accenture

# Global Incident Report: Russia-Ukraine Crisis | June 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 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.
- While various "carrots" and "sticks" appear to motivate Russian hackers' support for Russian strategic goals, "sticks" such as the threat of imprisonment have become more prominent since the leadup to the war with Ukraine.
- The targeting and timing of some Russia-origin cyber threat incidents appear aimed at influencing decisions, an apparent tactic reminiscent of the Russian military doctrine of "escalate to de-escalate."

# 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 updated June 10 discusses: a hack-and-leak operation targeting United Kingdom (UK) politics; pro-Russian disruptive operations against Italy, Costa Rica, and other countries; cyber threat incidents, the targeting and timing of which appear aimed at influencing decisions, reminiscent of Russian doctrine of "escalate to de-escalate"; the use of Russian hacker prowess as a deterrent; new insights

[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

into the evolving relationships between hackers and intelligence agencies in Russia; and dates to watch. This version continues to focus on selected issues of the most concern at the time of its publication. The themes in the May 27 and May 13 release remain relevant as of 8 June 2022.

The Global Incident Report dated May 27 discusses: Russian-aligned hacktivists' and ransomware operators' threats against countries; Conti group developments; DDoS and ransomware attacks associated with information operations; new reports of state cyber groups' activities; and a new Russian cybersecurity decree. This version focuses on selected issues of the most concern at the time of its publication.

The Global Incident Report dated May 13 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. This version focuses on selected issues of the most concern at the time of its publication.

**ADDITIONAL VERSION INFORMATION:**

The March 10 and earlier versions of the Global Incident Report presented a chronological compendium of incidents.

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

## Update for 11 May 2022: 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.

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]

[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
[8] https://cert.gov.ua/article/39086

- 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 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]

[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
[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/

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:

- **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:

---

[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/
[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

- **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 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.

[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
[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

## 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 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]

[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/
[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/

## 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 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

[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
[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

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.

# Update for 25 May 2022: Fear, uncertainty, and doubt

Over the period of 11–25 May 2022, Russia-origin ransomware actors and pro-Russian hacktivists boasted of disabling whole countries. At the same time, changes in the ransomware group landscape left researchers guessing about those group members' motives, organization, and future threats. Meanwhile, reports continued to elucidate the ongoing activity of cyber espionage actors.

## Sowing Fear: Ransomware actors and hacktivists threaten countries

As previous versions of this report mentioned, cybersecurity officials in the US and other Five Eyes countries warned that "Russia-aligned" threat groups could threaten critical infrastructure in countries around the world.[51] Broad attacks and threats against government websites in countries such as Costa Rica, Germany, and Italy continued for two weeks in mid-May 2022.

### Killnet hacktivists

The pro-Russian hacktivist group Killnet claimed responsibility for DDoS attacks against European countries and made further threats, which follow:

- On 7 May, Killnet's Telegram channel claimed responsibility for DDoS attacks on multiple German government entities—the Ministry of Defense, the Bundestag, the federal police, and the police authorities of several states—in retaliation for Germany having provided weapons to Ukraine.[52]
- On 10 and 14 May, Killnet actors coordinated DDoS attacks against the international singing competition Eurovision Song Contest, which banned Russia's participation in the 2022 season (ACTI had previously predicted Russia-linked actors may try to disrupt events that banned Russia's participation). During the Eurovision Song Contest voting on 14 May, the Killnet actors coordinating the

[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/
[51] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[52] https://www.dw.com/ru/rossijskie-hakery-atakovali-pravitelstvennye-sajty-frg/a-61722443

attack inexplicably called it off after 13 minutes.[53] Other Killnet operations appear to have failed.[54]

- On 11 and 12 May, Killnet claimed to be the group "Legion" and took responsibility for taking offline the websites of Italy's Senate, military, and National Institute of Health, as well as the Italian Automobile Club, in a probable DDoS attack.[55] One of Killnet's postings said "Italy and Spain is being torn to pieces by the 'MIRAI' detachment. And Sakura and Jackie get Poland and Germany,"[56] with Mirai and Sakura referring to botnets.
- On May 14, after its brief attack on Eurovision, Killnet's Telegram channel announced it "officially declares war on 10 countries, including the deceitful police of Italy."[57] Possibly in connection with the threat against the Italian police, the police website was unavailable on 16 May.[58]
- On 17 May, Killnet (a.k.a. Legion) specified the 10 countries it was targeting: the US, the UK, Germany, Italy, Poland, Romania, Latvia, Estonia, Lithuania, and Ukraine, although the group claimed it would only target the governments of these countries, not the populations.[59]
- A 24 May posting on the Killnet site said: "We have just received information that Italian and American WiFi routers are carrying out a cyber attack on the FBI's Cyber Crime Investigation Unit. It's amazing, how could this happen?" The posting showed a screenshot depicting the FBI's Internet Crime Complaint Center (IC3). The ic3.gov site was inaccessible at 6:30 p.m. US ET on 24 May and was intermittently unavailable on the morning of 25 May. The Killnet posting's reference to an attack by Wi-Fi routers suggests the use of a botnet as part of a DDoS attack.

