2023

CISCO TALOS

YEAR IN REVIEW

Introduction

Ransomware, commodity loaders and APTs dominated the threat landscape in 2023. As we'll outline in the second annual Cisco Talos Year in Review, global conflict influenced cybersecurity trends, shifting many threat actors' tactics and approaches in operations ranging from espionage to cybercrime.

Cisco's global presence and Talos' world-class expertise provided a massive amount of data to sift through — endpoint detections, incident response engagements, network traffic, email corpus, sandboxes, honeypots and much more. Thankfully, our teammates include subject matter experts from all ends of the cybersecurity space to help us turn this intelligence into actionable information for defenders and users. Leveraging these rich, complex sources of information, we analyzed the major trends that shaped the threat landscape in 2023.

Ransomware continued to threaten enterprises globally in 2023, with LockBit remaining the top threat in this space for the second year in a row. Health care was the top targeted industry this year, as adversaries maintained their focus on entities that have cybersecurity funding constraints and low downtime tolerance. Not all things were the same, though, as we saw actors such as Clop deploy a collection of zero-day exploits, behavior we usually associate with advanced persistent threat (APT) activity. At the same time, leaked ransomware source code allowed low-skilled actors to enter the fray. Further complicating matters, we observed a new trend of ransomware actors turning to pure extortion, skipping encryption altogether while threatening to leak sensitive data.

Commodity loaders are still being used to deliver these ransomware threats, and many of the same families as last year remained prevalent, such as Qakbot and IcedID. This is reflected in our telemetry, as the most commonly spoofed brands were in financial services and shipping, hallmarks of these adversaries. But these loaders are shedding all remnants of their banking trojan past as they position themselves more as sleek payload delivery mechanisms. Developers and operators are adapting to improved defenses, finding new ways to bypass increasing security updates and compromise victims. And although we again observed a takedown of a large botnet, this year being Qakbot, our experience shows that this does not necessarily mean that the threat has been eliminated.

One of the newer cross-regional trends we have observed this year is an increase in the targeting of network devices from APTs and ransomware actors. Both groups rely on exploiting recently disclosed vulnerabilities and weak/default credentials, one of the reasons why the use of valid accounts was consistently a top weakness in Talos IR engagements. Whatever the sophistication and intent of the adversary is, the reason behind the targeting is the same: network devices are extremely high value while possessing many security weaknesses.

Geopolitical instability is manifesting in APT activity. This is reflected in our telemetry, which shows a rise in suspicious traffic during major geopolitical events. For Chinese groups, as relationships with the West and Asia Pacific become further strained, we see an emboldening in operations, such as a greater willingness to cause destruction. We also observe this in their targeting of telecommunications organizations, which possess numerous critical infrastructure assets in strategically important geographies such as Guam and Taiwan. For Russian APTs, Gamaredon and Turla targeted Ukraine at an accelerated pace, but Russian activity in general for 2023 did not reflect the full range of destructive cyber capabilities we have seen it deploy in the past, potentially because of the concerted efforts of defenders.

One bright spot this year was Cisco's determined efforts to create and deliver inventive security solutions that help strengthen our partners. Talos' Ukraine Task Force continues to thwart attacks against critical Ukrainian partners. This year, we spear-headed an effort to stabilize Ukraine's power grid against the effects of global positioning system (GPS) jamming on the battlefield by delivering modified Cisco switches into an active war zone. Cisco also launched the Network Resilience Coalition with leading industry partners, focusing on increasing awareness and providing actionable recommendations for improving network security. Relatedly, Talos's Vulnerability Discovery and Research Team made investigating small office, home office (SOHO) and industrial routers a major priority, reporting 289 vulnerabilities to vendors to date, published across 141 Talos advisories.

As conflict in the Middle East worsens, we are once again positioned to help protect our customers and partners. Therefore, perhaps the overarching story of 2023 is this: as the daringness, sophistication, and persistence of our adversaries grows, so too does the resolve of defenders to interdict them in any way we can.

Table of contents

CISCO TALOS

YEAR IN REVIEW

2023

Telemetry trends

Section highlights

- Suspicious network traffic captured by Cisco Security products revealed sharp increases in activity that often corresponded with major geopolitical events and global cyber attacks.
- The most targeted vulnerabilities were older security flaws in common applications, consistent with the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) findings in recent years. Most of the top-targeted vulnerabilities we observed received maximum- or high-severity scores by Cisco Kenna and the Common Vulnerability Scoring System (CVSS) and were also included in CISA's Known Exploited Vulnerabilities catalog. The high frequency of targeting attempts against these CVEs, paired with their significant impact, underscores adversaries' preference to target unpatched systems that can cause major disruptions.
- Threat actors abused common file extensions and spoofed well-known brands, common techniques that underscore the use of social engineering to enable operations like phishing and business email compromise (BEC). Adversaries are likely responding to Microsoft's disabling of macros in 2022 by using different file types to hide their malware, such as PDFs, which was the top blocked file extension this year.
- Financial services and shipping companies accounted for the brands we observed being spoofed most often in email telemetry, suggesting longstanding phishing themes for email-based commodity loaders like Emotet, Qakbot and Trickbot are still at play. Relatedly, phishing accounted for a quarter of known initial access vectors in Talos IR engagements this year, highlighting actors' continued reliance on this technique.
- The use of valid accounts was a top-observed MITRE ATT&CK technique, underscoring adversaries' reliance on compromised credentials and use of existing accounts for various stages of their attacks. This is consistent with Talos IR data, which showed compromised credentials/valid accounts accounted for nearly a third of known initial access vectors in 2023.

Regional trends over time

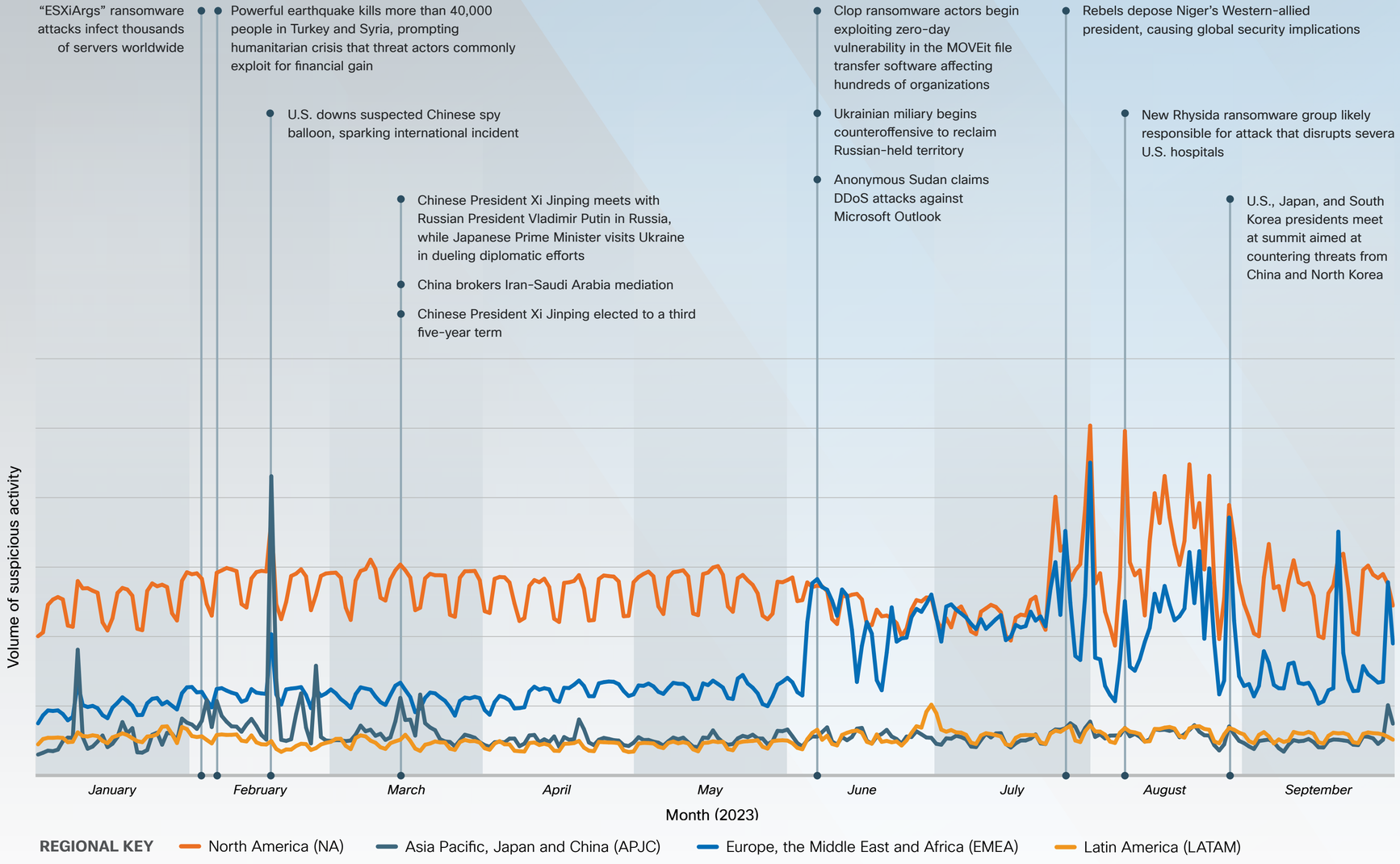
Suspicious traffic includes a wide variety of categorized information sourced from multiple Cisco Security products, including Umbrella, Secure Endpoint, Email Security Appliance (ESA), Meraki, SSE and Secure Firewall. Examples include malicious domains blocked by Umbrella, records with malicious dispositions from Secure Endpoint, phishing emails from ESA, triggered Snort signatures from Secure Firewall and Meraki, and many others.

In North America, Europe, the Middle East and Africa (EMEA), and Latin America, suspicious network traffic was periodic, following a Monday - Friday workday pattern for much of the year. Starting mid-year, we saw a break from this pattern marked by a dramatic increase in traffic blocked by our security products, often quadrupling the early part of the year's normal behavior.

In mid-February, these regions experienced various spikes in web spam. While spam volume was up globally, it disproportionally affected the Asia Pacific, Japan and China (APJC) region.

In APJC, suspicious traffic was less periodic and experienced large swings in volume between January and April. These changes leveled out through the spring and early summer.

Various international events and major cyber attacks overlayed on the graph suggest how such activity can affect the threat landscape. While it's impossible to prove causation, there are obvious correlations between the suspicious global and regional traffic patterns we observed and significant world events.



Top targeted vulnerabilities

In 2023, cyber threat actors exploited older software vulnerabilities in common applications. In many cases, the vulnerabilities were more than 10 years old, consistent with CISA's finding that adversaries have targeted old security flaws more than newly disclosed ones in recent years. In fact, four of the top five most-targeted vulnerabilities we observed were also cited by CISA as being frequently exploited in prior years, further highlighting this point. This underscores the need for entities to regularly install software updates, as many of these systems were likely unpatched given the age of the targeted vulnerabilities.

The top targeted vulnerabilities are found in common applications, like Microsoft Office. This finding is also substantiated by CISA, which noted that actors in 2022 prioritize CVEs that are more prevalent in their targets' networks. Adversaries likely prioritize targeting widespread vulnerabilities because the exploits developed for such CVEs can have long-term use and high impact.

Lastly, most of the vulnerabilities on our list would cause substantial impact if exploited, with six receiving a maximum vulnerability risk score of 100 from Cisco Kenna and seven receiving the highest "critical" score from the Common Vulnerability Scoring System (CVSS). Most of the CVEs are also listed in CISA's Known Exploited Vulnerabilities catalog, which is meant to inform users on the security flaws for which they should prioritize remediation. The high frequency of targeting attempts against these CVEs, paired with their severity, underscores the risk to unpatched systems.

Ranking	CVE	Vendor	Product	CISA findings	CISA KEV catalog	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office and WordPad	Routinely exploited in 2022	✓	100/9.3
2	CVE-2017-11882	Microsoft	Exchange server	Routinely exploited in 2022	✓	100/9.3+
3	CVE-2020-1472	Microsoft	Netlogon	Routinely exploited in 2022	✓	100/9.3
4	CVE-2012-1461	Gzip file parser utility	Multiple antivirus products		✗	58/4.3
5	CVE-2012-0158	Microsoft	Office	Commonly exploited by state-sponsored actors from China, Iran, North Korea, and Russia (2016-2019)	✓	100/9.3
6	CVE-2010-1807	Apple	Safari		✗	84/9.3
7	CVE-2021-1675	Microsoft	Windows (print spooler)		✓	100/9.3
8	CVE-2015-1701	Microsoft	Windows (kernel-mode driver)		✓	72/7.2
9	CVE-2012-0507	Oracle	Java SE		✓	100/10
10	CVE-2015-2426	Microsoft	Windows (font driver)		✓	100/9.3

Source: Cisco Secure Endpoint

CISA sources: Top Routinely Exploited Vulnerabilities, 2022 and 2016-2019.

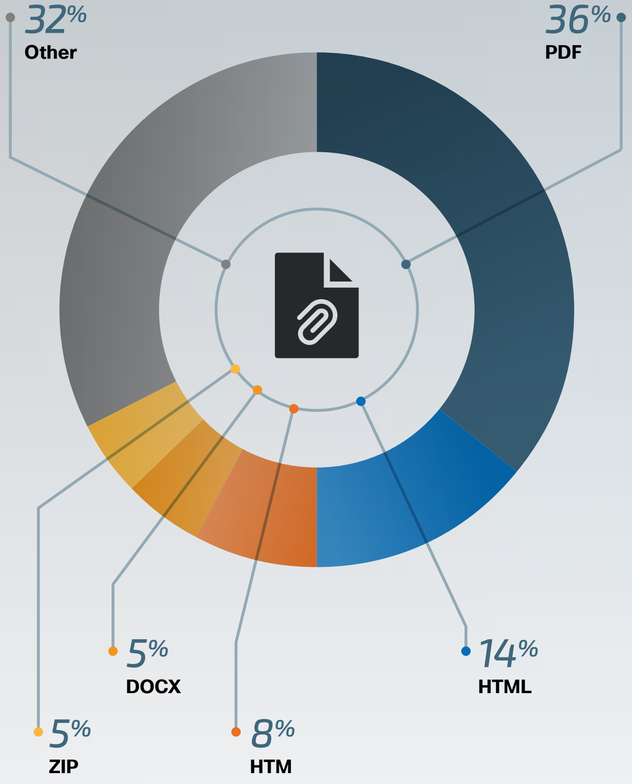
Email findings

TOP BLOCKED ATTACHMENT FILE EXTENSIONS

Phishing emails are one of the most common ways adversaries compromise victims and this has consistently been a top-ranked threat in Talos IR findings for years. In the last year alone, 25 percent of the initial access vectors identified in Talos IR engagements were comprised of phishing (this refers to chart 3b). This observation is consistent with U.S. government findings, with the FBI noting that phishing was the top incident reported to its Internet Crime Complaint Center (IC3) in 2022.

Threat actors commonly send unsolicited emails requesting users download or open an attachment to deliver malware. While file extension is not necessarily indicative of file type, actors frequently try to hide malware under well-known file extensions to appear less suspicious, so users are more likely to open them. For example, earlier this year, Japan's Computer Emergency Response Team (JP-CERT) warned that adversaries were embedding malicious Word documents in PDF files to bypass detection, a strategy we have seen threat actors rely on for years.

Threat actors' file type preference was also likely affected by Microsoft's 2022 decision to block macros, which adversaries had heavily abused up to that point. With this change, actors have moved away from using Microsoft Office files like Word and Excel as frequently as they once did. In 2023, we saw the commodity loader Ursnif incorporate malicious PDF attachments into their phishing operations for the first time as this actor and other groups looked for ways to avoid relying on macros.



