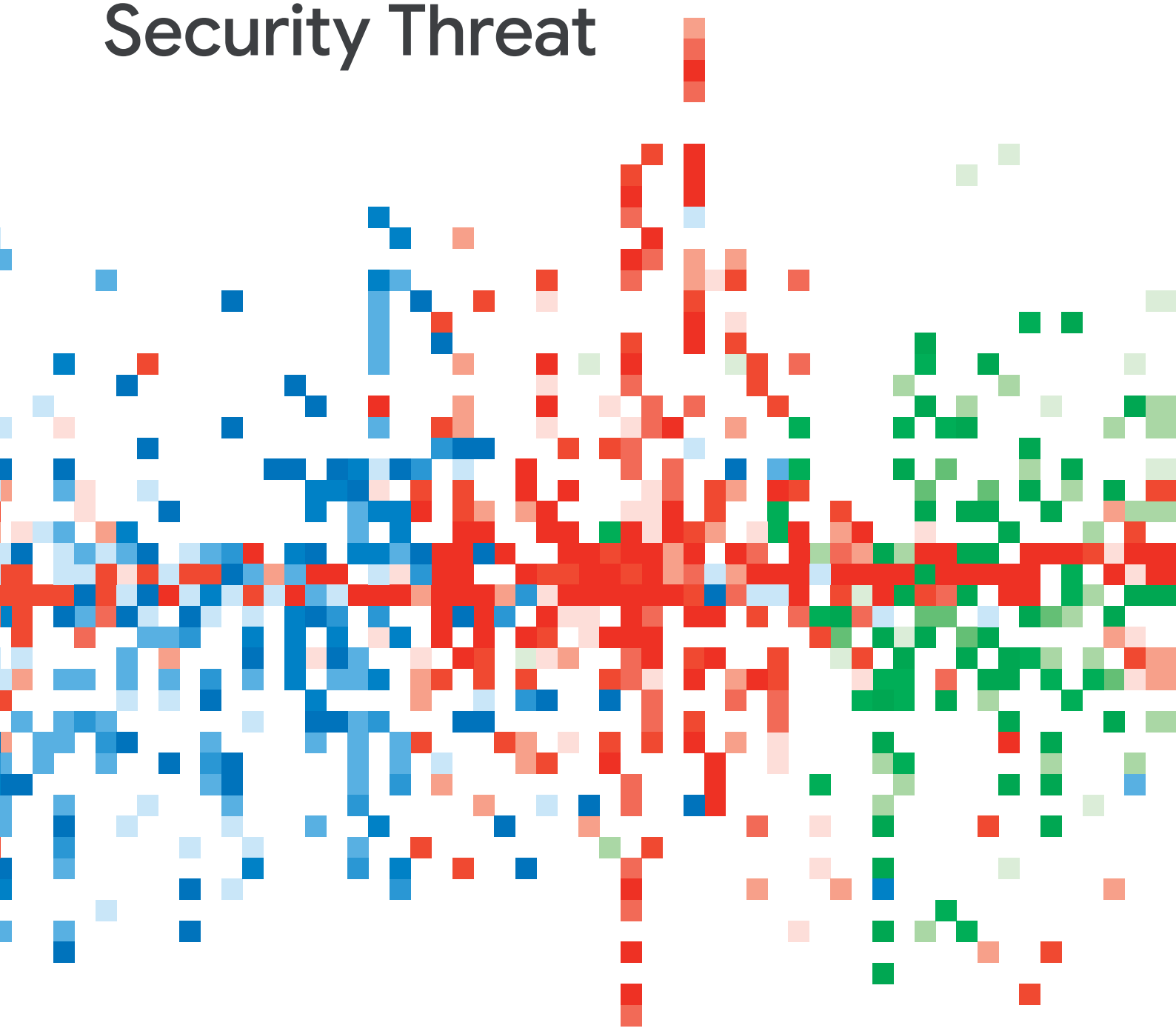
Cybercrime: A Multifaceted National Security Threat



Google

2025 February

Table of contents

About the Authors

Google Threat Intelligence Group brings together the Mandiant Intelligence and Threat Analysis Group (TAG) teams, and focuses on identifying, analyzing, mitigating, and eliminating entire classes of cyber threats against Alphabet, our users, and our customers. Our work includes countering threats from government-backed attackers, targeted zero-day exploits, coordinated information operations (IO), and serious cyber-crime networks. We apply our intelligence to improve Google's defenses and protect our users and customers.

Executive Summary

Cybercrime makes up a majority of the malicious activity online and occupies the majority of defenders' resources. In 2024, Mandiant Consulting responded to almost four times more intrusions conducted by financially-motivated actors than state-backed intrusions. Despite this overwhelming volume, cybercrime receives much less attention from national security practitioners than the threat from state-backed groups. While the threat from state-backed hacking is rightly understood to be severe, it should not be evaluated in isolation from financially-motivated intrusions.

A hospital disrupted by a state-backed group using a wiper and a hospital disrupted by a financially-motivated group using ransomware have the same impact on patient care. Likewise, sensitive data stolen from an organization and posted on a data leak site can be exploited by an adversary in the same way data exfiltrated in an espionage operation can be. These examples are particularly salient today, as criminals increasingly target and leak data from hospitals. Healthcare's share of posts on data leak sites has doubled over the past three years, even as the number of data leak sites tracked by GTIG has increased by nearly 50% year over year. The impact of these attacks mean that they must be taken seriously as a national security threat, no matter the motivation of the actors behind it.

Cybercrime also facilitates state-backed hacking by allowing states to purchase cyber capabilities, or co-opt criminals to conduct state-directed operations to steal data or engage in disruption. Russia has drawn on criminal capabilities to fuel the cyber support to their war in Ukraine. GRU-linked APT44 (aka Sandworm), a unit of Russian military intelligence, has employed malware available from cybercrime communities to conduct espionage and disruptive operations in Ukraine and CIGAR (aka RomCom), a group that historically focused on cybercrime, has conducted espionage operations against the Ukrainian government since 2022. However, this is not limited to Russia. Iranian threat groups deploy ransomware to raise funds while simultaneously conducting espionage, and Chinese espionage groups often supplement their income with cybercrime. Most notably, North Korea uses state-backed groups to directly generate revenue for the regime. North Korea has heavily targeted crypto- currencies, compromising exchanges and individual victims' crypto wallets.

Despite the overlaps in effects and collaboration with states, tackling the root causes of cybercrime requires fundamentally different solutions. Cybercrime involves collaboration between disparate groups, often across borders and without respect to sovereignty. Any solution requires international cooperation by law enforcement and intelligence agencies to track, arrest, and prosecute these criminals. Individual takedowns can have important temporary effects, but the collaborative nature of cybercrime means that the disrupted group will be quickly replaced by others offering the same service. Achieving broader success will require collaboration between countries and public and private sectors on systemic solutions such as increasing education and resilience efforts.

Section 1

Stand-alone cybercrime is a threat to countries' national security

Financially-motivated cyber intrusions, even those without any ties to state goals, harm national security. A single incident can be impactful enough on its own to have a severe consequence on the victim and disrupt citizens' access to critical goods and services. The enormous volume of financially-motivated intrusions occurring every day also has a cumulative impact, hurting national economic competitiveness and placing huge strain on cyber defenders, leading to decreased readiness and burnout.