Russian state TV interviewed Killnet actors on 23 May. According to independent, open-source intelligence researcher Cyberknow20, in the interview, the Killnet actors "Said they are conducting much more than DDoS attacks. That they are outnumbered but holding their own."[60]

Russian state actors have carried out politically motivated "hybrid DDoS operations" in the past. The purportedly hacktivist group Cyber-Berkut, which NATO and the UK government have linked with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), carried out DDoS attacks against Ukraine and

[53] https://inforesist.org/italiya-otbila-neozhidanno-korotkuyu-kiberataku-rf-na-servera-evrovideniya-vo-vremya-finala-konkursa
[54] https://cyberknow.medium.com/killnet-pro-russian-hacktivists-e916ac7201a3, https://www.pwndefend.com/2022/05/18/killnet-area-they-really-a-threat/
[55] https://www.reuters.com/world/europe/pro-russian-hackers-target-italy-defence-ministry-senate-websites-ansa-news-2022-05-11/, https://twitter.com/Cyberknow20/status/1524687251262873601, https://therecord.media/italy-killnet-hacking-military-parliament-national-health-institute/
[56] https://twitter.com/Cyberknow20/status/1524410228246302725
[57] https://govinfosecurity.com/new-cyberattacks-on-italy-include-eurovision-disruption-a-19081
[58] https://www.euronews.com/culture/2022/05/16/eurovision-2022-russian-hackers-targeted-contest-say-italian-police
[59] hxxps://www.securitylab[.]ru/news/531675.php
[60] https://twitter.com/Cyberknow20/status/1528736348437303301

NATO in 2014;[61] and Russian military intelligence personnel associated with SNAKEMACKEREL activity conducted DDoS attacks against the World Anti-Doping Agency website in 2016, according to a US indictment.[62]

### Continued Conti ransomware threats in Costa Rica

The Conti ransomware operators continued to threaten the Costa Rican government and denounced that country's relationship with the US, as the following illustrates:

- On 12 May, ACTI observed an account calling itself "unc1756" posting an ad on the Russia-based exploit[.]in forum, offering to buy access to "MSP TOP WORLD," likely referring to managed service providers (MSPs). In the posting, unc1756 claimed responsibility not only for the breaches of Peru's Digimin and Costa Rican agencies but also of Ruby Receptionists, a US-based MSP. unc1756 wrote: "We really can shake down a small country." Offering to split the profits 50-50 with anyone who would provide access to MSPs, unc1756 concluded, "We don't work with mother***ers or with pro-Americans." unc1756's message appeared the day after the Five Eyes countries issued an alert warning of threats to MSPs[63] and could be read as a taunting response to that warning.
- On 14 May, a Conti leak site posting, titled "FOR COSTA RICA AND US TERRORISTS (BIDEN AND HIS ADMINISTRATION)", read "Just pay before it's too late, your country was destroyed by 2 people, we are determined to overthrow the government by means of a cyber attack, we have already shown you all the strength and power, you have introduced an emergency. Now we are putting together a campaign against the current government... we have defeated you! I appeal to every resident of Costa Rica, go to your government and organize rallies so that they would pay us as soon as possible if your current government cannot stabilize the situation? Maybe it's worth changing it?"[64] Later that day, the Conti authors bolstered their argument urging Costa Ricans to oust the current pro-US president. They changed the posting to add that "the Americans simply sacrifice" Costa Rica, apparently referring to Conti actors' earlier claim that the US was causing hardship for Costa Rica by advising it not to pay the ransom.
- In a 20 May posting, the Conti actors also harangued Russian-American cybersecurity researchers and expressed extreme hostility to the current US leadership. They wrote, "You don't know anything about us and about our motives, you are just traitors who work for the USA (the USA is a cancer on the body of the earth, you make people suffer, not so long ago we attacked https://www.securityweek.com/hackers-hit-web-hosting-provider-linked-oregon-elections, the fbi paid us money, why are you preventing us from doing this in costa rica, we hope that soon the usa power will change [sic]."[65]

[61] https://wired.com/story/russias-cyber-threat-to-ukraine-is-vast-and-underestimated/, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf
[62] https://www.justice.gov/opa/page/file/1098481/download
[63] https://www.cisa.gov/uscert/ncas/alerts/aa22-131a
[64] https://twitter.com/vxunderground/status/1525463875872870400
[65] https://twitter.com/NatSecGeek/status/1527770125260181504

Analysts still seek consensus on the mix of political and financial motives behind Conti actors' activity, whether they are acting on their own or in coordination with Russian intelligence services, and whether they are reorganizing, as this report discusses below. Regardless, the Conti actors clearly seek to intimidate political leaders in Costa Rica and other target countries, and they arrogate to themselves the power to affect politics.

## Sowing uncertainty and doubt

Developments in the cyber threat landscape over the 11-25 May period sparked debates among researchers on threat groups' organization and intentions. In addition, new reports provided examples of threat actors seeking to use disruptive or destructive activities as part of information operations to demoralize and sway adversaries.

### Attribution challenges

Developments in the Conti ransomware ecosystem have left analysts guessing and debating not only their motives and organization but also their future, making attribution difficult.