Source: *Cisco Email Security Appliance*

Note: *Common image-related filetypes – like JPG, JPEG, PNG and GIF – were excluded from this list because they appear frequently in an overwhelmingly high volume of benign emails, such as those containing graphics in senders' signatures or in the email body.*

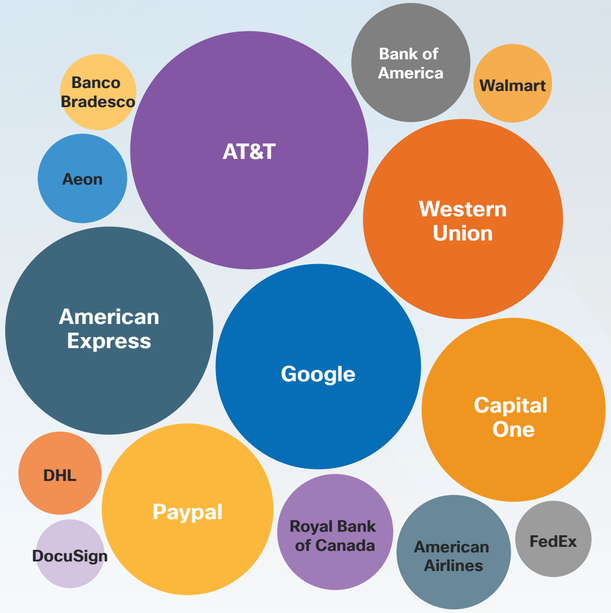
TOP INITIAL ACCESS VECTORS, ACCORDING TO TALOS IR

Note: *Initial access vector is often hard to determine due to a variety of reasons – including insufficient logging or lack of visibility into the affected environment – resulting in "unknown" being highly represented.*

TOP BRANDS SPOOFED IN SENDER NAMES

Cybercriminals and other malicious actors rely heavily on social engineering tactics to compromise users, which is why they commonly imitate well-known companies in their phishing emails. Commodity loaders like Emotet, Qakbot and Trickbot, for instance, routinely use fake invoices, bank statements, or shipping notifications as phishing themes to feign legitimacy. This is reflected in our list of top spoofed brands, where we see that financial services entities and shipping services were among those that actors most frequently spoofed.

Business email compromise (BEC) operations also leverage spoofed company names to enhance legitimacy. BEC is a scam in which cybercriminals send emails to targets that appear to come from a known source making a legitimate request. The goal is to prompt the target to make unauthorized money transfers to the threat actor. Actors may impersonate well-known and trusted brands, like those represented in our list, to trick users. BEC has been on the rise in recent years, according to the FBI, and resulting in $2.7 billion in losses in 2022.



Source: *Cisco Email Security Appliance*

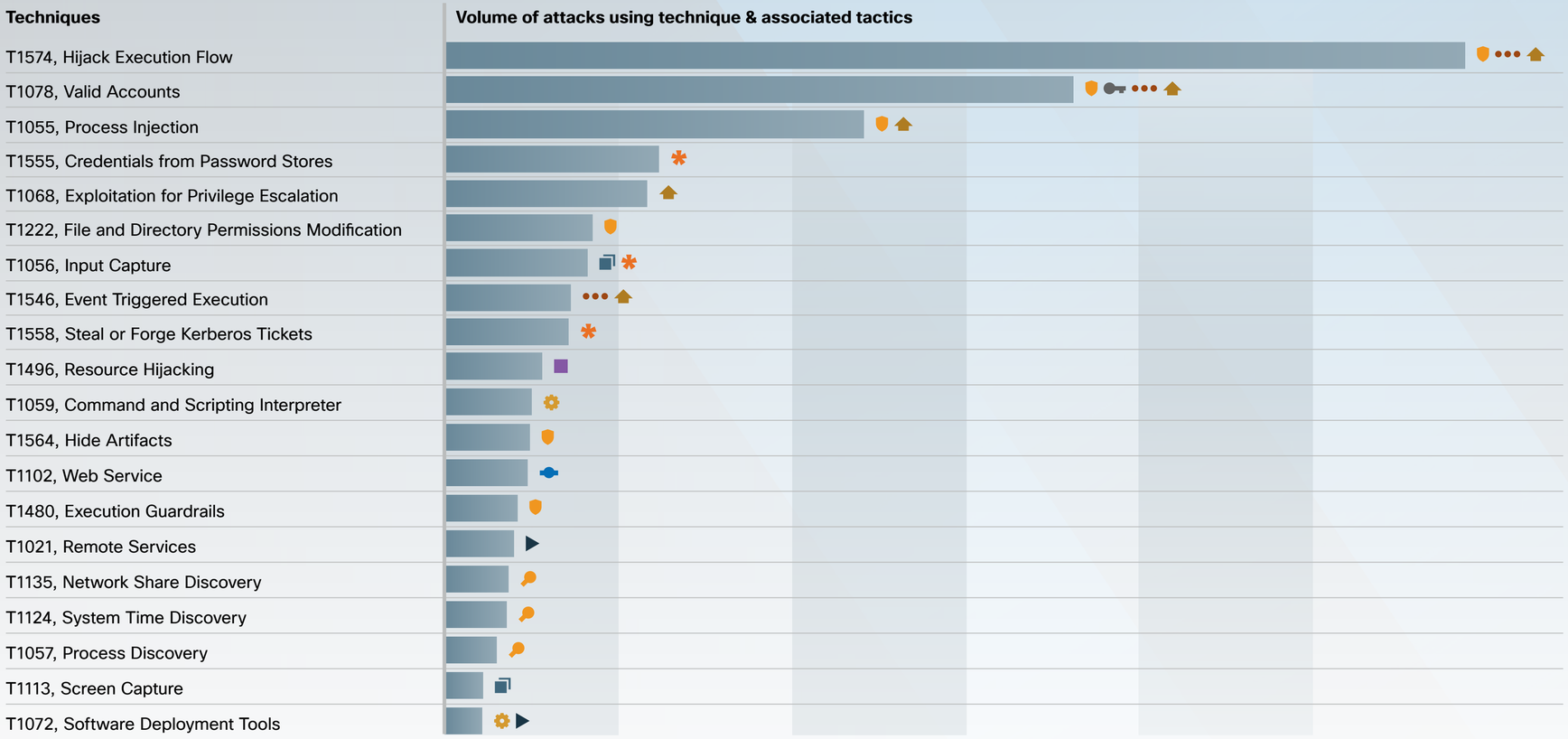
Top MITRE ATT&CK techniques

Notably, nearly a third of the top 20 most common MITRE ATT&CK techniques fall under the **defense evasion** tactic, suggesting actors are devoting substantial resources to this phase of the attack chain. Techniques relating to **privilege escalation** and **persistence** also ranked high, highlighting their importance in the attack lifecycle.

Hijack execution flow was the most common technique, appearing nearly twice as often as the next highest result. Hijacking execution flow refers to actors co-opting the way an operating system runs programs on a target endpoint. DLL side-loading is a common example of this, whereby actors essentially position their malware alongside the victim application so that when the program searches for its legitimate DLL, it also unwittingly executes the malicious payload. This is an effective way for actors to hide their activities under legitimate and trusted software, a technique we commonly see leveraged by APTs and cybercriminals.

The use of **valid accounts** was the second-most common technique we observed, underscoring adversaries' reliance on compromised credentials and use of existing accounts. Actors use this technique to enable various stages of the attack chain. We commonly see commodity loaders deploying information-stealing malware for this very purpose. Relatedly, **credentials from password stores** ranked in the top five, further highlighting actors' focus on obtaining user credentials. These findings are consistent with Talos IR data, which showed compromised credentials/valid accounts accounted for nearly a quarter of known initial access vectors in 2023.

Resource hijacking, which ranked in the top 10, is a technique we typically see associated with the deployment of cryptocurrency mining malware, which hijacks an endpoint's processing power for profitable gains. Cryptocurrency mining threats are highly common, as this is a low-level type of attack typically carried out by unsophisticated actors. We often see this type of malware deployed, especially soon after new vulnerabilities are disclosed, before victims have time to patch and/or in conjunction with other, more complex, malware.



CISCO TALOS

YEAR IN REVIEW

2023

Ransomware and extortion

Section highlights

- Ransomware and pre-ransomware incidents continue to affect customers at a consistent rate — totaling the same 20 percent of Talos IR incidents as last year — with health care being the most targeted vertical.
- For the second year in a row, LockBit was the most prolific ransomware-as-a-service (RaaS) gang, based on our findings, consistent with CISA's assessment that it is the most deployed ransomware variant. LockBit was one of the most frequently observed ransomware threats in Talos IR this year, and affiliates accounted for more than 25 percent of the total number of victim posts on data leak sites across some 40 ransomware groups we monitor.
- ALPHV, Clop and BianLian also dominated the threat landscape, accounting for another quarter of all ransomware and/or data extortion compromises publicized on dark web actor sites.
- We saw Clop affiliates consistently exploit zero-day vulnerabilities, a highly unusual tactic given the expertise, personnel and access required to develop such exploits, suggesting the group possesses a level of sophistication and/or resources matched only by advanced persistent threats (APTs).
- New ransomware variants are emerging that leverage leaked source code from other RaaS groups, allowing less skilled actors to enter this space. At the same time, we also see highly sophisticated operators like Clop leveraging zero-day vulnerabilities at an unprecedented pace, an interesting dichotomy demonstrating the breadth of actors in this space.
- Actors are turning to data extortion more than ever, with this being the top threat that Talos IR responded to in Q2 2023 (April - June). Data theft extortion looks very similar to pre-ransomware activity, creating challenges for defenders.
- Some actors are abandoning ransomware use altogether, opting for extortion instead, a trend likely influenced by ongoing law enforcement operations, better industry detections and lower operational costs.

Ransomware and extortion

The ransomware space remained dynamic in 2023, with groups continuing to rebrand or merge, actors often working for multiple ransomware-as-a-service (RaaS) outfits at a time, and new groups continually emerging. The skill levels varied greatly as well, with experienced actors developing sophisticated exploits for zero-day vulnerabilities, while less-skilled actors relied on repurposed ransomware code to create their own threats. We also saw an emerging trend in this space, as more actors began to abandon the use of ransomware and resort to pure data theft extortion without encrypting files, presenting a new line of challenges for defenders. Despite these changes, one thing remains constant: Ransomware remains a top threat to entities worldwide.

Ransomware attacks persist at steady pace

Ransomware and pre-ransomware made up 20 percent of the total incidents that Talos IR responded to this year, a very slight drop compared to last year. It can be difficult for defenders to determine what constitutes a pre-ransomware attack if a ransomware binary is never executed and encryption does not take place. However, there are some indications analysts use to assess if ransomware is the likely final objective, such as the use of adversary simulation frameworks like Cobalt Strike and/or credential-harvesting tools like Mimikatz, the targeting of certain critical assets such as backups, or enumeration and discovery techniques.

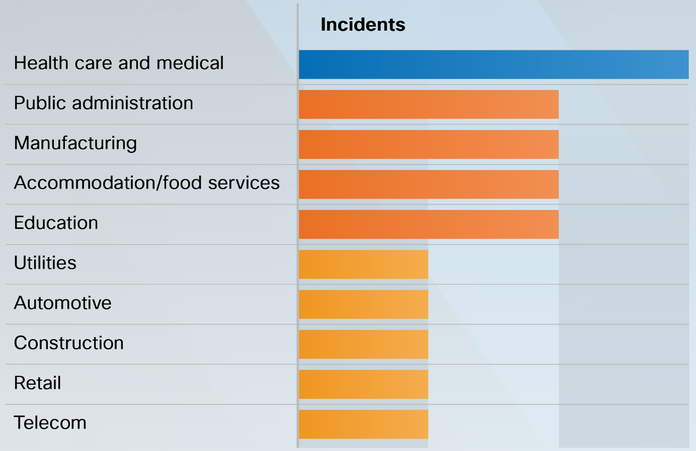
The health care and public health sector was the most targeted vertical in Talos IR ransomware and pre-ransomware engagements this year, compared to the education sector in 2022, as reported in last year's Year in Review report **(see Figure 1)**. Healthcare organizations are highly vulnerable to cyber attacks given their low downtime tolerance, often underfunded cybersecurity budgets, and possession of protected health information (PHI) that is valuable to threat actors. The COVID-19 pandemic likely exacerbated this situation in recent years, with healthcare providers strained from a resource perspective and downtime being even less tolerable.

Old foes are top offenders as LockBit remains top threat

For a second year in a row, LockBit was the most active RaaS group, accounting for over 25 percent of the total number of posts made to data leak sites. LockBit, ALPHV, Clop and BianLian accounted for nearly 50 percent of the total posts made to leak sites this year **(Figure 2)**.

FIGURE 1

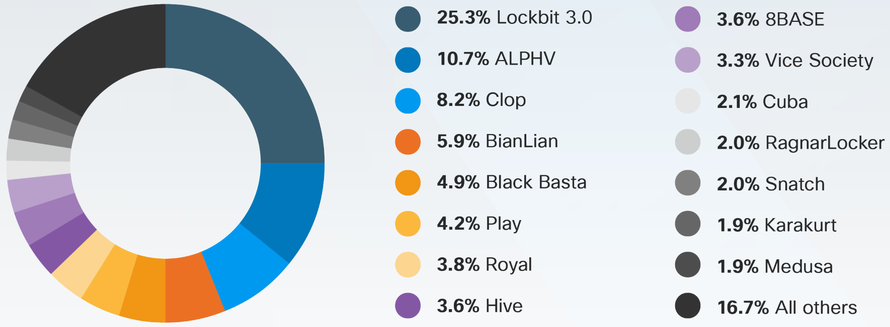
Talos IR ransomware and pre-ransomware incidents per sector



"The health care and public health sector was the most targeted vertical in Talos IR ransomware and pre-ransomware engagements this year, compared to the education sector in 2022."

FIGURE 2

Number of posts made to ransomware data leak sites



Talos IR responds to LockBit incident affecting IT and OT networks

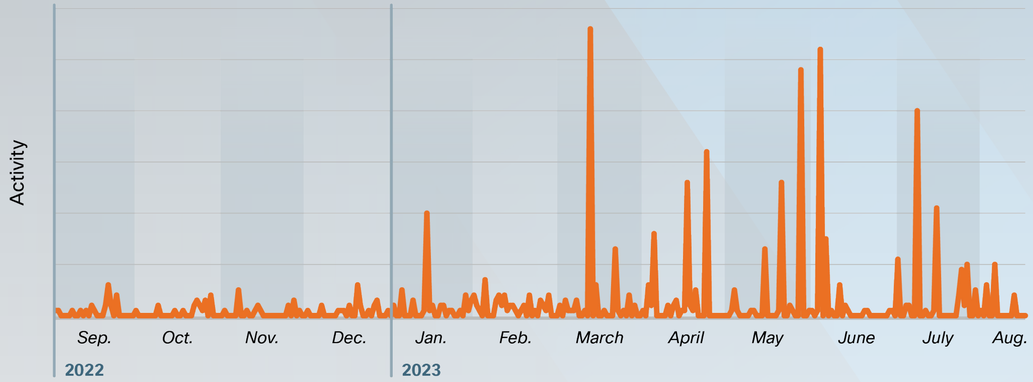
Talos IR responded to a LockBit ransomware incident affecting a utilities company where ransomware infiltrated the organization's IT and OT networks, causing significant impact to the victim and downstream disruptions to customers. The ransomware affiliate gained initial access using valid router credentials authenticating over VPN where multi-factor authentication (MFA) was not implemented. The attackers encrypted production servers, including those monitoring the electrical grid, and three of four domain controllers were encrypted, as well.