A single financially-motivated operation can have severe effects

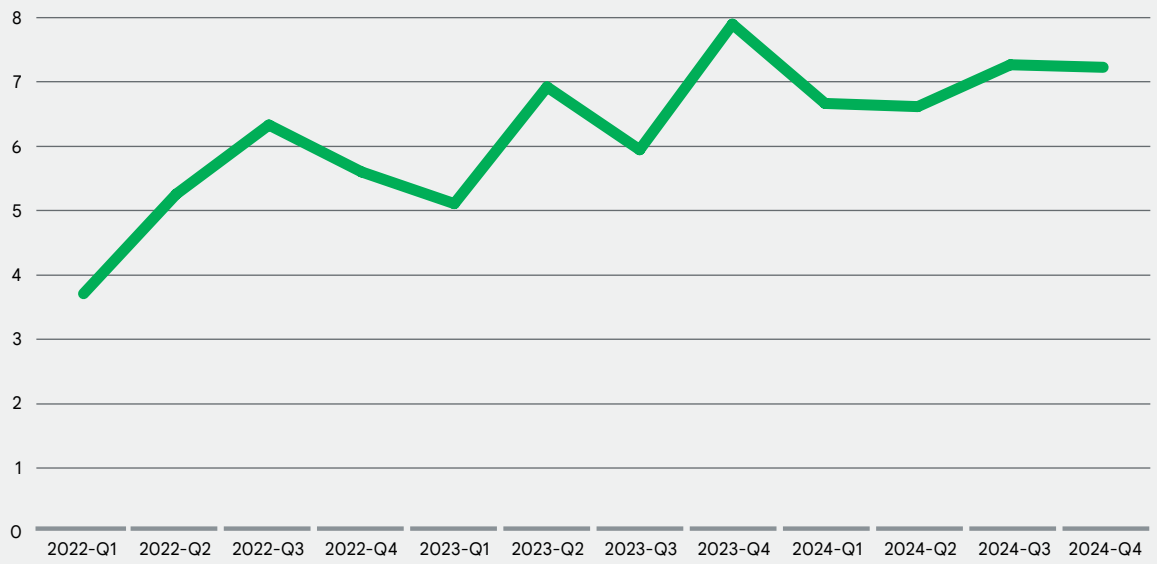
Cybercrime, particularly ransomware, is a serious threat to critical infrastructure. Disruptions to energy infrastructure, such as the 2021 Colonial Pipeline attack, a 2022 incident at the Amsterdam-Rotterdam-Antwerp refining hub, and the 2023 attack on Petro-Canada, have disrupted citizens' ability to access vital goods. While the impacts in these cases were temporary and recoverable, a ransomware attack during a weather emergency or other acute situation could have devastating consequences.

Beyond energy, the ransomware attacks on the healthcare sector have had the most severe consequences on everyday people. At the height of the pandemic in early 2020, it appeared that ransomware groups might steer clear of hospitals, with multiple groups making statements to that effect, but the forbearance did not hold. Healthcare organizations' critical missions and the high impact of disruptions have led them to be perceived as more likely to pay a ransom and led some groups to increase their focus on targeting healthcare. The healthcare industry, especially hospitals, almost certainly continues to be a lucrative target for ransomware operators given the sensitivity of patient data and the criticality of the services that it provides.

Since 2022, Google Threat Intelligence Group (GTIG) has observed a notable increase in the number of data leak site (DLS) victims from within the hospital subsector. Data leak sites, which are used to release victim data following data theft extortion incidents, are intended to pressure victims to pay a ransom demand or give threat actors additional leverage during ransom negotiations.

- In July 2024, the Qilin (aka "AGENDA") DLS announced upcoming attacks targeting U.S. healthcare organizations. They followed through with this threat by adding a regional medical center to their list of claimed victims on the DLS the following week, and adding multiple healthcare and dental clinics in August 2024. The ransomware operators have purportedly stated that they focus their targeting on sectors that pay well, and one of those sectors is healthcare.
- In March 2024, the RAMP forum actor "badbone", who has been associated with INC ransomware, sought illicit access to Dutch and French medical, government, and educational organizations, stating that they were willing to pay 2–5% more for hospitals, particularly ones with emergency services.

SHARE OF DATA LEAK SITES' VICTIMS WHO ARE IN THE HEALTHCARE INDUSTRY



Studies from academics and internal hospital reviews have shown that the disruptions from ransomware attacks go beyond inconvenience and have led to life-threatening consequences for patients. Disruptions can impact not just individual hospitals but also the broader healthcare supply chain. Cyberattacks on companies that manufacture critical medications and life-saving therapies can have far-reaching consequences worldwide.

A recent study from researchers at the University of Minnesota-Twin Cities School of Public Health showed that among patients already admitted to a hospital when a ransomware attack takes place; "in-hospital mortality increases by 35-41%."

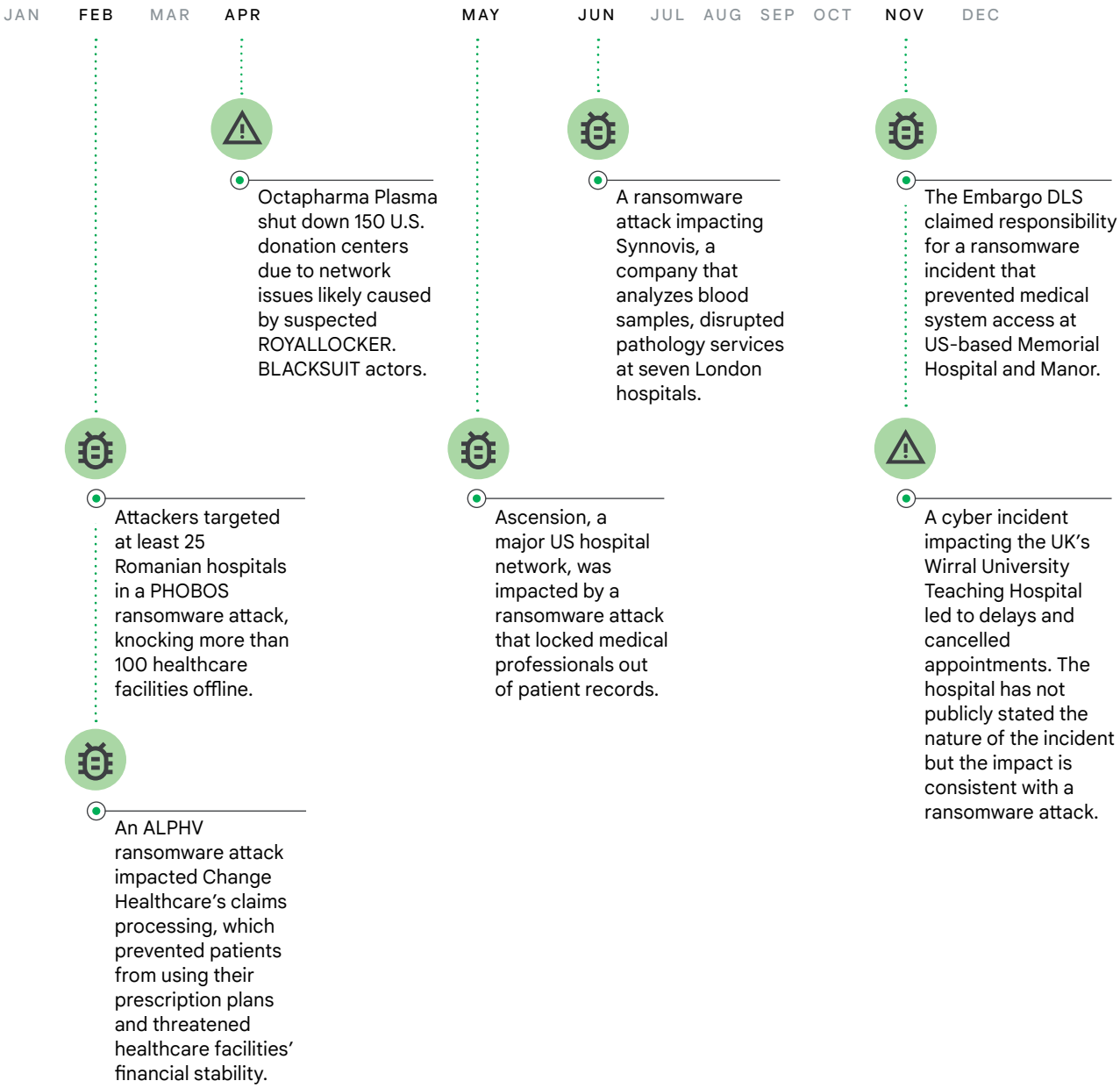
Public reporting of UK National Health Service Data stated that a June 2024 ransomware incident at a contractor led to multiple cases of "long-term or permanent impact on physical, mental or social function or shortening of life-expectancy," with more numerous cases of less severe effects.