Researchers from the cybersecurity company AdvIntel named 19 May as "Conti's official date of death." They said Conti actors closed "all the infrastructure related to negotiations, data uploads, and hosting of stolen data" although the ransomware group's "Conti News" website continued to publicize statements. AdvIntel hypothesized that: data extortion operations using BlackByte, BlackBasta, and Karakurt (Turkish for Black Wolf) malware are spinoffs of the formerly unified Conti organization; Conti operators worked as "collective affiliates" with Hive, AvosLocker, AlphV (a.k.a. BlackCat), and HelloKitty (a.k.a. FiveHands) ransomware groups; and Conti actors carried out the ransomware operation and political threats against Costa Rica to distract attention from Conti's disappearance.[66] Determining the validity of these claims will require further research. Analysts have found evidence both for and against a link between Conti and BlackBasta,[67] while the Conti leak site itself has denied Conti and BlackBasta are the same.[68] In addition, the relationship between the Conti organization and the threat entity calling itself unc1756 requires further clarification. Also unclear is why the Conti leak site and the Hive leak site both claimed responsibility for the same breach simultaneously on 24 May.[69]

Similarly confusing is a new ransomware strain called Nokoyawa, targeting mainly South America, that shares some characteristics with Hive, Babuk, Karma, and Nemty. Some early ransom notes have Chinese characters, suggesting Asian targeting as well.[70]

[66] https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape
[67] https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html
[68] https://twitter.com/BrettCallow/status/1524387838531301377/photo/1
[69] https://twitter.com/ValeryMarchive/status/1529103060299132928
[70] https://www.fortinet.com/blog/threat-research/nokoyawa-variant-catching-up
https://trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html

### Destructive and disruptive activity tied to information operations

The WhisperGate wiper and DDoS operations against Ukraine before the 24 February invasion included efforts to demoralize Ukrainians and sow Ukrainian-Polish hostility[71] and, as this report mentioned above, Russian state actors have carried out politically motivated "hybrid DDoS operations" in the past. Events such as the following, which the 11–25 May reporting period covered, have cast further light on relationships between disruptive or destructive operations—such as ransomware attacks, wiper activity, or DDoS operations—and information operations:

- A wiper operation targeting a Ukrainian organization coincided with a 16 March operation in which threat actors hijacked a Ukrainian news feed with the false message that Ukraine was surrendering to Russia.[72]
- Researchers at cybersecurity firm Nisos explored documents that Ukrainian activists leaked in 2020; the documents described a Federal Security Service of the Russian Federation (FSB)-commissioned botnet known as Fronton, which is a DDoS and social media manipulation tool that Russian IT company 0Day Technologies (a.k.a. Zeroday Technologies or 0Dt) designed.[73] The creation of false and manipulative social media accounts is a major tactic in Russian "active measures" to demoralize and influence adversaries.[74]

### Reports outline state-sponsored threat actors' ongoing activity

Reports emerging in the 11-25 May period provided new details on ongoing state-sponsored operations; these reports include the following:

- ESET reported on the evolution of a malware loader ESET said Sandworm group threat actors had used in the Industroyer2 operation.[75]
- Recorded Future analyzed nine wipers associated with the Russia-Ukraine conflict. The study found a worm component—HermeticWiper—in only one of them. The threat actors behind HermeticWiper had designed the worm to spread only within a victim network, apparently in an attempt to prevent the uncontrolled spillover that occurred with Petya.A/NotPetya in 2017. The study also found that the threat actors had designed the wipers merely for destruction, not for information exfiltration.[76]
- Researchers at Malwarebytes discovered at least two malicious English-language documents, purportedly about the Russia-Ukraine crisis or about purported chemical agents in Ukraine, that exploit the MSHTML remote code execution

[71] https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/, https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces/
[72] https://www.mandiant.com/resources/information-operations-surrounding-ukraine
[73] https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/fronton-report.pdf
[74] https://www.armyupress.army.mil/Portals/7/nco-journal/images/2022/January/Social-Media/The-Info-Domain-Part%201.pdf
[75] https://welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
[76] https://go.recordedfuture.com/hubfs/reports/mtp-2022-0512.pdf

vulnerability CVE-2021-40444.[77] A previous report reported on a campaign exploiting this vulnerability to target dissidents in Russia.

- German speakers received documents with purported updates on the Ukraine crisis that dropped a custom PowerShell remote access Trojan, which stole data and then exfiltrated it to the domain kleinm[.]de. Malwarebytes researchers reporting on the operation speculated that a Russian group could be responsible but acknowledged they could not be sure.[82]
- Turla (a.k.a. BELUGASTURGEON) has created typo-squat domains resembling those of the Austrian Federal Economic Chamber, an Estonian military college, and a NATO e-learning portal. The domains host a malicious "War Bulletin" document that contains no malicious macros but does have an embedded.png file that can inform the attackers about victims' IP addresses and Microsoft Word versions, according to cybersecurity firm Sekoia.[78]

In other reports on state-sponsored threat actors, the US Cybersecurity and Infrastructure Security Agency (CISA) urgently warned that unspecified state-sponsored threat actors were exploiting VMware remote code execution vulnerabilities CVE-2022-22954 and CVE-2022-22960 to drop the Dingo J-spy webshell and gain root privileges.[79] In a separate alert on "unintentional insider threats," the US Department of Defense urged organizations to warn their employees against interacting with manipulated media and inadvertently compromising security.[80]

**Putin signs cybersecurity decree**

During the 11-25 May period, there were continued reports of DDoS attacks or data-theft efforts targeting Russian systems, including Russian video platform RuTube, Russian state nuclear company Rosatom, and three Russian airports.[81]

In a May 20 address to the Russian Security Council, President Putin said Russia had "essentially become the target of aggression, of an information war" that included attacks by "state-run structures."[82] On 24 May, Putin signed a decree "On additional Measures to Ensure the Information Security of the Russian Federation." The decree called for Russian state and critical infrastructure entities to allow Russia's Federal Security Service remote access to their Internet-connected information systems. It also set a 2025 deadline for such entities to cease the use of foreign-made anti-virus tools.[83]