LockBit continued to conduct prolific ransomware operations in 2023, a finding that aligns with CISA's assessment that it is the most deployed ransomware variant. LockBit attacks can be very impactful, affecting an organization's information technology (IT) networks and operational technology (OT), the hardware and machines responsible for physical processes, as we have observed in Talos IR engagements. In October, CISA published guidance for securing OT environments, underscoring how significant the impact can be to these systems. LockBit was also deployed during the exploitation of two vulnerabilities in the PaperCut software, a print management solution widely used across entities in the government and education verticals, among others.

Posts made to the group's data leak site ebbed and flowed throughout the year, with detections of LockBit activity appearing to spike in March, partially coinciding with LockBit's deployment against vulnerable instances of the printer management software PaperCut, where it has remained consistently high **(Figure 3)**.

FIGURE 3

LockBit activity throughout the year



Ransomware space remains crowded with new and rebranded groups

Ransomware groups' constant rebranding and/or turnover was a prominent trend this year. Multiple leaks of ransomware source code and builders – components essential to creating and modifying ransomware – have had a significant effect on the ransomware threat landscape. These leaks allow ransomware operators to rebrand or give unsophisticated actors the ability to generate their own ransomware more easily with little effort or knowledge. As more actors enter this space, Talos is seeing an increasing number of ransomware variants emerge leveraging leaked ransomware code, often leading to more frequent attacks and new challenges for cybersecurity professionals and defenders, particularly regarding actor attribution.

The volume of new ransomware variants based on leaked source code also highlights the speed at which actors take advantage of such public disclosures. Most recently, we observed a surge in new ransomware strains emerging from the Yashma ransomware builder. First appearing in May 2022, Yashma is a rebranded version of the Chaos ransomware builder (v5), which was leaked in April 2022. Since early 2023, we have seen several new Yashma strains emerge, including ANXZ and Sirattacker, likely deployed by smaller or groups of affiliates with fewer resources given their lack of widespread adoption and notoriety in the landscape. In April, we discovered a new ransomware actor,

RA Group, deploying their ransomware variant based on the leaked Babuk source code. Since an alleged member of the Babuk group leaked the full source code of its ransomware in September 2021, several new variants based on the leaked code have emerged, with many appearing in 2023, including ESXiArgs, Rorschach and RTM Locker.

While these changes in the threat landscape have largely benefitted affiliates, security researchers and defenders also have an advantage with access to the leaked code. It allows security researchers to analyze the source code and understand the attacker's TTPs and develop effective detection rules, potentially aid in the creation of decryptors and enhance security products' capabilities in combating ransomware threats.

Affiliates turning to data theft extortion over ransomware deployment

Even with the expanding number of RaaS options, some have found success in extorting funds without deploying ransomware. In these extortion instances, an adversary steals the victim's data but does not encrypt it. The common double extortion tactic is thereby eliminated, with the actor relying solely on the threat of leaking the information rather than also demanding payment to unlock the files. This trend is also reflected in Talos IR engagements, where extortion was the most observed threat in Q2 2023, accounting for almost a third of threats seen, a 25 percent increase from the prior quarter (January-April) **(Figure 4)**.

Several well-known ransomware gangs — including Babuk, BianLian and Clop — have opted for data theft extortion over ransomware, a departure from the groups' typical ransomware attack chain **(Figure 5)**.

Several factors have likely contributed to some threat actors' preferences for data theft extortion instead of deploying ransomware. U.S. and international law enforcement have aggressively pursued ransomware actors in recent years, conducting major disruptions against well-known groups. Advancements in endpoint detection and response (EDR) capabilities have likely been a significant obstacle for threat actors seeking to deploy ransomware and encrypt data. Adversaries appear to consider the technique a viable way to receive a payout, demonstrating how ransomware actors are constantly working around advancements in EDR, law enforcement operations and other barriers.

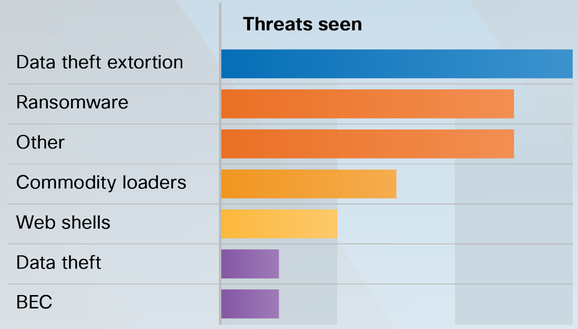
While extortion has proven to be a serious and effective threat, it has not yet outpaced the ransomware threat that has been a challenge for organizations and defenders for the past several years. We are continuing to monitor the long-term effects of this trend.

Some ransomware groups consistently leverage zero-days, often affecting multiple organizations

While many inexperienced adversaries relied on code reuse this year, we also continued to see highly sophisticated operators exploiting zero-day vulnerabilities at an unprecedented pace, highlighting the broad technical diversity of actors and TTPs in this space. Ransomware actors, well-known for being opportunistic, are quick to exploit flaws when made public. When Clop, a high-profile ransomware

FIGURE 4

Data theft extortion was the top threat in Q2 (April - June 2023), according to Talos IR



What is the impact of leaked ransomware source code?

When ransomware source code or builders are leaked, it becomes easier for aspiring cybercriminals who lack the technical expertise to develop their own ransomware variants by making only minor modifications to the original code. Additionally, by using leaked source code, threat actors can confuse or mislead investigators, as security professionals may be more likely to misattribute the activity to the wrong actor.

(From research posted on the Talos blog)

FIGURE 5

Prominent groups increasingly turn to data theft extortion in recent years

Babuk

A former ransomware group that publicly announced their shift to data theft extortion in April 2021.

Karakurt

A data theft extortion group that first appeared in June 2021.

RansomHouse

A data theft extortion group that first appeared in December 2021.

Lapsus$

A data theft extortion group that first appeared in December 2021.

Clop

A ransomware group that also conducted lucrative data theft extortion attacks in 2023.

BianLian

A ransomware group that has conducted data theft extortion since January 2023.

FIGURE 6

Timeline of ransomware groups leveraging notable vulnerabilities

JAN 2023

Clop ransomware group launches campaign using a zero-day vulnerability (CVE-2023-0669) to target the GoAnywhere MFT platform.

APR 2023

Malicious actors start exploiting vulnerabilities in PaperCut (CVE-2023-27350) beginning in mid-April 2023.

PaperCut becomes aware of unpatched servers being exploited in the wild attributed to Clop.

PaperCut actively exploited by malicious actors for remote code execution (RCE) to deploy LockBit ransomware.

MAY 2023

BI00dy ransomware gang exploits vulnerable PaperCut servers.

Clop begins exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution.

and data extortion group, claims public responsibility for exploiting a zero-day vulnerability, additional ransomware affiliates quickly follow suit, scanning for affected systems before patches are issued **(Figure 6)**.

In April, shortly after print management software company PaperCut became aware of unpatched servers being exploited in the wild by Clop, other ransomware groups began to exploit the critical remote code execution (RCE) vulnerability (CVE-2023-27350) as part of their attack chain. This highlights the widespread nature of this activity and ransomware operators' strategy, often based on the disclosure of other groups leveraging high-profile security flaws to increase chances of eliciting payouts from victims.

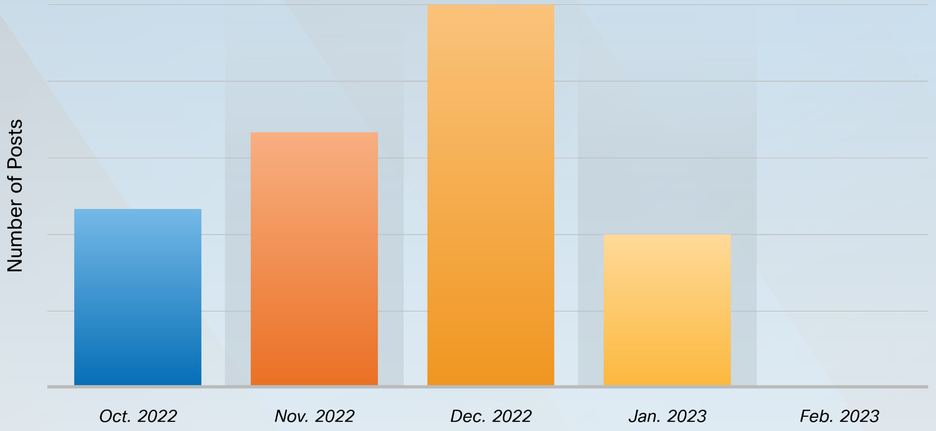
Clop's repeated efforts to exploit zero-day vulnerabilities is highly unusual for a ransomware group given the resources required to develop such capabilities. We saw many instances of this in 2023, beginning in January, when the Clop ransomware group launched a campaign leveraging a zero-day vulnerability, (CVE-2023-0669) to target the GoAnywhere MFT platform. In May, Clop claimed responsibility for attacks involving another zero-day flaw (CVE-2023-34362) affecting Progress Software's file transfer solution, MOVEit Transfer. These attacks also demonstrate Clop's expanded toolkit, as the operators deployed a previously unseen web shell, dubbed LemurLoot, to exfiltrate victims' data and extort payments on systems running MOVEit.

The vulnerabilities leveraged by ransomware affiliates/groups highlighted above all received high- or critical-severity CVSS scores, were found to be easily exploitable by Cisco Kenna, and were included in CISA's Known Exploited Vulnerabilities catalog.

Given the resources required to develop or identify such exploits, it is possible that Clop, and/or certain members, possess a level of sophistication and funding matched only by APTs. There is no known chatter on underground forums about how Clop may have obtained these exploits, though we assess the group may have access to a sophisticated developer that appears to be focusing on identifying vulnerabilities in third-party file management systems and other network peripherals.

FIGURE 7

Posts made to Hive's data leak site since late 2022



Landscape shifts in the RaaS space due to law enforcement disruptions

Ransomware groups experienced disruptions, forcing them to adapt and/or join other RaaS outfits. In January 2023, the U.S. Justice Department announced it had disrupted the Hive ransomware group. By late January, we saw this reflected in our data, with a general dropoff in posts made to Hive's data leak site **(Figure 7)**.

When ransomware infrastructure gets disrupted, operators often continue their work with other groups, creating a whack-a-mole scenario for law enforcement and network defenders. For example, when Hive's infrastructure was disrupted, many former Hive members attempted to join other ransomware groups within days of the disruption, according to our sources. This greater democratization, with an influx of new groups leveraging code from the same ransomware builders, introduces complexities for defenders attributing activity to specific groups as TTPs remain consistent across groups.

CISCO TALOS

YEAR IN REVIEW

2023

Network infrastructure

Section highlights

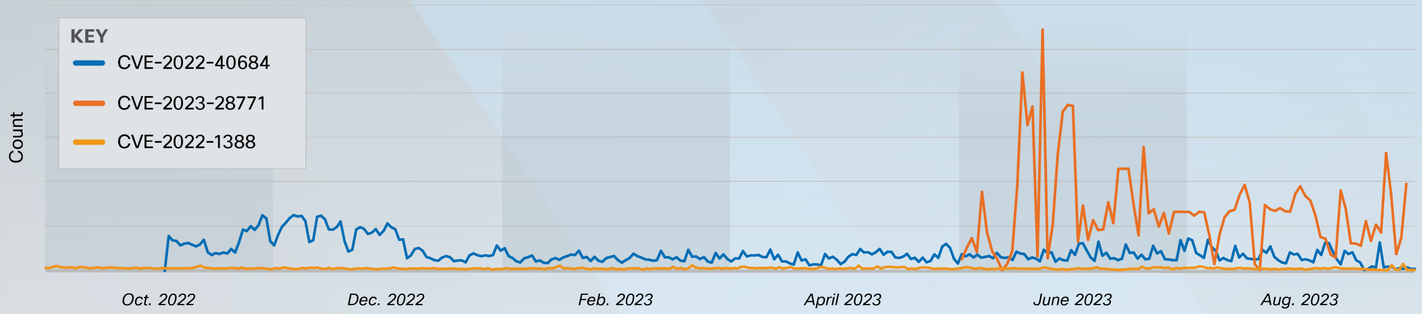
- Advanced actors are attacking networking devices at a concerning rate this year, particularly China and Russia-based groups looking to advance espionage objectives and facilitate stealthy operations against secondary targets.
- Other cybercriminals are starting to follow suit, adopting this technique to sell unauthorized access to these devices on the dark web or pivot into targeted networks and deploy ransomware.
- Actors take advantage of security weaknesses, such as default credentials and unpatched vulnerabilities, to gain initial access to the targeted device.
- Three of the five most targeted device vulnerabilities in this space are critical or severe, and exploitation can, in some instances, lead to full device takeover. This could provide adversaries unfettered access to core components of a target's network and security perimeter.
- Exploitation attempts against vulnerabilities in this space typically remained consistent throughout 2023 with occasional spikes after the vulnerabilities' public disclosure. This suggests that targeted organizations are often failing to patch their devices in a timely manner, and actors therefore continue to see value in exploiting CVEs, even as they age.
- To remain hidden post-compromise and establish additional methods of access without raising alarm bells, actors take steps to weaken defenses within the environment and will even introduce new vulnerabilities to exploit.
- Talos is helping to combat this threat by supporting the Network Resilience Coalition, a group of industry leaders from network equipment vendors, network operators, and security companies that focuses on securing critical data networks.

Talos observed an increase in sophisticated attacks on networking devices this past year, particularly by state-sponsored actors seeking to advance espionage objectives and facilitate stealthy operations. Our investigations have largely involved threat groups affiliated with Russia and the People's Republic of China (PRC), though it is reasonable to assume any sufficiently capable APT is, or will be, developing the capability to target network infrastructure as the success of these attacks garners increased attention. We have also recently observed targeting activity from other cybercriminals, including initial access brokers and ransomware actors seeking to profit off unauthorized access to targeted devices.

Networking equipment is an attractive target for malicious cyber actors due to the large attack surface it presents and potential access to a victim network it can offer. Though these devices are key components of an organization's IT infrastructure and often conduits of sensitive network traffic, they are infrequently examined from a security perspective and typically poorly patched. Further, they often do not run on standard operating systems, but rather custom firmware unique to the vendor, meaning they cannot be protected or monitored with standard, one-size-fits-all security solutions. The dichotomy of high value and weak security in these devices makes them a prime target for exploitation. Because of the large presence of Cisco network infrastructure around the world, we are well-positioned to investigate and report on top-tier attackers and their campaigns.

FIGURE 8

Exploitation attempts of network device CVEs released in 2022 or 2023



Weak security often exploited for initial access

We have seen malicious actors predominately gain initial access to networking devices by exploiting unpatched vulnerabilities, weak or default credentials, or insecure device configurations. While security professionals may not be able to implement standard EDR solutions on networking devices as referenced above, this observation demonstrates that an organization's defenses against this threat can be greatly improved simply through routine patching, enhanced monitoring, and improved credential management. Once initial access is obtained, threat actors will typically take further advantage of the device's limited security by destroying evidence of an intrusion, such as wiping or disabling logs.

Exploitation of vulnerabilities spike after public disclosure

Over the last year, exploitation activity against vulnerabilities in network devices typically remained consistent, though sometimes spiked following public disclosure, based on our telemetry. A spike in exploitation attempts could be due to several factors, such as a singular and very large campaign conducted by an advanced threat actor, or widespread targeting activity that was suddenly impeded by highly publicized reporting and recommendations to patch. Comparatively, the consistent targeting levels in the months after disclosure suggests affected organizations are failing to patch their devices in a timely manner and actors therefore continue to see value in exploiting these older vulnerabilities even as they age.

