Global Incident Report: Russia Ukraine Crisis March 10

Key Findings

- The Russian military action that began 24 February 2022 against Ukraine has cyber and information-warfare components.
- Residents in Ukraine, Belarus, and/or 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.
- 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. This offensive also has a cyber component that could potentially affect parties in multiple locations, including Ukraine, NATO countries, and/or their allies, according to United States (US) and United Kingdom (UK) government assessments.[1]

[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

This report update includes information on incidents affecting the financial, automotive, communications, energy, and other sectors in multiple countries, as well as a new suspected Russian state-sponsored information operation using artificial intelligence (AI)-created faces, and studies on Border Gateway Protocol vulnerabilities and on the state of Ukraine's physical internet infrastructure.

MITIGATIONS are available at the end of this report.

Analysis

As part of the military confrontation, essential businesses and government services within Ukraine, such as commerce, electricity, and transportation, could experience not only kinetic disruptions but also cyber-enabled disruptions like those resulting from the CRASHOVERRIDE and Petya/NotPetya attacks of 2016-2017.

Threat groups aligned with Russian state interests, and Russian-based hacktivists, could also use cyber threat activity in an attempt to discredit the current Ukrainian government and undermine the population's will to fight. Other potential cyber activity could include Russia-based cyber criminals perpetrating ransomware or other disruptive attacks against government or critical infrastructure.

Depending upon how the crisis unfolds, Russian aligned activity could remain the greatest threat; however, other malicious actors may attempt to take advantage of the situation by increasing their activities, which could potentially include conducting false-flag operations.

As countries impose restrictive sanctions on Russia, anyone doing business with Russia could also experience economic activity disruptions. Further, organizations in, or doing business with, Russia or its neighboring countries might see the invocation of emergency censorship and restrictions on internet traffic.

Cyber-related Events Involving Ukraine, Russia and Belarus

Although this situation continues to evolve, several noteworthy cyber-related events have already occurred:

- On the night of 13-14 January 2022, the so-called WhisperGate attack disrupted 70 Ukrainian websites, severely damaged six and defaced 22, with the message: "Ukrainians! All information about you has become public… Be afraid and expect worse."[2]
    - On 15 January, Microsoft announced the discovery of a multi-stage destructive malware on dozens of Ukraine-based government, non-profit, and IT organizations. Although posing as ransomware, it lacks a ransom recovery mechanism and simply overwrites the Master Boot Record[3]. This tactic resembles that of the Russian military-linked NotPetya pseudo-ransomware operation in 2017[4]. The attackers reportedly exploited an OctoberCMS vulnerability (CVE-2021-

[2] https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers
[3] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[4] https://www.sentinelone.com/blog/dissecting-notpetya-so-you-thought-it-was-ransomware/

32648) at an IT firm managing affected websites and had access to the networks months before the attack, suggesting cyber espionage activity[5].

- On 15 February, a DDoS attack briefly disrupted two state-owned banks and two military websites in the country[6]. Ukrainian officials said the threat actors also spread text messages falsely claiming that ATMs belonging to those banks were down, commenting, "The purpose of this attack was to sow panic and destabilize the situation"[7].

  The US and UK governments subsequently attributed these operations to Russia's military intelligence service, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, which most refer to as the GRU[8]; and, on 19 February, the US Cybersecurity and Information Security Agency (CISA) issued an alert warning of foreign operations pairing cyber threat activity with disinformation to undermine security and hinder the functioning of critical infrastructure.[9]

- During the night of 17-18 February, cellphone service in several government-held cities in eastern Ukraine experienced disruptions for hours. The phone company attributed it to "vandalism" of the fiber optic lines[10]. Ukrainian journalist Margo Gontar quoted the Ukrainian Interior Ministry as having said "This is part of Russia's plan to destabilize situation in Ukraine. We must understand sabotage at communications facilities will continue."[11]

- **HermeticWiper:** On 23 February, cybersecurity firm ESET reported the discovery of a new data wiper malware on hundreds of machines in Ukraine[12]. Judging from one timestamp, threat actors have been deploying this malware since as early as December 2021. According to ESET, "The wiper abuses legitimate drivers from the EaseUS Partition Master software in order to corrupt data…" Samples of the wiper are present in Lithuania and Latvia[13]. Sentinel Labs has provided additional analysis and indicators of compromise (IOCs) of this malware, which it calls HermeticWiper.[14]
  - In a 24 February report on HermeticWiper, Symantec noted it had found the malware targeting the financial, defense, aviation, and IT services sectors. The report additionally noted that "ransomware was also deployed against affected organizations at the same time as the wiper," likely as a "decoy or distraction from the wiper attacks." A screenshot of the ransom note shows it has a political message; its title begins: "The only thing that we learn from new elections is we learned nothing from the old!"[15].
  - A 1 March ESET report provided additional detail on HermeticWiper and described another wiper targeting Ukraine.[16] ESET found that HermeticWiper has used a variety of initial-access vectors, including group policy objects and a worm. The article stated that "Malware artifacts suggest that the attacks had been planned for several months." ESET also detected on 24 February a second destructive

[5] https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
[6] https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine
[7] https://twitter.com/ersincmt/status/1493940639649742853 and https://thedigital.gov.ua/news/mikhaylo-fedorov-ukraina-zmogla-vidbiti-naybilshu-za-vsyu-istoriyu-kraini-kiberataku
[8] https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/ and https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine
[9] https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf
[10] https://twitter.com/lapatina_/status/1494431566310916099 and https://abcnews.go.com/International/wireStory/ukraines-volatile-east-day-shelling-outages-fear-82976148
[11] https://twitter.com/MargoGontar/status/1494639246606581762
[12] https://twitter.com/esetresearch/status/1496581903205511181?s=21
[13] https://www.scmagazine.com/analysis/apt/ukraine-organizations-hit-by-new-wiper-malware
[14] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
[15] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
[16] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

attack against a Ukrainian governmental network, during which attackers used a less-sophisticated wiper ESET named IsaacWiper. These threat actors moved laterally using tools like Impacket. ESET also found the remote access tool RemCom on some attacked machines along with IsaacWiper.

- In a 2 March report, the Insikt Group analyzed both HermeticWiper and the associated fake ransomware, which it dubbed PartyTicket. The Insikt Group noted that using a wiper resembles other operations attributed to SANDFISH, such as WhisperGate and NotPetya. Though not definitive proof, the timing and methodology point to a Russian state origin for HermeticWiper, the Insikt Group wrote.[17]
- On 3 March, in Twitter threads, cybersecurity researchers proposed the name “Sunflower Seed” to describe Hermetic Wiper and FoxBlade malware and discussed its relationship with other Russian- origin wipers[18].

- **Cyclops Blink:** On 23 February, the UK National Cyber Security Centre reported that US and UK officials identified a new SANDFISH malware called Cyclops Blink[19], which recruits compromised machines as botnets and appears to supersede the SANDFISH malware VPNFilter. A Shadowserver report provided additional IOCs[20].
  - In a 24 February report on Cyclops Blink[21], Shadowserver stated that as of 23 February 2022, more than half of the 1,573 possibly compromised WatchGuard network devices are in either the US (686), France (85), Italy (85), Canada (85) or Germany (74); Ukraine only has 14 WatchGuard devices with suspected infections.
  - On 3 March, Shadowserver updated its list of Cyclops Blink-infected IP addresses. The majority of these were in the US, France, Italy, and Canada[22].

- Also on 23 February, Ukraine’s Ministry of Digital Transformation said a massive DDoS attack—the second in a week—had affected several government websites and banks that afternoon. Additionally, CNBC reported that websites for Ukraine’s Foreign Ministry, Security Service, Cabinet of Ministers, and parliament were down.[23]

- In the early hours of 24 February, residents in the separatist-occupied city of Donetsk reported an electricity blackout and spotty internet coverage as armored columns moved into the city, according to social media accounts.[24]

- On 24 February, US media reported that President Biden was considering options for offensive cyber threat activity against Russia. "Among the options: disrupting internet connectivity across Russia, shutting off electric power, and tampering with railroad switches to hamper Russia’s ability to re-supply its forces,” MSN reported, citing three sources[25].

  However, White House spokeswoman Jen Psaki tweeted, “This report on cyber options being presented to @POTUS is off base and does not reflect what is actually

[17] https://www.recordedfuture.com/hermeticwiper-partyticket-targeting-computers-ukraine/

[18] https://twitter.com/juanandres_gs/status/1499075039727075338 and https://twitter.com/instacyber/status/1499277784228806656

[19] https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter

[20] https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/

[21] https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/

[22] https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/

[23] https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html

[24] https://twitter.com/Blake_Allen13/status/1496572901717331971 and hxxps://t[.]me/itsdonetsk/9423

[25] https://www.msn.com/en-us/news/world/biden-has-been-presented-with-options-for-massive-cyberattacks-against-russia/ar-AAUghSb

being discussed in any shape or form."[26]

- On 24 February, Netblocks reported internet disruptions in Ukrainian cities of Kharkiv and Mariupol[27]. The Internet Protection Society, a Russian non-profit, listed the cities of Kyiv, Kharkiv, Donetsk, Kherson, Vinnitsyia, Luhansk, Sumy, and Khmelnytskyi as experiencing connectivity problems[28].
    - On 26 February, after continued Internet and phone disruptions in major Ukrainian cities, entrepreneur Elon Musk arranged to provide Starlink satellite Internet service in Ukraine[29].

