Global Incident Report: Russia-Ukraine Crisis | May 13

Key Findings

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

worldwide should remain vigilant for renewed Russian activity designed for maximum service disruption and psychological impact.

- Revelations of a sophisticated 8 April operation intended to cripple the Ukrainian energy grid have led some analysts to assess that a cyberwar has begun.
- Some cyber criminal operations appeared to align with Russia's long-term, strategic priorities of maintaining the country’s dominance in fossil fuel export markets and eroding the perceived US-dominated “unipolar” world order. ACTI assesses with medium-to-high confidence that these have been part of Russia’s “long game” for years.

Summary

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

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

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

This Global Incident Report contains an overview of trends and noteworthy incidents that occurred from 27 April to 11 May 2022, including new developments in the tactics, techniques, and procedures (TTPs) of state-associated threat groups, an assessment that certain ransomware incidents dovetail with Russian strategic interests, and information on cyber criminals threatening cybersecurity researchers. Whereas previous versions of this report presented a chronological compendium of incidents, this version focuses on selected issues of the most concern at the time of its publication.

ADDITIONAL VERSION INFORMATION:

The Global Incident Report dated March 10 provided ongoing updates of cyber threat activity and connectivity-related issues affecting Ukraine and Russia as well as those affecting other countries, along with information on pro-Ukrainian and pro-Russian hacktivist activity.

The Global Incident Report dated April 28 provided new and developing information on: incidents affecting Russia and Ukraine; ransomware and other disruptive incidents worldwide that appeared related to the Russia-Ukraine war, particularly those involving the energy and transportation industries; and both pro-Russian and pro-Ukrainian hacktivist activity. The reports also contained ongoing updates on Russia's isolation from the global internet and the apparent lull in Russian state-sponsored cyber threat activity, and government warnings and expert assessments about threats to critical infrastructure, as well as information on related threat groups and capabilities.

MITIGATIONS are available at the end of this report.

Analysis: Hot War, Cold War

Perceptions of Russian cyber threats have fluctuated. In the first weeks after the invasion, analysts remarked on the apparent absence of massive global Russian cyber attacks. Later, as reports emerged in April of Russia's extensive use of wipers and targeting of operational technology to cripple energy entities, analysts began stating a cyber war had begun.

However, by 10 May 2022, US intelligence chief Avril Haines said: "We have not seen the level of attacks... that we expected,"[2] and United Kingdom (UK) intelligence chief Jeremy Fleming said the threat of a cyber war may have been "overhyped."[3] Analysts have hypothesized that Ukrainian and Western deterrence strategies have worked, that Russia is keeping destructive cyber strikes on NATO countries as a tactic in reserve,[4] and that Russia significant global cyber attacks still hold: kinetic strikes are more efficient than cyber strikes for the most common objectives in wartime; Russian threat actors continue to preposition for broader offensive cyber activity in case there is an existential conflict; and some cyber strikes have already occurred, with the world having slowly realized their seriousness, as the Viasat Hack and Industroyer2 campaigns reflected. The US, UK, and European Union governments officially attributed the Viasat hack to Russia on 10 May.[5] Further, a 27 April Microsoft report summarizes the breadth and depth of Russian cyber attacks on Ukraine.[6]

The hot war on the ground in Ukraine continues, and the risk of a massive cyber attack is still serious. In an urgent joint alert on 20 April, cybersecurity authorities from the US, UK, Canada, Australia, and New Zealand (the Five Eyes countries) issued the joint advisory "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure,"[7] warning organizations against complacency.

[2] https://twitter.com/martinmatishak/status/1524029069309927433
[3] https://www.ft.com/content/d5657df5-a962-4acf-b0bd-b892c6b15361
[4] https://www.nytimes.com/2022/05/03/world/europe/russia-ukraine-war-nato.html
[5] https://www.pcmag.com/news/eu-and-uk-blame-russia-for-hack-that-disrupted-viasats-satellite-internet
[6] http://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[7] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

As ACTI previously assessed, future Russian cyber threat activity will likely occur ahead of elections or moments of major decisions, and some Russia-origin criminal activities align with Russia's long-term strategic priorities. These priorities include maintaining Russia's leading position in fossil fuel markets and eroding the "unipolar" dominance it perceives the US has in the international political and financial systems. Barring a major change in Russian leadership policies, ACTI assesses with medium-to-high confidence that this "long game" will continue even if and when the hot war subsides.