[77] https://twitter.com/h2jazi/status/1524012184010997760, https://twitter.com/h2jazi/status/1524408606363471873
[78] https://www.bleepingcomputer.com/news/security/russian-hackers-perform-reconnaissance-against-austria-estonia/
[79] https://www.cisa.gov/uscert/ncas/alerts/aa22-138b
[80] https://dhra.mil/Portals/52/Documents/perserec/reports/20220413_PERS_Rpt_RN-21-14_Deepfakes.pdf
[81] https://nbcnews.com/tech/tech-news/rutube-down-russia-hack-attack-ukraine-rcna28299
https://www.ibtimes.com/anonymous-challenges-russias-supposed-cyber-prowess-repeat-rosatom-breach-leaks-data-3505131; hxxps://tass[.]ru/proisshestviya/14620147
[82] hxxp://en.kremlin[.]ru/events/president/news/68451
[83] hxxp://static.kremlin[.]ru/media/events/files/ru/51DUJhHHAb0tNBBbC6xWgbDo1Fu9znRO.pdf

## Update for 8 June 2022: War of attrition

Initial massive ground offensives have given way to slow, grinding battles over cities and villages in eastern Ukraine. In recently occupied areas, Russian officials have sought to consolidate control over communications mediums, including the internet; they have switched the country codes of phone numbers in those areas to Russia's country code and have routed traffic through Russian rather than Ukrainian providers.[84]

The conflict has turned into a war of attrition, as NATO Secretary General Jens Stoltenberg has put it.[85] ACTI and other analysts have argued that Putin seeks to wear down the current Western united front, taking advantage of differences of opinion over oil and gas embargoes, grain sale blockades, and other topics. Edward Luce of the Financial Times said, "The war is being fought on two levels—on the ground in Ukraine and in the information battle for control of the global narrative. Both have entered a period of attrition."[86]

For their part, Pro-Ukrainian hackers continue to wreak havoc on Russian systems. They have disrupted Russian video site RuTube, breached Russian radio stations to play Ukrainian songs, and claimed responsibility for DDoS attacks or data breaches against targets such as Russian media websites, Russian law firms, Russian Railway employees, and Belarus ministries.[87] Additionally, US Cyber Command chief Paul Nakasone said the US has carried out unspecified offensive cyber operations in support of Ukraine. In US terminology, "offensive cyber operations" can include both active intelligence and more-disruptive operations, and it is unclear what offensive activity the US has undertaken.[88]

Pro-Russian ransomware actors and hacktivists have continued disruptive activity that includes declaring "war" on whole countries. The timing of some of those operations appears consistent with a Russian military strategy called "escalate to de-escalate," which refers to coercive threats or demonstrative attacks that force an adversary to capitulate.[89] Since mid-May, new information (described below) has emerged about the complicated relationship between the pro-Russian hackers carrying out disruptive activity and the Russian state officials who both protect and threaten those hackers. Organizations in countries supporting Ukraine should expect continued Russian targeting of such countries, intimidation with the threat of ransomware, and attempts to sow inflammatory, false, or misleading information.

---

[84] hxxps://iz[.]ru/1340975/2022-05-27/v-gosdume-obiasnili-perekhod-zaporozhia-i-khersona-na-rossiiskii-telefonnyi-kod; https://twitter.com/tass_agency/status/1531508347387752448; https://twitter.com/netblocks/status/1531321609633538048

[85] https://www.msn.com/en-us/news/world/west-must-brace-for-long-haul-in-ukraine-nato-chief/ar-AAY0KKO

[86] https://www.ft.com/content/80faf9af-d11f-476f-8fc7-88d2c28e3620

[87] https://twitter.com/HumanBrotherho1/status/1530331900400783365; https://twitter.com/cyber_etc/status/1529470209815457792; hxxps://inforesist[.]org/na-treh-populyarnyh-v-rf-radiostancziyah-neskolko-chasov-zvuchali-ukrainskie-i-antivoennye-pesni/; https://twitter.com/cyber_etc/status/1530635346366562308; https://twitter.com/cyber_etc/status/1530596640851210242; https://twitter.com/PucksReturn/status/1530302169223778305; https://twitter.com/LorianSynaro/status/1530980049909911555

[88] https://twitter.com/ILDannyMoore/status/1532841218643738625

[89] https://www.russiamatters.org/analysis/escalate-deescalate-part-russias-nuclear-toolbox

## Active Measures

Operations and statements by pro-Russian hacktivists and Russia-aligned ransomware groups appear consistent with an attempt to influence global opinion and sow distrust among and against the US and NATO countries. Since Soviet days, Russia has used a strategy of taking "active measures," which are cyberspace, media, or real-world activities a nation-state's intelligence services take to influence the politics of another state. These measures may include influencing with an election, swaying popular opinion, or engineering the ouster of a country's leader, among others, and are part of psychological or information warfare.[90] To the extent pro-Russian hacktivists and ransomware actors received targeting inspiration from Russian intelligence services, those actors' operations fit the definition of "active measures" as well.

## Battlegrounds: Europe and the Global South

Disruptive operations continued in Europe. The Killnet pro-Russian hacker group, which declared "war" on Italy in mid-May, on 28 May called for a second wave of DDoS attacks against Italian government agencies to begin on May 30.[91] In the first days of June, Twitter user @KILLNET_LEGION claimed to have taken down websites of Italy's President of the Republic and of the Italian military, as well as systems at numerous Italian ports.[92] Furthermore, on 3 June, an apparent ransomware attack crippled municipal services and online portals of the Italian city of Palermo for at least three days.[93] In England, a threat group that several third-party analysts tentatively identified as the FSB-linked Russian state hacker group Callisto created a website and, on 25 May, posted to that site documents purporting to show machinations by Richard Dearlove (former head of the British Secret Intelligence Service, MI6) and others to help Boris Johnson defeat former British Prime Minister Theresa May in 2019 to ensure the implementation of Brexit (Britain's separation from the European Union).[94] ACTI tracks Callisto under the name WINTERFLOUNDER, under which ACTI also tracks Gamaredon activity.