Ransomware operators are aware that their attacks on hospitals will have severe consequences and will likely increase government attention on them. Although some threat actors have devised strategies to mitigate the blowback from these operations, the potential monetary rewards associated with targeting hospitals continue to drive attacks on the healthcare sector.

The actor "Firewalker" who has recruited partners for REDBIKE (aka Akira) ransomware operations, indicated a willingness to accept access to government and medical targets, but in those cases a different ransomware called FOULFOG would be used.

Leaked private communications broadly referred to as the "ContiLeaks" reveal that the actors expected their plan to target the US healthcare system in the fall of 2020 to cause alarm, with one actor stating "there will be panic."

2024 CYBERCRIME INCIDENTS IMPACTING HOSPITALS AND ASSOCIATED SERVICES (EXAMPLES)



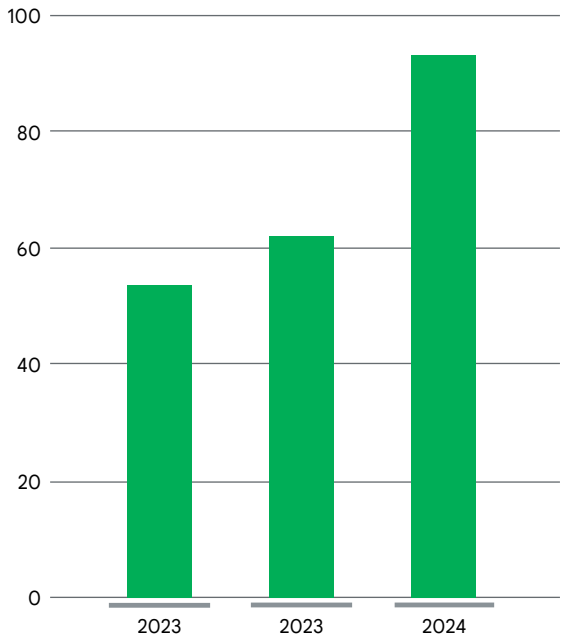
Economic disruption

On May 8, 2022, Costa Rican President Rodrigo Chaves declared a national emergency caused by CONTI ransomware attacks against several Costa Rican government agencies the month prior. These intrusions caused widespread disruptions in government medical, tax, pension, and customs systems. With imports and exports halted, ports were overwhelmed and the country reportedly experienced millions of dollars of losses. The remediation costs extended beyond Costa Rica: Spain supported the immediate response efforts and in 2023, the US announced $25 million USD in cybersecurity aid to Costa Rica.

While the Costa Rica incident was exceptional, responding to a cybercrime incident can involve significant expenses for the affected entity, such as paying multi-million dollar ransom demands, loss of income due to system downtime, providing credit monitoring services to impacted clients, and paying remediation costs and fines. In just one example, a U.S. healthcare organization reported $872 million USD in "unfavorable cyberattack effects" after a disruptive incident. In the most extreme cases, these costs can contribute to organizations ceasing operations or declaring bankruptcy.

In addition to the direct impacts to individual organizations, financial impacts often extend to taxpayers and can have significant impacts on the national economy due to follow-on effects of the disruptions. The US Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) has indicated that between October 2013 and December 2023, business email compromise (BEC) operations alone led to $55 billion USD in losses. The cumulative effect of these cybercrime incidents can have an impact on a country's economic competitiveness. This can be particularly severe for smaller or developing countries, especially those with a less diverse economy.

DATA LEAK SITES TRACKED BY GOOGLE THREAT INTELLIGENCE GROUP



Data leak sites add additional threats

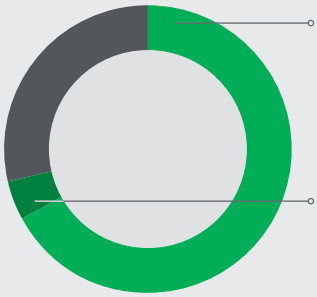
In addition to deploying ransomware to interfere with business operations, criminal groups have added the threat of leaking data stolen from victims to bolster their extortion operations. This now standard tactic has increased the volume of sensitive data being posted by criminals and created an opportunity for it to be obtained and exploited by state intelligence agencies.

Threat actors post proprietary company data—including research and product designs—on data leak sites where they are accessible to the victims' competitors. GTIG has previously observed threat actors sharing tips for targeting valuable data for extortion operations. In our research, GTIG identified Conti "case instructions" indicating that actors should prioritize certain types of data to use as leverage in negotiations, including files containing confidential information, document scans, HR documents, company projects, and information protected by the General Data Protection Regulation (GDPR).

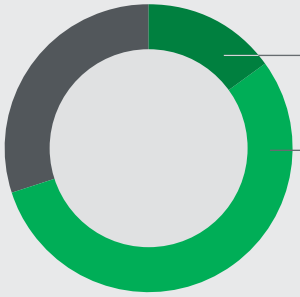
Data leak sites has proliferated, with the number of sites tracked by GTIG almost doubling since 2022. Leaks of confidential business and personal information by extortion groups can cause embarrassment and legal consequences for the affected organization, but they also pose national security threats. If a company's confidential intellectual property is leaked, it can undermine the firm's competitive position in the market and undermine the host country's economic competitiveness. The wide-scale leaking of personally identifiable information (PII) also creates an opportunity for foreign governments to collect this information to facilitate surveillance and tracking of a country's citizens.

The toll of combating cybercrime

The large volume and constant pressure of cybercrime activity means it dominates defender attention. This steady drumbeat taxes resources, and can crowd out investigations into state-backed activity. For example:



In 2024 **67%** of the intrusions that Mandiant Managed Defense identified and attributed to a threat group were attributed to financially-motivated groups, compared to just **4.5%** attributed to espionage-motivated groups.



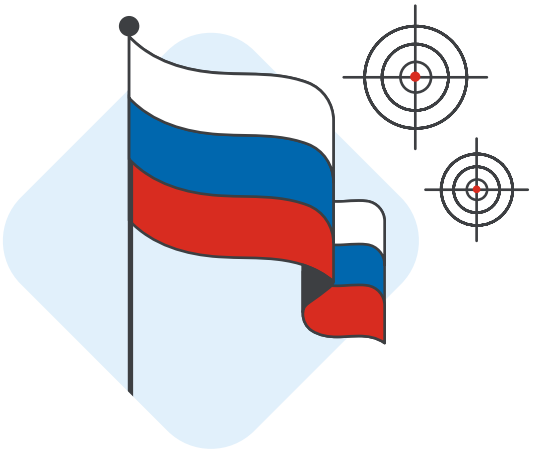
Among the intrusions identified by Mandiant Incident Response, **15%** were conducted by a group whose goal was espionage, while **55%** were conducted by financially-motivated groups.