- On 24 February, security experts Dmitri Alperovitch and Rob Lee both expressed surprise that the Russians had not undertaken more-active cyber threat or electronic warfare activity to disrupt Ukrainian military and civilian communications[30].

- On 25 February, the State Special Communications Service of Ukraine warned of a phishing attack in which Ukrainians received emails "with attached files of uncertain nature"[31].

- Although the alert provided few specifics, one phishing campaign allegedly targeted Ukrainian soldiers' private "i.ua" and "meta.ua" email accounts. The malicious emails urge recipients to click a link and verify their contact information or risk the suspension of their email accounts. The Computer Emergency Response Team of Ukraine (CERT-UA) attributed that campaign to UNC1151, an espionage group that Ukrainian officials have also blamed for WhisperGate; many analysts also associate it with an information campaign called Ghostwriter. UNC1151 cooperates with Belarusian intelligence services, according to Mandiant research[32]. However, based on linguistic evidence in UNC1151 content, ACTI assesses it is likely a joint Russian-Belarusian group.
    - On 28 February, RiskIQ reported additional phishing domains UNC1151 uses[33].
    - On 28 February, Meta (formerly Facebook) reported on a suspected Ghostwriter campaign that used compromised email accounts to log into the Facebook accounts of Ukrainian politicians, military leaders, and journalists to spread pro-Russian propaganda. The campaign's tactics included the use of false profiles with AI-generated "deepfake" faces[34]. Google's Threat Analysis Group also observed and took action against this campaign[35].
    - On 1 March, Proofpoint reported a campaign that may represent the "next stage" of the UNC1151 campaign CERT-UA described. A "likely nation state-sponsored phishing campaign used a possibly compromised Ukrainian armed service member's email account to target European government personnel involved in managing the logistics of refugees fleeing Ukraine," Proofpoint stated.
    - According to Proofpoint, the phishing campaign email contained a lure document about a 23 February NATO meeting and a malicious attachment that attempted to download a malware called SunSeed. The goal of the campaign appeared to be to

[26] https://twitter.com/presssec/status/1496919281535111211?s=21
[27] https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K
[28] https://twitter.com/safe_runet/status/1497131808881795079
[29] https://twitter.com/elonmusk/status/1497701484003213317
[30] https://twitter.com/DAlperovitch/status/1497021630220218371
[31] https://twitter.com/dsszzi/status/1497103078029291522
[32] https://www.bleepingcomputer.com/news/security/ukraine-links-phishing-targeting-military-to-belarusian-hackers/
[33] https://community.riskiq.com/article/e3a7ceea/description
[34] https://www.nbcnews.com/tech/internet/facebook-twitter-remove-disinformation-accounts-targeting-ukrainians-rcna17880, https://www.politico.com/news/2022/02/28/meta-belarus-hacking-campaign-ukraine-00012214
[35] https://twitter.com/ShaneHuntley/status/1498382034732937217

  - “gather intelligence around the movement of refugees from Ukraine,” Proofpoint assessed[36].
  - A 3 March Secureworks report listed additional domains linked to the reported Ghostwriter phishing activity CERT-UA and other security firms had flagged.
  - On 7 March, CERT-UA reported on a new Ghostwriter campaign targeting Ukrainians with a .zip file purportedly about defending against artillery attacks and a file with the filename “file.htm” that contained a malicious VBScript that installs the MicroBackdoor malware, a publicly available backdoor. More information and IOCs appear on CERT-UA’s website[37].

- Also on 25 February, Ukrainian media sources, citing “intelligence sources,” outlined “Russia’s plan to seize Kyiv.” In addition to kinetic attacks, the purported plan would involve sabotage to cut Kyiv’s electricity and communications to cause panic, as well as a cyberattack on government websites[38].

- Additionally on 25 February, the Premise micro-tasking platform suspended operations in Ukraine after accusations of the platform's use to fine-tune Russian artillery targeting[39].

- On 26 February, Anonymous tweeted that the “Anonymous Liberland & the PWN-BAR Hack Team” had leaked purported Belarusian bomb blueprints to the DDoSecrets transparency website[40]. DDoSecrets’ founder tweeted on 26 February that the leak had arrived almost a week previously[41] and noted that such posts should be approached with due skepticism[42]. One cybersecurity researcher cast doubt on the leak’s veracity and noted that someone maliciously impersonated him in an email advertising the leak[43].

- On 27 February 2022, *POLITICO* magazine reported that a suspected Russian cyber-attack took down websites and email servers of Ukrainian embassies and consulates around the world, on the same day that Ukrainian president Zelensky had invited foreigners to contact Ukrainian embassies if they wanted to join a foreign legion to defend Ukraine.

- On 28 February Ukrainian officials warned that the FSB is sending central government agencies emails masquerading as Ukraine’s SBU domestic intelligence service claiming to provide details about evacuation plans[44].

- On 28 February, Curated Intelligence, an international intelligence-sharing project, announced a GitHub platform providing free threat intelligence (threat reports, vendor support, and open-source intelligence sources) to help organizations in Ukraine[45].

- On 28 February, a RIPE (Réseaux IP Européens) Network Coordination Center study, using Atlas internet connectivity probes, concluded that the physical internet

[36] https://www.proofpoint.com/us/blog/threat- insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
[37] hxxps://cert.gov[.]ua/article/37626
[38] https://twitter.com/KyivIndependent/status/1497086361509187584
[39] https://www.premise.com/blog/premises-response-to-allegations-of-influence-in-ukraine/
[40] https://twitter.com/YourAnonNews/status/1497532671269945345
[41] https://twitter.com/NatSecGeek/status/1497684185552769038
[42] https://twitter.com/NatSecGeek/status/1497587401501327361/photo/1
[43] https://twitter.com/juanandres_gs/status/1497673732181184516
[44] https://ua.interfax.com.ua/news/general/803862.html, https://www.unian.net/techno/okkupanty-ot-imeni-sbu-rassylayut-pisma-ob-evakuacii-v-centralnye-organy-vlasti-11722078.html
[45] https://github.com/curated-intel/Ukraine-Cyber-Operations

infrastructure in Ukraine “has been mostly intact and functioning since the start of the conflict”[46].

- On 28 February, Internet users uploaded to VirusTotal 12 recent malicious Office documents associated with the so-called GlowSpark campaign. Microsoft first identified that campaign in early February and attributes it to the group ACTI calls WINTERFLOUNDER (Gamaredon)[47].

- On 1 March, ACTI observed continued turmoil in Russian underground communities as they took sides in the Russian-Ukrainian conflict. Attacks on major Jabber servers that Russian Dark Web actors use are hindering communications. Some major players, including administrators of the RAMP community, blame pro-Ukrainian actors for the Jabber attacks, saying they are unfair because those underground communities are "outside of politics."

- Between 23 February and 2 March, the Kyivstar mobile provider suffered outages at 500 of its cellular phone base stations due to infrastructure damage and power outages, according to Netblocks[48]. This damage likely resulted from physical military activity.

- On 3 March, cyber firm Wordfence reported a huge wave of cyber attacks against Ukrainian WordPress sites since the invasion, with 144,000 recorded attacks on February 25 alone. Several of the attacks were successful and resulted in defacements, with a group known as “theMxonday” taking credit[49].

- On 3 March, Ukraine’s Defense Ministry warned that the Russians are planning a deepfake video that will purport to show President Zelensky capitulating. Such a video would be “intended to sow panic, to disorient, to cause despair, and to incline [Ukrainian] troops toward capitulation”[50].

- On 3 March, a cybersecurity source told Lenta[.]ru, a relatively independent Russian news site, that Russian hacker group RaHDit had disabled 750 Ukrainian government sites and defaced them with a message from Russian soldiers criticizing the current Ukrainian government addressed to Ukrainians. Lenta[.]ru said it could not confirm this report[51].

- On 3 March, Russian space agency Roscosmos said the pace of cyber attacks against it had lessened after strikes against unspecified “centers of cyber operations” in Ukraine[52]. Pro-Ukrainian hacktivists had claimed on 1 March to have breached it and stolen information.

- On 4 March, Ukrainian cyber authorities warned Ukrainians that emails from the address jowhar@xintongwood[.]club contain a malicious attachment that downloads the Formbook (a.k.a. XLoader) malware, a credential harvester and keylogger[53].

[46] https://labs.ripe.net/author/emileaben/the-ukrainian-internet/
[47] https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/
[48] https://twitter.com/netblocks/status/1499003625116512258
[49] https://www.bleepingcomputer.com/news/security/ukrainian-sites-saw-a-10x-increase-in- attacks-when-invasion-started/
[50] http://web.archive.org/web/20220303151512/ and https://www.rbc.ua/rus/news/rossiya-gotovit-feykovoe-video-zelenskim-1646278231.html
[51] https://lenta.ru/news/2022/03/03/hackers_ukraine/
[52] hxxps://www.kp[.]ru/online/news/4651806/
[53] https://twitter.com/dsszzi/status/1499740427783651336

- On 4 March, Netblocks reported a disruption in fixed-line and mobile networks in the Kherson region[54].

