178] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a
[179] https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/
[180] https://buzzfeednews.com/article/sheerafrenkel/inside-the-hunt-for-russias-hackers

- 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.
- 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 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:
  - 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.

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.