Cyber Espionage groups target Ukraine and NATO countries

Russian state-sponsored groups continue to target Ukraine and other countries with espionage. Reports emerging in the 27 April-11 May 2022 period illustrate the groups' evolving tactics; the following summarizes these reports:

- A recent Gamaredon (a.k.a. WINTERFLOUNDER) operation leveraged Ukrainian-language and English-language lure documents purportedly related to humanitarian assistance for Ukrainian refugees. Targets reportedly included Latvia, a NATO member.[8]
- ACTI identified an overlap in infrastructure between Gamaredon and the cyber criminal Cobalt Group's malware, suggesting the groups possibly share tools.
- The SolarWinds cyber espionage actors have undertaken new phishing campaigns against European, US, and Asian diplomats; as part of these operations, they introduced two malware families in 2022 and sought to evade detection through retooling and abuse of Atlassian's Trello service, according to Mandiant.[9]
- A newly identified group that Mandiant calls UNC3524 has TTPs that overlap with APT28 (a.k.a. SNAKEMACKEREL) and APT29 (a.k.a. JACKMACKEREL).[10] Masquerading as the Computer Emergency Response Team for Ukraine (CERT-UA), SNAKEMACKEREL sent malicious messages asking recipients to download an "UkrScanner" that drops the CredoMap_v2 malware. The threat actors use a subdomain of pipedream[.]net, possibly in a deliberate taunt of using the name of the PIPEDREAM industrial control systems (ICS) malware.[11]

Criminal Targeting Dovetails with Russian Strategic Priorities

As the joint alert from the Five Eyes countries warned, some Russia-origin criminal groups have expressed support for Russia[12] and could undertake disruptive activity against Russia's enemies. While unable to confidently analyze the motives for particular cyber criminal acts, ACTI assesses some of these operations align with Russian strategic

[8] https://cert.gov.ua/article/39086
[9] https://www.mandiant.com/resources/tracking-apt29-phishing-campaigns
[10] https://www.mandiant.com/resources/unc3524-eye-spy-email
[11] https://cert.gov.ua/ARTICLE/40102
[12] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

goals not only to defeat Ukraine but also to preserve Russia’s domination of fossil fuel markets, and to restore a “multipolar world” by ending the perceived US dominance of international institutions.

Defeating Ukraine and Undermining its Supporters

Attacks on government and national security entities of countries supporting Ukraine continue. Ransomware groups have targeted:

- A Bulgarian refugee agency after Bulgaria refused Russian demands to pay for gas in rubles,[13]
- A German weapons manufacturing city as Germany was deciding to provide weapons to Ukraine,[14]
- The US agricultural industry during critical times, such as the harvest and preparations for planting.[15]

DDoS attacks affected Estonian government sites during a NATO cybersecurity exercise in April 2022[16] and websites in Czechia and Moldova.[17]

On 28 April, a week after the Five Eyes countries issued their warning about Russian state and criminal threat actors targeting critical infrastructure,[18] ACTI observed BlackBasta ransomware actors posting ads on underground forums showing particular interest in the Five Eyes countries. They wrote: "We buy and sell access to the corporate networks of the following countries: USA, CA, UK, AU, NZ," referring to the United States, Canada, the United Kingdom, Australia, and New Zealand, respectively.

Maintaining Fossil Fuel Markets

Russia’s economic survival relies heavily on its dominant position in fossil fuel exports. Ransomware incidents and other malicious activity have affected organizations and people associated with:

- Moments of decision that could affect Russia’s energy market position,
- Liquefied natural gas (LNG) and other sources of energy that are playing a growing role as an alternative to dependence on Russia,[19]
- Alternative energy, especially wind power.

Ransomware incidents that have affected moments of decision that could affect Russia’s energy market position include:

[13] https://www.cyberscoop.com/lockbit-ransomware-attack-bulgarian-refugee-agency/
[14] https://twitter.com/darktracer_int/status/1521313526119223296
[15] https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks; https://europe-cities.com/2022/05/01/killnet-attacked-several-websites-of-state-institutions-in-the-republic-of-moldova/
[16] https://news.err.ee/1608573376/ddos-cyberattacks-temporarily-disrupt-estonian-government-websites
[17] https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks; https://europe-cities.com/2022/05/01/killnet-attacked-several-websites-of-state-institutions-in-the-republic-of-moldova/
[18] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[19] https://www.washingtonpost.com/technology/2022/04/13/pipedream-malware-russia-lng/; https://ig.ft.com/europes-race-to-replace-russian-gas/

