



 | TALOS

2022 **YEAR IN** **REVIEW**





INTRODUCTION

Welcome to the inaugural Cisco Talos Year in Review. This report represents an unprecedented effort within Cisco to tell a comprehensive story of our work in the past year, relying on a wide variety of data and expertise.

As a large security organization with global reach, the data we use as the basis for our research presents us with both a gift and a curse. The gift lies in the diversity of inputs, ranging from endpoint detections, incident response engagements, network traffic, email corpus, data from our sandboxes and honeypots, and much, much more from customers all over the world. The curse is that with the multitude of telemetry we have access to and the urgency of some of the work we do, it can be difficult to take a step back and look at the bigger picture, like trying to make sense of a Monet with your nose up against the frame.

This is what inspired us to create the Cisco Talos Year in Review. We wanted to get insight from dozens of subject matter experts all throughout Cisco, including our reverse engineers, detection specialists, data scientists, linguists, managed hunt providers, incident responders, and threat intelligence analysts. To this diverse group, we posed a few key questions:

1. What were the major security events Cisco responded to in 2022 and what is their current status and impact?
2. What are the major trends in the threat landscape and what do we think may change?
3. What are the top threats we observed in 2022 and what is their current state?

This report tells a story based on responses to these questions from our experts and their year-long data. Through the upcoming weeks, we will be highlighting different aspects of this story, including our efforts in Ukraine, the disastrous Log4j vulnerabilities, adversaries' use of offensive frameworks and software native to the victim's machine, shifts in the ransomware landscape, the ever-present threat of commodity loaders/trojans, as well as an overview of some of the advanced persistent threats (APTs) we are most concerned with. Throughout the story, one key theme is clear: adversaries are adapting to shifts in the geopolitical landscape, actions from law enforcement, and the efforts of defenders. Defenders will need to track and address these shifts in behavior in order to maintain resilience.

We expect this data-driven story will shed some insight into Cisco's and the security community's most notable successes and remaining challenges. In addition, as these Year in Review reports continue in the future, we aim to provide data and narratives that help explain how the threat landscape changes from one year to the next. We hope you find this report as elucidating to read as it was to research and write, and that it arms the security community with the information and context needed to continue fighting the good fight.



TABLE OF CONTENTS

MAJOR EVENTS

Ukraine

A strategic overview of Ukraine’s threat landscape since the start of the war, from cyber criminals and Russia-aligned threat actors to nation-state activities. Specific telemetry findings give insight into top threats and trends 5

Log4j

Log4j exploitation attempts was one of the most common threats affecting Cisco customers in 2022. In this section, we look at the ongoing threat to organizations based on our historic telemetry and incident response data 14

THREAT LANDSCAPE

Review of the general threat landscape in 2022

An overview adversaries’ continued use of dual-use tools, living-off-the-land-binaries (LoLBins), and the reemergence of older techniques like USB attacks..... 19

Ransomware threat landscape

Review of the increasing "democratization" of ransomware, a top threat this year, along with the most affected industries..... 28

Commodity loaders

Insight into the four most active commodity loaders observed: Qakbot, Emotet, IcedID and Trickbot, despite several takedown efforts..... 37

ADVANCED PERSISTENT THREAT ACTIVITY

Advanced persistent threats

A highlight of our most significant APT findings from state-sponsored actors in Russia, China, Iran, North Korea and more..... 50

Conclusion 65

 | TALOS

2022 **YEAR IN REVIEW**

UKRAINE





Figure 1. Current Cisco support for Ukrainian critical infrastructure and government partners since the beginning of the Russia-Ukraine war.

UKRAINE

Talos’ ongoing support for Ukraine has been a large focus of our operational efforts this year. Driven by our core mission of protecting the Ukrainian people and infrastructure from cyber attacks, our work has also enhanced our knowledge of the Russian adversary and wartime cyber threat landscape—information that will inform and enrich our analysis, defenses, and strategies for addressing similar crises in the future. In this section, we look back on our Ukraine-related work from 2022 and provide some strategic takeaways about the threat landscape and adversary behavior, based on Cisco telemetry, Cisco Talos Incident Response (CTIR) data, and case studies from our ongoing internal Ukraine task unit.