- On 4 March, as Russia blocked many foreign and independent news sources, BBC News offered shortwave radio dispatches[55].

- On 4 March, US-funded Russian-language news source Current TimeTV broadcasted a QR code that links to its Telegram channel[56].

- As of 4 March, Cyberknow20's chart of cyber groups includes 37 pro-Ukraine groups and 142 pro-Russia groups[57].

- On 4 March, Russia's government blocked its citizens' access to Twitter and Facebook as well as many foreign news outlets[58]. Additionally, BBC News suspended reporting from Russia due to Russian laws barring independent journalism[59].

- On 4 March, Cisco's BGPStream reported a "possible BGP hijack." The Russian ASN NETGRUP announced the prefix 31.148.149.0/24, which Ukrainian ASN NGROUP normally announces[60], but it is unclear whether this was intentional.

- On 5 March, Ukrainian cybersecurity authorities warned of constant DDoS attacks originating from Russia against Ukrainian government ministry sites, including those of the Interior Ministry, Defense Ministry, Presidency, Parliament, and Cabinet of Ministers. The largest attack was 100 GBs, but the cybersecurity officials' statement claimed the websites were continuing to function[61].

- On 5 March, the website of Ukraine's Energoatom national atomic energy company reported significant cyber attacks, leading administrators to temporarily take the website offline[62]. A cybersecurity official said Ukrainian nuclear power stations are well protected from cyber attacks, but that physical attacks are a much more serious risk to Ukraine's critical infrastructure[63].

- On 6 March, a Netblocks graphic showed network connectivity for Ukrainian operator Ukrtelecom had dipped to just above 50 percent of full connectivity on 4 March, to just above 40 percent on 5 March, and had ended the day of 6 March at about 70 percent of full connectivity[64]. The provider attributed the disruptions to "combat damage," suggesting the cause of the disruption was physical attacks or military signal- jamming operations rather than malware-driven activity[65].

- On 7 March, Google's Threat Analysis Group (TAG) posted a blog saying it was tracking three campaigns against Ukraine in the past two weeks[66]. These included the following:

[54] https://twitter.com/netblocks/status/1499735002313015300
[55] https://www.nytimes.com/2022/03/03/business/media/bbc-shortwave- radio-ukraine.html
[56] https://twitter.com/CurrentTimeTv/status/1499736910318686209
[57] https://twitter.com/Cyberknow20/status/1499725665490599940/photo/1
[58] https://www.bleepingcomputer.com/news/technology/russia-blocks-access-to-facebook-twitter-foreign-news-outlets/
[59] https://www.reuters.com/world/uk/bbc-halts-reporting-russia-after-new-law-passes-2022-03-04/
[60] https://bgpstream.com/event/287556
[61] https://cip.gov.ua/ua/news/rosiiski-khakeri-bezperervno-prodovzhuyut-atakuvati-ukrayinski- informaciini-resursi
[62] hxxps://ukrinform[.]ua/rubric-technology/3421124-sajt-energoatomu-zaznav-kiberataki.html
[63] https://www.washingtonpost.com/national-security/2022/03/04/ukraine-nuclear-cyberattack/
[64] https://twitter.com/netblocks/status/1500462190591197187
[65] https://twitter.com/netblocks/status/1500189246673637378
[66] https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/

    - UNC1151 activity against Polish and Ukrainian targets, as this report described previously.
    - A SNAKEMACKEREL (a.k.a. APT28, FancyBear) credential-phishing campaign targeting users of Ukrainian media company ukr[.]net, using newly created Blogspot domains to redirect targets to credential phishing campaigns.
    - A campaign targeting European organizations with lures related to the Ukrainian invasion—with malicious attachments, using tracking pixels known as “web bugs” to identify people who are prone to clicking on social engineering emails, with file names such as 'Situation at the EU borders with Ukraine.zip‘[67].

- On 7 March, Ukraine’s State Service of Special Communications and Information Protection (SSCIP) claimed the country had undergone 2,800 cyber attacks since 15 February, with the single-day record being 271 DDoS attacks[68].

- On 7 March, the Xahnet team, a pro-Russian group, claimed to have attacked regional Ukrainian communications provider’s domain vinfast.net, allegedly in retribution for attacks on Russian mobile operator Beeline. The Xahnet team wrote: “We have a fairly large list of providers under our control. And if the attacks on the infrastructure of the Russian Federation continue, we will be forced to respond, regardless of the ‘side effects’ that will hurt those whom we really don’t want to hurt.”[69] The group’s actual capabilities and intentions remain unclear.

- On 8 March, Trend Micro reported on a new wiper called RU_Ransom, which has targeted a few entities in Russia. In a fake Russian-language ransom note, threat actors wrote they were carrying out their attack in response to the Russian killing of innocent civilians in Ukraine. The note ends: “And yes, it was translated from Bangla into Russian using Google Translate,” implying \ the authors were in South Asia[70].

- On 8 March, ACTI observed a posting by threat actor “Burgir” on the XSS underground forum that read (translated): “I pay up to $10,000 in BTC for PWN’ing (taking control) of certain LED screens/jumbotrons in a specified country (Eastern Europe region)! The goal is to display content of my choice on these large screens [sic].” It is unclear what country the threat actor planned to target. In 2014, the threat group SNAKEMACKEREL, hiding behind the hacktivist persona CyberBerkut, claimed to have hijacked electronic billboards in Kyiv and shown images of wartime atrocities to undermine the incumbent president[71].

- On 8 March, the International Atomic Energy Agency said it was not receiving remote data transmission from monitoring systems at Ukraine's decommissioned Chernobyl nuclear power plant. The incident follows a loss of data from the active Zaporizhzhia plant[72].

- On 9 March, NetBlocks reported a power blackout and “major disruption to telecommunications services” in the vicinity of the Chernobyl plant[73].

[67] https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european
[68] hxxps://www.ukrinform[.]ua/rubric-society/3422396-iz-seredini-lutogo- ukrainski- resursi-zaznali-blizko-2800-kiberatak.html
[69] https://twitter.com/Cyberknow20/status/1500715129226231810
[70] https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html
[71] https://www.bbc.com/news/world-europe-30453069
[72] https://www.iaea.org/newscenter/pressreleases/update-15-iaea-director-general-statement-on-situation-in-ukraine
[73] https://netblocks.org/reports/severed-power-line-heightens-safety-concerns-at-chernobyl-nuclear-power-plant-eBOQke8Z

A timeline of Russia-linked cyber incidents is available at https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html

Pro-Ukrainian Hacktivist Activities

- On the evening of 24 February, the main Russian government website was unreachable; websites of the Kremlin and the Russian parliament were also down[74]. Initial Russian media reporting said it was a cyber-attack[75], but later the Kremlin spokesman said the Kremlin site was functioning and denied that a DDoS attack on the site had occurred.[76] Later that evening, these Russian government sites were functioning but inaccessible to IP addresses outside of Russia[77]. Cybersecurity analyst Thaddeus Grugq speculated that this selective unavailability could be related to Russia's effort to control cross-border internet traffic ostensibly for defensive purposes.[78]

- On the night of 24 February, Russian media outlet RT experienced brief DDoS activity. The hacktivist group Anonymous claimed responsibility, saying it was acting "in response to [sic] Kremlin's brutal invasion of #Ukraine"[79].

- On 25 February, Anonymous-linked Twitter user @SebastianDAlex tweeted: "We are now looking into all Russian IP's that are actively scanning and attacking Ukraine's Networks. We Will be attempting to breach into any that we can or Shut Down whatever we cannot breach [sic]." The tweet provided a link to a target list[80].

- **YourAnonTV:** On 25 February the account @YourAnonTV announced it would "intensify cyber-attacks on the Kremlin this afternoon"[81].
  - On 25 February, the YourAnonTV Twitter account published a link to a purported database with employees' private data on mil[.]ru, the Russian Defense Ministry website; however, Twitter removed the link early on 26 February[82].
  - Throughout the day on 26 February, numerous Russian government and state media sites were unavailable. At midnight, Russian state media outlet RIA Novosti reported (translated): "The Digital Ministry informs you that it is encountering an unprecedented scale of cyber-attacks, including a series of professional targeted attacks against the State Services portal. Security center specialists are successfully repelling all the attacks"[83]. The State Services portal was on the target list of the Ukrainian government-sponsored "IT Army," described below.