The remainder of activity is attributed to a group whose motivations we do not have sufficient data to assess. However, we do not expect these groups to materially affect the distribution of motivations.

Section 2

Cybercrime directly supporting state activity

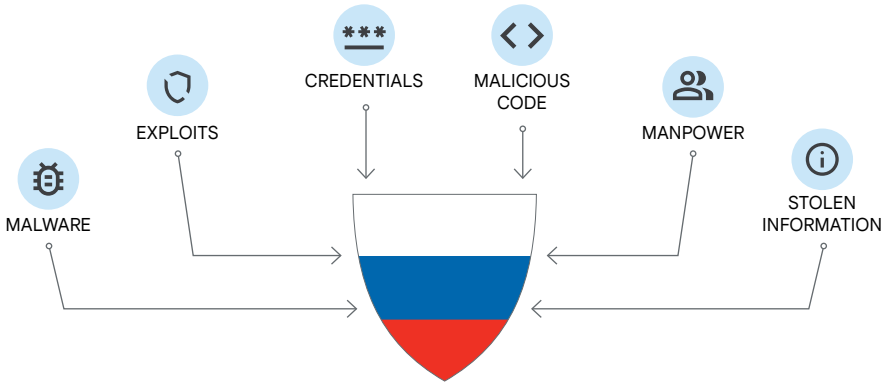
Since the earliest computer network intrusions, financially-motivated actors have conducted operations for the benefit of hostile governments. While this pattern has been consistent, the heightened level of cyber activity following Russia's war in Ukraine has shown that, in times of heightened need, thelatent talent pool of cybercriminals can be paid or coerced to support state goals. Operations carried out in support of the state, but by criminal actors, have numerous benefits fortheir sponsors, including a lower cost and increased deniability. As the volume of financially-motivated activity increases, the potential danger it presents does as well.



States as a customer in cybercrime ecosystems

Modern cybercriminals are likely to specialize in a particular area of cybercrime and partner with other entities with diverse specializations to conduct operations. The specialization of cybercrime capabilities presents an opportunity for state-backed groups to simply show up as another customer for a group that normally sells to other criminals. Purchasing malware, credentials, or other key resources from illicit forums can be cheaper for state-backed groups than developing them in-house, while also providing some ability to blend in to financially-motivated operations and attract less notice.

Russian state increasingly leveraging malware, tooling sourced from crime marketplaces



Google assesses that resource constraints and operational demands have contributed to Russian cyber espionage groups' increasing use of free or publicly available malware and tooling, including those commonly employed by criminal actors to conduct their operations. Following Russia's full-scale invasion of Ukraine, GTIG has observed groups suspected to be affiliated with Russian military intelligence services adopt this type of "low-equity" approach to managing their arsenal of malware, utilities, and infrastructure. The tools procured from financially-motivated actors are more widespread and lower cost than those developed by the government. This means that if an operation using this malware is discovered, the cost of developing a new tool will not be borne by the intelligence agency; additionally, the use of such tools may assist in complicating attribution efforts. Notably, multiple threat clusters with links to Russian military intelligence have leveraged disruptive malware adapted from existing ransomware variants to target Ukrainian entities.

APT44 (Sandworm, FROZENBARENTS)

APT44, a threat group sponsored by Russian military intelligence, almost certainly relies on a diverse set of Russian companies and criminal marketplaces to source and sustain its more frequently operated offensive capabilities. The group has used criminally sourced tools and infrastructure as a source of disposable capabilities that can be operationalized on short notice without immediate links to its past operations. Since Russia's full-scale invasion of Ukraine, APT44 has increased its use of such tooling, including malware such as DARKCRYSTALRAT (DCRAT), WARZONE, and RADTHIEF ("Rhadamanthys Stealer"), and bulletproof hosting infrastructure such as that provided by the Russian-speaking actor "yalishanda", who advertises in cyber criminal underground communities.

- APT44 campaigns in 2022 and 2023 deployed RADTHIEF against victims in Ukraine and Poland. In one campaign, spear-phishing emails targeted a Ukrainian drone manufacturer and leveraged SMOKELOADER, a publicly available downloader popularized in a Russian-language underground forum that is still frequently used in criminal operations, to load RADTHIEF.
- APT44 also has a history of deploying disruptive malware built upon known ransomware variants. In October 2022, a cluster we assessed with moderate confidence to be APT44 deployed PRESSTEA (aka Prestige) ransomware against logistics entities in Poland and Ukraine, a rare instance in which APT44 deployed disruptive capabilities against a NATO country. In June 2017, the group conducted an attack leveraging ETERNALPETYA (aka NotPetya), a wiper disguised as ransomware, timed to coincide with Ukraine's Constitution Day marking its independence from Russia. Nearly two years earlier, in late 2015, the group used a modified BLACKENERGY variant to disrupt the Ukrainian power grid. BLACKENERGY originally emerged as a distributed denial-of-service (DDoS) tool, with later versions sold in criminal marketplaces.

UNC2589 (FROZENVISTA)

UNC2589, a threat cluster whose activity has been publicly attributed to the Russian General Staff Main Intelligence Directorate (GRU)'s 161st Specialist Training Center (Unit 29155), has conducted full-spectrum cyber operations, including destructive attacks, against Ukraine. The actor is known to rely on non-military elements including cybercriminals and private-sector organizations to enable their operations, and GTIG has observed the use of a variety of malware-as-a-service tools that are prominently sold in Russian-speaking cybercrime communities.

In January 2022, a month prior to the invasion, UNC2589 deployed PAYWIPE (also known as WHISPERGATE) and SHADYLOOK wipers against Ukrainian government entities in what may have been a preliminary strike, using the GOOSECHASE downloader and FINETIDE dropper to drop and execute SHADYLOOK on the target machine. U.S. Department of Justice (DOJ) indictments identified a Russian civilian, who GTIG assesses was a likely criminal contractor, as managing the digital environments used to stage the payloads used in the attacks. Additionally, CERT-UA corroborated GTIG's findings of strong similarities between SHADYLOOK and WhiteBlackCrypt ransomware (also tracked as WARYLOOK). GOOSECHASE and FINETIDE are also publicly available for purchase on underground forums.

Turla (SUMMIT)

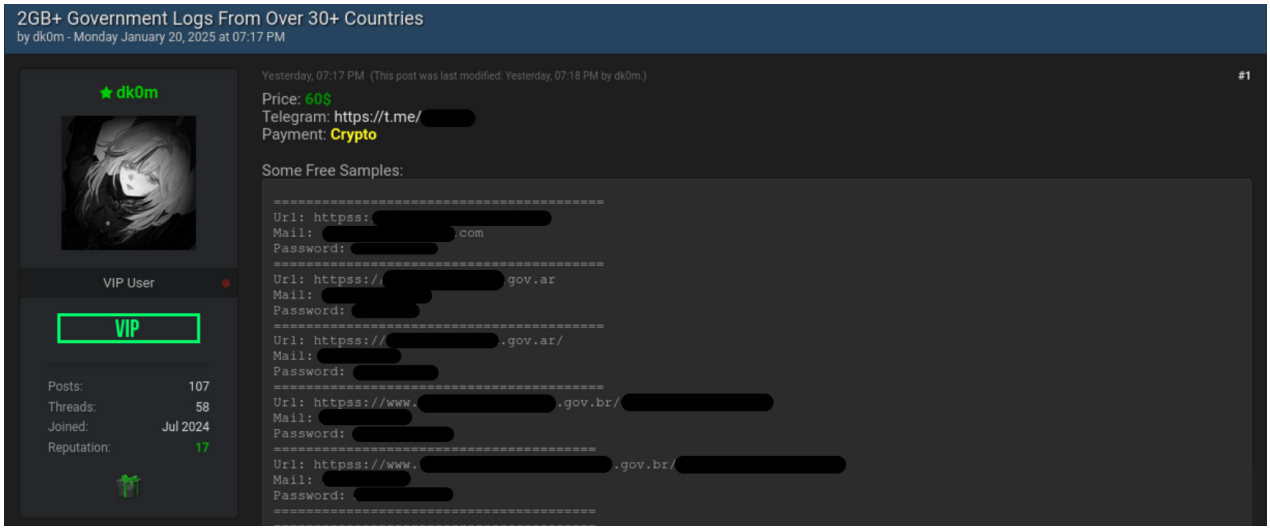
In September 2022, GTIG identified an operation leveraging a legacy ANDROMEDA infection to gain initial access to selective targets conducted by Turla, a cyber espionage group we assess to be sponsored by Russia's Federal Security Service (FSB). Turla re-registered expired command-and-control (C&C or C2) domains previously used by ANDROMEDA, a common commodity malware that was widespread in the early 2010s, to profile victims; it then selectively deployed KOPILUWAK and QUIETCANARY to targets in Ukraine. The ANDROMEDA backdoor whose C2 was hijacked by Turla was first uploaded to VirusTotal in 2013 and spreads from infected USB keys.

