accenture

Global Incident Report: Russia Ukraine Crisis

Update February 25

Key Findings

The Russian military action that began 24 February 2022 against Ukraine has cyber and information-warfare components.

According to media and intelligence reports, 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.

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 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.

Summary

After a several-month military buildup on Ukraine's borders in February 2022, Russian President Vladimir Putin formally recognized two separatist regions of eastern Ukraine and, on 24 February, sent in troops for the "demilitarization and denazification" of Ukraine.[1] 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.

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

[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

Russian state interests, and Russian-based hacktivists, could also use cyber threat activity 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.

If Western countries follow through on their threats to cut Russia off from the SWIFT financial messaging service, anyone doing business with Russia could also experience economic activity disruptions. As of 24 February 2022, US President Joseph Biden said a SWIFT cutoff was "always an option"[2] and the EU and ECB are also "considering the possibility to use this tool" and will hold talks in the coming days to explore.[3]

Cyber-related Events

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."[4] On 15 January, Microsoft announced the discovery of a multi-stage destructive malware on dozens of Ukraine-based government, nonprofit, and IT organizations. Although posing as ransomware, it lacks a ransom recovery mechanism and simply overwrites the Master Boot Record.[5] The attackers reportedly exploited an OctoberCMS vulnerability (CVE-2021-32648) at an IT firm managing affected websites and had access to the networks months before the attack, suggesting cyber espionage activity.[6]
- On 15 February a distributed denial of service (DDoS) attack briefly disrupted two state-owned banks and two military websites in the country.[7] 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."[8] 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[9] [10]; and, on 19 February, the US Cybersecurity and Information Security Agency (CISA) issued an alert warning of foreign operations pairing cyber threat

[2] https://www.barrons.com/articles/joe-biden-russia-sanctions-ukraine-51645726170
[3] https://www.bloomberg.com/news/videos/2022-02-25/eu-to-consider-ousting-russia-from-swift-gentiloni-says-video
[4] https://ua.interfax.com[.]ua/news/telecom/793663.html
[5] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[6] https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html
[7] https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine
[8] https://twitter.com/ersincmt/status/1493940639649742853, https://thedigital.gov.ua/news/mikhaylo-fedorov-ukraina-zmogla-vidbiti-naybilshu-za-vsyu-istoriyu-kraini-kiberataku
[9] https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/
[10] https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine

activity with disinformation to undermine security and hinder the functioning of critical infrastructure.[11]

- 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.[12] 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."[13]
- On 23 February, cybersecurity firm ESET reported the discovery of a new data wiper malware on hundreds of machines in Ukraine.[14] 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.[15] Sentinel Labs has provided additional analysis and indicators of compromise (IOCs) of this malware, which it calls HermeticWiper.[16]
- 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 thus: “The only thing that we learn from new elections is we learned nothing from the old!”[17]
- Meanwhile, US and UK officials have identified a new SANDFISH malware called Cyclops Blink,[18] which recruits compromised machines as botnets and appears to supersede the SANDFISH malware VPNFilter. A Shadowserver report provided additional IOCs[19].
- In a 24 February report on Cyclops Blink,[20] Shadowserver stated that as of 23 February 2022, more than half 1,573 possibly compromised WatchGuard network devices are in either the United States (686), France (85), Italy (85), Canada (85) or Germany (74); Ukraine only has 14 WatchGuard devices with suspected infections.
- 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.[21]

---

[11] https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf
[12] https://twitter.com/lapatina_/status/1494431566310916099, https://twitter.com/MargoGontar/status/1494639246606581762 and https://abcnews.go.com/International/wireStory/ukraines-volatile-east-day-shelling-outages-fear-82976148
[13] https://twitter.com/MargoGontar/status/1494639246606581762
[14] https://twitter.com/esetresearch/status/1496581903205511181?s=21
[15] https://www.scmagazine.com/analysis/apt/ukraine-organizations-hit-by-new-wiper-malware
[16] https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
[17] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
[18] https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
[19] https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/
[20] https://www.shadowserver.org/news/shadowserver-special-reports-cyclops-blink/
[21] https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html