For example, detections for Snort IDs (SIDs) 60726 and 60725, which alert on attempts to exploit the aforementioned Fortinet vulnerability (CVE-2022-40684), spiked right after the security flaw was disclosed in mid-October 2022, then significantly lowered to a consistent level in early 2023 **(Figure 8)**. In comparison, attempts against vulnerable Zyxel devices (CVE-2023-28771; SID 6185) began in mid-May 2023, shortly after the CVE was publicized in April, and remained relatively level for months afterward.

Top vulnerabilities targeted are highly critical, easily exploitable and widespread

The vulnerabilities affecting network devices that were most frequently targeted in 2023 have high severity scores, meaning they are easily exploitable and can cause significant operational impact. Of the five most targeted vulnerabilities in this space, three have a CVSS score of 9.8 or 10, scores that are reserved for only a small number of the most serious CVEs. Exploitation of critical and severe security flaws in network devices can, in some instances, lead to full device takeover, allowing adversaries unfettered access to core components of a target's network and security perimeter.

Furthermore, many of the affected devices are widely used by enterprises and governments globally, further exacerbating the potential impact and scope of successful compromise. Threat actors may uncover thousands of vulnerable devices when conducting mass scanning after flaws are disclosed and can often find publicly available exploits as well.

Finally, the variety of vendors represented in the list below demonstrates how universal this issue is for device providers. This is further supported by Russian intelligence contracting documents, also known as the Vulkan Files, that Talos obtained samples of this past year. These documents showed that any network device brand was vulnerable to targeting, with one scanning component targeting almost 20 different router and switch manufacturers.

Most of the CVEs listed below are also included in CISA's lists of vulnerabilities that are commonly targeted and/or have known exploitation. Our top two vulnerabilities were also included in a CISA advisory on threats to U.S. critical infrastructure, demonstrating just how impactful exploitation of these vulnerabilities can be.

1. **CVE-2020-5902 (SID 54462):** A remote code execution vulnerability in F5 BIG-IP's Traffic Management user interface.
2. **CVE-2019-1653 (SID 48949):** An information disclosure vulnerability in Cisco RV series routers.
3. **CVE-2022-40684 (SIDs 60725 and 60726):** An authentication bypass vulnerability in Fortinet FortiOS, FortiProxy and FortiSwitchManager.
4. **CVE-2023-28771 (SID 61865):** An unauthenticated command injection vulnerability in multiple Zyxel firewalls.
5. **CVE-2020-3452 (SID 54598):** A directory traversal vulnerability in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software.

CVE descriptions sourced from the National Institute of Standards and Technology (NIST) website and Snort IDs sourced from the Snort website.

Malware sometimes installed post-compromise to establish footholds

In some instances, we observed actors, particularly China-affiliated APTs, installing malware onto devices post-compromise to establish footholds in the network and enable follow-on activity. Some of the capabilities enabled by the malware we have seen include:

- Bypassing access control lists (ACLs) so that traffic cannot be properly blocked by the router.
- Allowing for authenticated access to devices outside of normal authentication methods.
- Enabling the ability to corrupt and disable the device.
- Redirecting actor-defined traffic to actor-controlled infrastructure.

In many instances, we see actors using living-off-the-land binaries (LoLBins) either in conjunction with or instead of malware deployment to advance their operations and avoid detection.

In a more recent instance of malware being installed post-compromise, actors began exploiting a previously unknown critical vulnerability (CVE-2023-20198) in September and October 2023 to gain access to certain network devices running Cisco's IOS XE software. This allowed attackers to gain privilege level 15 access to the device, which they used to exploit a second zero-day vulnerability (CVE-2023-20273) to deploy their malware.

Notably, the CVE-2023-20198 vulnerability specifically affects devices that are exposed to the internet and have the HTTP or HTTPS Server function enabled, features the U.S. government had previously warned about.

This activity underscores Cisco's recommendations, which are consistent with best practices and guidance the U.S. government has provided in the past on mitigating risk from internet-exposed management interfaces. This is also in line with Cisco's ongoing work with industry partners as part of the Network Resilience Coalition, covered in more detail below.

Collection of network information essential to high-stakes operations

Russian and Chinese APTs use their visibility into compromised devices to capture sensitive network information, facilitating further access to more valuable data. Actors seek to intercept and abuse data such as legitimate credentials, details of trusted domain relationships, network diagrams, contracts with network customers, and configuration information. This information can provide a roadmap for actors seeking to elevate their privileges and pivot into networks of interest for intelligence collection.

APTs will also take steps to weaken defenses within the environment and carve out additional paths for long-term access. These methods include disabling logging, modifying memory to reintroduce vulnerabilities that had been patched, modifying configurations to enable privileged activity and replacing firmware with older and legitimate firmware that can be modified in memory. This variety of activities demonstrates that adversaries have a very high level of comfort and expertise working within the confines of compromised networking equipment. Additionally, in establishing these footholds within a target environment, actors seek to erode the variable barriers in an organization's defense-in-depth security architecture. Organizations must update and enhance their system hardening efforts and network monitoring capabilities to defend against these threat groups.

Numerous compromised devices form anonymizing network for malicious traffic

While the techniques described thus far are typically highly specialized to target specific victims, actors also conduct widespread and indiscriminate targeting of network devices to facilitate stealthy operations against secondary targets. We have observed China-affiliated APTs compromising numerous networking devices globally, with limited consideration of the device's owner, to form an anonymizing network that functions similarly to Tor. The actors use this network of compromised devices to route malicious traffic to and from a targeted network, thereby obfuscating the origin of their attack. These APTs can also bypass a target's security defenses that block traffic from certain geographic regions by having the C2 traffic emanate from internet service providers (ISPs) local to the victim.

We have seen China-affiliated actors conducting widespread campaigns to exploit critical vulnerabilities associated with networking devices within days of public disclosure, meaning the type of infrastructure targeted is often largely opportunistic.

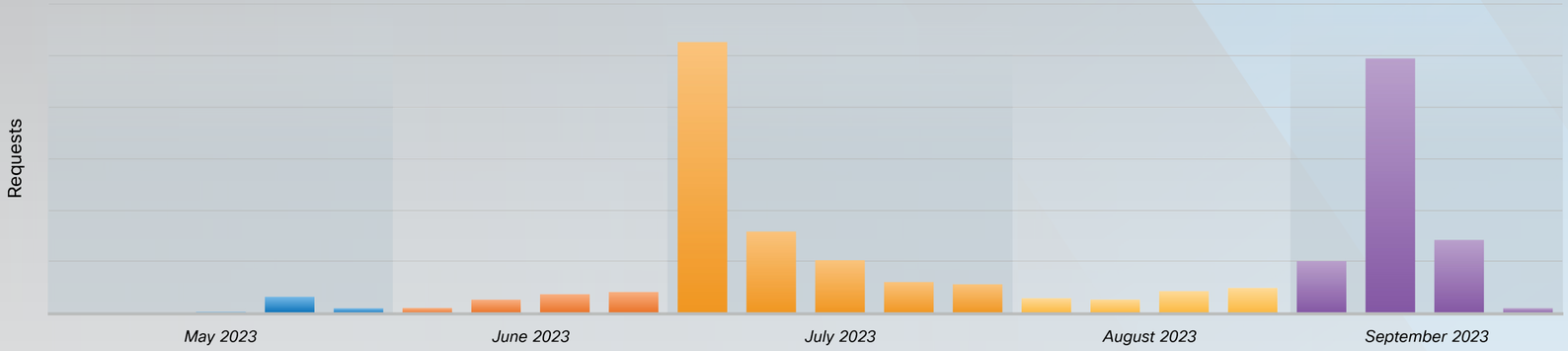
How are we countering this growing threat?

Cisco launched the Network Resilience Coalition with leading industry partners in July 2023. This alliance focuses on increasing awareness of this issue, understanding its full scope, and providing actionable recommendations for improving network security that supports global economic and national security.

Talos has led efforts to address this threat, contributing a significant amount of research and technical information that has been published in U.S. government advisories on this topic. We have also increased messaging to customers and network defenders on how to improve network infrastructure resilience. We actively engage in research and information sharing efforts with other vendors as well to bolster overall device security. For example, this past year, our Talos Vulnerability Discovery and Research Team made investigating small office, home office (SOHO) and industrial routers a major priority. As a direct result of this effort, we have reported 289 vulnerabilities to vendors to date, published across 141 Talos advisories. These reports resulted in new Snort network intrusion detection coverage and several security improvements from each vendor. These fixes help customers who deploy Cisco Security solutions and improve the security posture of anyone using these devices once the vulnerabilities are patched.

FIGURE 9

Spikes in WebVPN-related requests that coincide with activity targeting ASA devices



Ransomware actors and initial access brokers abuse weak credentials and monetize access

Initial access brokers and ransomware affiliates have also become more active in targeting network devices this past year, predominately compromising weak or default credentials, then either selling the unauthorized access on dark web marketplaces or using it to deploy ransomware onto targeted networks.

This year, we responded to a campaign targeting Cisco Adaptive Security Appliance (ASA) devices configured with WebVPN in which cybercriminals likely gained unauthorized access to the devices via brute force and password spraying attacks. In July, we observed a significant spike in activity targeting ASA devices configured with WebVPN, coinciding with much of the public reporting on in-the-wild activity targeting ASA devices **(Figure 9)**. Additionally, a September 2023 spike in WebVPN requests coincides with Cisco's security advisory on a vulnerability disclosure for CVE-2023-20269. Exploitation of this vulnerability allows a remote attacker to conduct brute-force attacks or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user. The ability to perform a brute-force attack, combined with widespread use of weak or default credentials, facilitated high impact against a large number of devices. This activity also highlights the frequency in which adversaries will attempt to exploit vulnerabilities soon after they are made public.

Akira and LockBit ransomware groups were publicly tied to this activity starting in August 2023, though it is unclear if these actors conducted the credential spraying attacks or if they purchased access from initial access brokers. These two threat groups have also been observed conducting similar activity against other device vendors, such as FortiGuard. Talos believes that third-party brokers may be responsible for initial access in many of the ransomware cases based on volume and timing of the targeting activity and nature of follow-on actions post-compromise. The aforementioned security advisory included mitigation recommendations and indicators of compromise to help defenders protect against this threat, highlighting the importance of implementing proper MFA and limiting the number of consecutive failed login attempts, which would significantly reduce exposure to this threat.

"Initial access brokers and ransomware affiliates have also become more active in targeting network devices this past year, predominately compromising weak or default credentials..."

CISCO TALOS

YEAR IN REVIEW

2023

Advanced persistent threats: China

Section highlights

- China-affiliated activity occurred at a rigorous pace this year, likely in response to geopolitical events that strained the country's relationships with the West and Asia Pacific.
- Based on our analysis of numerous malicious campaigns, it appears Beijing may be directing more aggressive intelligence collection and prepositioning for future attacks against targets in these regions.
- Actors have improved in terms of deeply entrenching themselves in targeted networks and dodging detection or incident response efforts, placing a heavier burden on targeted organizations to keep their networks safe.
- Talos observed several instances of ransomware actors compromising a target closely following a long-term, covert APT intrusion by using similar methods of initial access and deploying ransomware. While the connection, if any, between the APT and ransomware groups is undetermined, the timing of the operations and overlap in TTPs suggests the ransomware operators may at least have prior knowledge of the espionage campaigns.
- Telecommunications organizations were a top target of Chinese cyber operations in 2023, particularly those offering services in areas of strategic interest to China, such as Guam and Taiwan. These entities are particularly attractive targets for these actors, as unauthorized access can enable widespread intelligence collection across several critical sectors.
- The organizational structure of telecommunications organizations and victims' geographical locations often poses challenges to incident responders, including limited visibility into all affected networks and political sensitivities when investigating or assigning attribution to China.

While APTs emanating from many parts of the world remained active, most of our investigations and research this year focused on China, Russia and the Middle East, which are featured in this section of the report.

Advanced persistent threats: China

China-linked APTs operated at a rapid pace this year, conducting sophisticated and stealthy intrusions into the networks of numerous high-value targets. According to our research, the actors responsible for these campaigns often seek long-term access to targeted networks, establishing multiple methods of maintaining persistence while avoiding targets' detection mechanisms.

TTPs largely centered on evading detection and attribution

China-affiliated APTs appear to considerably reduce their malicious activity on a network if detected or the actor becomes aware of incident response efforts. Operators are likely maintaining undiscovered footholds and waiting until the target is no longer operating at a level of heightened awareness to resume their activity, underscoring the importance of aggressive remediation and eviction efforts, and keeping incident response plans updated. Their success in maintaining this access is evidenced by long dwell times on compromised networks, with one intrusion we investigated this past year having a dwell time of at least seven years. This demonstrates the severe impact these types of campaigns can have on targeted organizations, as complete remediation often requires comprehensive analysis of all network assets, long-term support of advanced incident response teams, and organization-wide action such as password resets and system updates. If targeted entities cannot commit to these response efforts, the malicious actors will likely quickly and quietly resume their activities once they sense the target feels the environment is safe.

Other TTPs used by China-linked APTs this past year include LoLBins to evade detection, exploitation of public vulnerabilities, targeting of network devices, and use of shared, open-source or commercial tools, all of which are largely unchanged from last year. We also continued to see these APTs conducting operations in which access to the targeted entity can facilitate compromise of many victims, with actors especially employing this methodology against telecommunications organizations.

New trend of ransomware deployment following long-term espionage operations

In a few instances, following a long-term, sophisticated and espionage-oriented APT intrusion, Talos observed a secondary threat group targeting the victim network by using similar methods of gaining initial access, such as exploiting public-facing vulnerabilities, and then deploying ransomware payloads. We have observed this trend in certain industries, such as semiconductors, and regions, such as Guam, that the PRC places a high degree of strategic importance on. Though we have yet to determine a connection, if any, between the two groups of attackers in these instances, several scenarios are possible:

- They could be illustrative of these APTs engaging in destructive attacks. There are several examples of Chinese APTs incorporating ransomware into their operations, such as Bronze Starlight or APT41.
- They could be comprised of actors affiliated with the original attackers, such as opportunistic associates seeking financial gain.
- These groups may also not be affiliated with China at all, though this is probably less likely given the timing of the follow-on ransomware operations and overlap in methods of obtaining initial access.

Whether it has resulted from strategic collaboration, financial cooperation, or just unaffiliated actors finding their way in due to some other element, such as noisier tradecraft from the original adversaries, these attacks potentially represent a dangerous new destructive element to PRC-affiliated APT attacks that we assess reveals an escalation from previous years.

More rigorous pace of operations likely linked to shifts in geopolitical environment

Activity conducted by China-affiliated APTs occurred at a fast tempo this past year, likely due in part to geopolitical factors that Chinese leadership perceived as threats to the Communist Party of China's (CCP's) governance. We quantified this increase in activity based on the number of government partner intelligence shares, collaboration projects with CISA, related infrastructure targeting cases, and high-priority investigations into China-affiliated activity affecting Cisco customers.

This shift in tempo may reflect a difference in intent, a type of signaling we have not observed in years past. Beijing typically directs cyber activity with the intent of collecting intelligence to address the economic, political and strategic goals of the CCP. Though some of these goals, such as their Five-Year Plans, are routinely set as long-term objectives for growth, other provisional needs are determined based upon China's relationships with other nations. For example, if a relationship with a nation China relies on for exports deteriorates, Chinese

"Activity conducted by China-affiliated APTs occurred at a fast tempo this past year, likely due in part to geopolitical factors that Chinese leadership perceived as threats to the Communist Party of China's (CCP's) governance."

Threat actor highlight: Volt Typhoon

Volt Typhoon is a China-affiliated threat group that made headlines this past year for their long-term operation targeting U.S. critical infrastructure organizations and military bases.