TASK UNIT DRIVES TALOS’ UKRAINE SUPPORT, SERVES AS MODEL FOR FUTURE CRISIS RESPONSE

In the weeks and months leading up to Russia’s February invasion of Ukraine, [Cisco Talos quickly spun up a vast effort](#) to support our Ukrainian friends and partners. This effort was unprecedented in scope and pace, as we rapidly expanded our Ukraine coverage, deployed and managed Cisco security products on new Ukrainian endpoints, and refocused parts of our workforce to surge their monitoring and detection capabilities in support of this effort. Much of this work continues today as part of an ongoing, comprehensive wartime effort to protect the people of Ukraine and enhance the resilience of Ukrainian organizations.

As part of this work, we developed an internal Ukraine task unit that has become a prototype for how we can respond to future global events that are likely to have significant, ongoing cyber implications (**Figure 1**).



Figure 2. Major cyber attacks against Ukraine.

The task unit is comprised of about 45 volunteers from across the Talos organization, including threat hunters, malware reverse engineers, incident responders, data scientists, and others. These experts monitor around 30 Ukraine-based Cisco customers from various critical infrastructure sectors, providing critical support while also gathering information that has been instrumental to enhancing our knowledge of the adversary and wartime cyber threat space. Our observations from the task force helped inform this section of the report.

UKRAINE THREAT LANDSCAPE SEES DIVERSE SET OF ACTORS, THREATS

Since the start of the war in February, we have [observed](#) an unprecedented number of adversaries—driven by different motivations and of varying skill levels—clustered in the same threat landscape. This level of activity is in some ways familiar for Ukraine and its allies, as the country has been defending itself from a variety of sophisticated cyber attacks since at least 2014 (Figure 2). The variety of actors involved in this most recent conflict has presented a diverse set of challenges for customers, partners, and defenders who have had to respond to ongoing changes in adversary tactics, techniques, and procedures (TTPs), new and evolving threats, and difficulties attributing activity to specific groups. This diverse set of actors has remained active throughout the year.





Cybercriminals, wiper malware, and APTs were quick to enter the threat landscape

Cybercriminals, known for being highly opportunistic, are a mainstay in this threat space. Since the beginning of the war, we have [observed](#) threat actors sending email lures with themes related to the conflict, including humanitarian assistance and various types of fundraising (**Figure 3**). These emails are primarily used for scam activity but have also delivered a variety of threats, including remote access trojans (RATs). This pattern is consistent with what we typically see following global events or crises, such as the COVID-19 pandemic, when opportunistic cybercriminals attempt to exploit high public interest for their own gain, underscoring their adaptability.

We also [observed](#) cybercriminals attempting to exploit Ukrainian sympathizers by offering offensive cyber tools to target Russian entities that were in fact malware. In one such instance, we observed an actor named “disBalancer” offering a purported distributed denial-of-service (DDoS) tool, “Liberator,” on Telegram to attack Russian propaganda websites (**Figure 4**). The downloaded file is actually an information stealer that infects the unwitting victim with malware designed to dump credentials and harvest cryptocurrency-related information.

State-sponsored threat actors and other sophisticated adversaries have also been highly active throughout the war. The Russian state-sponsored advanced persistent threat (APT) Gamaredon, for example, has been a major player. The group has historically targeted predominantly Ukrainian entities—particularly those responsible for the country’s defense, diplomacy, and internal security—and those activities have only increased since Russia’s invasion in February. In September, we identified a new [Gamaredon campaign](#) infecting Ukrainian users with custom information-stealing malware that can exfiltrate victim files of interest and deploy additional payloads. We also discovered likely Russian state-sponsored actors deploying a modified version of the [GoMet](#) open-source backdoor against a Ukrainian software