- **"IT Army":** On 25 February, the Ukrainian government advertised on local hacker forums for volunteers to help it defend Ukrainian systems and to conduct espionage against Russian systems, according to media reports. Ukrainian cybersecurity firm Cyber Unit Technologies plans to coordinate the effort.[84]
  - On 26 February, the verified Twitter account of Ukraine's Minister of Digital Transformation, Mykhailov Fedorov, announced the creation of an "IT Army of

[74] https://twitter.com/safe_runet/status/1496876823979909126
[75] hxxps://ria[.]ru/20220224/kiberataki-1774863604.html
[76] hxxps://www.rbc[.]ru/politics/24/02/2022/6217ab749a79473b77b219d9
[77] https://twitter.com/olliecarroll/status/1496936638723006466
[78] https://twitter.com/thegrugq/status/1496906043636404236
[79] https://www.thedailybeast.com/anonymous-hackers-claim-responsibility-for-cyberattacks-against-russian-state-news-site-rtcom
[80] https://twitter.com/SebastianDAlex/status/1497318426922172416
[81] https://twitter.com/YourAnonTV/status/1497176425014648835
[82] https://twitter.com/YourAnonTV/status/1497273131567828992
[83] https://twitter.com/rianru/status/1497684385683935241
[84] https://www.jpost.com/international/article-698601

  Ukraine" to "fight on the cyber front."[85] Multiple social media outlets reposted an IT Army of Ukraine post that encouraged others to launch DDoS attacks or other mechanisms against the provided Russian state agencies and Kremlin-friendly companies.[86]
  - On 27 February, the social media accounts of @itarmyofukraine and other groups posted numerous claims of cyber-attacks on Russian targets[87].
  - On 28 February, Ukrainian officials posted on social media, asking readers to contribute information on vulnerabilities in Russian cyber defenses to its Cyber Front chatbox, @stop_russian_war_bot[88].
  - On 28 February, Ukraine's Digital Ministry claimed that website of the Russian Federal Security Service FSB) is down. Kommersant and several other news sites were also down on 1 March[89].
  - On 28 February, anti-Russian hacktivist groups announced operations against Russian targets, including the following:
    - Sberbank[90]
    - The Moscow Stock Exchange[91]
    - Petroleum and machinery company Severnaya Kompaniya[92]
    - Russian Railways[93]
    - Russian contractor “promen48[.]ru”[94]
    - The Joint Institute for Nuclear Research at State University Dubna[95]
    - Electric vehicle charging stations in Russia itself, which hacktivists have defaced to display crude messages about Putin[96]
    - Russian TV transmissions, which hacktivists have interrupted with the Ukrainian national anthem[97]
  - On 1 March, Twitter user @Cyberknow20 listed 22 groups that have been carrying out cyber-attacks supporting Ukraine and nine groups carrying out cyber-attacks supporting Russia or Belarus[98].

- On 28 February, Microsoft announced that just hours before Russia invaded Ukraine, it detected a malware package it calls FoxBlade. The destructive malware, "precisely targeted" at Ukraine's digital infrastructure, can use a victim's PC to carry out DDoS attacks. Microsoft has since updated its Windows Defender anti-malware service[99] in response.

- On 28 February, the Kremlin promised a "harsh response" to "EU citizens and structures involved in supplying lethal weapons and fuel and lubricants to the Armed Forces of Ukraine"[100]. This "harsh response" could include cyber threat activity targeting energy and transportation companies and infrastructure.

[85] https://twitter.com/FedorovMykhailo/status/1497642156076511233?cxt=HHwWgsC5meXm2MgpAAA
[86] https://pbs.twimg.com/media/FMkVCicVgAIFE4c.png
[87] https://twitter.com/itarmyofukraine
[88] https://t.me/SBUkr/3762 and https://twitter.com/dsszzi/status/1498245709031776258
[89] https://www.ukrinform.ru/rubric-technology/3415929-sajt-fsb-rossii-leg-mincifry.html
[90] https://twitter.com/YourAnonTV/status/1498031979555659776
[91] https://twitter.com/Cyberknow20/status/1498211564356194306
[92] https://twitter.com/xxNB65/status/1498221706263019520
[93] https://twitter.com/AgainstTheWest_/status/1498349260013813760
[94] https://twitter.com/AgainstTheWest_/status/1498351312110600200
[95] https://twitter.com/AgainstTheWest_/status/1498342663564804097
[96] https://www.hackread.com/anonymous-hack-russian-tv-electric-charging-station/
[97] https://www.hackread.com/anonymous-hack-russian-tv-electric-charging-station/
[98] https://twitter.com/Cyberknow20/status/1498620110000787458
[99] https://www.geekwire.com/2022/microsoft-detected-destructive-cyberattacks-against-ukraine-several-hours-before-russian-invasion-began/
[100] https://www.currenttime.tv/a/russia-ukraine-war/31726786.html and https://www.dailymail.co.uk/news/article-10562199/Russia-promises-EU-face-harsh-response-support-Ukraine.html

- On 28 February, cybersecurity firm CheckPoint reported a 196 percent uptick in cyber-attacks on Ukraine's government (time period unknown)[101]. However, the pro-Ukrainian IT Army and Cyber Front attacks attract more attention because they publicize themselves.[102]

- A 28 February Russian media report cited Russian cybersecurity experts saying they had observed three times as many attacks on Russian entities in the four days following Russia's 24 February 2022 attack on Ukraine as they had in the same four days of 2021. The largest attacks exceeded 750 gigabits per second. However, most were smaller-scale attacks; of the 175 DDoS attacks Rostelekom- Solar recorded, the largest reached just 63 Gbps[103].

- On 1 March, reports listed additional Russian entities that had suffered hacktivist attacks:
  - The Control Center of the Russian Space Agency, Roscosmos[104]; this report prompted the Roscosmos head to deny the reports and to warn: "Offlining the satellites of any country is actually a casus belli, a cause for war"[105].
  - Russian companies Gazprom, Lukoil, Nornikel, and Yandex, as well as government entities the Pension Fund and Roskomnadzor[106].
  - The Selyatino agricultural site near Moscow[107].

- On 1 March, one particularly active hacktivist group, AgainstTheWest, announced it was ceasing operations because Anonymous was taking credit for its breaches[108]. Then AgainstTheWest reappeared, targeting both Russia and China[109].

- On 1 March, a group called Killnet claimed it had been conducting cyber attacks against Anonymous[110].

- On 3 March, the @YourAnonTV Twitter feed claimed that, as part of its ongoing #OpRussia campaign, Anonymous-affiliated groups had hacked more than "2500 websites of Russian & Belarusian government, state media outlets, banks, hospitals, airports, companies and pro-Russian 'hacking group' [sic]"[111].

- On 3 March, the Ukraine-sponsored IT army of Ukraine launched an "Internet forces of Ukraine" initiative to inform Russians on the Russia-Ukraine war[112].

- On 5 March, the Dutch General Intelligence and Security Service warned Dutch private entities not to take part in cyber attacks against Russian targets, according to cybersecurity researcher Matthijs Koot[113]. Numerous analysts have warned of the risks that hacktivism poses, with Talos summarizing the problem thus: the actors who carry out such attacks are unpredictable, misattribution could lead to an escalation among states, and threat actors could exploit recently disclosed vulnerabilities. Talos

[101] https://twitter.com/joetidy/status/1498281962422910976
[102] https://twitter.com/campuscodi/status/1498283610092277774
[103] https://www.kommersant.ru/doc/5238079
[104] https://twitter.com/YourAnonTV/status/1498792639877074945
[105] https://reuters.com/world/russia-space-agency-head-says-satellite-hacking-would-justify-war-report-2022-03-02/
[106] hxxps://lenta[.]ru/news/2022/03/01/hackers/
[107] hxxps://www.securitylab[.]ru/news/530388.php
[108] https://twitter.com/AgainstTheWest_/status/1498817861929816064
[109] https://twitter.com/AgainstTheWest_/status/1498915840229580802, https://twitter.com/IntelStrike/status/1498983958943391747 and https://twitter.com/Cyberknow20/status/1499342034166956033
[110] https://www.securitylab.ru/news/530382.php
[111] https://twitter.com/YourAnonTV/status/1499513585915019278
[112] https://twitter.com/Cyberknow20/status/1499669130504331269
[113] https://twitter.com/mrkoot/status/1500102753380704258

also listed 10 vulnerabilities they consider threat actors will most likely exploit; most involve Windows and Google Chrome products[114].

- Between 4 and 7 March, pro-Ukrainian hacktivist groups claimed attacks on the following targets:
  - A Russian government vehicle database[115].
  - Russia's Joint Institute for Nuclear Research and "Information Department"[116].
  - Russia's Federal Security Service[117].

- On 5 March, Russia's National Coordination Centre for Computer Incidents (NKTsKI), which is part of the FSB, released a list of 17,500 IP addresses supposedly launching DDoS attacks against Russian networks and entities[118].

- On 8 March, Network Battalion 65 (NB65), the same hacktivist persona that claimed to have breached the Russian Space Agency, tweeted, "Stay tuned for Kaspersky source code leak…I'm sure you'll find interesting relationships in this code. Glory to Ukraine"[119].