While GTIG has continued to observe ANDROMEDA infections across a wide variety of victims, GTIG has only observed suspected Turla payloads delivered in Ukraine. However, Turla's tactic of piggybacking on widely distributed, financially-motivated malware to enable follow-on compromises is one that can be used against a wide range of organizations. Additionally, the use of older malware and infrastructure may cause such a threat to be overlooked by defenders triaging a wide variety of alerts.

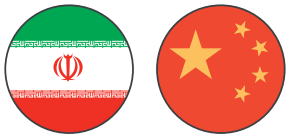
In December 2024, Microsoft reported on the use of Amadey bot malware related to cyber criminal activity to target Ukrainian military entities by Secret Blizzard, an actor that aligns approximately with what we track as Turla. While we are unable to confirm this activity, Microsoft's findings suggest that Turla has continued to leverage the tactic of using cybercrime malware.

APT29 (ICECAP)

In late 2021, GTIG reported on a campaign conducted by APT29, a threat group assessed to be sponsored by the Russian Foreign Intelligence Service (SVR), in which operators used credentials likely procured from an infostealer malware campaign conducted by a third-party actor to gain initial access to European entities. Infostealers are a broad classification of malware that have the capability or primary goal of collecting and stealing a range of sensitive user information such as credentials, browser data and cookies, email data, and cryptocurrency wallets An analysis of workstations belonging to the target revealed that some systems had been infected with the CRYPTBOT infostealer shortly before a stolen session token used to gain access to the targets' Microsoft 365 environment was generated.



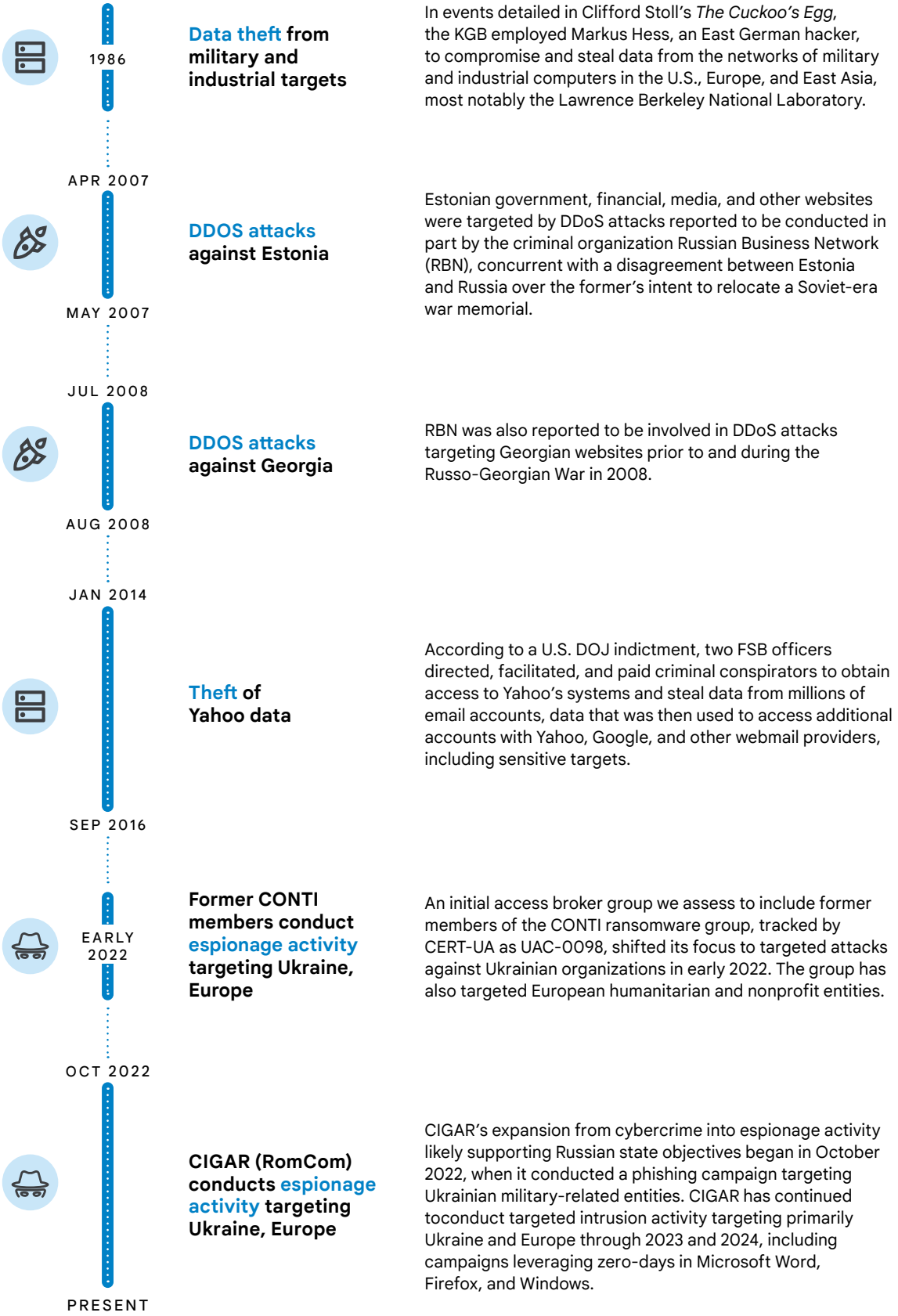
An example of the sale of government credentials on an underground forum



Use of cybercrime tools by Iran and China

While Russia is the country that has most frequently been identified drawing on resources from criminal forums, it is not alone. For instance, in May 2024, GTIG identified a suspected Iranian group, UNC5203, using the aforementioned RADTHIEF backdoor in an operation using themes associated with the Israeli nuclear research industry.

In multiple investigations, the Chinese espionage operator UNC2286 was observed ostensibly carrying out extortion operations, including using STEAMTRAIN ransomware, possibly to mask its activities. The ransomware dropped a JPG file named “Read Me.jpg” that largely copies the ransomware note delivered with DARKSIDE. However, no links have been established with the DARKSIDE ransomware-as-a-service (RaaS), suggesting the similarities are largely superficial and intended to lend credibility to the extortion attempt. Deliberately mixing ransomware activities with espionage intrusions supports the Chinese government’s public efforts to confound attribution by conflating cyber espionage activity and ransomware operations.