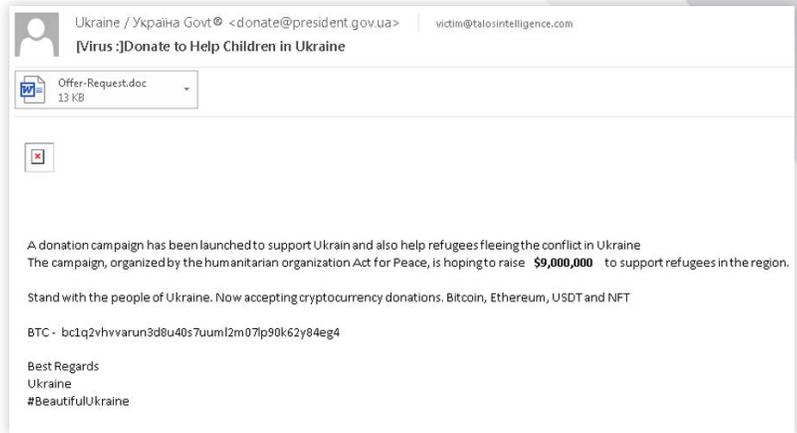


Figure 3. Malspam message themed as humanitarian aid request for Ukrainian refugees.

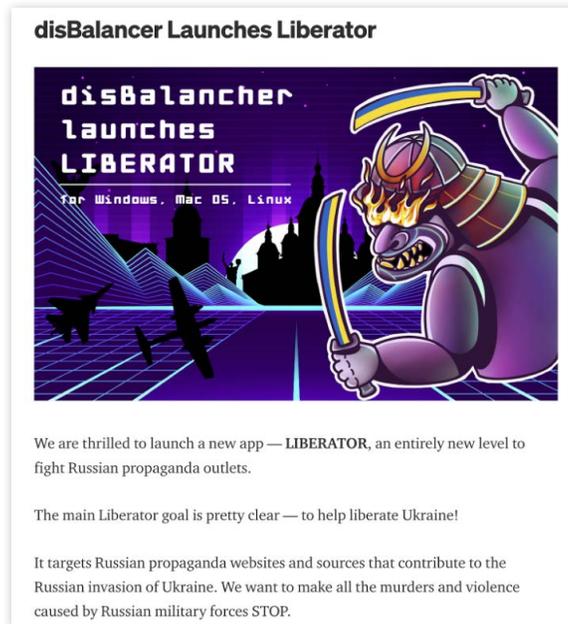


Figure 4. Screenshot showing disBalancer’s “Liberator” advertisement.



As the war wages on, we are seeing new groups emerge motivated by clear political objectives, highlighting the dynamic threat space and continued impact of geopolitical events on the cyber landscape.

company. This was possibly an attempted supply chain attack, as the target’s software is widely used by Ukrainian government entities and the malware was designed to establish persistent access.

We also saw other sophisticated actors leverage the war to their advantage, often by creating themed lures to deliver malware to victims. Corresponding with Russia’s invasion in February, the China-based threat actor [Mustang Panda](#) began conducting phishing campaigns against European entities, including Russian organizations. Some phishing messages contained malicious lures masquerading as official European Union (EU) reports on the war and its effects on North Atlantic Treaty Organization (NATO) countries. Other phishing emails delivered fake "official" Ukrainian government reports, both of which download malware onto compromised machines.

We have discovered or analyzed countless other threats that, while unattributed to specific actors, highlight the variety of adversaries and malware that persist in this threat landscape. Leading up to and immediately following Russia’s invasion of Ukraine, threat actors began deploying a variety of destructive wipers and other malware against Ukrainian targets, including [WhisperGate](#), [HermeticWiper](#), [CaddyWiper](#), [DoubleZero](#), and [CyclopsBlink](#). Some of these threats were likely deployed by state-sponsored adversaries, based on our analysis and U.S. government [reports](#). More recently, Talos’ internal Ukraine task unit has identified a wide variety of threats affecting our Ukrainian partners. These range from common threats like the IcedID commodity loader and Sality malware to more sophisticated, targeted threats like WannaCry ransomware, Industroyer2 destructive malware, GrimPlant backdoor, and GraphSteel information-stealer.