Cyber-related Events in Other Countries

- On 19 January 2022, a cyber-attack disabled certain functions of Global Affairs Canada, the country's diplomatic and external affairs agency, after Canadian officials extended their support to Ukraine. Canadian officials refrained from making an attribution, but an unnamed Canadian national security source blamed Russian-backed actors.[120]

- In late January, ransomware incidents affected logistics and port companies in Germany, Belgium, and the Netherlands and related to the petrochemical industry, disrupting automated loading and unloading systems and forcing client companies to reroute supplies[121].

  The incidents involved BlackCat and Conti ransomware. Dutch and Belgian officials said they had no evidence of state links as of 4 February[122], but the ransomware gangs that control the BlackCat and Conti ransomware are based in Russia[123]

- On 24 February, threat actor DataFor posted on the XSS underground forum, claiming to have 90,000 records of alleged US intelligence officers. The actor, who emerged on the forum in early 2021, has a low reputation score but has repeatedly posted anti-Ukrainian threads on XSS and has shared data leaks in the past. ACTI has no evidence regarding the validity of the alleged leak but notes that the threat actor was sharing it without asking for money, suggesting a political rather than financial motivation.

[114] https://blog.talosintelligence.com/2022/03/ukraine-update.html
[115] https://twitter.com/IntelStrike/status/1500071124566089733/photo/1
[116] https://twitter.com/IntelStrike/status/1500773254281129985
[117] https://kyivindependent.com/uncategorized/anonymous-claim-to-have-taken-down-fsb-website/
[118] https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/
[119] https://twitter.com/xxNB65/status/1501265001037795335
[120] https://globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/
[121] https://www.vrt.be/vrtnws/nl/2022/02/01/verschillende-havenbedrijven-slachtoffer-van-cyberaanval/ and https://www.bleepingcomputer.com/news/security/german-petrol-supply-firm-oiltanking-paralyzed-by-cyber-attack
[122] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say/
[123] https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/

- **KA-SAT:** On 24 February, the date Russia invaded Ukraine, KA-SAT, a European subsidiary of US satellite communications firm ViaSat suffered what initially appeared to be a DDoS attack linked to the 23 February DDoS attack on Ukrainian websites preceding the Russian invasion[124].
  - On 27 February, German IT news site Golem.de cited an email Viasat sent to its telecommunication provider clients saying: "This appears to have initially started with the KA-SAT service in Ukraine and then spread to almost the entire KA-SAT footprint"[125]. The KA-SAT attack affected tens of thousands of satellite Internet customers throughout Europe[126].
  - On 28 February, German wind turbine maker Enercon reported it had lost remote control capabilities for 5,800 turbines due to the "massive disruption" of satellite connections on 24 February. The satellite disruption also affected a company that provides "connection services and solutions for industrial applications and safety-critical infrastructures." Experts initially hypothesized that the wind farm incident could have originated from a cyber attack, deliberate electronic interference, or a missile attack on a satellite system ground station, according to Handelsblatt[127]. This incident has political resonance, as Germany has vowed to speed up wind projects to reduce reliance on Russian gas[128]. Victims of the satellite failure included emergency services, according to a 3 March German media report[129].
  - On 3 March, a Polish cybersecurity periodical published an analysis by a tech-savvy customer affected by the incident. According to this analysis, the threat actors reportedly erased the firmware of all modems that were connected to the satellite network at the time of the attack[130].
  - On 5 March, Der Spiegel published an update on the KA-SAT outage. Citing a German government document, it wrote: "On February 24 at 5 a.m., the attackers activated a faulty update, causing KA-SAT customers to lose their network access." The German authorities suspected "a connection with the Ukrainian conflict" due to the timing and because the Ukrainian military uses the affected satellite segment in Central and Eastern Europe. As for the German wind farm, the German government assesses it as "cyber collateral damage" and did not observe additional effects on Germany's electricity supply or other critical infrastructure. According to Der Spiegel, the satellite operator itself claimed that "in the Central/Eastern Europe segment, the end devices were sabotaged by commercial customers." The meaning of this statement is unclear[131].
  - On 6 March (11 days after the initial attack), Netblocks reported continued outages in at least one European ISP that the satellite company serves[132].
  - On 7 March, Spain-based researcher Ruben Santamarta (a.k.a. ReverseMode), citing his own BlackHat conference presentations and other researchers' reports on vulnerabilities in the Viasat modems' firmware, concluded: "there are multiple ways to permanently damage a KA-SAT SATCOM terminal"[133].

[124] https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid-russia-fears-12554004

[125] https://www.golem.de/news/ukraine-krieg-satelliteninternet-ka-sat-ausgefallen-2202-163468.html

[126] https://www.securityweek.com/cyberattack-knocks-thousands-offline-europe

[127] https://web.archive.org/web/20220228160735/ and https://app.handelsblatt.com/unternehmen/ener gie/erneuerbare-energien-massive-stoerung-der-satellitenverbindung-enercon-meldet-fast-6000- betroffene-windanlagen/28114360.html

[128] https://news.yahoo.com/germany-turns-renewables-russian-invasion-123511545.html

[129] https://www.tagesschau.de/investigativ/russland-cyberattacken-105.html

[130] https://zaufanatrzeciastrona.pl/post/tysiace-terminali-internetu-satelitarnego-powaznie-uszkodzonych-w-dniu-ataku-na-ukraine/

[131] https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa- gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024

[132] https://twitter.com/GossiTheDog/status/1500422232534835202

[133] https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in- europe.html

- On 25 February, hacktivists opposed to the Russian military buildup unleashed ransomware on Belarus Railways, hoping to slow troops' movements[134]
  - On 27 February, the hacktivists renewed their attack.[135]

- On 25 February, Polish officials reported that unknown actors targeted government email servers, the website of the national payment clearing system, and networks at Poland's top power utility.[136]

- **Snatch:** On 25 February, the Russian-language Snatch ransomware team announced a leak of stolen data from McDonald's on its victims list[137]. The Snatch team has stolen national security-related data from US and German government contractors in the past[138], and it sometimes gives away data for free, suggesting its motives are less financial than political. Whether financially or politically motivated, the 25 February data leak from an iconic American restaurant has the effect of a symbolic strike against the US.
  - On 28 February, the founder of the DDOSecrets transparency website tweeted that the Snatch Team had just "dropped" data it had stolen from a Swedish automaker and a US-based aerospace company[139]. The data may have come from a December 2021 Snatch operation against the same carmaker, suggesting that the Snatch group may have held the leak in reserve until after the sanctions announcement.[140]

- **Conti:** In a 25 February posting on its website, the Conti ransomware group wrote, "The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyber-attack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy [sic]," according to screenshots several researchers have posted[141].

  The message appears to have caused dissension within the cyber criminal ranks. The group has subsequently modified its message to remove the threat against critical infrastructure and to say the group does "not ally with any government and we condemn the ongoing war."[142]
  - On 27 February, vx-underground, a clearinghouse for malware code and analysis, posted a message purportedly from a Conti member who broke with the group's pro-Russian stance. The message announces a leak of chats among purported Conti group members and concludes with: "Glory to Ukraine!"[143].
  - Nevertheless, the threat of retaliatory action by ransomware actors remains. The US government warned in September 2021 that Conti operators have targeted national security-related entities[144]. Other ransomware actors have also explicitly encouraged targeting of the US; a REvil spokesperson did so in June 2021[145]. Wazawaka, a LockBit actor who also appears to be behind Babuk ransomware

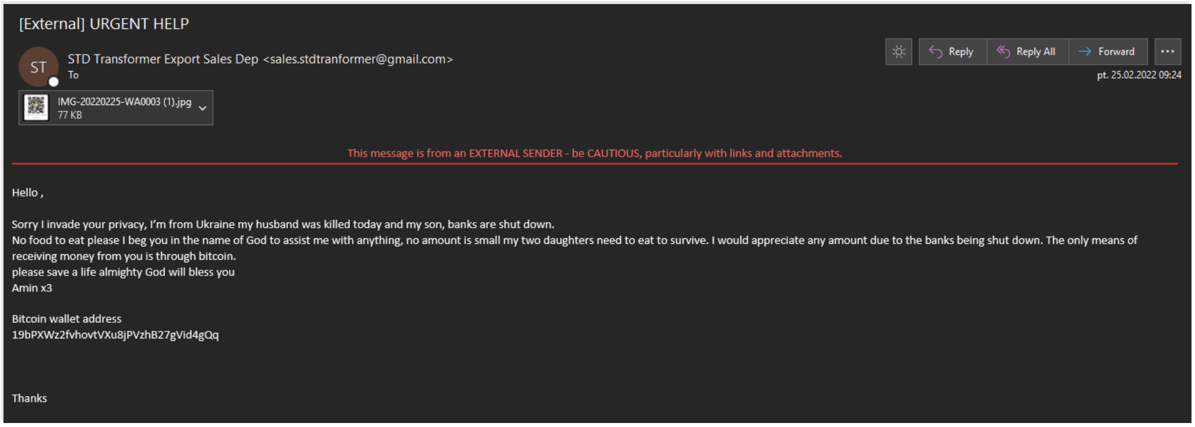
[134] https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/
[135] https://twitter.com/cpartisans/status/1497930273425661958
[136] https://reuters.com/technology/poland-sees-more-cyberattacks-government-servers-official-says-2022-02-25/
[137] https://www.dailymail.co.uk/news/article-10553013/Russia-linked-hacker-gang-claims-ransomware-attack-McDonalds.html
[138] https://ddosecrets.com/wiki/Perceptics
[139] https://twitter.com/NatSecGeek/status/1498395468514144263
[140] https://cisomag.eccouncil.org/did-snatch-ransomware-snitch-volvo-cars-rd-data/
[141] https://www.vice.com/en/article/y3vxnm/russian-ransomware-gang-says-it-will-support-russian-government
[142] https://cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure.
[143] https://twitter.com/vxunderground/status/1498060366445613056
[144] https://www.cisa.gov/news/2021/09/22/cisa-fbi-and-nsa-release-conti-ransomware-advisory-help-organizations-reduce-risk
[145] http://web.archive.org/web/*/https://t.me/Russian_OSINT/791

activity, said in January 2022: "I declare war on the USA!"[146]. Over the years, ACTI has also observed underground forum actors specifically seeking to buy compromised credentials from US government and critical infrastructure entities or threatening to send sensitive stolen data to Russian intelligence services.