1986
Data theft from military and industrial targets
In events detailed in Clifford Stoll's *The Cuckoo's Egg*, the KGB employed Markus Hess, an East German hacker, to compromise and steal data from the networks of military and industrial computers in the U.S., Europe, and East Asia, most notably the Lawrence Berkeley National Laboratory.
APR 2007
MAY 2007
DDOS attacks against Estonia
Estonian government, financial, media, and other websites were targeted by DDoS attacks reported to be conducted in part by the criminal organization Russian Business Network (RBN), concurrent with a disagreement between Estonia and Russia over the former's intent to relocate a Soviet-era war memorial.
JUL 2008
AUG 2008
DDOS attacks against Georgia
RBN was also reported to be involved in DDoS attacks targeting Georgian websites prior to and during the Russo-Georgian War in 2008.
JAN 2014
SEP 2016
Theft of Yahoo data
According to a U.S. DOJ indictment, two FSB officers directed, facilitated, and paid criminal conspirators to obtain access to Yahoo's systems and steal data from millions of email accounts, data that was then used to access additional accounts with Yahoo, Google, and other webmail providers, including sensitive targets.
EARLY 2022
Former CONTI members conduct espionage activity targeting Ukraine, Europe
An initial access broker group we assess to include former members of the CONTI ransomware group, tracked by CERT-UA as UAC-0098, shifted its focus to targeted attacks against Ukrainian organizations in early 2022. The group has also targeted European humanitarian and nonprofit entities.
OCT 2022
PRESENT
CIGAR (RomCom) conducts espionage activity targeting Ukraine, Europe
CIGAR's expansion from cybercrime into espionage activity likely supporting Russian state objectives began in October 2022, when it conducted a phishing campaign targeting Ukrainian military-related entities. CIGAR has continued toconduct targeted intrusion activity targeting primarily Ukraine and Europe through 2023 and 2024, including campaigns leveraging zero-days in Microsoft Word, Firefox, and Windows.

Criminals supporting state goals

In addition to purchasing tools for state-backed intrusion groups to use, countries can directly hire or co-opt financially-motivated attackers to conduct espionage and attack missions on behalf of the state. Russia, in particular, has leveraged cybercriminals for state operations.

Current and former Russian cybercriminal actors engage in targeted activity supporting state objectives

Russian intelligence services have increasingly leveraged pre-existing or new relationships with cybercriminal groups to advance national objectives and augment intelligence collection. They have done so in particular since the beginning of Russia's full-scale invasion of Ukraine. GTIG judges that this is a combination of new efforts by the Russian state and the continuation of ongoing efforts for other financially-motivated, Russia-based threat actors that had relationships with the Russian intelligence services that predated the invasion. In at least some cases, current and former members of Russian Cybercriminal groups have carried out intrusion activity likely in support of state objectives.

CIGAR (UNC4895, RomCom)

CIGAR (also tracked as UNC4895 and publicly reported as RomCom) is a dual financial and espionage-motivated threat group. Active since at least 2019, the group historically conducted financially-motivated operations before expanding into espionage activity that GTIG judges fulfills espionage requirements in support of Russian national interests following the start of Russia's full-scale invasion of Ukraine. CIGAR's ongoing engagement in both types of activity differentiates the group from threat actors like APT44 or UNC2589, which leverage cybercrime actors and tooling toward state objectives. While the precise nature of the relationship between CIGAR and the Russian state is unclear, the group's high operational tempo, constant evolution of its malware arsenal and delivery methods, and its access to and exploitation of multiple zero-day vulnerabilities suggest a level of sophistication and resourcefulness unusual for a typical cybercrime actor.

Targeted intrusion activity from CIGAR dates back to late 2022, targeting Ukrainian military and government entities. In October 2022, CERT-UA reported on a phishing campaign that distributed emails allegedly on behalf of the Press Service of the General Staff of the Armed Forces of Ukraine which led to the deployment of the group's signature RomCom malware. Two months later, in December 2022, CERT-UA highlighted a RomCom operation targeting users of DELTA, a situational awareness and battlefield management system used by the Ukrainian military.

CIGAR activity in 2023 and 2024 included the leveraging of zero-day vulnerabilities to conduct intrusion activity. In late June 2023, a phishing operation targeting European government and military entities used lures related to the Ukrainian World Congress, a nonprofit involved in advocacy for Ukrainian interests, and a then-upcoming NATO summit, to deploy the MAGICSPELL downloader, which exploited CVE-2023-36884 as a zero-day in Microsoft Word. In 2024, the group was reported to exploit the Firefox vulnerability CVE-2024-9680, chained together with the Windows vulnerability CVE-2024-49039, to deploy RomCom.

CONTI

At the outset of Russia's full-scale invasion of Ukraine, the CONTI ransomware group publicly announced its support for the Russian government, and subsequent leaks of server logs allegedly containing chat messages from members of the group revealed that at least some individuals were interested in conducting targeted attacks, and may have been taking targeting directions from a third party. GTIG further assessed that former CONTI members comprise part of an initial access broker group conducting targeted attacks against Ukraine tracked by CERT-UA as UAC-0098.

UAC-0098 historically delivered the IcedID banking trojan, leading to human-operated ransomware attacks, and GTIG assesses that the group previously acted as an initial access broker for various ransomware groups including CONTI and Quantum. In early 2022, however, the actor shifted its focus to Ukrainian entities in the government and hospitality sectors, as well as European humanitarian and nonprofit organizations.

Chinese-language operator supports espionage goals

UNC5174 ("Uteus")

UNC5174 uses the "Uteus" hacktivist persona who has claimed to be affiliated with China's Ministry of State Security, working as an access broker and possible contractor who conducts for-profit intrusions. UNC5174 has weaponized multiple vulnerabilities soon after they were publicly announced, attempting to compromise numerous devices before they could be patched. For example, in February 2024, UNC5174 was observed exploiting CVE-2024-1709 in ConnectWise ScreenConnect to compromise hundreds of institutions primarily in the U.S. and Canada, and in April 2024, GTIG confirmed UNC5174 had weaponized CVE-2024-3400 in an attempt to exploit Palo Alto Network's GlobalProtect appliances. In both cases, multiple China-nexus clusters were identified leveraging the exploits, underscoring how UNC5174 may enable additional operators.

Hybrid groups enable cheap capabilities

Another form of financially-motivated activity supporting state goals are groups whose main mission may be state-sponsored espionage that are, either tacitly or explicitly, allowed to conduct financially-motivated operations to supplement their income. This can allow a government to offset direct costs that would be required to maintain groups with robust capabilities.

Moonlighting among Chinese contractors

APT41

APT41 is a prolific cyber operator working out of the People's Republic of China and most likely a contractor for the Ministry of State Security. In addition to state-sponsored espionage campaigns against a wide array of industries, APT41 has a long history of conducting financially-motivated operations. The group's cybercrime activity has mostly focused on the video game sector, including ransomware deployment. APT41 has also enabled other Chinese espionage groups, for example by stealing digital certificates that are then used by other Chinese groups. APT41's cybercrime has continued since GTIG's 2019 report, with the United States Secret Service attributing an operation that stole millions in COVID relief funds to APT41, and GTIG identifying an operation targeting state and local governments.

Iranian groups deploy ransomware for disruption and profit

Over the past several years, GTIG has observed Iranian espionage groups conducting ransomware operations and disruptive hack-and-leak operations. Although much of this activity is likely primarily driven by disruptive intent, some actors working on behalf of the Iranian government may also be seeking ways to monetize stolen data for personal gain, and Iran's declining economic climate may serve as an impetus for this activity.