The leaks became public on the same day the so-called Partygate report—the results of an investigation into Johnson's alleged violations of COVID-19 protocols—became public. A different scandal called Swedengate—a wave of social media postings claiming Swedes are racist and inhospitable—briefly rocked Twitter and Reddit on 30 May.[95] It is unclear who made these postings "go viral," but the timing of this, not long after Sweden had formerly applied to join NATO on 17 May,[96] is consistent with an attempt to influence the discussion of Sweden's NATO accession.

---

[90] https://www.lawfareblog.com/kremlins-return-active-measures
[91] https://twitter.com/KILLNET_LEGION/status/1530591712858472453; https://therecord.media/italy-killnet-hacking-military-parliament-national-health-institute/; https://www.politico.eu/article/italys-eni-to-open-ruble-accounts-for-gas-payments/; https://www.ilgiorno.it/mondo/anonymous-killnet-attacco-italia-telegram-1.7729173; https://www.bleepingcomputer.com/news/security/italy-warns-organizations-to-brace-for-incoming-ddos-attacks/
[92] https://web.archive.org/web/20220601195302/https://twitter.com/KILLNET_LEGION/status/1532087703084351488; https://twitter.com/KILLNET_LEGION/status/1533144560276230146
[93] https://www.bleepingcomputer.com/news/security/italian-city-of-palermo-shuts-down-all-systems-to-fend-off-cyberattack/;
[94] https://reuters.com/technology/exclusive-russian-hackers-are-linked-new-brexit-leak-website-google-says-2022-05-25/
[95] https://www.newsweek.com/dinner-guests-colonialism-how-swedengate-took-over-internet-1711640
[96] https://www.businessinsider.com/sweden-formally-applies-join-nato-reports-2022-5; https://www.nato.int/cps/en/natohq/news_195468.htm

Additionally, as a previous version of this Global Incident Report mentioned, whoever controls the REvil ransomware leak site claimed responsibility for the attack on Oil India on the eve of US President Biden's phone call urging India to reduce purchases of Russian oil.[97] Cyber threat activity has also continued against Latin American countries, with Costa Rica experiencing yet another ransomware attack against a public service; this time, the Hive ransomware group, rather than Conti, took responsibility for the attack.[98] As ACTI argued in the 13 May and 27 May updates to this report, such attacks align with the long-term Russian foreign policy goal of reducing US influence in Latin American countries such as Costa Rica and, more broadly, US global dominance. More immediately, the attacks helped set a negative tone on the eve of the US-hosted Summit of the Americas that began on 6 June. ACTI assesses with medium confidence that these operations align with Russian diplomatic efforts in the "Global South"[99] countries of Latin America, Africa, and Asia. Many such countries have expressed lukewarm support for punishing Russia.[100]

### Escalate to de-escalate

In past Global Incident Reports, ACTI has urged organizations to expect to see Russian cyber-enabled information operations pegged to moments of decision, such as elections or decisions affecting Russia's monopoly on fossil fuel exports. Sometimes such operations appear aimed at retaliation for a decision unfavorable to Russia; other times, they occur before or during negotiations, which is incompatible with the theory of a retaliatory motive. A possible motive for attacks occurring earlier in the negotiation process is that such operations are aimed at having a deterrent effect on the counterparty by emphasizing the fearsome cyber threat activity Russia could unleash should negotiations result in an unfavorable outcome for that country.

Numerous disruptive incidents that have occurred since mid-May appear circumstantially linked to the Russia-Ukraine war. Not all have definitive ties with the Russian state, but they form a pattern that aligns with a known Russian nuclear war strategy termed "escalate to de-escalate." This strategy involves carrying out limited strikes that raise the stakes beyond what an adversary can tolerate, doing so in an effort to force the adversary to make concessions.[101] ACTI assesses with medium confidence that this concept, applied to the sphere of cyber conflict, helps explain threat operations that have occurred during promising negotiations—operations that otherwise seem to make no sense strategically.[102] The following incidents came during moments of decision-making that affected Russia's strategic goals:

- On 24 May, Indian airline Spicejet announced unspecified actors had attempted a ransomware attack on it. Hundreds of passengers faced delays and many web pages remained inaccessible on 25 May.[103] This occurred on the same day global

[97] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220428_TLP-WHITE-FINAL.pdf.pdf
[98] https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/
[99] https://journals.sagepub.com/doi/pdf/10.1177/1536504212436479
[100] https://www.reuters.com/article/apps-south-column/column-ukraine-war-unleashes-battle-for-global-south-hearts-and-minds-idINL3N2W91UE
[101] https://www.russiamatters.org/analysis/escalate-deescalate-part-russias-nuclear-toolbox
[102] https://www.cyberwarcon.com/juice-worth-the-squeeze
[103] https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/

media showed Indian President Narendra Modi shaking the hand of US President Biden during a meeting of the so-called Quad countries (India, US, Australia, and Japan).[104] In light of the earlier-mentioned Oil India breach, ACTI assesses that the targeting and timing of the Spicejet incident aligns with Russian state interests in discouraging Indian rapprochement with Western countries.