  - Messages in the leaked chats prove that the Conti group takes orders from the FSB, according to investigative group Bellingcat.[147]
  - As of 2 March, Conti had reportedly shut down and wiped its server infrastructure[148].
  - As of 7 March, Conti's leak site was functional, advertising sample customer data from US- based industrial firm Cummins-Wagner[149]. The firm's customers include US military and government entities[150]. This targeting seems consistent with Conti's encouragement of attacks on the US. An attacker could easily confuse the target company's name with that of Cummins Inc, a major provider of engines to US and other militaries[151].

- On 25 February, a large Canada-based aluminum company confirmed an unspecified cyber incident in its IT systems[152]. The victim's parent company, a Norwegian firm, suffered a LockerGoga attack in 2018; ACTI and other researchers have assessed that attack to be part of a broader Russian operation to deter Norway from supporting NATO[153].

- On 25 February 2022, Poland-based employees of a large multinational received Ukrainian crisis-themed phishing emails. One such email purported to be from a woman whose husband and son had just died and who could not withdraw money because the banks were shut down. The sender begged for a Bitcoin donation (Exhibit 1). In addition, ACTI has observed multiple social media postings purporting to raise money for Ukraine; their veracity could not be determined.



[External] URGENT HELP

STD Transformer Export Sales Dep <sales.stdtranformer@gmail.com>
To

pt. 25.02.2022 09:24

This message is from an EXTERNAL SENDER - be CAUTIOUS, particularly with links and attachments.

Hello ,

Sorry I invade your privacy, I'm from Ukraine my husband was killed today and my son, banks are shut down.
No food to eat please I beg you in the name of God to assist me with anything, no amount is small my two daughters need to eat to survive. I would appreciate any amount due to the banks being shut down. The only means of receiving money from you is through bitcoin.
please save a life almighty God will bless you
Amin x3

Bitcoin wallet address
19bPXWz2fvhovtVXu8jPVzhB27gVid4gQq

Thanks

Exhibit 1: Phishing Email from 25 February 2022 Targeting Poland-based employees

- On 27 February, LockBit operators wrote on their Tor leak site: "Warning: Official Statement on the Cyber Threat to Russia: ALL AVAILABLE DATA WILL BE

[146] https://krebsonsecurity.com/2022/02/wazawaka-goes-waka-waka/
[147] https://twitter.com/christogrozev/status/1498387134604001285
[148] https://twitter.com/campuscodi/status/1499115864112644096
[149] https://twitter.com/IntelStrike/status/1500743053853835269 and https://www.redpacketsecurity.com/conti-ransomware-victim-https-www-cummins-wagner-co/
[150] https://www.cummins-wagner.com/state/maryland/cooling-towers-md/
[151] https://www.cummins.com/news/releases/2021/07/30/us-army-awards-cummins-inc-87m-contract-deliver-advanced-combat-engine and https://www.militarysystems-tech.com/suppliers/military-diesel-engines/cummins-ltd
[152] https://www.tvanouvelles.ca/2022/03/01/cyberattaque-lusine-de-pneus-bridgestone-de-joliette-forcee-a-larret-complet
[153] https://www.dragos.com/blog/industry-news/spyware-stealer-locker-wiper-lockergoga-revisited/

PUBLISHED!"[154] It is unclear whether the LockBit operators are referring to the ongoing attacks on Russia by Anonymous and the Ukraine IT Army or to the reports that President Biden was considering offensive cyber activity against Russian critical infrastructure, reports that US officials have denied, as the above describes. This threat is consistent with LockBit actor wazawaka's declaration of war against the US described above.

- On 27 February, CERT-EU issued TLP:Green Security Guidance 22-002, "Hardening Signal." In this document, CERT-EU reports "sustained nation-state activity against Signal," a secure instant message service. CERT-EU urges Signal users to download Signal apps only from official websites; regularly update apps; verify the identity of anyone who requests to become a contact; enable registration lock and screen lock; activate notification privacy and disappearing messages features; and reboot their phones at least once a day.

- On 27 February, LockBit's leaks site announced it had stolen data from First Financial Credit Union, a New Mexico bank, and would publish it if they did not receive a ransom payment by 6 March.[155] However, later that day LockBit operators backtracked as Conti had, writing: "For us it is just business and we are all apolitical....We will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts"[156].

- On 28 February, a major Japanese carmaker announced it was halting production due to a cyber-attack on a company that supplies the carmaker with plastic parts. The Japanese Prime Minister, responding to questions about a possible link to Japanese sanctions on Russia, said: "It's hard to answer without thoroughly checking."[157] Other sources do mention suspicions of Russian involvement but have not identified any concrete proof.[158]

- On 28 February, a US satellite communications firm suffered a DDoS attack that appeared linked to the 23 February DDoS attack on Ukrainian websites preceding the Russian invasion.[159]

    - On 28 February, a major German wind turbine maker lost remote control capabilities for 5,800 turbines due to a "massive disruption" of satellite connections on 24 February, the same date in which the Russian invasion of Ukraine began. The satellite company is a subsidiary of the above-mentioned US-based company that suffered the DDoS attack. Experts told media outlet Handelsblatt that the wind farm incident could have originated from a cyber attack, deliberate electronic interference, or a missile attack on a satellite system ground station. The satellite disruption also affected a company that provides "connection services and solutions for industrial applications and safety-critical infrastructures."[160]

[154] https://twitter.com/AShukuhi/status/1497973628993945612/photo/1
[155] https://twitter.com/IntelStrike/status/1497979609874419716
[156] https://twitter.com/GossiTheDog/status/1498011275506458627
[157] https://uk.news.yahoo.com/toyota-halts-japan-plants-reported-105523941.html
[158] https://www.forbes.com/sites/peterlyon/2022/02/28/russia-is-suspect-in-cyberattack-that-will-force-toyota-to-shut-down-plants-in-japan/?sh=98e0414563a0
[159] https://news.sky.com/story/satellite-giant-viasat-probes-suspected-broadband-cyberattack-amid-russia-fears-12554004
[160]https://web.archive.org/web/20220228160735/https://app.handelsblatt.com/unternehmen/energie/erneuerbare-energien-massive-stoerung-der-satellitenverbindung-enercon-meldet-fast-6000-betroffene-windanlagen/28114360.html

  - This incident has political resonance, as Germany has vowed to speed up wind projects to reduce reliance on Russian gas[161].

- On 1 March, a Finnish bank reported that unknown actors had carried out a DDoS attack that had slowed some of its online services[162]. Some Internet users voiced suspicion that Russian-aligned actors slowed the bank's services to prevent users from authenticating votes on an initiative to have Finland join NATO[163], although this is unproven.

- On 1 March, the Stormous (a.k.a. Stormus, Stourmous) ransomware gang, an Arabic-speaking group[164], issued a message declaring support for the Russian government and threatening to attack Western infrastructure[165]. The Stormous gang writes in Modern Standard Arabic, making it difficult to determine the group's country of origin. However, word choices and cultural references suggest the authors are from Egypt. In recent days, Stormous operators have claimed responsibility for breaches against Ukraine's Foreign Ministry, a Ukrainian aircraft engine maker, and a US military contractor. They have also targeted entities in Morocco, the Philippines, Japan, and India, and leaked data from a US industrial automation company and educational entities in the US and Brazil. This variety of targets suggests they could be hackers for hire[166].
  - On 8 March, Israeli cybersecurity company Kela claimed that Stormous ransomware was falsely claiming responsibility for operations that other threat actors had actually carried out[167].

- On 1 March, Ukrainian officials listed Telegram channels that Military Unit 26165 (a.k.a. the 85th Main Center of Special Service) of Russia's GRU military intelligence service is coordinating to spread disinformation[168]. The US and other countries have attributed the activity tracked as being that of the cyber threat group SNAKEMACKEREL (a.k.a. APT28, Fancy Bear) to Unit 26165[169].

