accenture

Global Incident Report: Russia-Ukraine Crisis March 17

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.
- 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. 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 10 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.

This report update includes new information on the 24 February 2022 Viasat hack, information about ransomware and other incidents that might have links with the Russia-Ukraine conflict, new pro-Russian and pro-Ukrainian hacktivist attacks, and new Internet disruptions and phishing activity targeting Ukraine. It also contains expanded analysis on the extent of Russia's isolation from the global Internet and on the apparent lull in Russian state-sponsored cyber threat activity.

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 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[1].

[1] https://blog.talosintelligence.com/2022/03/threat-advisory-cybercriminals.html

- 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.[2] 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.[3]

- On 10 March, CyberScoop detailed how criminals are posing as fundraisers for Ukraine to steal cryptocurrency.[4]

- 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".[5]

- 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.[6]

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

- 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.[9]

- 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 Signal" to learn of Russian troop movements.[10]

- 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.[11]

---

[2] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/?sh=58cf1f516573
[3] hxxps://mediasat[.]info/2022/03/15/triolan-prodolzhaet-vosstanavlivat-set-posle-kiberataki-gde-uzhe-dostupen-internet/
[4] https://www.cyberscoop.com/cybercriminals-are-posing-as-ukraine-fundraisers-to-steal-cryptocurrency/
[5] https://twitter.com/DougMadory/status/1502038861584740357
[6] https://twitter.com/OliverLinow/status/1502589239053238272
[7] hxxps://cert.gov[.]ua/article/37704
[8] https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/
[9] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[10] https://www.datacenterknowledge.com/networks/battle-intensifies-keep-ukraine-online
[11] https://twitter.com/dsszzi/status/1502683855639171083

- 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”.[12]

- 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[13].

- 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.[14]

- 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.[15]

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, listed 46 pro-Ukrainian and 18 pro-Russian groups.[16].

- 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,

[12] https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K
[13] https://twitter.com/ESETresearch/status/1503436423818534915
[14] https://www.cnn.com/2022/03/14/europe/ukrainian-railways-war-intl-cmd/index.html
[15] https://www.vice.com/en/article/v7djda/ukraine-arrests-hacker-routing-calls-for-russian-troops
[16] https://twitter.com/Cyberknow20/status/1502619395037618180

Roskomnadzor, as an act of information warfare.[17]

- 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.[18]

- 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.[19] On 1 March, NB65 had also claimed it would leak data from Roscosmos, the Russian state space agency.[20]

- 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".[21]

- 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.[22]

- 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[23]..

- 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.[24]

- On 13 March, #LeakTheAnalyst claimed it would release sensitive US military research data from research organization SRI International.[25] On 14 March, the same entity announced it was leaking information of job candidates for the UK Defense Ministry on its victim list.[26] 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

[17] 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
[18] https://twitter.com/S0ufi4n3/status/1501851883882921987
[19] http://web.archive.org/web/20220313070149/
[20] https://twitter.com/YourAnonTV/status/1498792639877074945
[21] 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/
[22] https://www.reuters.com/article/ukraine-crisis-russia-hack-idCNL5N2VE4EU
[23] hxxps://www.securitylab[.]ru/news/530582.php
[24] https://www.bbc.com/news/technology-60697261
[25] https://twitter.com/S0ufi4n3/status/1503057681506095105/photo/1
[26] https://twitter.com/darktracer_int/status/1503378378555940864

pipelines and refineries".[27]

- 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[28], had sent over 20 million messages.[29]
- 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.[30]
- On 14 March, Ukrainian media reported that Ukraine's amateur "IT Army" had reached 300,000 members.[31]
- 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".[32]

Cyber-related Events in Other Countries

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

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

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

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

---

[27] https://www.spiegel.de/netzwelt/web/bundeskriminalamt-ermittelt-hackerangriff-auf-rosneft-deutschland-a-74e3a53a-e747-4500-8198-ea6780a7d79a
[28] https://twitter.com/AnonymousVideo/status/1503484842809438208
[29] https://twitter.com/squad3o3/status/1503428370306113536
[30] https://twitter.com/IAmMrGrey2/status/1503396245477502980
[31] hxxps://tech.segodnya[.]ua/tech/v-ukrainskoy-kiberarmii-uzhe-300-tysyach-chelovek-kak-tuda-popast-i-chem-oni-zanimayutsya-1608837.html
[32] https://twitter.com/Cyberknow20/status/1503699552989167617