- A 24 May incident disrupted government services and email traffic in the Austrian state of Carinthia for several days. ALPHV (a.k.a. BlackCat) ransomware operators demanded US$5 million to unlock the regional government's computers, published sample screenshots of sensitive data, and attempted a DDoS attack in retribution for non-payment of the ransom.[105] The initial disruption occurred three days before Austrian Chancellor Karl Nehammer held a 45-minute phone call with Putin and agreed to discuss a prisoner swap and to honor previous Russian natural gas delivery contracts.[106] As previous Global Incident Reports have shown, threat actors have used ALPHV in several operations that aligned with Russian strategic priorities.[107]

- In Italy, the first wave of Killnet attacks on 11-12 May (described in the 27 May update, above) occurred as Italy wavered between a hard line and concessions toward Russia; Italian state energy company Eni was deciding how to respond to Russia's demand to pay for gas in rubles; and Italian Prime Minister Draghi, after speaking with US President Biden, had proposed the idea of an oil consumer "cartel" to counter Russian demands.[108] The European Union met on 30 May to discuss Draghi's proposal for imposing a cap on prices paid to Russia for gas. Killnet called for a renewed "war" on Italy to take place on the same day, 30 May.[109]

**Russian hackers as a sword of Damocles**

Official statements and actions bolster the idea that Russian hackers act as "a sword of Damocles"[110] to threaten and deter Russia's adversaries. On 6 June, Russian cybersecurity negotiator Andrey Krutskikh issued a statement claiming the US had instigated pro-Ukrainian hacktivist attacks on Russia and was failing to cooperate in UN negotiations on international information security. Krutskikh warned, "we do not recommend that the United States provoke Russia into retaliatory measures - a rebuff will certainly follow, it will be firm and resolute. However, the outcome of this 'mess' could be catastrophic, because there will be no winners in a direct cyber clash of states." Krutskikh has issued similar threats in the past, as previous versions of this report

[104] https://therecord.media/us-australia-india-and-japan-announce-cybersecurity-initiatives-on-software-supply-chains/; https://therecord.media/spiceject-ransomware-attack-flights-grounded/
[105] https://www.derstandard.at/story/2000136284267/kaernten-hack-erbeutete-private-daten-im-netz-veroeffentlicht
[106] https://www.usnews.com/news/world/articles/2022-05-27/putin-ready-to-deliver-gas-discuss-prisoner-swap-austria
[107] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220428_TLP-WHITE-FINAL.pdf.pdf; https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220527_TLP-WHITE-CLEAN.pdf
[108] https://www.ft.com/content/a7984e58-a2f7-4436-9c83-efe4d2db42a2
[109] https://www.theguardian.com/business/2022/may/30/could-a-cartel-of-large-energy-consumers-cut-oil-and-gas-prices
[110] https://greekreporter.com/2022/05/25/sword-damocles-power-ancient-greece/

have noted.[111] Krutskikh's most recent threat occurred during UN committee deliberations on a cyber crime treaty. During the negotiations, scheduled for 30 May–10 June in Vienna, Russia and numerous countries of the Global South have backed Russia's version of the treaty, which critics have warned would legitimize controls on free speech.[112]

**Case Study: REvil**

"Hopes of Russian help on ransomware are officially dead," the Washington Post reported on 1 June, citing a report from the semi-independent Russian news source Kommersant.[113] The Kommersant article, titled "Russian Hackers Don't Matter to America: Prosecution of REvil Suspects Is at a Dead End,"[114] cited a lawyer for one of the suspected REvil ransomware group members, whom Russian authorities arrested in January after investigating leads the US had provided. The lawyer said the case remained in limbo and that his client remained in pre-trial detention after four months, reportedly without even facing questioning. This paralysis supposedly resulted from the failure of US law enforcement to produce evidence to document the group's victims and their losses. Indeed, the Russian courts database shows that the Moscow City Court opened Case No. 10-9644/2022 under article 187 of the Russian Criminal Code on 6 May 2022; the case apparently went to an appeals court, which sent it back to the lower court on 17 May 2022.[115]

According to Kommersant, defense lawyers suggested the suspects could make a deal with the prosecutors. In return for dropping the charges, according to possible proposals for such a deal, the state could confiscate the suspects' allegedly ill-gotten property, or the suspects could donate it for humanitarian relief in the war-torn eastern Ukraine "republics." "Besides," Kommersant concluded, "the unique experience of the former suspects would probably be useful to Russian intelligence in the fight against the hackers from Ukraine, who have become active recently."[116] The Washington Post and other commentators understood this as a veiled threat of further state-inspired Russian criminal activity against the enemies of Russia.[117]

The defense lawyer's statements, claiming the US was to blame for Russia's failure to combat Russian cyber crime, echoed points that Russian Deputy Security Council chief Aleksey Khramov made in interviews that Russian state media published in early April and mid-May.[118] Soon after Khramov's April interview, an underground leak site purportedly belonging to REvil reappeared,[119] as if to show how the supposed US failure to cooperate with Russia could allow the resurgence of cyber crime. However, the