- On 1 March, researchers identified several scam websites and Twitter spam notices featuring appeals for Ukraine-related charitable donations[170]. These appeals appear to have come from cyber criminals using the crisis as a lure.

- On 2 March, Polish officials warned of a disinformation campaign using text messages purporting to come from the Polish military and falsely telling recipients they must immediately go to the country's military recruitment station[171].

- On 3 March, the head of Latvia's CERT (CERT.LV) said that, over the last week, cyber attacks on the country had grown significantly and that these were "serious planned attacks on the organs of state power, critical infrastructure and service suppliers" and that some of the attacks had succeeded. She also noted that "vulnerability

[161] https://news.yahoo.com/germany-turns-renewables-russian-invasion-123511545.html
[162] https://twitter.com/Nordea_Aspa/status/1498681430993473542
[163] https://news.ycombinator.com/item?id=30518421
[164] http://web.archive.org/web/20211226192808/ and https://cybershafarat.com/2021/12/26/stormous-ransomware/
[165] https://twitter.com/Cyberknow20/status/1498661852108054528/photo/1 and https://twitter.com/darktracer_int/status/1498644747316981762
[166] https://twitter.com/hashtag/stormous?src=hashtag_click
[167] https://twitter.com/Intel_by_KELA/status/1501197181184888834
[168] https://twitter.com/dsszzi/status/1498721540971585545?s=20&t=ZS8L1nOFS9zU0s8ghMwA1g
[169] https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
[170] https://twitter.com/malwrhunterteam/status/1498673731920617476 and https://twitter.com/0xDanielLopez/status/1498722180238131206
[171] https://twitter.com/MON_GOV_PL/status/1499052596199370753

scanning was happening across the whole spectrum"[172].

- On 3 March, US media reported that US bank executives say they have seen "a subtle but intensified assault on banks' technological infrastructure" after the US and other countries announced sanctions against Russian banks, but that no significant breaches had occurred[173].

- On 3 March, ACTI became aware of US-based public service entities that say their stakeholders "have received emails that are part of a sophisticated spear-phishing campaign built upon pre-existing and legitimate conversations." In these emails, bad actors spoofed the From address to impersonate senior-level leadership and attached malware-infected ZIP files.

- A 4 March report from Bitdefender indicated threat actors are using a Ukraine-themed spam campaign to install remote access Trojans like Remcos and Agent Tesla[174].

- On 6 March, UK tabloids reported on a so-called Russian "Covid for computers." Vaguely citing a "former cyber spy," the tabloids claim that Russian threats could attack readers' devices through porn sites[175]. ACTI assesses that this is an information campaign designed to spread panic among a UK audience.

- On 7 March, the Lapsus$ data extortion group leaked confidential data from South Korean electronics firm Samsung[176]. This occurred two days after the company suspended deliveries to Russia due to sanctions[177]. Lapsus$ has breached a wide variety of targets in the past, including Brazilian and Portuguese government and media entities and a US-based chipmaker[178], raising questions about the group's origin and motives. Samsung said the threat actors had leaked some source code for the company's Galaxy phone but had not leaked customer or employees' personal information and had not affected its business operations[179].

- On 4 March, a cyber attack on PressReader blocked access to electronic editions of over 7,000 publications worldwide, five days after PressReader had announced it was providing content for free to Ukrainians[180]. ACTI assesses the attack was likely intended to block news access for Ukrainians, but it also affected the platform globally.

- On 7 March, Romanian media reported that a "complex cyber attack" had affected some digital services at a Romanian petrol company, but that its gas stations and refinery were operating normally[181]. Romania has played a key role in NATO operations supporting Ukraine, but it is unclear whether this incident directly relates to the conflict.

[172] https://rus.lsm.lv/statja/novosti/obschestvo/nekotorie-iz-poslednih-kiberatak-uvenchalis-uspehom-no-bez-posledstviy--certlv.a446170/
[173] https://nypost.com/2022/03/01/russian-cyber-attacks-against-us-banks-increasing/
[174] https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine
[175] https://www.dailystar.co.uk/news/world-news/russia-could-use-covid-computer-26398061
[176] https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/
[177] https://www.bloomberg.com/news/articles/2022-03-04/samsung-suspends-shipments-of-phones-chips-to-russia
[178] https://www.crn.com/news/security/nvidia-hacks-ransomware-gang-back-to-block-data-leaks-group
[179] http://www.koreaherald.com/view.php?ud=20220307000961
[180] http://web.archive.org/web/20220307010913/https://gazette.com/news/local/cyber-attack-disrupts-thousands-of-publications-including-gazette/article_bdb8bdc4-9d80-11ec-9119- 6300b0f08c7e.html
[181] https://economie.hotnews.ro/stiri-telecom-25416147-surse-atac-cibernetic-rompetrol-mai-multe-masini-sunt-criptate-firma-unde-are-hosting.htm

- On 7 March, ACTI observed a Russian underground forum actor offering free, compromised credentials to supervisory control and data access (SCADA) systems around the world, including a fusion power plant in Pakistan, a US oil refinery, a water supply system in Turkey, and heating and cooling systems in Europe.

- On 7 March, the US intelligence community released its annual Worldwide Threats Assessment[182]. The document noted: "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."

- On 7 March, the Snatch ransomware team—whose past politicized leaks appeared earlier in this SITREP—claimed to have targeted a US-based undersea fiber optic cable manufacturer[183]. This raises anxiety considering the US Annual Threat Assessment that stated Russia is interested in undersea cables.

- A 7 March report by Bloomberg cites Los Angeles-based Resecurity as saying that in February 2022 hackers had compromised computers of current and former employees at nearly two dozen companies involved in liquefied natural gas (LNG) production, including at least five named US companies. Resecurity said it obtained the information by tracing underground forum participants who sought to buy access to these companies, then using a vulnerability to obtain files from the hackers' machines. Resecurity assessed this was a prepositioning effort in advance of the invasion. Bloomberg noted that one of the threat actors had links to SNAKEMACKEREL (a.k.a. Fancy Bear or APT28)[184].

- On 8 March, Cloudflare briefly experienced issues with its load balancers at various datacenters[185]. Twitter, Spotify, and Discord use Cloudflare for content delivery network and/or domain name system (DNS) services.

- On 8 March, Bleeping Computer reported that the Hive ransomware group had carried out the Rompetrol attack and was demanding US$2 million in ransom[186].

- On 8 March, Netblocks wrote: "#Spotify users around the world have been logged out of the service and are unable to stream, as chat app #Discord reports API errors resulting in service outages. The incidents come shortly after Twitter experienced intermittent failures"[187]. Over the prior 24 hours, Twitter had experienced outages in multiple countries due to an issue affecting an internal Twitter API[188]. The source of these disruptions is unknown.

- In an 8 March 2022 posting, Internet-of-things (IoT)-focused cybersecurity company Armis reported on three new critical zero-day vulnerabilities in cloud-connected Smart Uninterruptible Power Supply (Smart-UPS) devices that APC, a Schneider Electric subsidiary, makes. Critical facilities rely on UPS for backup power in case of emergency. These flaws (CVE-2022-22806, CVE-2022-22805, and CVE-2022- 0715) could affect almost 80 percent of companies, according to Armis. Threat actors can

[182] https://docs.house.gov/meetings/IG/IG00/20220308/114469/HHRG-117-IG00-Wstate-HainesA-20220308.pdf
[183] https://twitter.com/S0ufi4n3/status/1500934560627970058
[184] https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine
[185] https://www.cloudflarestatus.com/incidents/75509v4081bm
[186] https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive- ransomware/
[187] https://twitter.com/netblocks/status/1501272743735668738
[188] https://twitter.com/netblocks/status/1501215060638769161

use the UPS as an entry point into the internal corporate network for further malicious activities. More dramatically, they can cause cyber-physical effects: by exploiting these vulnerabilities in a test setting, the researchers remotely caused a UPS device to burst into flames[189]. The CVE-2022-0715 flaw in particular allows a threat actor to send malicious firmware updates—a tactic that threat actors appear to have used in the 24 February Viasat outage described above.

- On 8 March, Der Spiegel reported that Germany's BSI intelligence service has warned of the threat of an imminent cyber attack on high-value German targets such as military or energy-related entities. They reported on Ghostwriter phishing campaigns on German targets with emails sent from the address "theaktuellenews.de@comcast.net"[190].

Analytical Notes: Fall Out from Sanctions

The ever-widening list of sanctions against Russia, particularly the move to ban some Russian banks from the SWIFT international payments system and the curb on certain transactions of the Russian central bank, has raised fears that Russia will undertake cyber threat activity in retaliation[191]. After Iran's expulsion from SWIFT in 2012, massive DDoS attacks originating from Iran hit US banks in 2012-2013 in what analysts see as a retaliatory action[192] and SANDFISH disrupted the Pyeongchang 2018 Olympics reportedly in retaliation for the Russian team's doping-related exclusion from those games[193].