Talos investigated a sustained Volt Typhoon intrusion targeting the telecommunications sector in Guam, which is notably the site of a U.S. military base significant for the defense of Taiwan. Our research revealed the actors maintained persistent access to and exfiltrated data from networks of a service provider and certain high-value customers for at least a year and a half. Talos continues to closely collaborate with public and private partners on hunting this threat group's activity and investigate the group's anonymization infrastructure.

actors may seek to exfiltrate proprietary data, focused on espionage yet deliberately quiet, that can boost their self-reliance in developing whatever that export is. If a relationship with a nation becomes increasingly contentious, China may seek to establish footholds in the networks of that nation's critical infrastructure and preposition themselves for future destructive attacks.

Numerous geopolitical events affected China's relationships with the West and Asia Pacific this year, potentially leading to CCP directives for more aggressive targeting activity. Talos performed intensive incident response operations for strategic targets in both of these regions.

Deepening divide between China and the West

One major factor that has deepened the divide between China and the West this year has been the PRC's alliance with Russia, particularly as other world leaders have vehemently denounced Moscow's actions in the Russia-Ukraine war. The two countries have strengthened their trade relationship, and China's rapidly increasing exports to Russia have tempered the impact of numerous Western sanctions that have been levied against the country since its invasion of Ukraine. Russia and China have also united to expand their presence in the Middle East and developing countries, conducting joint military exercises in the Gulf of Oman in March 2023, and inviting numerous nations to join BRICS group in August 2023, bolstering the trade bloc against competition from the West.

U.S. policies and positions regarding China have not softened this year, with the U.S. continuing to categorize China as a top security threat. The Director of National Intelligence named China the "most consequential threat" to U.S. national security in 2023, and the U.S. has steadily expanded sanctions against Chinese companies and organizations because of such concerns. These security issues were exemplified by an incident in early 2023 when a Chinese spy balloon flew over the U.S., gathered intelligence from military bases, and transmitted the information back to Beijing before being shot down. The U.S., Japan and South Korea also bolstered their alliance in 2023, with the countries' leaders meeting at Camp David in August and committing to work together to address security challenges from China and North Korea. Beijing swiftly criticized this meeting, publicly stating attempts to form military blocs in the Asia Pacific will be met with "vigilance and opposition."

Growing conflict in the Asia Pacific

Meanwhile, China is already facing conflict with neighboring nations in the Asia Pacific. Tensions have been rising between China and Taiwan, exacerbated by U.S. support in expanding Taiwan's self-defense capabilities. The People's Liberation Army (PLA) has upped its military pressure on the island, routinely sending warplanes, drones and ships past the median line of the Taiwan Strait in shows of force. China has also become increasingly aggressive in the South China Sea, doubling down on their claims to sovereignty over almost all of the disputed area. Their robust military presence in the region has incurred standoffs and conflict throughout the past year with neighboring countries that have competing claims for the territory, as well as with the U.S. military that is present there. Finally, China's relationship with Japan has also seen challenges in the past year, with events like Japan restricting exports of semiconductors and Tokyo's decision to release water from the Fukushima Daiichi nuclear power plant, which elicited criticism from Beijing.

Targeting of the telecommunications sector expands collection and prepositions actors for future attacks

We responded to several intrusions into telecommunications providers by China-affiliated APTs this year, particularly in areas that are of strategic interest to Beijing.

Telecommunications organizations are attractive targets for these groups, as they often control numerous critical infrastructure assets in the country, such as national satellite systems, internet services, and telephone networks that are vital to the private and public sectors. China-affiliated APTs can use their unauthorized access to establish footholds to disrupt critical services, such as communication infrastructure, in the event of a conflict with the targeted nation. They can also pivot into the networks of additional high-value targets of interest and conduct widespread exfiltration of sensitive data.

There are several ways in which use of this latter technique can challenge remediation efforts. A service provider may not immediately realize or have visibility into the extent of an intrusion targeting other businesses, subscribers or third-party providers, giving the actors ample time to burrow themselves deeper into compromised networks. The guidance for notifying customers of a breach also varies by country, potentially delaying incident response based on the geographic location of the initial victim. Finally, given delicate diplomatic relations that may exist between the targeted country and adversary, U.S.-based incident response teams may face challenges and political sensitivities when assisting in certain regions. Victims in certain countries may be hesitant to assign attribution to a particular threat group, could have strong organizational ties to China, and/or may be wary of sharing key details of the compromise with American teams.

CISCO TALOS

YEAR IN REVIEW

2023

Advanced persistent threats: Russia

Section highlights

- Russian state-sponsored APT Gamaredon has remained a major player in threats against Ukraine and was the top threat that the Cisco Talos Ukraine Task Unit responded to this year.
- In 2023, Gamaredon primarily targeted entities in North America and Europe, with a disproportionate number of victims in Western Europe. Additionally, over half of the entities targeted were in the transportation and utilities sectors, reflecting Russia's focus on critical infrastructure.
- Turla, another Russian government-affiliated APT, was largely active between September 2022 and February 2023, but their operations diminished significantly around May 2023, coinciding with the U.S. Justice Department's disruption of Turla's Snake malware.
- The number of affected sectors and volume of victims between these two groups vastly differed, contrasting Gamaredon's broader targeting with Turla's more limited activity against highly selective victims.
- Beyond Gamaredon and Turla activity, we also observed a spike in SmokeLoader activity – malware used by a variety of different groups – in late April and early May, aligning with CERT-UA's reporting of mass distribution of SmokeLoader targeting Ukrainian entities.
- To stabilize Ukraine's power grid against the effects of global positioning system (GPS) jamming on the battlefield, Cisco hardware and software engineers modified one of our commercial network switches to provide holdover for Ukraine's power grid equipment during these outages.

Advanced persistent threats: Russia

Threats from Russian state-sponsored or state-aligned APTs remain a mainstay in our threat tracking and research efforts this year. Since the onset of the Russian invasion of Ukraine, Russian APTs' engagement in cyber espionage, cyber influence, and destructive attacks has intensified. In line with activity reported in last year's report, Russian APTs continue to adapt to geopolitical challenges stemming from the war and NATO and allied nations' military assistance to Ukraine. Additionally, 2023 saw a global law enforcement effort to dismantle the Snake malware, considered one of the most prolific and sophisticated cyber espionage tools in the Federal Security Service of the Russian Federation's (FSB) arsenal commonly deployed against systems globally.

Gamaredon and Turla remain top threats, targeting patterns vary

Russia-affiliated APT groups Gamaredon and Turla continue to persist as top threats in this space, updating aspects of their attacks and toolkits to support their TTPs, despite international efforts to combat the Russian cyber threat.

Cisco Talos closely tracks activities associated with Gamaredon, an APT broadly suspected to be a team of Russian government-supported actors based in Crimea. While the group in recent months has concentrated their efforts on cyberespionage against Ukrainian entities, they also target entities globally, with a less focused victimology as compared to other Russian APTs operating in this space. Turla also conducts long-term espionage and data exfiltration operations that are in line with Russian intelligence priorities that the U.S. government attributes to a unit within the FSB. In contrast to Gamaredon, who we observed targeting a range of sectors in 2023 (Figure 10), Turla is known for much more targeted operations against a smaller number of strategically important entities. Turla, who is publicly assessed to operate on behalf of a different unit than Gamaredon in the FSB, is likely capable of compromising a much broader spectrum of entities worldwide but limits their operations to what they perceive to be high-value targets.

The number of sectors and volume of victims that Gamaredon and Turla targeted vastly differed, based on our telemetry **(Figures 10 and 11)**.

FIGURE 10

Industry verticals targeted by Gamaredon

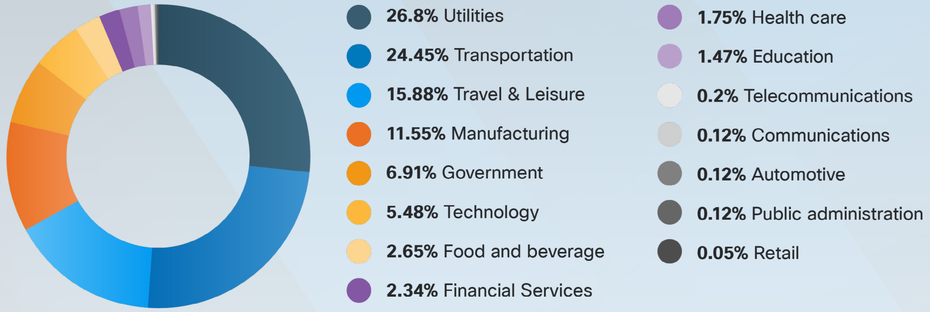
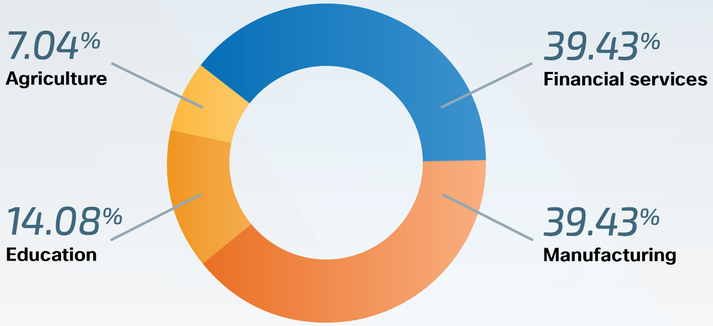


FIGURE 11

Industry verticals targeted by Turla



Note: *Percentages may not equal 100% due to rounding.*

FIGURE 12

Gamaredon malicious download activity throughout the year

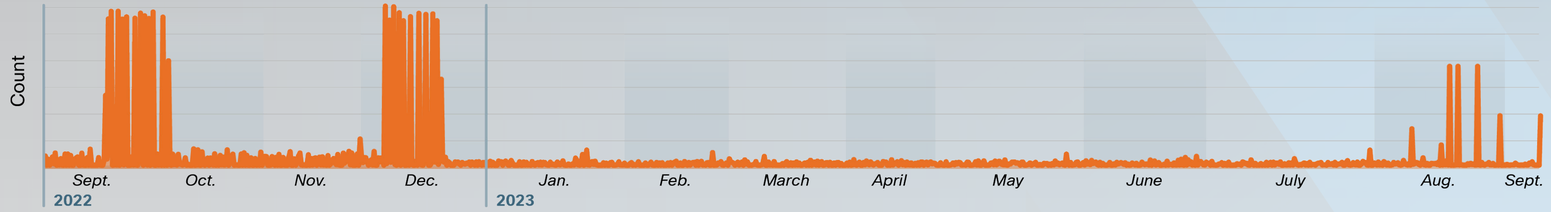
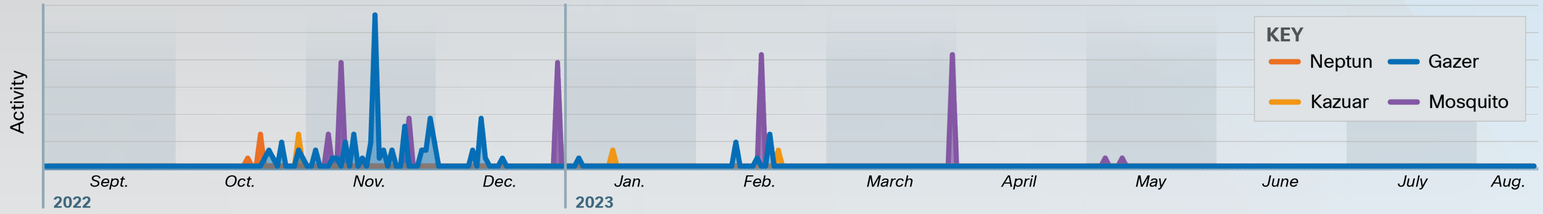


FIGURE 13

Activity across Turla malware variants Gazer, Kazuar, Mosquito and Neptun this year



"Beyond highlighting the sectors that Gamaredon and Turla targeted this year, the data is also largely representative of the volume of attacks Snort helped prevent."

The largest spread of Gamaredon victims were located in North America, followed by Europe and the Middle East, with a disproportionate number of victims in western Europe. Over half of Gamaredon's targeting activity impacted the utilities and transportation industry sectors, consistent with Russia's targeting of critical infrastructure entities, likely to cause the most disruption to strategic entities to stymie Ukraine's war efforts.

In September and December 2022 and September 2023, we saw three clear spikes in Gamaredon activity **(Figure 12)**, potentially representing clusters of specific targeted operations. The ramped up Gamaredon activity as seen in Figure 12 in August 2023 is consistent with the group's activity levels according to a report by Ukraine's National Coordination Center for Cybersecurity (NCCC).

In contrast to the range of industry verticals Gamaredon targeted this year, Turla targeted fewer victims across a smaller number of sectors and geographies, in line with the group's precise operations. The manufacturing and financial services sectors were equally impacted, with education and agriculture targeted to a lesser degree **(Figure 11)**. Beyond highlighting the sectors that Gamaredon and Turla targeted this year, the data is also largely representative of the volume of attacks Snort helped prevent.

Malware deployed by and custom to Turla, including various backdoors and implants used for persistent access, are seen to congregate in a series of events largely occurring between September 2022 and February 2023. While the reason for the heightened activity during that period is unknown, we asses it is likely to have stemmed from an increased operational tempo in response to the Russian invasion on Ukraine. These four malware families – Gazer, Kazuar, Mosquito and Neptun – while not an exhaustive list of Turla malware, are part of Turla's large arsenal of bespoke malware and modified open-source malware, which are constantly updated or replaced with more advanced versions.

This clustering over time, as seen in Figure 13, of custom Turla malware continues to convey the narrative of Turla's operational tempo, likely highly based on the selectivity of targets. Notably, the depiction of Turla malware activity in Figure 13 (while not an exhaustive list) diminishes significantly around May 2023, coinciding with the U.S. Justice Department's disruption of Turla's Snake malware. For nearly 20 years, Turla deployed Snake to steal and exfiltrate data from targeted systems through numerous relay nodes scattered around the world. While the effects of the Snake disruption on Turla's current and future operations are still unknown, the diminished malware activity may represent changes in Turla's toolkit as a result of the disruption.

FIGURE 14

Top threats in Ukraine task force investigations

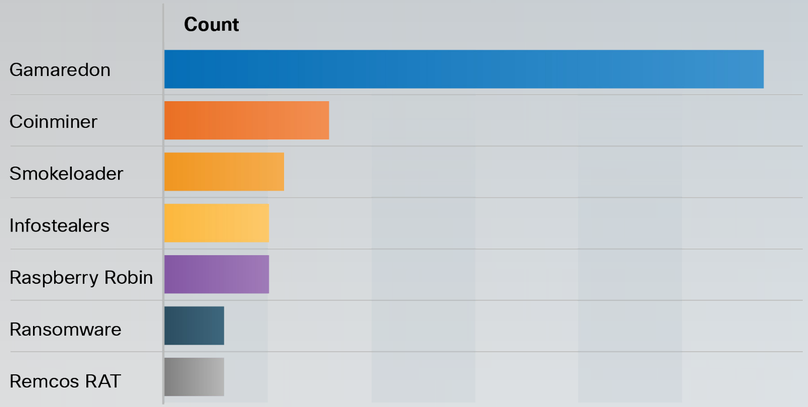
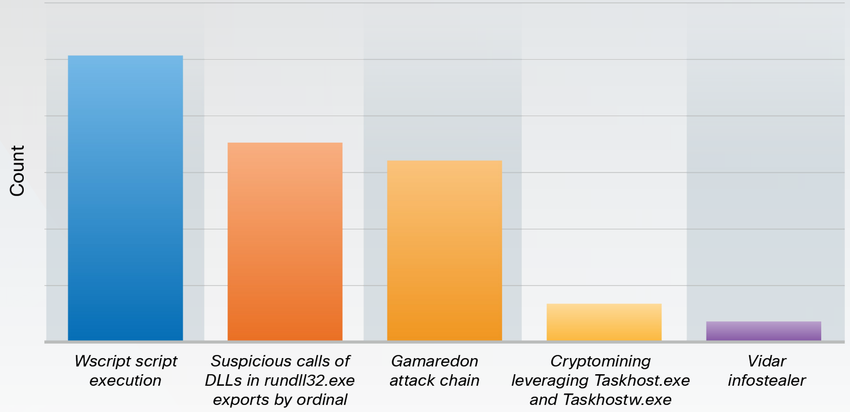


FIGURE 15

Top five malicious activities affecting Ukraine partners



Internal Task Unit continues to monitor threats to Ukraine

Talos' ongoing support for Ukraine continues to be a large focus of our operational efforts this year. As part of the Task Unit's work, we monitor suspicious activity in endpoint telemetry for nearly three dozen Ukrainian partners across critical infrastructure sectors, including government, utilities, financial services, health care and transportation, among others.