Russia-aligned actors target NATO countries

As the war wages on, we are seeing new groups emerge motivated by clear political objectives, highlighting the dynamic threat space and continued impact of geopolitical events on the cyber landscape. One such adversary is Killnet, a hacktivist group that conducts distributed denial-of-service (DDoS) attacks in support of pro-Russian interests. The group has been active since February 2022—coinciding with the start of the war—and has garnered media attention for a spate of attacks against Western nations, including several U.S. states and major U.S. airports.

The group launched its first DDoS attacks against two dozen Ukrainian government websites in response to the Anonymous hacktivist group targeting Russian entities. Over the next several months, Killnet quickly began targeting websites of pro-Ukraine countries, including Poland, Norway, Lithuania, Italy, Romania, Estonia, and Japan. Killnet attacked Lithuania, for example, in response to the country blocking the transit of goods to Russia. The DDoS attacks have been targeted at various



government websites that typically affect multiple services and operations, such as Ministries of Defense, transportation, banking, and police.

While Killnet’s operations have so far been limited to disruptive attacks, there are some indications that the group may look to expand its attack arsenal going forward. Earlier this year, Killnet reportedly sought to recruit ransomware gangs to attack entities on their behalf, suggesting that they may develop their own variant or purchase one from an underground market to conduct more destructive attacks. Additionally, Killnet reportedly leveraged the Mirai botnet to scale their attack capabilities earlier this year, further highlighting the group’s interest in expanding their malware arsenal.

Killnet’s offensive operations are unsophisticated and do not leverage custom tools or malware. Victims are often able to recover quickly from the DDoS attacks, suggesting that Killnet is more intent on garnering media attention for their cause rather than inflicting maximum damage or disruption against their targets. Killnet’s decentralized structure, fervent Russian nationalism, and high-profile victims suggest that countries or organizations perceived to be pro-Ukraine or anti-Russia are viable targets in the months ahead.

TELEMETRY REVEALS TOP THREATS, ACTIVITY TRENDS SINCE BEGINNING OF WAR

Based on a review of our endpoint telemetry between January and September, we gained unique insights into historic threat trends since the start of the conflict. These findings are based on Behavioral Protections (BP) data, which is an engine in Cisco Secure Endpoint that detects and blocks malicious activity based on rules that we write. Based on this data, we derived a list of the top 10 most active BP signatures across Ukrainian entities customers and partners (Figure 5).