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.[33] 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.[34] In January, Israeli pilots reported GPS spoofing from the Russian airbase at Khmeimim in Syria.[35]

- 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.[36]

- 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.[37]

  - 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.[38]

  - 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.[39]

---

[33] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf
[34] https://www.gpsworld.com/finnish-airline-finds-gps-interference-near-russian-border/
[35] https://www.middleeastmonitor.com/20220201-russia-refuses-israeli-demand-to-stop-jamming-gps-of-flights-into-tel-aviv/
[36] https://www.bleepingcomputer.com/news/security/cisa-updates-conti- ransomware-alert-with-nearly-100-domain-names/
[37] https://twitter.com/S0ufi4n3/status/1502032449643192325
[38] https://www.msn.com/en-us/entertainment/gaming/ubisoft-says-it-experienced-a-e2-80-98cyber-security-incident-e2-80-99/ar-AAUWMgW
[39] https://twitter.com/S0ufi4n3/status/1501269430025826311

- 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.[40]

- According to a dox (i.e., a release of personal information) from March 7[41], 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.[42]

- Previous attacks on Toyota and Volvo had led to suspicions of connections between the attacks and Japan's and Sweden's support for Ukraine.[43].

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.[44]

On 11 March, Bridgestone Americas confirmed it had suffered a ransomware attack. The LockBit ransomware group has indeed leaked data belonging to Bridgestone.[45] LockBit actors had previously vowed to leak data from anti-Russian countries and entities.[46]

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

[40] https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/
[41] hxxps://doxbin[.]com/upload/white
[42] https://twitter.com/BleepinComputer/status/1503888889007939586
[43] https://www.cnn.com/2022/03/01/business/toyota-japan-cyberattack-production-restarts-intl-hnk/index.html, SITREP version 8.1
[44] https://www.independent.ie/regionals/kerryman/news/kerry-county-council-on-cyber-attack-alert- over-suspicious-russian-online-activity-41439254.html
[45] https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware- attack-lockbit-leaks-data/
[46] https://acn-marketing-blog.accenture.com/wp- content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog- 14MARCH22.pdf

Russia invaded Ukraine.[47]. 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".[48]

- On 15 March, NetBlocks reported that KA-SAT's network "remains heavily impacted," 18 days after the 24 February cyber attack.[49]

    - 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.[50]

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.[51] Putin's September 2020 speech had demanded that the US not "intervene" in Russian affairs.[52] Russian officials interpret "interference" broadly to include any criticism of the country[53].

- 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.

[47] https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
[48] https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html
[49] https://twitter.com/netblocks/status/1503791987161505801
[50] https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/
[51] hxxps://tass[.]ru/politika/14063755
[52] https://www.nytimes.com/2020/09/25/world/europe/russia-cyber-security-meddling.html
[53] https://www.dw.com/en/world-leaders-condemn-navalny-sentence-russia-denounces-interference/a-56436335

- Some analysts interpreted Syromolotov's comment as a veiled threat from Russia to unleash criminals REvil actors.[54] 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[55],, were scheduled to be eligible for release on bail on 13 March.[56]

- 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.[57]

- 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".[58]

- 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".[59] 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.

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 Rostelecom and Russian mobile provider MegaFon (https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/).However, on 3 March, the Internet Corporation for Assigned Names and

[54] https://twitter.com/C_C_Krebs/status/1503395668387377155
[55] https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest/index.html
[56] https://twitter.com/Zilla57826895/status/1482064786770776066
[57] https://rus.lsm.lv/statja/novosti/obschestvo/v-latvii-uchastilis-sluchai-kiberatak.a448086/
[58] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html
[59] https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

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[60].