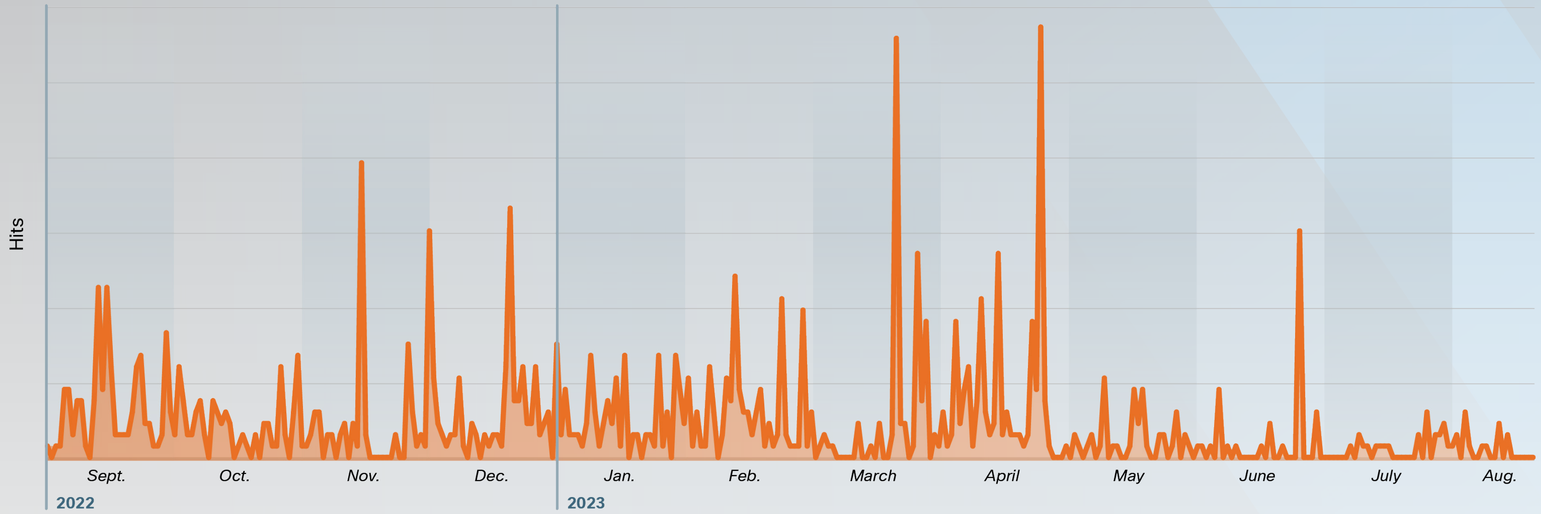
While the threats against these organizations may not all be designated as APT activity, the volume of threats and volatile geopolitical climate they are deployed in poses a significant risk to network defenders protecting critical assets.

Gamaredon is the most dominant threat to Ukraine that our task force has responded to **(Figure 14)**. The group has historically targeted predominantly Ukrainian entities – particularly those responsible for the country's defense, diplomacy and internal security.

Gamaredon, and portions of their attack chain, consistently appear in top threat hunting alerts from Cisco Secure Endpoint that notified our Ukrainian partners (Figure 15). For example, these top five behaviors demonstrate the consistent use of LoLBins and the techniques associated with them, such as Wscript execution – a legitimate Windows process likely used to masquerade malware deployment under the guise of expected activity – that continue to be leveraged to support a variety of threats across an attack lifecycle. Activity commonly linked to financially motivated cybercriminals, like the deployment of cryptocurrency mining and information stealers, also continue to impact Ukrainian organizations across numerous industries, speaking to the broad range of threats facing Ukraine.

FIGURE 16

SmokeLoader malware activity throughout the year



"The significant cyber defense resources we continue to devote to protecting our Ukrainian partners has undoubtedly had a significant impact on this threat space as well, thwarting significant disruptions by mitigating attacks in the early stages."

Beyond highlighting the consistent tempo of Gamaredon activities above, Figures 14 and 15 also help to demonstrate the multitude of threats the Task Unit has responded to this year. This includes activities from malware threats such as loaders, information stealers, ransomware, cryptocurrency miners and Raspberry Robin, a prolific malware family covered in last year's annual report, which remains a consistent threat to enterprise environments. For example, SmokeLoader is a downloader leveraged by a variety of groups that the Task Unit has repeatedly responded to this year **(Figure 14)**. Typically delivered via email, SmokeLoader drops malware on infected machines and since early May, has been consistently reported by Ukraine's Computer Emergency Response Team (CERT-UA) further highlighting its persistent use in the threat landscape.

We observed a spike in SmokeLoader activity in late April and early May, aligning with CERT-UA's reporting of mass distribution of SmokeLoader targeting Ukrainian entities (Figure 16).

While the Task Unit has continuously responded to a myriad of cyber threats since the onset of the Russia-Ukraine war, the observed activity in 2023 was far less sophisticated than what is typically associated with the sophisticated adversaries we would expect to see in this space. The activity was dynamic this year but does not reflect the full range of destructive cyber capabilities Russia has previously demonstrated against Ukraine and/or its NATO allies. The reasons behind this have been debated by industry partners and experts, and it is likely the result of combined efforts from the cybersecurity industry, U.S. government, foreign partners, and Ukraine's own commitment to protecting its people. The significant cyber defense resources we continue to devote to protecting our Ukrainian partners has undoubtedly had a significant impact on this threat space as well, thwarting significant disruptions by mitigating attacks in the early stages.

Project PowerUp: Keeping the lights on in Ukraine

Leveraging Talos' unique relationships with industry, government, and Ukraine, we spearheaded an effort to help stabilize Ukraine's power grid against the effects of GPS jamming on the battlefield.

Faced with the complex problem of how to make Ukraine's substations resistant to operational failures caused by downed GPS signals, Cisco hardware and software engineers modified one of our commercial network switches, the Cisco Industrial Ethernet switch, to provide holdover for Ukraine's power grid equipment during these outages.

After months of development and coordination with various partners, the devices were delivered to Ukraine and installed in substations around the country, no small feat during an active war zone. This story will be featured in Cisco's annual Purpose Report later this year. This example further demonstrates how Cisco's efforts have helped safeguard Ukraine's critical infrastructure from severe Russian cyberattacks in 2023.

How is Ukraine's power grid affected when GPS goes down?

Many of Ukraine's high-voltage electrical substations – which play a vital role in the country's domestic transmission of power – make extensive use of the availability of precise GPS timing information to help operators anticipate, react and diagnose a complex high-voltage electric grid. When GPS signals are widely disrupted, substations cannot synchronize their time reporting accurately because they cannot assign accurate timestamps. Without good synchronized data, efforts to manage loads between different parts of the system can be affected, and this management avoids outages and failure, especially during peak demand and surge times. This disruption can be widespread, causing wide areas to lose GPS service for long periods of time.

FIGURE 17

YoroTrooper threat actor matrix

Aliases	Unknown
Affiliations	Kazakhstan
Active since	2022
Goals	Espionage, data theft to support state objectives.
Victimology	European governing entities with a special focus on the Commonwealth of Independent States (CIS) countries.
Notable TTPs	Social engineering, spear-phishing, data exfiltration, custom-built and commodity malware.
Malware & tooling	YoroTrooper employs a variety of self-developed and commodity malware families such as AveMaria/Warzone RAT, LodaRAT.

Some YoroTrooper members hail from pro-Russia Kazakhstan

Earlier this year, Cisco Talos disclosed information on a new threat actor we named "YoroTrooper," who we assess with high confidence consists, at least in part, of individuals from Kazakhstan. YoroTrooper is a highly motivated threat actor whose low sophistication is complemented with aggressive targeting of entities using a multitude of commodity malware families. Since 2022, the group has conducted operations aimed at espionage and data theft against victims in the government or energy sectors in Azerbaijan, Tajikistan, Kyrgyzstan and other members of the Commonwealth of Independent States (CIS).

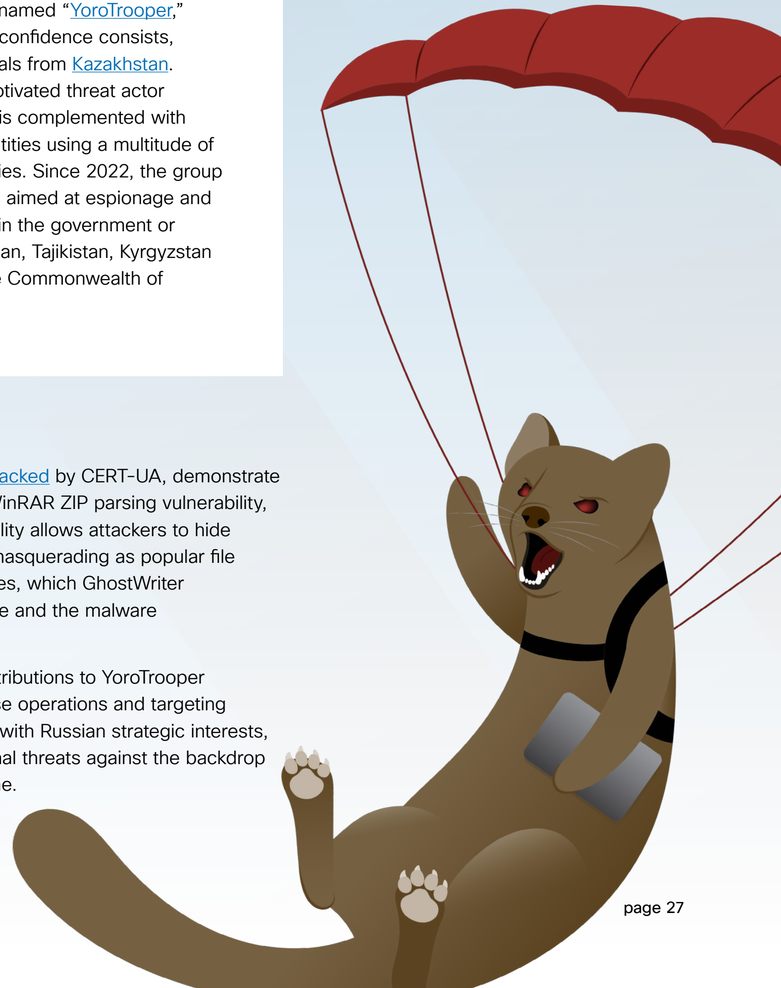
APT activity from Russian allies

Talos' research and monitoring efforts of regional threats have expanded to APT activity attributed to countries formerly part of the Soviet Union, whose intelligence goals, TTPs and victimology often align with the Kremlin. Given the long-standing political union between these governments, collaboration is plausible. However, we do not have direct evidence of Russian government involvement.

We assess YoroTrooper also targets organizations of strategic value across European and Turkish governments **(Figure 17)**. For example, YoroTrooper has compromised accounts for at least two international organizations, including a critical European Union (EU) health care agency and the World Intellectual Property Organization (WIPO). Successful compromises also included embassies of European countries including Azerbaijan and Turkmenistan.

This year, Talos has also been monitoring GhostWriter operational activities, which is a group allegedly linked to the Belarusian government, according to CERT-UA. We have observed several GhostWriter campaigns against government entities, military organizations and civilian users in Ukraine and Poland. We judge that these operations, often seen promoting anti-NATO narratives that aim to undermine regional security cooperation, are very likely aimed at stealing information and gaining persistent remote access. Recent activities, also tracked by CERT-UA, demonstrate the group's exploitation of the WinRAR ZIP parsing vulnerability, CVE-2023-38831. The vulnerability allows attackers to hide malicious code in ZIP archives masquerading as popular file formats including JPG or TXT files, which GhostWriter leveraged to deploy Cobalt Strike and the malware downloader, PicassoLoader.

We cannot rule out Russian contributions to YoroTrooper or GhostWriter at this time. These operations and targeting patterns, often strongly aligning with Russian strategic interests, are key for understanding regional threats against the backdrop of the Russian invasion of Ukraine.



CISCO TALOS

YEAR IN REVIEW

2023

Advanced persistent threats: Middle East

Section highlights

- Events in early October 2023 between Hamas and Israel contributed to several politically motivated hacktivist groups launching uncoordinated and mostly unsophisticated attacks against both sides, similar to what we observed at the beginning of the Russia-Ukraine war.
- The Middle East's complicated geopolitical environment continued to be dynamic this year, and we will likely see that impact the cyber realm going forward. As longtime regional adversaries attempt to normalize ties, and decades-old conflicts spark new violence, major cyber players with economic and political interests in the Middle East, like China and Iran, may be more motivated to influence outcomes through direct or proxy operations.
- Middle East-based APT groups targeted telecommunications firms in the region, following the trend we have seen of sophisticated adversaries targeting this sector. As part of this activity, we identified a new intrusion set, ShroudedSnooper, deploying novel implants we dubbed HTTPSnoop and PipeSnoop against related entities.
- The Iran state-sponsored MuddyWater APT group relied less on the commonly used Syncro tool — essential for remote access and malware deployment — than in previous years, likely in response to the cybersecurity industry's action against known MuddyWater TTPs.

Advanced persistent threats: Middle East

Regional state-sponsored groups continue to conduct pervasive cyber attacks against entities in North America, Europe, the Middle East and Asia. Telecommunications companies endured the most of these attacks, a trend that has transcended multiple APTs, as outlined in other parts of this report. Our work in this space resulted in the discovery of a new actor we named ShroudedSnooper that appears intent on targeting major telecommunications entities in the region. The Iran state-sponsored MuddyWater APT actor remains a key player in this threat space and was the focus of much of our research efforts this year. While the group continues to use many of the same techniques to advance their primary goals of stealing intellectual property and collecting intelligence, industry action has likely influenced the group's ability to use certain tools, including the Syncro remote management and monitoring (RMM) platform that the group was using at the end of 2022.

The Middle East is arguably the most complicated geopolitical region in the world, and the conflict that ignited between Hamas and Israel in October 2023 reminds us that events with global consequences can unfold quickly and with little notice. The everchanging geopolitical landscape here will undoubtedly affect cyber activity going forward, as established regional players like Iran remain intent on achieving certain geopolitical goals and new actors like China seek to expand its influence.

Hamas-Israel conflict brings influx of hacktivist groups

Hamas' surprise attack on Israel in October not only had global implications but also has affected the cyber realm, immediately drawing in actors from both sides of the conflict. Politically motivated hacktivist groups — including well-known actors like Killnet and Anonymous Sudan as well as lesser-known groups — launched uncoordinated and mostly unsophisticated attacks at the outset, as the threat space was quickly flooded with many different actors. Several hacktivist groups quickly announced support for both sides in the Israel-Hamas conflict, posted threatening political messages, called on followers to join in and claimed responsibility for DDoS attacks against targets of interest — typical hacktivist TTPs. This is broadly consistent with what we observed at the start of the Russia-Ukraine war, when an influx of cyber activity became concentrated on these countries seemingly overnight.