UNC757

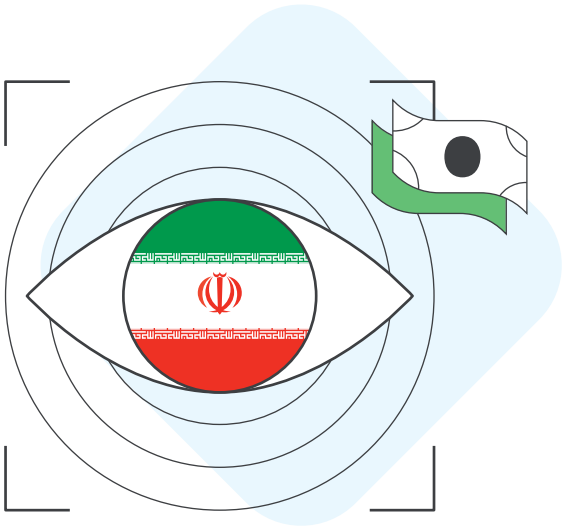
In August 2024, the U.S. Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Department of Defense Cyber Crime Center (DC3) released a joint advisory indicating that a group of Iran-based cyber actors known as UNC757 collaborated with ransomware affiliates including NoEscape, Ransomhouse, and ALPHV to gain network access to organizations across various sectors and then help the affiliates deploy ransomware for a percentage of the profits. The advisory further indicated that the group stole data from targeted networks likely in support of the Iranian government, and their operations were likely not sanctioned by the Government of Iran.

GTIG is unable to independently corroborate UNC757's reported collaboration with ransomware affiliates. However, the group has historical, suspected ties to the persona "nanash" that posted an advertisement in mid-2020 on a cybercrime forum claiming to have access to various networks, as well as hack-and-leak operations associated with the PAY2KEY ransomware and corresponding persona that targeted Israeli firms.

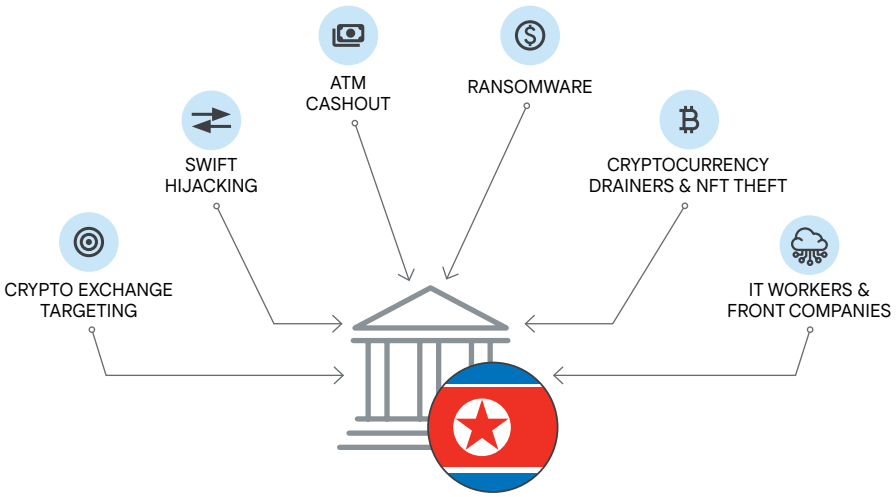
Examples of dual motive (financial gain and espionage)

In multiple incidents, individuals who have conducted cyber intrusions on behalf of the Iranian government have also been identified conducting financially-motivated intrusions.

- A 2020 U.S. DOJ indictment indicated that two Iranian nationals conducted cyber intrusion operations targeting data "pertaining to national security, foreign policy intelligence, non-military nuclear information, aerospace data, human rights activist information, victim financial information and personally identifiable information, and intellectual property, including unpublished scientific research." The intrusions in some cases were conducted at the behest of the Iranian government, while in other instances, the defendants sold hacked data for financial gain.
- In 2017, the U.S. DOJ indicted an Iranian national who attempted to extort HBO by threatening to release stolen content. The individual had previously worked on behalf of the Iranian military to conduct cyber operations targeting military and nuclear software systems and Israeli infrastructure.



DPRK cyber threat actors conduct financially-motivated operations to generate revenue for regime, fund espionage campaigns



Financially-motivated operations are broadly prevalent among threat actors linked to the Democratic People's Republic of Korea (DPRK). These include groups focused on generating revenue for the regime as well as those that use the illicit funds to support their intelligence-gathering efforts. Cybercrime focuses on the cryptocurrency sector and blockchain-related platforms, leveraging tactics including but not limited to the creation and deployment of malicious applications posing as cryptocurrency trading platforms and the airdropping of malicious non-fungible tokens (NFTs) that redirect the user to wallet-stealing phishing websites. A March 2024 United Nations (UN) report estimated North Korean cryptocurrency theft between 2017 and 2023 at approximately $3 billion USD.

APT38

APT38, a financially-motivated group aligned with the Reconnaissance General Bureau (RGB), was responsible for the attempted theft of vast sums of money from institutions worldwide, including via compromises targeting SWIFT systems. Public reporting has associated the group with the use of money mules and casinos to withdraw and launder funds from fraudulent ATM and SWIFT transactions. In publicly reported heists alone, APT38's attempted thefts from financial institutions totaled over $1.1 billion USD, and by conservative estimates, successful operations have amounted to over $100 million USD. The group has also deployed destructive malware against target networks to render them inoperable following theft operations. While APT38 now appears to be defunct, we have observed evidence of its operators regrouping into other clusters, including those heavily targeting cryptocurrency and blockchain-related entities and other financials.

UNC1069 (CryptoCore), UNC4899 (TraderTraitor)

Limited indicators suggest that threat clusters GTIG tracks as UNC1069 (publicly referred to as CryptoCore) and UNC4899 (also reported as TraderTraitor) are successors to the now-defunct APT38. These clusters focus on financial gain, primarily by targeting cryptocurrency and blockchain entities. In December 2024, a joint statement released by the FBI, DC3, and National Police Agency of Japan (NPA) reported on TraderTraitor's theft of cryptocurrency then valued at $308 million USD from a Japan-based company.

APT43 (Kimsuky)

APT43, a prolific cyber actor whose collection requirements align with the mission of the RGB, funds itself through cybercrime operations to support its primary mission of collecting strategic intelligence, in contrast to groups focused primarily on revenue generation like APT38. While the group's espionage targeting is broad, it has demonstrated a particular interest in foreign policy and nuclear security, leveraging moderately sophisticated technical capabilities coupled with aggressive social engineering tactics against government organizations, academia, and think tanks. Meanwhile, APT43's financially-motivated operations focus on stealing and laundering cryptocurrency to buy operational infrastructure.

UNC3782

UNC3782, a suspected North Korean threat actor active since at least 2022, conducts both financial crime operations against the cryptocurrency sector and espionage activity, including the targeting of South Korean organizations attempting to combat cryptocurrency-related crimes, such as law firms and related government and media entities. UNC3782 has targeted users on cryptocurrency platforms including Ethereum, Bitcoin, Arbitrum, Binance Smart Chain, Cronos, Polygon, TRON, and Solana; Solana in particular constitutes a target-rich environment for criminal actors due to the platform's rapid growth.

APT45 (Andariel)

APT45, a North Korean cyber operator active since at least 2009, has conducted espionage operations focusing on government, defense, nuclear, and healthcare and pharmaceutical entities. The group has also expanded its remit to financially-motivated operations, and we suspect that it engaged in the development of ransomware, distinguishing it from other DPRK-nexus actors.