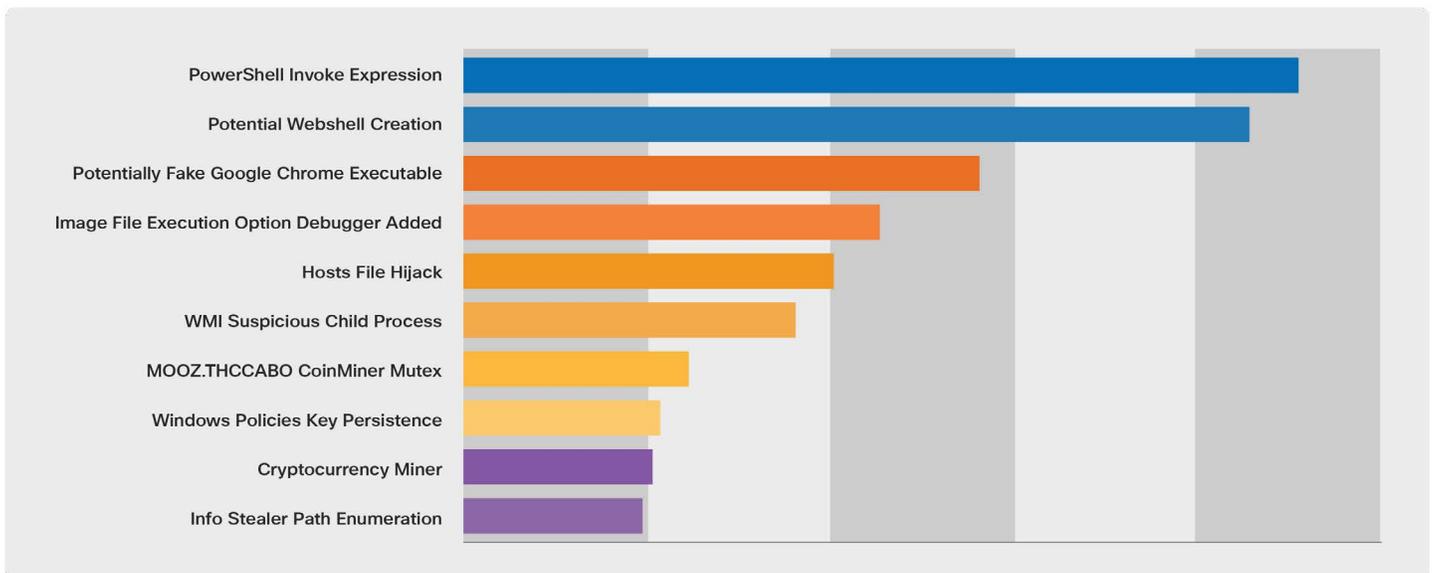


Figure 5. Most active Behavioral Protections rules from Cisco Secure Endpoint across Ukrainian customers where Cisco Secure Endpoint has been deployed.



Given that this data displays total counts rather than unique endpoints, one or several endpoints could have been firing on the same BP for days or weeks at a time. Still, the graph sheds light on some of the utilities (PowerShell, WMI), techniques (use of Windows Policies Keys to establish persistence and fake Google Chrome executables), and malware (information stealers and cryptocurrency miners) that were prevalent so far during the war. The top offender, “Potential WebShell Creation,” could allow an attacker to control a victim machine via a webUI. That would rely on the victim machine being accessible over HTTP(s) ports, which implies the affected endpoint is a server and not an individual user’s desktop or laptop. The top two most active BPs, “Potential WebShell Creation” and “PowerShell Invoke Expression,” also alerted on the first and second highest number of total days, respectively, meaning that their prevalence is further indicated by the frequency with which we observed them over time.

Upon reviewing results from our Exploit Prevention data, which is another Cisco Secure Endpoint detection engine similar to BPs, we see that the number of detections for the “Signed binary proxy execution using rundll32” signature steadily increased beginning in May (**Figure 6**).

This activity is an exact match to the MITRE ATT&CK technique “System Binary Proxy Execution: Rundll32” (T1218.011). Adversaries use this technique for defense evasion by abusing “rundll32.exe” to proxy execution of malicious code. This helps them avoid triggering security tools that may not monitor execution of the “rundll32.exe” process because of allowlists or false positives from normal administrative operations. Rundll32 is also commonly associated with executing DLL payloads. Interestingly, this technique is also becoming increasingly common during attacks across all customers globally, based on our telemetry (**Figure 7**). According to [MITRE](#), a variety of threat actors are known to use this technique, including Russia-linked groups Gamaredon, APT28, and APT29.



Figure 6. rundll32 detections across Ukraine customers.

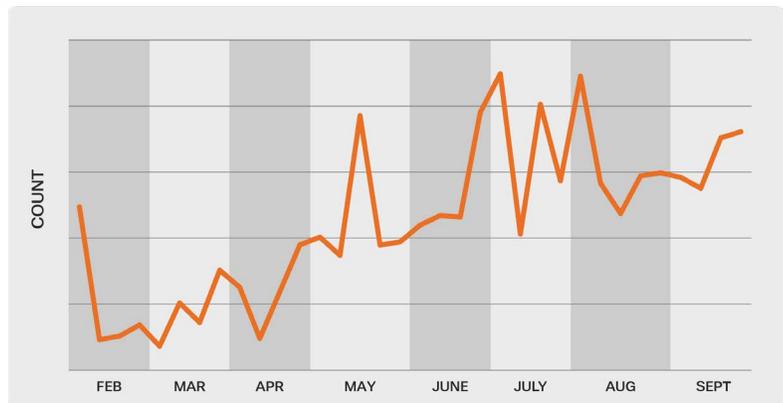


Figure 7. rundll32 detections across all Cisco customers.