[111] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220428_TLP-WHITE-FINAL.pdf.pdf
[112] https://riskybiznews.substack.com/p/risky-biz-news-lockbit-and-mandiant?s=r; https://unodc.org/unodc/en/cybercrime/ad_hoc_committee/home; https://www.washingtonpost.com/opinions/2022/06/07/us-russia-conflict-is-heating-up-cyberspace/
[113] https://www.washingtonpost.com/politics/2022/06/01/hopes-russian-help-ransomware-are-officially-dead/
[114] http://web.archive.org/web/20220527011707/https://www.kommersant.ru/doc/5369361
[115] hxxp://xn--90afdbaav0bd1afy6eub5d[.]xn--p1ai/68321031/extended
[116] http://web.archive.org/web/20220527011707/https://www.kommersant.ru/doc/5369361
[117] https://www.washingtonpost.com/politics/2022/06/01/hopes-russian-help-ransomware-are-officially-dead/
[118] hxxps://tass[.]ru/politika/14657587
[119] https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/05/ACTI_POV_UkraineCrisis_20220428_TLP-WHITE-FINAL.pdf.pdf

prospects for real cooperation with Russia to combat cyber crime always remained dim. In the past, when Russian law enforcement agencies have received intelligence from their US counterparts, they have sometimes tipped off the Russian suspect or co-opted them to help Russia instead.[120] The Russian government has also brought treason charges against several Russian cybersecurity investigators who worked closely with Western law enforcement agencies; this likely also has a chilling effect on any Russian official who might consider sharing information with Western counterparts.[121] As another sign of lack of commitment to effective cooperation against cyber crime, on 6 June, Russia banned the main US negotiator on such cooperation efforts from entering Russia.[122] In the case of REvil, a Russian law enforcement raid netted eight people but did not search for or arrest the more-infamous REvil suspect, FBI-wanted Yevgeniy Polyanin.[123] While the REvil suspects remain in prison, intelligence officers have the opportunity to co-opt them. In addition, Russian law enforcement officials confiscated suspects' servers and devices, from which the officials probably learned extensive information about the whole threat group organization. Russia could hold that information in reserve as needed to pressure other group members to take part in state-directed cyber threat activity.

### Sticks over carrots

"Carrots" like the opportunity to make money with relative impunity appear to have become less important than Russian law enforcement wielding of "sticks," which namely consist of a heightened threat of arrest. The pressure has only grown since mid-2021, as Russian authorities have arrested people ranging from cybersecurity company chief Ilya Sachkov to suspects in cases involving TrickBot, REvil, and other ransomware.[124]

As previous versions of this report have noted, Russian prison officials have broached the idea of hiring imprisoned hackers and IT specialists for remote work.

Former CISA head Christopher Krebs tweeted on 1 June: "I've long thought one of the reasons the Russians permitted ransomware unchecked was to provide OTJ [on-the-job] training and foster a cyber workforce they could call on at a later date in support of the state's security services. Looks like that deal might be on the table."[125] Another former top US official from the Department of Homeland Security (DHS), Suzanne Spaulding, similarly hypothesized the following in a tweet:[126]

> *these arrests were also intended to send a message to cyber criminals operating out of Russia that they better cooperate with 'requests' from the government or risk a similar fate. Don't need actual prosecution. The threat is there. …. the 'requests' by the Kremlin of these cyber criminals would be/are to attack targets of*

[120] https://rferl.org/a/cyber-crime-us-russia-cooperation-mess/28459178.html
[121] https://www.youtube.com/watch?v=ntwsAxk_Tmw; https://www.rferl.org/a/group-ib-sachkov-cybersecurity-treason/31483812.html
[122] https://www.washingtonpost.com/opinions/2022/06/07/us-russia-conflict-is-heating-up-cyberspace/
[123] hxxps://dailystorm[.]ru/rassledovaniya/blesk-i-nishcheta-koroley-hakerskogo-mira-daily-storm-publikuet-profayly-podozrevaemyh-po-delu-gruppirovki-revil; https://www.fbi.gov/wanted/cyber/yevgyeniy-igoryevich-polyanin/download.pdf
[124] https://therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/
[125] https://twitter.com/C_C_Krebs/status/1531978125873225728
[126] https://twitter.com/SpauldingSez/status/1532505158571130890?cxt=HHwWlICwkc_UxsQqAAAA

*Kremlin's choosing. The threat of prosecution is a way to ensure the proxies can be counted on.*

**Russian hackers working for the motherland or money**

Russian hackers, both criminals and employees of legitimate IT companies, have often lent their services over the years for the "motherland," reflecting patriotic feelings, desires for heroic self-images, and the pure love of achievement. The following provide some examples of this behavior:

- Self-proclaimed hacker Pavel Sitnikov, who claims to have worked with "security agencies," including a Russian contractor that develops tools for the FSB,[127] in a 2020 interview sketched out his vision of an ideal world for hackers: "where we will feel comfortable, and the government will come and ask us nicely, with a cookie, 'Here you go, guys. Now we need you to destroy another country...'" To this, in Sitnikov's imagined world, the hackers would answer "'No question about it! Let's do it!!'" Sitnikov has boasted of breaching the US National Security Agency (NSA) and other US entities, because "we want to destabilize America. You know, destroy it, just as they want to destroy us."[128] Russian authorities arrested Sitnikov in 2021.[129]
- On 1 June, the Killnet spinoff group called Legion, in an apparent effort to attract young followers, tweeted "Legion is the sword and shield of Russia in cyberspace. Yes, it is made up of young people, and so what? The whole world is wetting its pants at the sound of Your name. Develop your skills, love your motherland, and protect it! No one but us -- We are the cyber special forces!"[130]
- A wide variety of Russian sympathizers have joined the attacks on Italy, as former financial police general told Italian newspaper Il Giornale on 1 June, "Russia has found support in Brazilian hackers and in experts recruited from all over the world, with a kind of digital volunteering. Not only are there Putin's sympathizers, but many other stakeholders. For example, the anti-vaxxers who collaborate with Killnet to discover the military secrets behind the vaccine."[131]