- On 26 February, the Internet Protection Society (IPS), a Russian internet-freedom advocacy group, released a purported message that Russia's Ministry of Digital Development, Communications, and Mass Media had sent to software developers and government entities within Russia[194]. This purported Russian government warning to Russian government and IT entities cited the risk of internet cutoffs and of poisoned software updates or code libraries.
    - According to the (translated) posting, the ministry urged recipients to "immediately download from GitHub, global repositories, foreign open-source software sites and similar resources everything they need to allow them to continue designing and developing their own software under conditions in which access to these resources will be closed off, or in which deliberately compromised materials will be uploaded. They are afraid it will come to that."
    - This appears to reflect a fear that the broad sanctions Western countries adopted on 26 February could include disconnection from GitHub and other repositories[195].
    - Alternatively, it could be a warning that the Russian government might proactively isolate itself from the global internet. Russian authorities have already selectively blocked access to international platforms Twitter and Meta[196]. More broadly, Russia's government has been developing the legal foundation and

[189] https://www.armis.com/research/tlstorm
[190] https://www.theaktuellenews.com/technologie/die- sicherheitsbehoerde-rechnet-in-naher-zukunft-mit-einem-cyberangriff-auf-hochwertige-deutsche- ziele/
[191] https://www.reuters.com/markets/europe/us-banks-prepare-cyber-attacks-after-latest-russia-sanctions-2022-02-27/
[192] https://www.justsecurity.org/61067/planning-cyber-fallout-iranian-nuclear-deal/
[193] https://www.fdd.org/analysis/2020/06/04/nsa-report-attributes-malware-to-russia
[194] https://twitter.com/safe_runet/status/1497560901519646730/photo/1
[195] https://dgap.org/en/research/publications/russias-quest-digital-sovereignty
[196] https://twitter.com/netblocks/status/1497941791177416711

    technical capability to cut its entire internet segment off from the rest of the world, ostensibly to defend against massive outside attacks[197].

  - While warning their own people against code poisoning and malicious updates, Russian strategists may also be considering offensive uses of these attack techniques. Russian state threat actors have themselves used software updates to deliver malware, such as in the Petya/NotPetya attacks. Given the strength of the Russian software industry, software developers worldwide have incorporated Russian-developed code libraries and software components into their own products. Until the time all such products come with a software bill of materials[198], organizations, including those in critical infrastructure sectors, could risk compromises via poisoned code or malicious updates.

- 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[199].

- On 4 March, Tier-1 backbone Internet provider Cogent told its several dozen Russian customers, including state-owned telecommunications provider Rostelecom, that it is terminating their contracts with the provider in compliance with EU sanctions[200]. Despite this termination, Cogent told ZDNet it was "not otherwise restricting or blocking traffic originating from or destined for Russia"[201]. Disconnecting customers will slow international Internet traffic into and out of Russia and will have downstream impacts on some of Russia's neighbors in Central Asia and the Caucasus, according to network operator Kentik. Another backbone carrier, Lumen, said on 8 March that it was ceasing to provide local Lumen services to its enterprise customers in Russia[202].

- On 4 March, amid rumors that the Russian government might soon impose martial law, the Krebs Stamos Group issued recommendations for companies to consider a controlled exit from Russia, including securing data accesses, within hours of receiving notice[203].

- During the week of 7 March, rumors circulated that Russia's government was going to disconnect itself from the global Internet on 11 March. These are exaggerated. Russia's Ministry of Digital Development had written a telegram to federal government entities with tasks the completion of which were due on that day. They were to provide an inventory of their network infrastructure, bandwidth, and user load, and "data on necessity of public resource being available outside of the Russian Federation." The Ministry had also instructed them to: switch to using DNS servers within Russia; delete JavaScript code loaded from foreign sources; and move government websites to Russian hosting, preferably to the .ru domain zone. "Essentially, the Kremlin was taking steps to allow its government websites to continue to work in the event of further cyberattacks, which have bombarded Russian online portals since the beginning of the Ukraine invasion," Vice said[204]. The listed measures are mostly modest steps to advance Russia's years-long efforts to achieve Internet "sovereignty," or self- reliance. The 2019 Internet Sovereignty law

[197] https://dgap.org/en/research/publications/russias-quest-digital-sovereignty
[198] https://www.forbes.com/sites/forbestechcouncil/2022/02/09/the-real-world-criticality-of-implementing-a-software-bill-of-materials/?sh=52c78efc54c1
[199] https://www.zdnet.com/article/icann-rejects-ukraines-request-to-block-russia-from-the-internet/#ftag=RSSbaffb68
[200] https://www.washingtonpost.com/technology/2022/03/04/russia-ukraine-internet-cogent-cutoff/
[201] https://www.zdnet.com/article/internet-service-provider- cogent-cutting-off-access-to-russian-customers/
[202] https://news.lumen.com/RussiaUkraine
[203] https://intel.ks.group/p/controlled-shutdown?s=r
[204] https://www.vice.com/en/article/88gevb/russia-is-preparing-to-cut-itself-off-from-the-global-internet and https://twitter.com/shakirov2036/status/1500649169454878724

called for building a self-sufficient DNS system, but such a system appears far from complete. The mandate to switch to Russia-based DNS services by 11 March, however, seems unrealistic.

- As of 7 March, ACTI has not yet observed a major uptick in sanctions-related threat activity aside from the LockBit attack on the New Mexico financial institution, which is not necessarily directly tied to Western financial sanctions on Russia. Numerous attacks have occurred since countries imposed harsh sanctions on Russia; these appear in the sections above. In many cases, only circumstantial evidence ties them to the Russia-Ukraine conflict.

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 4 March 2022, as part of the invasion of Ukraine and following the imposition of sanctions on Russia[205].

- 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.
  - They have undertaken operations that have not yet become public.
  - They are 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).
  - The limitations of cyber activity in a kinetic war.

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:

- 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[206]. They have

[205] 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

[206] 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[207].

- 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.

- 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.

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"[208].

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 Russians have encountered and some of the work that others have been able to prevent their actions"[209].

- 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

[207] https://www.bbc.com/news/world- europe-60600487
[208] https://www.youtube.com/watch?v=4XTTYr5rrrw&t=883s
[209] https://therecord.media/intel-chiefs-lawmakers-wait-for-other-shoe-to-drop-on-russian-cyberattacks- against-ukraine/

entities, US officials rapidly approved and funded the installation of Fortinet software on Ukrainian police servers[210].

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 potentially exploitable in a way that would spread malware in an automatic, self-sustaining way[211] wiper campaign. Russia-sympathetic cyber crime operators and the presence of cyber crime operations in Ukraine present additional opportunities for criminal actors to be involved in threat activity.

Primary Russian based Threat Groups

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

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

[210] https://www.ft.com/content/1fb2f592- 4806-42fd-a6d5-735578651471
[211] https://nakedsecurity.sophos.com/2022/01/12/wormable-windows-http-hole-what-you-need-to-know/

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[212]. 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.[213] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[214] 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[215]. UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors[216]

- **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[217]. The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics (TsNIIKhM) under Russia's Defense Ministry[218]. 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[219]. 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[220].

Recent WhisperGate Activity

Based on ACTI analysis, there are a few similarities between the mid-January 2022 WhisperGate campaign and SANDFISH's June 2017 NotPetya campaign. Both campaigns

[212] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[213] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[214] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
[215] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[216] 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
[217] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments
[218] https://home.treasury.gov/news/press-releases/sm1162
[219] https://home.treasury.gov/news/press-releases/sm845
[220] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

masqueraded as ransomware campaigns and employed a chain of compromise that several cyber criminal groups have leveraged. In particular, artifacts from both campaigns suggest a victim can recover files by paying a ransom when in fact the malicious code runs a Master Boot Record (MBR) wiper and a file corrupter makes files on the victim system unrecoverable. Although there are similarities, ACTI assesses this general overlap in modus operandi across the WhisperGate and NotPetya campaigns is insufficient to draw any further conclusions, as such overlaps could occur across many wiper or corrupter campaigns.

Mitigations

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

High-priority tactical mitigations:

- Patching externally facing infrastructure (virtual private network appliances, firewalls, web servers, load balancers, etc.) to the latest supported vendor releases, as threat actors often exploit vulnerabilities in externally facing infrastructure to gain initial access to an environment.
- Auditing domain controllers to log successful Kerberos TGS (ticket-granting service) requests and monitoring such events for anomalous activity.
- Having an adequate incidence response (IR) retainer in place to provide necessary surge support and domain-level IR expertise in the event of an incident.
- Treating malware detections for Cobalt Strike and webshells with high priority, as an attacker could use them for lateral movement and persistence.
- Testing and conducting backup procedures on a frequent, regular basis and isolating backups from network connections that could enable malware spreading.

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

- Monitoring service accounts and administrator accounts for signs of credential misuse and abuse, especially for accounts that should not have interactive logon rights.
- Monitoring installation of file transfer tools such as FileZilla and rclone as well as the processes associated with compression or archival tools.
- Creating, maintaining, and periodically exercising a cyber incident response and continuity of operations plan.
- Identifying a resilience plan that addresses how to operate, given a loss of access to or control of an information technology (IT) and/or operational technology (OT) environment.
- 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[221].

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:

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

- 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.

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

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

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