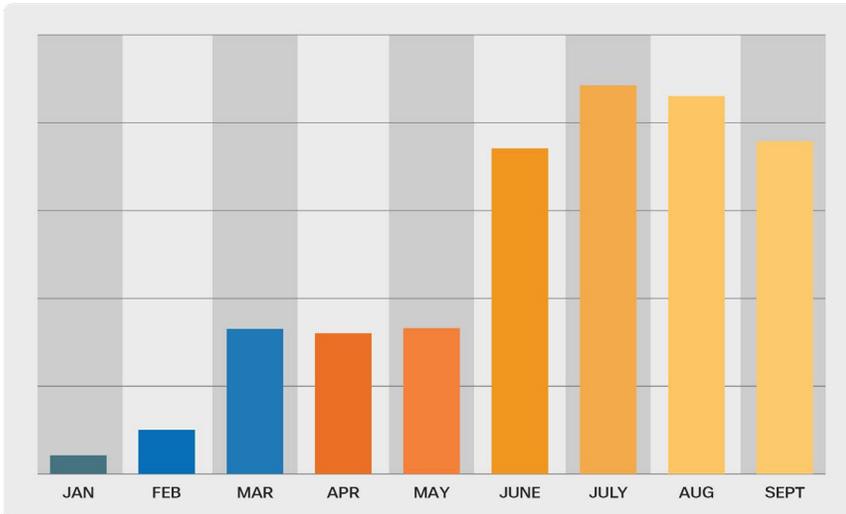


Figure 8. Total number of Behavioral Protection alerts across Ukrainian customers showing increases in activity in March and June.

39.175.68[.]100	192.241.221[.]160
207.249.96[.]145	128.14.225[.]243
128.1.42[.]231	117.208.234[.]11
45.83.192[.]134	152.32.200[.]79
103.178.237[.]134	143.244.135[.]246
85.198.141[.]6	61.52.46[.]172
31.43.190[.]200	167.172.69[.]26
206.189.37[.]136	152.32.153[.]235
185.218.200[.]1	178.128.103[.]166

Figure 9. Attacker IPs targeting Ukrainian entities based on custom detections

Looking at this data more broadly, we also see that there was a gradual uptick in BP detections across Ukrainian organizations since the start of the war (**Figure 8**). Activity between March and May stayed consistent, then dramatically increased in June, where it has remained consistently high.

Custom, native detection system yields new attacker IPs

When the war started and we began surging efforts to protect the Ukrainian people, we developed several new custom detection systems to help us better identify suspicious activity and potentially targeted attacks. One of those systems allows us to detect unique IP addresses that are targeting Ukrainian entities. IPs are flagged when they exceed a certain targeting threshold, as set by our data scientists. This list is then manually confirmed as malicious and the remaining IOCs are subsequently blocked.

Figure 9 shows a list of attacker IP addresses we have identified based on this detection system that have not been previously reported. All IPs have been blocked in Cisco security products.

INITIAL DROP IN TALOS IR OBSERVED THREATS SUGGESTS THREAT ACTORS FOCUSED ON RUSSIAN, UKRAINIAN TARGETS

In addition to our telemetry indicating that threat activity directed at Ukrainian entities has remained high over the last several months, our Cisco Talos Incident Response (CTIR) data also suggests that threat actors have been focused on the Russia-Ukraine attack space since the start of the war. Our incident responders observed fewer threats affecting Cisco customers in the first half of 2022. Threats like ransomware, information stealers, commodity malware, and exploitation of known vulnerabilities were notably lower between February and June, corresponding to the early months of the war. The volume of CTIR-observed threats returned to near-normal numbers around July.