- **India deciding whether to purchase Russian oil:** On 10 April, Indian government-owned Oil India Limited experienced a cyber incident just days before Indian president Narendra Modi held a video call with US President Joseph Biden, who urged Modi not to purchase Russian oil.[20] On 12 April, at least one Indian oil company removed Russian oil from its latest tender.[21] Actors using a new REvil leak site claimed responsibility for the Oil India breach. REvil is a Russian ransomware group with past targeting that has at times aligned with Russian strategic interests. The Russian government arrested six REvil group members in January, with those members presumably still in custody and potentially subject to Russian government pressure to cooperate in state cyber threat operations. It is unclear whether REvil actors still at large or the Russian government is controlling the new leak site.[22]

Malicious activity that has affected events related to LNG or other sources of energy that are playing a growing role as an alternative to dependence on Russia include:

- **PIPEDREAM malware:** The PIPEDREAM malware, as the April 28 report mentioned, appears to target ICSs, particularly in LNG and electric power environments.[23] Analysts previously warned that Russian threat actors could target LNG exports[24] and gasification facilities in the US and Europe.[25] It was employees of LNG facilities whose credentials Russian threat actors allegedly tried to harvest.[26]
- **ALPHV ransomware incidents:** ALPHV (a.k.a. BlackCat) ransomware operators targeted a major Latin American gas pipeline in early 2022. This attack resembles the 2021 attack on Colonial Pipeline in the US, which used a precursor of BlackCat malware. The attack on the Latin American pipeline syste[27] comes at a time when many countries are scrambling to find new supplies of fuel, including from Latin America, to lessen dependence on Russian fuel.
- **Chatter about new Colonial Pipeline targeting:** On 9 May, ACTI observed an actor nicknamed “Sheriff” posting on the “Breached” underground forum a request to buy login credentials for vpn1.colpipe.com, the website of Colonial Pipeline. The actor offered to pay between US$50,000 and US$150,000 for the login information and commented: “Love seeing these dirty … americans scramble for supplies” [sic]. It is unclear whether the author is serious and whether this actor is the same as the “Sheriff” who has threatened security researchers, as described below. ACTI had previously observed a similar posting

[20] https://www.business-standard.com/article/companies/oil-india-suffers-cyber-attack-receives-rs-57-crore-ransom-demand-122041301002_1.html; https://www.northeasttoday.in/2022/04/12/assam-cyberattack-on-duliajan-based-oil-india-limited-oil-office-it-systems-shut-down/; https://www.reuters.com/world/indian-pm-modi-suggests-direct-talks-between-putin-zelenskiy-2022-04-11/

[21] https://www.reuters.com/world/india/indian-oil-removes-russian-urals-latest-tender-sources-say-2022-04-12/

[22] https://twitter.com/S0ufi4n3/status/1517155603411468288

[23] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf

[24] https://www.brownwoodnews.com/2022/03/31/texas-power-grid-energy-sectors-facing-elevated-russian-cyber-threats-during-war-in-ukraine/

[25] https://www.dragos.com/blog/industry-news/assessing-threats-to-european-industrial-infrastructure/

[26] https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine

[27] https://www.bankinfosecurity.com/blackcat-attack-on-betting-company-disrupts-service-a-18886

from a threat actor nicknamed "Charles Carmakal" on the same forum on 20 March, as a previous version of this report describes.

Incidents involving renewable alternative energy sources include:

- **Attacks on wind power companies:** Wind power companies Nordex and Deutsche Windtechnik in Germany experienced ransomware attacks by Conti[28] and Black Basta, respectively.[29]
- **Compromised access to a solar company:** An underground forum participant advertised access to a Spanish company that works on solar projects.[30]

This battle over energy infrastructure goes both ways—pro-Ukrainian hacktivists have been breaching and leaking information of Russian entities related to energy production and exports, as previous editions of the report have illustrated.