DPRK IT Workers

DPRK IT workers pose as non-North Korean nationals seeking employment at a wide range of organizations globally to generate revenue for the North Korean regime, enabling it to evade sanctions and fund its weapons of mass destruction (WMD) and ballistic missiles programs. IT workers have also increasingly leveraged their privileged access at employer organizations to engage in or enable malicious intrusion activity and, in some cases, extort those organizations with threats of data leaks or sales of proprietary company information following the termination of their employment.

While DPRK IT worker operations are widely reported to target U.S. companies, they have increasingly expanded to Europe and other parts of the world. Tactics to evade detection include the use of front companies and services of "facilitators," non-North Korean individuals who provide services such as money and/or cryptocurrency laundering, assistance during the hiring process, and receiving and hosting company laptops to enable the workers remote access in exchange for a percentage of the workers' incomes.

Section 3

A comprehensive approach is required

We believe tackling this challenge will require a new and stronger approach that recognizes the cybercriminal threat as a national security priority requiring international cooperation. While some welcome enhancements have been made, more must—and can—be done. The structure of the cybercrime ecosystem makes it particularly resilient to takedowns. Financially-motivated actors tend to specialize in a single facet of cybercrime and regularly work with others to accomplish bigger schemes. While some actors may repeatedly team up with particular partners, actors regularly have multiple suppliers (or customers) for a given service.

If a single ransomware-as-a-service provider is taken down, many others are already in place to fill in the gap that has been created. This resilient ecosystem means that while individual takedowns can disrupt particular operations and create temporary inconveniences for cybercriminals, these methods need to be paired with wide ranging efforts to improve defense and crack down on these criminals' ability to carry out their operations. We urge policymakers to consider taking a number of steps:

Demonstrably elevate cybercrime as a national security priority

Governments must recognize cybercrime as a pernicious national security threat and allocate resources accordingly. This includes prioritizing intelligence collection and analysis on cybercriminal organizations, enhancing law enforcement capacity to investigate and prosecute cybercrime, and fostering international cooperation to dismantle these transnational networks.

Strengthen cybersecurity defenses

Policymakers should promote the adoption of robust cybersecurity measures across all sectors, particularly critical infrastructure. This includes incentivizing the implementation of security best practices, investing in research and development of advanced security technologies, enabling digital modernization and uptake of new technologies that can advantage defenders, and supporting initiatives that enhance the resilience of digital systems against attacks and related deceptive practices.

Disrupt the cybercrime ecosystem

Targeted efforts are needed to disrupt the cybercrime ecosystem by targeting key enablers such as malware developers, bulletproof hosting providers, and financial intermediaries such as cryptocurrency exchanges. This requires a combination of legal, technical, and financial measures to dismantle the infrastructure that supports cybercriminal operations and coordinated international efforts to enable the same.

Enhance international cooperation

Cybercrime transcends national borders, necessitating strong international collaboration to effectively combat this threat. Policymakers should prioritize the development of international frameworks for information sharing, joint investigations, and coordinated takedowns of cybercriminal networks, including by actively contributing to the strengthening of international organizations and initiatives dedicated to combating cybercrime, such as the Global Anti-Scams Alliance (GASA).

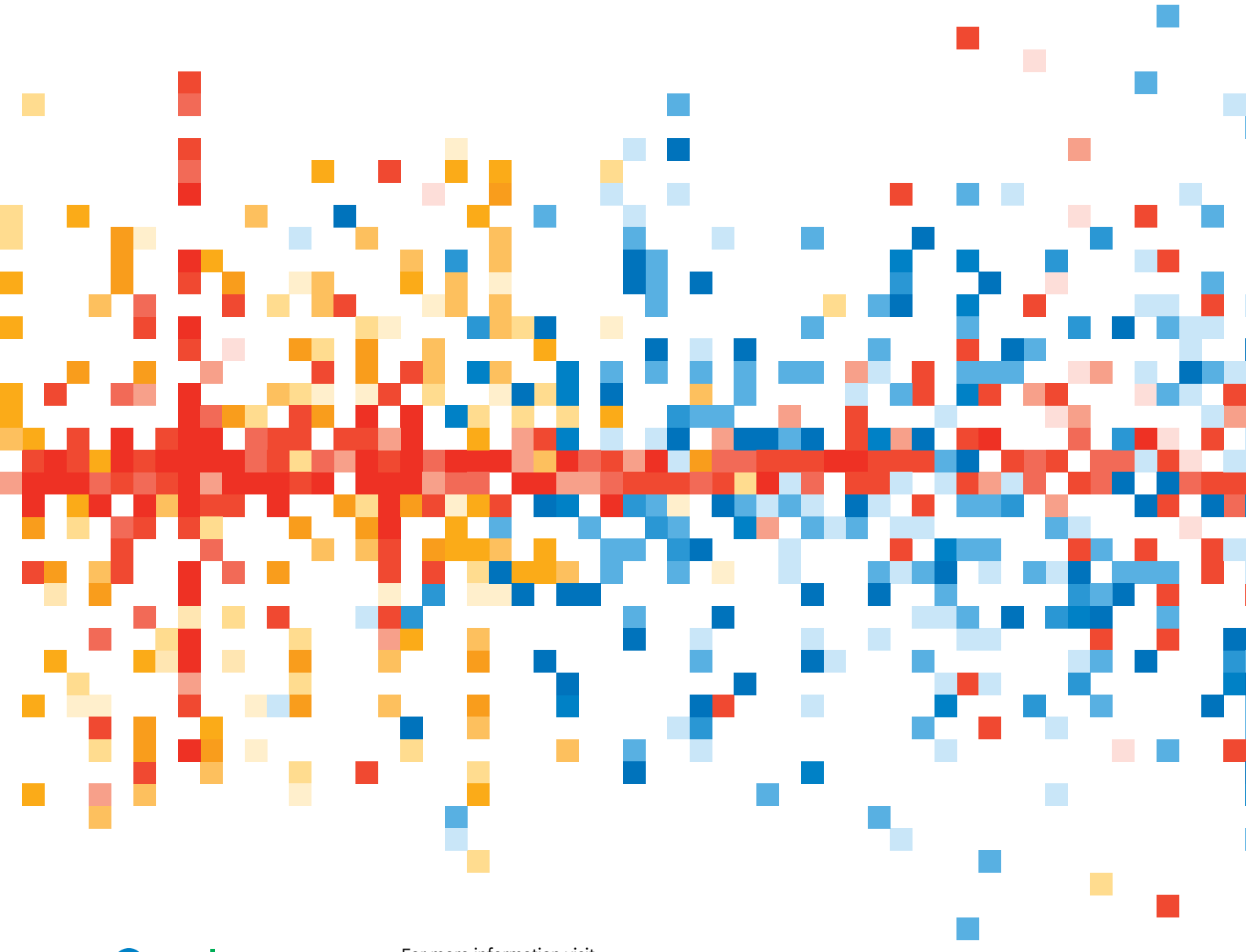
Empower individuals and businesses

Raising awareness about cyber threats and promoting cybersecurity education is crucial to building a resilient society. Policymakers should support initiatives that educate individuals and businesses about online safety, encourage the adoption of secure practices, empower service providers to take action against cybercriminals including through enabling legislation, and provide resources for reporting and recovering from cyberattacks.

Elevate strong private sector security practices

Ransomware and other forms of cybercrime predominantly exploit insecure, often legacy technology architectures. Policymakers should consider steps to prioritize technology transformation, including the adoption of technologies/products with a strong security track record; diversifying vendors to mitigate risk resulting from overreliance on a single technology; and requiring interoperability across the technology stack.

This report includes extensive research from dozens of sources and comes in print and online versions. The online version contains links to relevant sources.



Google

For more information visit
cloud.google.com