Significant geopolitical events like this also invite the participation of much more sophisticated adversaries, including those supported and funded by foreign state governments. We have seen this most recently in Ukraine, where advanced state-sponsored actors from Russia like Gamaredon and Turla have been relentless in their targeting of Ukranian entities since the start of the war. Likewise, we expect to see an increase in Iranian cyber activity in the Middle East following Hamas' attack on Israel. Iran and Israel are longstanding adversaries, and their decades-old conflict has major influence on Iran's cyber operations. Iran is also a key backer of several anti-Israel militant and terrorist groups, including Hamas, Hezbollah, and the Palestinian Islamic Jihad, which were all involved in this most recent spate of violence against Israel. Iran's support for these groups and Tehran's historical hostility with Israel strongly suggests Iran may use its cyber capabilities to influence the outcome of the crisis, much like other nations rely on cyber as an essential tool to advance foreign policy objectives.

"The Iran state-sponsored MuddyWater APT actor remains a key player in this threat space and was the focus of much of our research efforts this year. While the group continues to use many of the same techniques to advance their primary goals of stealing intellectual property and collecting intelligence, industry action has likely influenced the group's ability to use certain tools."

Chinese ambitions in the region portend possible cyber operations

While China has traditionally held a prominent economic role in the Middle East as one of the largest foreign investors, PRC leadership sought to also expand their political presence in the region this past year by engaging in regional conflict mediation. In March, Beijing brokered an agreement between longtime adversaries Iran and Saudi Arabia to reestablish diplomatic ties, and in September, China and Syria announced a strategic partnership, as Syrian President Bashar Assad begins to reenter the international fold after more than a decade of brutal civil war. The China-Syria deal may also provide great economic incentives for Beijing, which could become a major financial backer of Syria's reconstruction efforts. These strategic moves by China come at a time when the U.S. has largely withdrawn from the region following the post-9/11 period, and Beijing likely sees this as an opportunity to capitalize on waning U.S. involvement and influence there.

Because of China's growing political presence in the Middle East, we expect to see more Chinese APT activity in the region. We have observed Chinese APTs, among the most active and persistent of state-sponsored threats, supplementing financial endeavors with espionage operations in regions it is invested in, targeting private sector organizations and governments whose intellectual property aligns with economic goals. Future operations would likely be in-line with well-established Chinese APT TTPs, like targeting entities and individuals that operate in industries essential to China's strategic plans, establishing long-term and stealthy access to targeted networks, and stealing intellectual property and technology.

FIGURE 18

HTTPSnoop URLs masquerading as OfficeCore's LBS System

```
'http://+:80/1bsadmin/valve/',0
'http://+:80/1bsadmin/salon/',0
'http://+:80/1bsadmin/disorder/',0
'http://+:80/1bsadmin/cute/',0
'http://+:80/1bs/alpha/',0
'http://+:80/lbs/special/',0
'http://+:80/1bs/blue/',0
'http://+:80/1bs/mystery/',0
'http://+:80/1bswap/army/',0
'http://+:80/1bswap/problem/',0
'http://+:80/1bswap/goose/',0
'http://+:80/1bswap/useful/',0
```

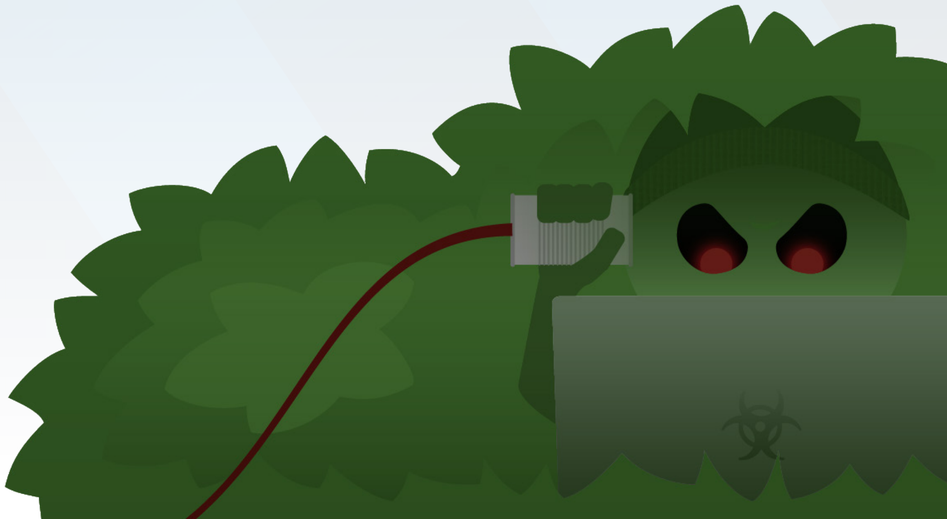
Because of China's growing political presence in the Middle East, we expect to see more Chinese APT activity in the region.

Telecommunications sector remains key target for regional threat actors

In 2023, we discovered a new intrusion set, ShroudedSnooper, deploying novel backdoor implants, HTTPSnoop and PipeSnoop, against telecommunications providers in the Middle East, a continuation of a trend we have been monitoring in which sophisticated actors frequently target this sector. There is currently not enough evidence to link ShroudedSnooper activity to a specific country. However, the group's consistent masquerading of software applications used by telecommunication firms in the region and impact to several regional providers highly aligns with likely state-sponsored actors and sophisticated adversaries around the world.

The HTTPSnoop and PipeSnoop implants consist of novel techniques to listen to incoming requests for specific HTTP(S) URLs and execute on an infected endpoint. Some of the HTTPSnoop implants use URLs that masquerade as those belonging to OfficeTrack, which is especially marketed toward telecommunication firms. OfficeTrack is an application promoted as a workforce management solution developed by OfficeCore, a software company that helps users manage administrative tasks. In several instances, we saw URLs ending in "lbs" and "LbsAdmin," references to the application's former name (OfficeCore's LBS System) before it was rebranded to OfficeTrack **(Figure 18)**.

Throughout our analysis of the ShroudedSnooper implants, the adversary used multiple URLs consisting of patterns mimicking provisioning services from telecommunications companies, including an Israeli telecommunications provider, likely to blend into typical network traffic. The DLL-based variants of HTTPSnoop usually rely on DLL hijacking in benign applications and services to get activated on the infected system, which was highlighted as a top technique this year in earlier sections of this report.



Industry actions likely affected MuddyWater operations

In late 2022, it was first reported that Iranian-backed APT group MuddyWater was using the Syncro remote management tool to take over target devices. This activity is consistent with Talos IR data from Q4 2022 (October - December 2022), where a growing number of adversaries were increasingly relying on Syncro, observed in nearly 30 percent of engagements.

In December 2022, Syncro released a statement addressing concerns about MuddyWater's deployment of Syncro in spear phishing campaigns targeting organizations in the Middle East and Asia. The company implemented additional verification measures for new trial account creation to limit the use of Syncro by illegitimate actors, and monitored for irregular account information and usage, terminating accounts that violate these new policies.

This swift action taken by Syncro most certainly has had an impact on MuddyWater operations, highlighting the direct effect industry can have on thwarting components of advanced adversaries' operations. While the reason for Syncro's increased usage in Q4 2022 was unknown, its use as a fully featured remote access platform for managed service providers (MSPs) and its ubiquity across enterprise environments likely made it an attractive option.

"This swift action taken by Syncro most certainly has had an impact on MuddyWater operations, highlighting the direct effect industry can have on thwarting components of advanced adversaries' operations."

Syncro leveraged to maintain access

In an incident affecting a telecommunications company, Talos IR identified company email accounts sending phishing emails with subject lines that translated from Arabic to "Staff Promotion." The emails contained OneDrive and OneHub phishing links with a compressed Microsoft Windows Installer (MSI) file that installed Syncro. The adversary used Syncro to stay connected to the targeted user's workstation. During analysis of the MSI file, multiple Syncro services were also installed, including SyncroRecovery (SyncroLive) and SyncroOvermind. The adversary's tactics appeared to focus on maintaining initial access through installation of Syncro. The lack of MFA for email access allowed the adversary to perform phishing attacks, highlighting the need to ensure MFA across all critical assets.

CISCO TALOS

YEAR IN REVIEW

2023

Commodity loaders

Section highlights

- Commodity loaders such as Qakbot, Ursnif, Emotet, Trickbot and IcedID represent some of the most impactful and pervasive threats, as actors routinely rely on them to enable key parts of their operations. Their use as downloaders for information-stealers, ransomware, and other malware have made them mainstays in the threat environment, indiscriminately affecting entities globally.
- All these loaders formerly functioned solely as banking trojans, and developers have diversified their capabilities in recent years to support more advanced operations. In 2023, new versions of IcedID, Ursnif, and Qakbot appeared to be tailored specifically for ransomware actors, based on their enhanced reconnaissance features, removal of functions that might trigger antivirus detections, and quick adoption by ransomware groups and initial access brokers.
- Microsoft's disabling of macros by default caused commodity loader actors to invent new ways to use macros undetected or avoid using them entirely. Qakbot operators used a wide variety of file types, scripting languages, packers, and exploits to deploy the loader. Emotet, IcedID, and Ursnif varied their techniques, although less frequently compared to Qakbot, and also tended to still rely on older TTPs.
- It can be challenging to eradicate the threat of commodity loaders even after the botnet is dismantled, as developers have been known to continue operating on behalf of different malware groups or rebuild their botnets. Furthermore, previously compromised infrastructure could be leveraged by other threat actors for malicious activity.

Actors have consistently relied on commodity loaders for years, and 2023 was no different. Many of these threats are widely available for purchase on underground forums, provide a low barrier of entry for unsophisticated actors, and are highly modular, allowing threat actors to carry out multiple phases of an attack. Throughout 2023, Qakbot, Ursnif, Emotet, Trickbot and IcedID stood out as the most impactful threats in this space.

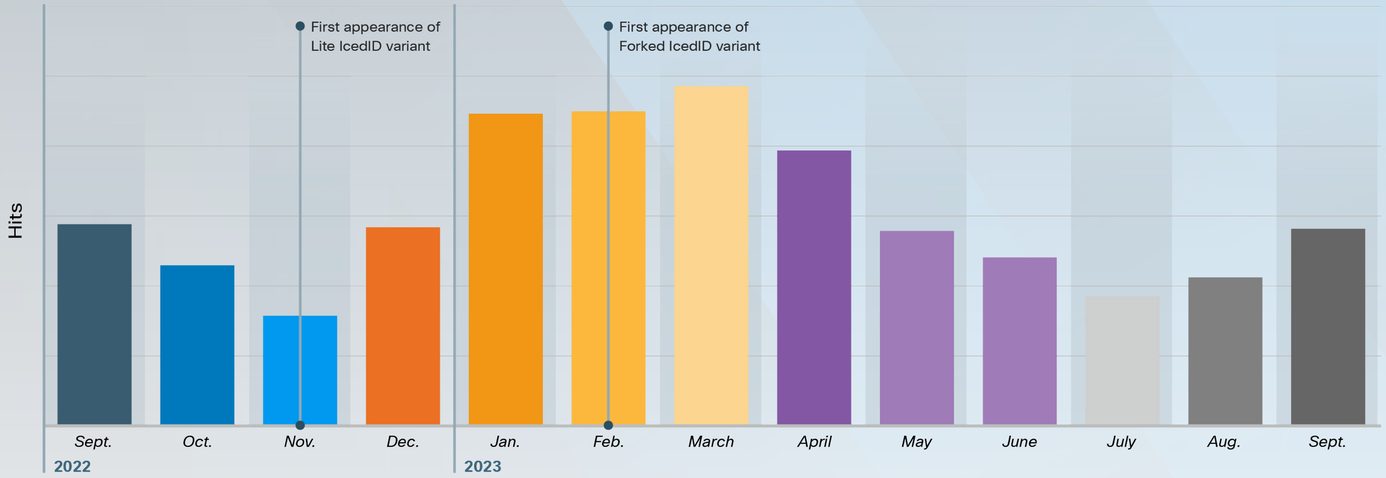
Commodity loaders' updates seem tailored to support ransomware activity

In late 2023, we observed the latest variants of IcedID and Ursnif, and a new automated feature in Qakbot, supporting ransomware deployment, following a trend of commodity loaders playing an integral part in the ransomware infection chain. These updates were tailored to enhance the malware's dropper functionalities, likely signifying a further shift away from their original intended use as banking trojans. Trickbot and Emotet are also known to facilitate ransomware attacks, however, they did not receive similar upgrades in 2023.

In November 2022 and February 2023, IcedID developers released two new versions that were stripped of their banking functionalities and designed to solely function as droppers. In 2023, these versions, dubbed "Forked" and "Lite," were used by initial access brokers, known for commonly selling network accesses to ransomware groups. While the original version was also used by initial access brokers and ransomware groups, the new versions are likely a more attractive option because they were stripped of functions that might trigger AV signatures, thereby making them stealthier. IcedID activity increased between November 2022 and February 2023—corresponding with the new versions' release—suggesting actors were keenly interested in trying out the threat's latest capabilities **(Figure 19)**.

FIGURE 19

IcedID activity increased around release of the new variant



The latest Ursnif variant, which was similarly retooled to exclude banking trojan functionality, was also seemingly intended to support ransomware deployment. In 2023, this updated version (released in 2022) was adopted by the prolific ransomware group Royal, the first instance of any ransomware gang incorporating Ursnif into their operations. Since Royal is the only group that has been observed leveraging this new variant, there may be a professional association between the developers. Royal is a group of sophisticated cyber criminals first active in September 2022, and suspected by many security professionals to be a rebrand of the prolific Russian ransomware group Conti. Royal tightly controls their malware and ransomware operations, unlike many other ransomware groups that arose in the last two years who chose to operate as a RaaS. Therefore, an exclusive partnering of the new Ursnif variant and Royal is likely intentional and could imply an affiliation between the developers.

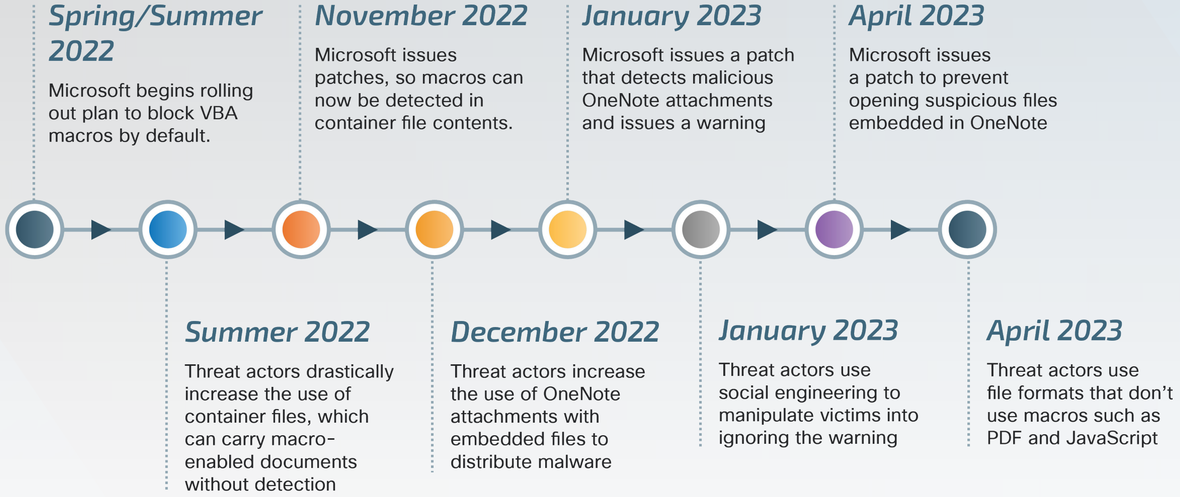
Finally, in late 2022, Qakbot deployed several new automated features, including a capability ideally suited to helping ransomware groups determine valuable targets prior to deployment. The updates included a list of reconnaissance commands to map out the customer's environment upon initial infection. The output of these commands enumerated data that would be most useful to ransomware groups, including domain groups, the domain name, and names of domain controllers. This information could assist with lateral movement resulting in Active Directory takeover, a tactic commonly used by ransomware groups. Qakbot's new automated reconnaissance capabilities also may have helped ransomware groups evade detection, because the gathered data could be used to formulate a detailed plan of attack, minimizing the time between initial infection and encryption.