While it's impossible to determine a direct cause for this drop, we assess that the Russia-Ukraine war likely played a key role. Many threat actors who would have traditionally been targeting entities across various geographic regions and sectors likely shifted their attention to pro-Russia or pro-Ukraine cyber efforts. This assessment is supported by the variety of threat actors and heightened activity we are seeing in the region, as detailed earlier in this report. Russia's invasion and harsh war tactics have drawn strong reactions from both pro-Russian and pro-Ukrainian supporters. This was reflected in the cyber landscape early on in the conflict, when we saw an influx of actors enter the Russia-Ukraine theater in support of both sides. This surge of interested actors reveals how the complex geopolitical environment can influence threat actor behavior.

In addition to shifting adversaries' attention away from traditional targets, the war has also caused conflict and infighting within different threat groups that may also have contributed to the early decline. Following Conti's public declaration of support for Russia, a disgruntled affiliate leaked the ransomware group's playbook that contained valuable operational information. A wave of distributed denial-of-service (DDoS) [attacks](#) in August and September caused operational and security challenges for several ransomware groups, discussed in more detail later in the report, likely further diverting their attention away from traditional operations.

CONCLUSION

We assess that the threat to Ukrainian and allied government and private sector entities will remain high throughout the duration of the war. Our telemetry, task unit findings, and threat hunting discoveries show no indication that the threat activity level against Ukrainian organizations is slowing down. While the variety of threats facing these entities will likely continue to vary, we assess that more destructive attacks are particularly more likely to occur given Russian adversaries' past preference for—and success in—deploying wiper malware against Ukrainian entities since 2014. As Russia doubles down on its objectives to occupy and annex portions of Ukraine, and as Moscow shows a consistent willingness to carry out dramatic, high-impact kinetic attacks against civilian and critical infrastructure entities, we judge that Russian cyber threat actors will similarly conduct aggressive and brazen attacks as necessary to affect the outcome of the war. Furthermore, we assess that the potential for increased cyber threat activity will likely continue past any future kinetic ceasefires on the battlefield.

The potential for increased cyber threat activity will likely continue past any future kinetic ceasefires on the battlefield.

 | TALOS

2022 **YEAR IN REVIEW**

LOG4J





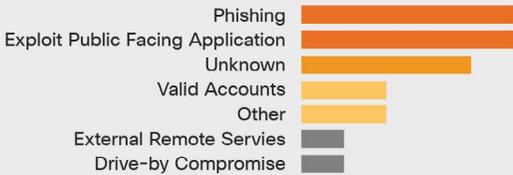
LOG4J

In [December 2021](#), the notorious vulnerabilities affecting the common Log4j library in Apache software were disclosed, kicking off an ongoing, months-long effort by Talos to mitigate associated threats. Due to organizations' widespread use of Log4j, the massive attack surface creates a multitude of potential entry points for adversaries to gain access to vulnerable systems. Moreover, Log4j libraries are often embedded within other systems, making it difficult for organizations to determine whether the vulnerabilities exist in their infrastructure and, if so, where and to what extent. Actors of all skill levels, including sophisticated APTs, continue to exploit vulnerable Log4j systems. The unique challenges posed by this set of vulnerabilities (CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105) indicate they will remain long-lasting challenges for organizations and cybersecurity providers. In this section, we provide an update on 2022 Log4j-related activity trends based on Talos telemetry to highlight one of the most impactful threats from this year and to remind organizations that active exploitation against older vulnerabilities remains a pervasive issue.

Top infection vectors, Q1



Top infection vectors, Q2



Top infection vectors, Q3

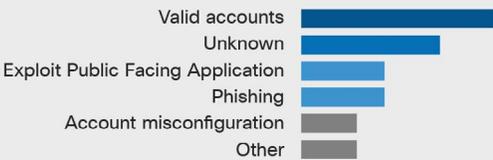


Figure 10. Top infection vectors based on Talos IR data.