- 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.[22]
- 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.[23] 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 being discussed in any shape or form."[24]
- The main Russian government website was unreachable on the evening of 24 February; websites of the Kremlin and the Russian parliament were also down.[25] Initial Russian media reporting said it was a cyberattack[26], but later the Kremlin spokesman said the Kremlin site was functioning and denied that a DDoS attack on the site had occurred.[27] Later that evening, these Russian government sites were functioning but inaccessible to IP addresses outside of Russia.[28]
- Russian media outlet RT experienced brief DDoS activity on the night of 24 February. The hacktivist group Anonymous claimed responsibility, saying it was acting "in response to [sic] Kremlin's brutal invasion of #Ukraine".[29] On 25 February the account @YourAnonTV announced it would "intensify cyberattacks on the Kremlin this afternoon."[30]
- 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.[31]
- On 24 February, Netblocks reported Internet disruptions in Ukrainian cities of Kharkiv and Mariupol (https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K). 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.[32]
- 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."[33]

---

[22] twitter.com/Blake_Allen13/status/1496572901717331971, hxxps://t[.]me/itsdonetsk/9423
[23] https://www.msn.com/en-us/news/world/biden-has-been-presented-with-options-for-massive-cyberattacks-against-russia/ar-AAUghSb
[24] https://twitter.com/presssec/status/1496919281535111211?s=21
[25] https://twitter.com/safe_runet/status/1496876823979909126
[26] hxxps://ria[.]ru/20220224/kiberataki-1774863604.html
[27] hxxps://www.rbc[.]ru/politics/24/02/2022/6217ab749a79473b77b219d9
[28] https://twitter.com/olliecarroll/status/1496936638723006466
[29] https://www.thedailybeast.com/anonymous-hackers-claim-responsibility-for-cyberattacks-against-russian-state-news-site-rtcom
[30] https://twitter.com/YourAnonTV/status/1497176425014648835
[31] https://www.jpost.com/international/article-698601
[32] https://twitter.com/safe_runet/status/1497131808881795079
[33] https://twitter.com/dsszzi/status/1497103078029291522

- 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.[34]

Outside of Ukraine, NATO members also incurred targeting, including the following:

- On 19 January 2022 a cyberattack disabled certain functions of Global Affairs Canada (GAC), the country's diplomatic and external affairs agency, after Canadian officials extended their support to Ukraine.[35]
- 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.[36] The incidents involved BlackCat and Conti ransomware. Dutch and Belgian officials said they had no evidence of state links as of 4 February 2022,[37] but the ransomware gangs that control the BlackCat and Conti ransomware are based in Russia.[38]
- For their part, hacktivists opposed to the Russian military buildup unleashed ransomware on Belarus Railways on 25 January, hoping to slow troops' movements.[39]
- 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. Accenture Cyber Threat Intelligence (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 motivation of undermining or denigrating US intelligence services.
- On 25 February 2022, we received examples of Ukrainian crisis-themed phishing emails sent to employees of a large global enterprise in Poland. 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.

[34] https://twitter.com/KyivIndependent/status/1497086361509187584
[35] https://globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/
[36] 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
[37] https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say/
[38] https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/
[39] https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/