Attacks on LATAM

The first months of 2022 have seen a rash of attacks using Russia-origin ransomware against Latin American countries. Some attacks appear consistent with an effort to amplify unrest and chaos in the US' backyard and weaken Latin American countries' relationship with the US.[31] Some such attacks include:

- On 21 April, a Conti ransomware group attack paralyzed numerous Costa Rican government systems. Former Costa Rican President Carlos Alvarado Quesada claimed the attacks were not financially motivated but "sought to threaten the stability of the country in a situation of transition" as the country prepared for the swearing-in of a new president on 8 May.[32] The new president promptly declared a national emergency.[33] The Conti ransomware group claimed responsibility for the attacks and issued a veiled threat: "in the chat we are open for private dialogue, …. keep stability in your beautiful country, you have beautiful nature, educated young people, developed business, we are waiting for you in the chat."[34] The Conti actors added that Costa Rica "cannot recover the information, they turned to the US for help and were told not to pay."[35] Conti actors have pledged support for Russia in the past, and an all-out attack on Costa Rican institutions would be consistent with Russian attempts to weaken the influence of the US in Latin America.[36] On 6 May, the US State Department offered a reward of up to US$10 million for information to bring Conti threat actors to justice; the

[28] https://twitter.com/BrettCallow/status/1514715780377575427
[29] https://twitter.com/IscsBalakrishna/status/1519745769515139072; https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/
[30] https://twitter.com/IscsBalakrishna/status/1519774951611727872
[31] https://www.realinstitutoelcano.org/en/analyses/latin-america-in-the-ukraine-crisis-a-pawn-in-the-game-for-putins-resurgent-russia/
[32] https://www.reuters.com/world/americas/costa-ricas-alvarado-says-cyberattacks-seek-destabilize-country-government-2022-04-21/
[33] https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
[34] https://twitter.com/NatSecGeek/status/1517980656676098054
[35] https://twitter.com/_bettercyber_/status/1518998432651878400
[36] https://warontherocks.com/2022/04/explaining-latin-americas-contradictory-reactions-to-the-war-in-ukraine/

announcement specifically named the attack on Costa Rican systems, saying the incident disrupted platforms for the country's foreign trade.[37]

- On 27 April, Conti actors announced they had stolen information from the Peruvian intelligence service, Digimin, and wrote: "please contact us if you do not want such consequences that occurred in Costa Rica not so long ago."[38]
- BlackCat (a.k.a. ALPHV) targeted an Argentinian pipeline, 12 manufacturing or industrial entities in Mexico, and a regional government in Ecuador.[39] BlackCat is the same ransomware responsible for crippling Oiltanking, the Antwerp port, and other energy- and transport-related infrastructure that NATO countries use. The US Federal Bureau of Investigation (FBI) issued an alert saying that, as of March 2022, the FBI had observed BlackCat-affiliated threat actors successfully infecting over 60 entities globally.[40]

IT Specialists as "Combat Resources" for the Russian State

Conti actors have a cozy relationship with the "cozy bears." Leaked internal chat messages from Conti ransomware operators show they take targeting guidance from "cozy bears," likely referring to Russian cyber threat group JACKMACKEREL, and the messages cited sponsors who apparently protect them from arrest by Russian law enforcement.[41]

Additionally, Russian prison officials have reportedly considered hiring imprisoned IT specialists out to Russian IT companies for remote work.[42] Previous Global Incident Reports have mentioned numerous IT specialists who are or have been in custody in Russia; these specialists include: REvil actors authorities arrested in January 2022; the Colonial Pipeline suspects; Ilya Sachkov, the head of the cybersecurity company Group-IB; Pavel Vrublevsky of Chronopay; and Dmitriy Pavlov of the Hydra underground network.

When Russian officials arrest cyber criminals, security experts question whether the Russian officials are preemptively arresting the criminals to prevent them from traveling abroad to avoid arrestation or to coopt them to conduct pro-Russian operations. A Ukrainian cybersecurity official made such an analysis recently.[43] The Russian government has often fought to prevent the extradition of Russian criminal suspects to the US after authorities arrested those suspects abroad. One Kremlin-friendly IT entrepreneur described IT specialists as a "combat resource" for the Russian state. Since the war started, one Russian IT expert said he was asked to list the "skills he could offer the military."[44] Furthermore, any Russia-based IT company could be forced to[45] use its