Commodity loader operators evolved TTPs in response to new security updates blocking macros, continuing a trend that began in mid-2022

In 2023, Microsoft blocked macros by default, a notable change that caused actors to modify their initial access and malware delivery techniques. Prior to the change, macros would run automatically when Microsoft Office documents were opened. Macros have been heavily abused by threat actors to execute malware automatically when a victim clicks on a malicious attachment in a phishing email. Now, the user receives a security warning if they click on a potentially malicious attachment, reducing the likelihood of downloading malware. Microsoft's disabling of macros continued to have an impact throughout 2023, as threat actors invented new ways to use macros undetected, or to avoid using macros entirely. When Microsoft created a new patch to update security features, threat actors were able to quickly change their TTPs in a game of cat-and-mouse **(Figure 20)**.

FIGURE 20

Commodity loaders allow threat actors to quickly change TTPs in response to changing security features



Sample reconnaissance commands we observed deployed by Qakbot affiliates in 2023

Threat actors conduct reconnaissance to gather information for additional operations. We observed Qakbot affiliates abusing common Windows utilities that allow for command execution in an attempt to hide among legitimate activity. Below are just a few examples to demonstrate the potential harmful impact of these commands.

Netstat -nao: Used to obtain a list of open ports that are particularly vulnerable to malicious attacks and a list of active connections between the infected host and other systems, such as a cloud environment, to determine whether the victim can access data that is of value to the threat actor.

Net localgroup: Used to identify administrator accounts (i.e., accounts with elevated privileges that can access sensitive data and make changes to the system). This information helps a threat actor know which accounts to prioritize in their targeting efforts.

Arp -a: Used to display the ARP cache, a record of each IP address and its corresponding MAC address that made a connection to the infected host. With this information, an attacker can position themselves between the communication of two or more networked devices to steal additional data or manipulate transmitted data.

In a trend that began in 2022 and continued throughout 2023, adversaries using commodity loaders repeatedly changed their TTPs in response to new Microsoft security updates. In November 2022, Microsoft issued two patches to detect and block macros-enabled content within container files, such as ZIP and LNK, which had been a popular method for surreptitiously using macros. Just a few weeks later, we observed a surge in threat actors, including those using Qakbot, Emotet and IcedID using OneNote file attachments to deploy malware. While using OneNote to deliver malware was not a new technique, it facilitated delivery of macros-enabled documents without being detected, which is highly favorable among affiliates wishing to bypass AV detection **(Figure 21)**.

Then in January, Microsoft quietly issued an update, so all macros-enabled documents embedded within OneNote files would be blocked by default, meaning the user would receive a security warning when opening a OneNote attachment embedded with macros. We still saw threat actors using OneNote, but with crafty social engineering techniques that manipulated victims into ignoring the warnings. In one observed campaign deploying IcedID, the threat actor used a DocuSign lure to trick the victim into clicking a button with an embedded link. The "Decrypt and View Message" button actually contained a malicious HTML Application (HTA) file **(Figure 22)**. When opened, the HTA file was dropped into the OneNote directory for execution.

FIGURE 21

Sample infection chain using OneNote with an embedded macro-enabled file to deliver malware

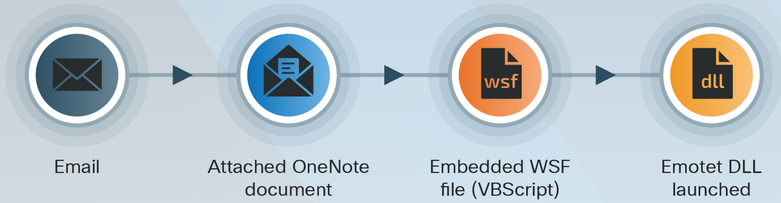


FIGURE 22

Sample infection chain attempting to manipulate victims into ignoring a security alert

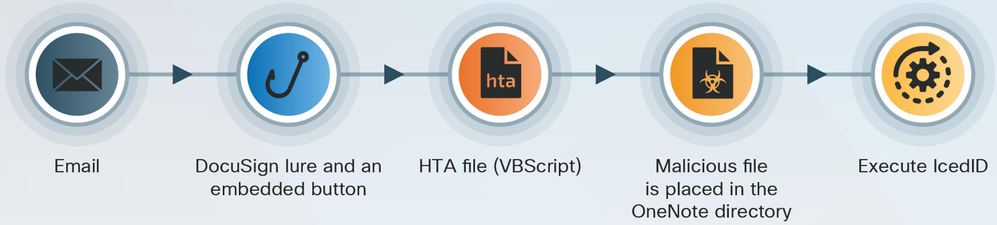


FIGURE 23

Sample infection chains that do not rely on macros

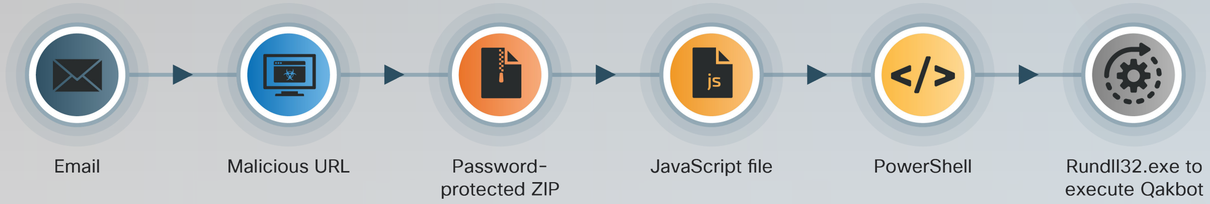
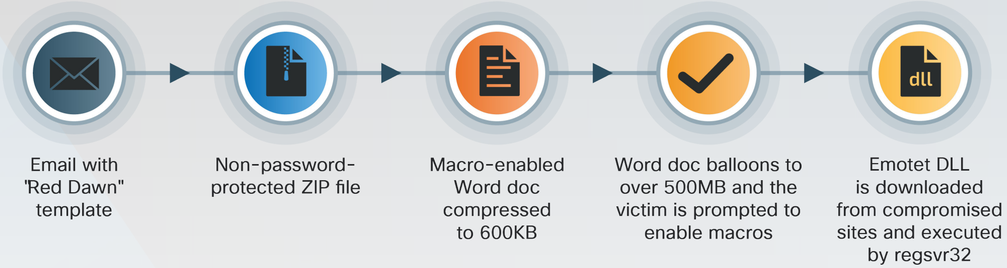


FIGURE 24

Emotet infection chain using binary padding



Finally, in April 2023, Microsoft issued another update that blocked users from opening files with a potentially dangerous extension embedded in OneNote. To open an attachment marked as potentially dangerous, OneNote users would need to save the file to their device and open it from there, allowing security applications running on the device to detect any malicious code in the attachment. This latest update caused many operators to abandon OneNote as a method to hide the use of macros. Instead, we observed actors turning to filetypes that execute malware without relying on macros, such as JavaScript files which rely on LoLBins for execution **(Figure 23)**.

Aside from OneNote, threat actors also experimented with other methods of deploying malware that did not rely on macros or could use macros without detection. Since at least December 2022, we have observed threat actors co-opting the Google Ads platform to deploy malware such as Ursnif, IcedID, and Trickbot, a method that completely avoids using macros. The attack chain in these campaigns begins with a user entering a search term for a software or service in the Google search engine. Once Google's results page loads, the malicious ads will typically be first in the list of results, as the actors have been observed using search engine optimization (SEO) to increase visibility. If the user clicks on the malicious ad, a Google Ad services URL will be generated, which then generates a secondary URL that leads the user to the malicious, spoofed domain with download links that deliver the various threats. Talos observed legitimate software products spoofed in these campaigns, such as Microsoft Teams and WhatsApp, and popular password managers like 1Password. Threat actors' use of Google Ads and Google Search makes their lures appear highly legitimate, as users are probably less likely to question the authenticity of paid advertisements prioritized at the top of their search results.

While many affiliates introduced new TTPs in 2023 in response to evolving security updates, we also observed commodity loaders using older methods. For example, Emotet, IcedID, and Ursnif were all observed using macros-enabled Office documents in the initial infection chain. Furthermore, we observed Emotet being delivered in phishing emails with old "RedDawn" templates first seen in 2020 **(Figure 24)**. While these operators may be capable of more sophisticated attacks, it's possible they have still found success using older TTPs, especially against unpatched, enterprise legacy systems.

Top five commodity loaders are similarly deployed against sectors globally in mass opportunistic campaigns

In 2023, we observed all five commodity loaders impacting businesses worldwide, primarily affecting North America and Europe **(Figure 25)**. These geographical targets do not necessarily reflect a coordinated preference among operators because the threats are sold as a malware-as-a-service (MaaS). Therefore, patterns in targeting are aligned with whatever group is executing the campaign and can vary.

We predominantly observed mass spam campaigns that opportunistically attempted to compromise vulnerable targets, likely with the intent to move laterally towards a more hardened target after the initial infection. Adversaries will typically tailor phishing lures for the targeted geography. For example, in 2023, we observed Ursnif predominantly deployed against businesses located in the U.S. and Italy in mass "spray and pray" spam campaigns using the languages of the targeted countries.

We have observed loaders primarily deployed against businesses, as opposed to targeting individuals' financial data, a shift that occurred as the malware was less frequently used as banking trojans. This is reflected in the phishing lures we observed. For example, in late-March, we saw an uptick in Emotet targeting U.S. businesses that pay quarterly taxes. The lures used themes related to the Internal Revenue Service (IRS) with subject lines such as "IRS Tax Forms W-9," which was also seen last year at the end of the November 2022 business quarter. W-9 forms are typically distributed by companies or financial institutions to their employees.

FIGURE 25

World map of regions impacted by commodity, from most to least targeted

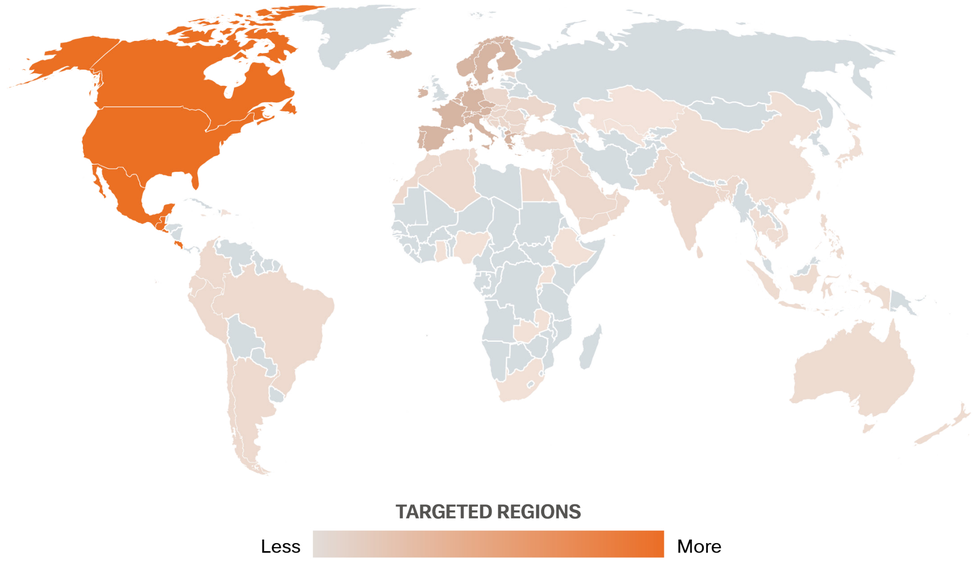
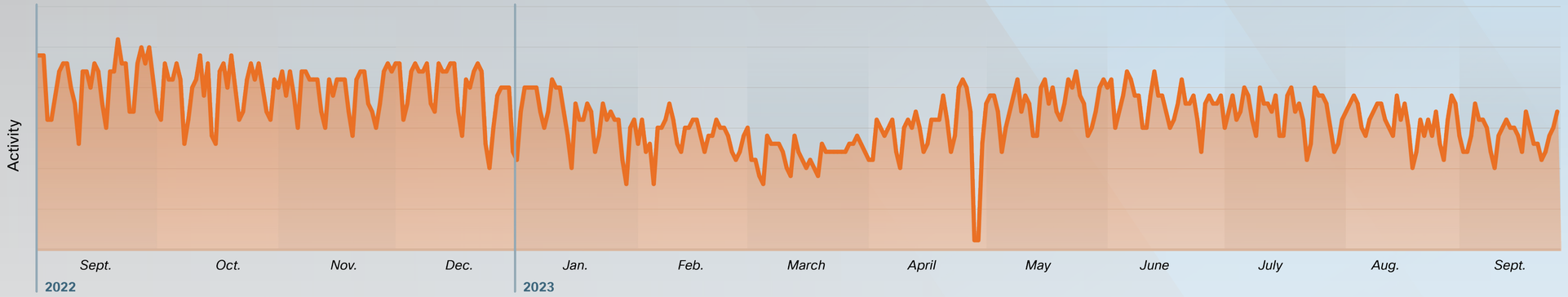


FIGURE 26

Trickbot activity over time



Threats from commodity loaders can persist long after their botnets are dismantled

In August 2023, the prolific Qakbot commodity loader was disrupted in a major global law enforcement operation, but dismantling botnet infrastructure does not always mean cybercriminals cease to operate. Going forward, it's possible Qakbot may reemerge after a several-month hiatus — as we have seen in similar scenarios involving other loaders like Emotet — further underscoring the need to monitor and report on this threat. Notably, the threat actors behind Qakbot were not apprehended during the global takedown, and our latest findings indicate they are still active—albeit delivering different threats – leaving open the possibility that they rebuilt the Qakbot botnet or rebrand themselves under a different name.

We have seen other malware developers also continuing to operate in the cyber threat landscape after their botnets were dismantled. For example, even after Trickbot took down its infrastructure in February 2022, the U.S. and UK still sanctioned the developers in February and September 2023, implying they are still active in the cyber threat landscape. The developers may have chosen to create other types of malware, or work with other groups they have had longstanding relations with, such as Emotet and Conti. In 2022, a series of leaks revealed close professional relations between developers of Trickbot and Conti and in 2021, Trickbot lent portions of its infrastructure to help rebuild the Emotet botnet.

Even if threat actors opt to cease cybercriminal activity, we may still observe zombie activity from infected Qakbot devices. We have seen this from Trickbot, where our telemetry picked up activity throughout 2023 even though their infrastructure was dismantled in February 2022. This is likely due to old infections that have yet to be remediated or threat actors leveraging previously compromised infrastructure. Looking at Trickbot activity over the past year, we can see it hovered around the same median number, supporting our assessment that the botnet is still active in some capacity, but the developers are not actively engaged in growing the botnet **(Figure 26)**. Any new campaigns or infrastructure, such as IPs or C2 servers, would likely be represented in the charts above by a more dramatic spike or irregular patterns.

Meanwhile there are always new commodity loaders to replace formerly prolific botnets like Qakbot and Trickbot. For example, IcedID may be a logical choice to fill the void left by Qakbot. There is a historical precedence, as IcedID attracted affiliates after Emotet was dismantled in 2021. Furthermore, many Qakbot affiliates are likely already familiar with IcedID because there are numerous instances of the two being deployed together as part of the same campaign. Finally, the recent advanced IcedID update shows the developers are capable of, and motivated to, maintain a high-quality product.