However, criminals balance out their patriotic duties with making money and avoiding prison time, according to an article in Russian investigative periodical Daily Storm. The article cited a hacker saying, "In the first week of the cyberwar, participants in Russian-language chats respectfully listened to the siloviki [law enforcement, military or intelligence personnel] and rushed to fulfill the tasks they set down.... In the second week, you could already hear phrases like 'well, the comrade majors set a task, but you can't fully trust them. If we reveal information about our tools, they will later come after us'. And in the third week, cyber criminals started to grumble, 'We have been slaving away for you for two weeks already; we are spending money on proxies, DDoS, servers. At least pay us back for our expenses.'" The law enforcement officials would urge them

[127] https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/fronton-report.pdf
[128] hxxps://expert[.]ru/expert/2020/39/oni-ne-pomnyat-nas-horoshih-pust-ne-zabudut-nas-plohih/
[129] https://therecord.media/russian-hacker-pavel-sitnikov-arrested-for-sharing-malware-source-code/
[130] https://twitter.com/KILLNET_LEGION/status/1532085139144163332
[131] https://www.ilgiornale.it/news/tecnologia/russia-ha-reclutato-3mila-cyber-mercenari-attaccare-litalia-2038553.html

to make sacrifices for the motherland and would hold over them the threat of arrest. For their part, hackers felt they had "worked a few weeks for the Motherland and that's good enough. It's time for the guys to make some money." However, the Daily Storm's hacker source noted that such hackers "fail to realize that the battles will end someday, whereas the statute of limitations on their crimes will not."[132] Already in January, the arrests of REvil suspects had shaken hackers' sense of impunity, according to a Digital Shadows' analysis of cyber crime forum posts.[133]

### Shape-shifting

Cyber criminal groups continue to evolve, hindering attribution.

As a previous version of this report described, analysts debate whether the Conti ransomware organization is disbanding and working with spinoff or otherwise-affiliated groups such as Hive and Karakurt. The ransom note attackers used in the 31 May breach of Costa Rica's public health service resembled that of the Hive group. The Hive group's leak site has also begun publishing leak announcements identical to ones on the Conti leak website, bolstering suspicions of a link between those groups.[134] One plausible hypothesis is that former Conti operators are rebranding to stay in business, as victims hesitate to pay ransom to the Conti organization after it explicitly declared support for Russia and after the US offered a reward for information leading to the arrest of Conti participants.

In another example of avoiding association with a sanctioned group, actors previously known for their use of the SocGholish (a.k.a. FAKEUPDATES) malware that some have associated with US-sanctioned group Evil Corp, have begun employing the more widely used LockBit ransomware for the encryption phase of their operations, apparently in an attempt to escape attribution and sanctions, according to a Mandiant report.[135] Days after Mandiant's publication of that report, the LockBit leak site claimed to have breached Mandiant and insisted, "our group has nothing to do with Evil Corp" and nothing to do with politics.[136] Mandiant says it has no evidence of a breach.[137]

### Dates to watch

Russian strategists might undertake or encourage cyber threat activity and/or information operations to exert influence during moments of decision such as the following:

- **30 May-10 June:** Second negotiating session of the Ad Hoc Committee on a UN cyber crime convention[138]
- **6-10 June:** Summit of the Americas in Los Angeles, California

[132] hxxps://dailystorm[.]ru/rassledovaniya/unikalnaya-myasorubka-hroniki-pervoy-mirovoy-kibervoyny
[133] https://www.digitalshadows.com/blog-and-research/life-in-prison-the-cybercriminal-perspective/
[134] https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/
[135] https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
[136] https://twitter.com/vxunderground/status/1533948505043124224
[137] https://www.bleepingcomputer.com/news/security/mandiant-no-evidence-we-were-hacked-by-lockbit-ransomware/
[138] https://unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

- **12 and 19 June:** French parliamentary elections
- **29-30 June:** NATO Summit in Madrid, during which heads of state and government from NATO member states and "key partners" will endorse NATO's new Strategic Concept and likely discuss Finland's and Sweden's accession to the alliance
- **September-October:** Elections in Austria, Sweden, Czechia, and Latvia
- **26 September-14 October:** The UN's International Telecommunications Union (ITU) Plenipotentiary Conference in Bucharest, Romania, which will include the election of a new ITU Secretary General, pitting an American candidate against a Russian candidate who also has ties to China; Russia has portrayed this election as key to promoting Russia's vision of the internet, which would allow countries to set their own rules in the name of "sovereignty"[139]
- **8 November:** US midterm elections

# 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.
- 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.

[139] https://www.itu.int/pp22/en/; https://www.washingtonpost.com/opinions/2021/05/04/russias-plot-control-internet-is-no-longer-secret/; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119863; https://www.atlanticcouncil.org/event/the-future-of-the-itu-how-will-russia-ukraine-affect-technology-standards

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.[140]
- "Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure".[141]
- Patching the vulnerabilities that Cisco Talos has assessed as most likely for threat actors to exploit.[142]"Russian State-sponsored and Criminal Cyber Threats to Critical Infrastructure," 20 April 2022.[143]

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[144] for guidance.
- Secure credentials.
- For organizations with OT or ICS, take note of any unexpected behavior such as reboots.
- Refer to the US alert on SatCom threats[145] 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

[140] https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
[141] https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf
[142] https://blog.talosintelligence.com/2022/03/ukraine-update.html
[143] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[144] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[145] https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

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).
- 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.