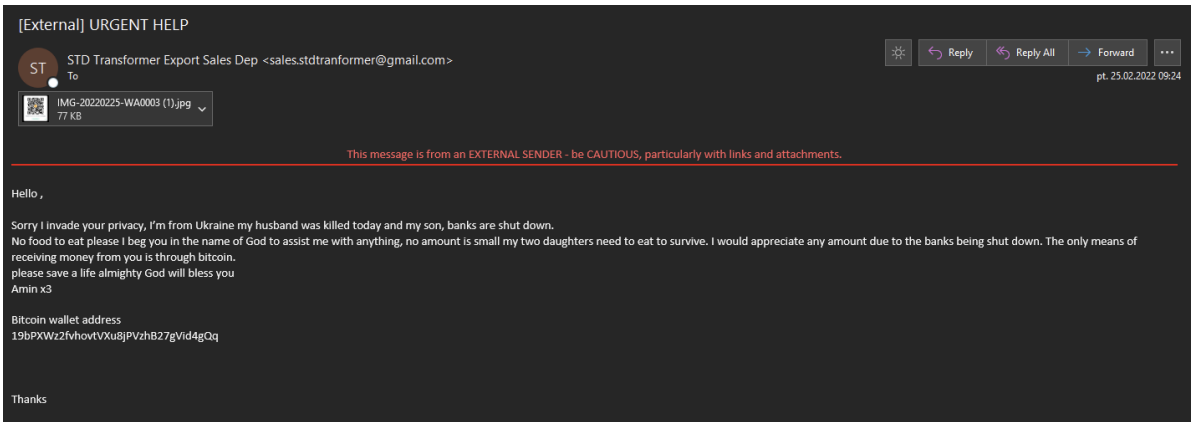

Exhibit 1: Phishing email targeting large global enterprise in Poland, 25 February 2022

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[40] wiper campaign. Russia-sympathetic cybercrime operators and the presence of cybercrime operations in Ukraine present additional opportunities for criminal actors to be involved in threat activity.

Primary Active Groups

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 in line with Russian foreign policy strategies, 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

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

targeting to include other nations in Eastern Europe, suggesting WINTERFLOUNDER's scope may widen as tensions increase.

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

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

- **BLACK GHOST KNIFEFISH (a.k.a. Dragonfly, Berserk Bear, Energetic Bear):** This group, which the US government has linked to the Russian government, is known for targeting energy entities in multiple countries.[41] 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.[42] An April 2018 US and UK government alert warned of additional BLACK GHOST KNIFEFISH[43] 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.[44] UK and US officials have alleged that the threat group has carried out false-flag operations framing Iranian threat actors.[45]

- **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.[46] The US government has linked ZANDER to the Central Research Institute for Chemistry and Mechanics (TsNIIKhM) under Russia's Defense Ministry.[47] 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.

---

[41] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[42] https://www.cisa.gov/uscert/ncas/alerts/TA18-074A
[43] https://www.cisa.gov/uscert/ncas/alerts/TA18-106A
[44] https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes
[45] 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

[46] https://www.slideshare.net/JoeSlowik/past-and-future-of-integrity-based-attacks-in-ics-environments
[47] https://home.treasury.gov/news/press-releases/sm1162

- **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.[48] 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.[49]

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 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 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 threat of cyber threats stemming from hostilities between Russia and 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:

To mitigate the threat of cyber threats stemming from hostilities between Russia and Ukraine, CIFR is treating the following mitigation suggestions with high priority:

- 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.

[48] https://www.wired.com/story/trickbot-malware-group-internal-messages/
[49] https://www.wired.com/story/trickbot-malware-group-internal-messages/ and https://www.cisa.gov/uscert/ncas/alerts/aa21-116a

- 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 (specific suggestions below).
- Identifying a resilience plan that addresses how to operate, given a loss of access to or control of an IT/OT environment (specific suggestions below).
- 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-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 U.S. 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).

Crisis Recommendations

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 and/or administrators).
- Identify critical supply chain vendors.

Week One

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

- Communicate to cybersecurity delivery leads the need to review current telemetry (hunt) for potentially missed IOCs related to Russian threat actors.
- Build a critical threats watchlist for known tactics, techniques, and procedures (TTPs) and ATT&CK model vectors.
- Review and prioritize BC/DR critical-asset lists to support potential response efforts.
- Review IT/OT cybersecurity vision completeness.
- Review availability of current staffing and delivery team to ensure capacity for major disruptions. Maintain IR teams with relevant IT and/or OT capabilities. In the event of suspicious activity or an attack, it is crucial to have the following types of third parties on standby:
    - One or more threat intelligence partners to receive bulletins and updates and validate findings.
    - One or more IR partner(s) to handle surge capacity in the event of an attack or to validate security operations center findings.
- Contact critical supply chain vendors to ensure both awareness and review of “ideal versus actual” process efficacy (e.g., use of multi-factor authentication and VPNs, and insider threat mitigations).

Long-Term

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

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

- Close monitoring of social media, news outlets, and threat intelligence partner bulletins for advance warnings of attacks.

RECOMMENDATIONS FOR SECURITY OPERATIONS AND DELIVERY TEAMS

Immediate

CIFR suggests that immediately after an incident, security 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, security 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, security 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.