[37] https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/
[38] https://twitter.com/darktracer_int/status/1519302162471292930
[39] https://www.linkedin.com/pulse/alerta-se-detecta-presencia-del-ransomware-blackcat-en-victor-ruiz; https://twitter.com/IscsBalakrishna/status/1519754103714623488
[40] https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/
[41] https://www.wired.com/story/conti-ransomware-russia/
[42] hxxps://tass[.]ru/obschestvo/14489179; https://krebsonsecurity.com/2022/05/russia-to-rent-tech-savvy-prisoners-to-corporate-it/
[43] https://therecord.media/from-the-front-lines-of-the-first-real-cyberwar/
[44] https://www.washingtonpost.com/world/2022/05/01/russia-tech-exodus-ukraine-war/
[45] hxxps://www.gazeta[.]ru/army/2017/08/26/10859996.shtml

software to steal information or introduce malware into the systems of its customers; the US government probed Kaspersky software based on these fears, according to a 9 May Reuters article.[46]

The competition for Russian IT talent goes both ways. US officials have discussed waiving some visa restrictions for Russians with high-tech skills, including cybersecurity skills, with the aim of weakening Russian productivity.[47]

Cyber criminals Take the Offensive Against Cybersecurity Researchers

Criminals have threatened DDoS attacks or physical violence against researchers. A Russian affiliate of the REvil ransomware crew with the nickname "Sheriff" claimed to have impersonated a law enforcement official and deceived Twitter into yielding account information on one of those researchers. To explain the reason for doing this, the actor stated: "i hate americans and i also hate researchers [sic]."[48]

On 6 May, the pro-Russian Killnet group vowed revenge after UK officials arrested a member on suspicion of attacking Romanian government sites. The Killnet Telegram site read: "If he is not released within 48 hours I will destroy your Romania, Great Britain and Moldova."[49] Addressing the UK, Killnet said: "I will destroy your entire information structure and even your Ministry of Health. All ventilators will be attacked."[50]

In some cases, this activity seems to fit with Russia's long-term objectives of preserving its position in fossil fuel export markets and restoring its status as a global power.

What To Expect

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

- Moments of decision such as elections, sanctions discussions, and court cases, or decisions related to NATO membership.
- High-profile events from which countries have excluded Russia, such as sporting events.

[46] https://www.reuters.com/technology/exclusive-ukraine-war-spurs-us-ramp-up-security-probe-software-maker-kaspersky-2022-05-09/
[47] https://ca.news.yahoo.com/news/bidens-proposal-ease-us-visa-053452268.html
[48] https://www.cyberscoop.com/twitter-emergency-disclosure-request-lalartu-aleksandr-sikerin-revil-ransomware-researcher-threats/; https://twitter.com/BleepinComputer/status/1465826315479789580; https://www.databreaches.net/silent-no-more-exposing-a-campaign-thatintimidated-researchers-and-journalists/
[49] https://metro.co.uk/tag/moldova/?ico=auto_link_news_P4_LNK1
[50] https://metro.co.uk/2022/05/06/russian-hacking-group-threatens-to-shut-down-uk-hospital-ventilators-16597589/

- 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.

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

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.
- 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" 11 January 2022.[51]
- "Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure".[52]
- Patching the vulnerabilities that Cisco Talos has assessed as most likely for threat actors to exploit.[53]"Russian State-sponsored and Criminal Cyber Threats to Critical Infrastructure," 20 April 2022.[54]

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

- Actively hunt for any indications of Russian state-sponsored tactics, techniques, and procedures (TTPs), using the abovementioned 11 January 2022 CISA document for reference.
- Know your network and any connectivity you have in Russia and surrounding territories.
- Mitigate public-facing vulnerabilities, particularly actively exploited ones, referring to CISA's Known Exploited Vulnerabilities catalog[55] for guidance.
- Secure credentials.

[51] https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
[52] https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf
[53] https://blog.talosintelligence.com/2022/03/ukraine-update.html
[54] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[55] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- For organizations with OT or ICS, take note of any unexpected behavior such as reboots.
- Refer to the US alert on SatCom threats[56] if satellite communication networks are in use.
- Take steps possible to maximize resilience.
- Dust off and exercise incident response plans, designate a crisis response team, ensure key personnel, test backups, test manual controls. Make sure your plans include contact information for the FBI and CISA and that you know in advance whom you would hire for incident response and legal services.
- Call the FBI field office quickly if you see social media posts indicating disinformation.
- Report to CISA or local FBI offices any anomalous activity even if it appears to be mundane or routine scanning.

Crisis Recommendations

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).

[56] https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

- Identify critical supply chain vendors.

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

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

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

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

Recommendations for Cybersecurity Operations and Delivery Teams

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

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

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

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

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

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

About Accenture

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

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

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

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.