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.[61] 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.[62] 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.[63]

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.[64]

Low Levels of Sophisticated Russian State Threat Activity Explained

ACTI and other analysts have admitted surprise at the relatively low level of disruptive and destructive cyber activity that Russian state and criminal threat actors have unleashed, as of 15 March 2022, as part of the invasion of Ukraine and following the imposition of sanctions on Russia[65].

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

[60] https://www.zdnet.com/article/icann-rejects-ukraines-request-to-block-russia-from-the-internet/#ftag=RSSbaffb68
[61] https://intelgraph.idefense.com/#/node/intelligence_alert/view/821210b8-16f1-47a3-8c75-1013c8329bd9
[62] https://www.thousandeyes.com/blog/russia-global-internet
[63] https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/
[64] https://www.bleepingcomputer.com/news/technology/russia-faces-it-crisis-with-just-two-months-of-data-storage-left/
[65] 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

- 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).

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 [66]. 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 (https://globalnews.ca/news/8533835/global-affairs-hit-with-significant- multi-day-disruption-to-it-networks-sources/), and Russian-origin criminal ransomware paralyzed fuel distribution and port infrastructure in Germany, Belgium, and the Netherlands (https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not- coordinated-officials-say/). 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[67]. They have

[66] https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/
[67] https://www.janes.com/defence-news/news-detail/behind-the-veil-information-warfare-in-ukraine-paves-a-shadowy-path-to-war

succeeded in convincing the Russian population but have not influenced global public opinion[68].

- **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"[69].

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, 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.
- 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.

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 and assessed why we have not seen more. Nakasone stated: "I think that's obviously some of the work that the Ukrainians have done, some of the challenges that the

[68] https://www.bbc.com/news/world-europe-60600487
[69] https://www.youtube.com/watch?v=4XTTYr5rrrw&t=883s

Russians have encountered and some of the work that others have been able to prevent their actions"[70].

- 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[71].

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[72].) 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

[70] https://therecord.media/intel-chiefs-lawmakers-wait-for-other-shoe-to-drop-on-russian-cyberattacks-against-ukraine/
[71] https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471
[72] https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

campaigns leveraged related topics, such as Ukraine and Russia casualty reports, troop movements, etc. More-recent targeting by WINTERFLOUNDER suggests Ukrainian collection is still a priority. However, ACTI has also observed additional targeting to include other nations in Eastern Europe, suggesting WINTERFLOUNDER's scope may widen as tensions increase.

- **WALLEYE (a.k.a. Zebrocy, Earworm):** Based on its victims since as early as 2018, WALLEYE's traditional intelligence mission focuses on gathering intelligence against state institutions, security bodies, and military industries in Eastern Europe, the Middle East, and South and Central Asia. While WALLEYE may sometimes share infrastructure with other Russia-based groups, WALLEYE's toolset and targeting remains distinct. In fact, unlike other Russia-based groups, there is little known WALLEYE targeting of Western European or North American countries, which is likely due to WALLEYE's mission, which appears to be aligned with that of a different part of a military and security establishment than, for example, SNAKEMACKEREL's (a.k.a. APT28, Swallowtail, Sofacy, Fancy Bear) mission.

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[73]. 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.[74] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[75] 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[76]. UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors[77]

- **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[78]. The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics

[73] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[74] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[75] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
[76] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[77] 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
[78] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments

(TsNIIKhM) under Russia's Defense Ministry[79]. 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[80]. WIRED, citing leaked private chats, alleged that TrickBot 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[81].

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.

[79] https://home.treasury.gov/news/press-releases/sm1162
[80] https://home.treasury.gov/news/press-releases/sm845
[81] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

Secondary strategic mitigations:

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

- Monitoring service accounts and administrator accounts for signs of credential misuse and abuse, especially for accounts that should not have interactive logon rights.
- Monitoring installation of file transfer tools such as FileZilla and rclone as well as the processes associated with compression or archival tools.
- Creating, maintaining, and periodically exercising a cyber incident response and continuity of operations plan.
- Identifying a resilience plan that addresses how to operate, given a loss of access to or control of an information technology (IT) and/or operational technology (OT) environment.
- 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" (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[82].

[82] https://blog.talosintelligence.com/2022/03/ukraine-update.html

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.

- 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 674,000 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.