LOG4J EXPLOITATION ATTEMPTS REMAIN CONSISTENTLY HIGH

Nearly a year after the Log4j vulnerabilities were discovered, threat actors continue to exploit the security flaws at a high rate, according to several Talos data sets. In mid-January, less than a month after the security flaws had been disclosed, we immediately saw mass exploitation attempts against VMware Horizon servers running vulnerable Log4j versions. Targeted organizations spanned across multiple sectors, highlighting the indiscriminate nature of the targeting attempts. We first began seeing this activity in our Cisco Secure Endpoint data and honeypot telemetry, and soon identified multiple clusters of post-exploitation behavior, including the deployment of various cryptocurrency miners and additional malware, the use of PowerShell reverse shells, and VMware commands issued for system information discovery.

The volume of associated threat activity quickly expanded, as did the variety of adversaries attempting to scan for and exploit vulnerable systems (**Figure 10**). In the [first quarter of 2022](#), Log4j exploitation attempts ranked number two among the most common threats affecting Cisco customers, according to Cisco Talos Incident Response (CTIR) data. This was second to ransomware, a constant mainstay as a top threat. Through the first half of 2022, exploitation of public-facing applications was tied with phishing

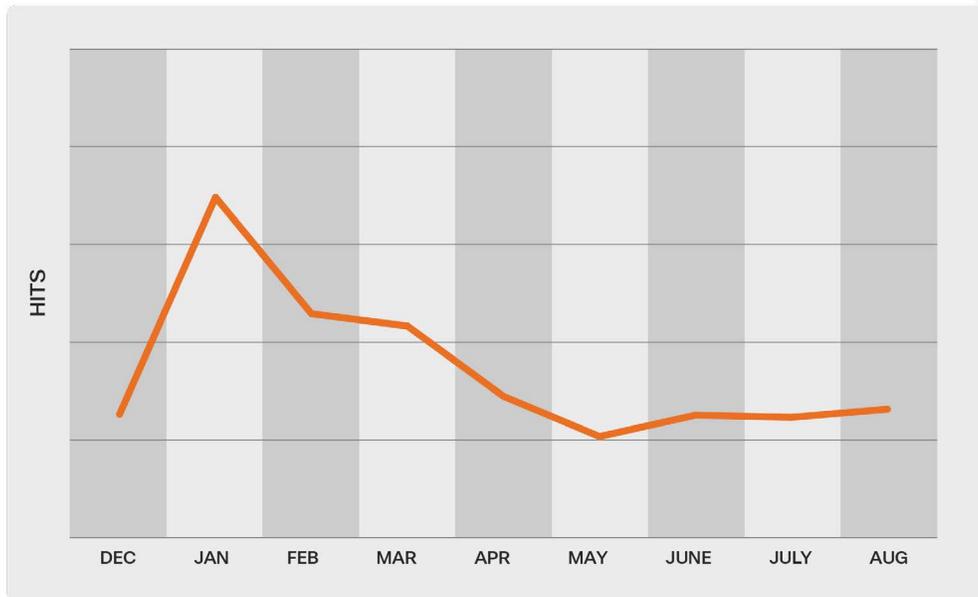


Figure 11. Total alerts on malicious network traffic identified as Log4j exploitation attempts.

as the top initial infection vector, according to CTIR findings, highlighting the presence of Log4j in incident response engagements. In Q3, nearly 15 percent of engagements saw adversaries identify and/or exploit misconfigured public-facing applications, including conducting Structured Query Language (SQL) injection attacks against external websites, exploitation of Log4Shell in vulnerable versions of VMware Horizon, and targeting of misconfigured and/or publicly exposed servers.

In addition to CTIR data, our Snort telemetry—which identifies malicious network traffic via signatures—helps paint a clear picture of the consistently high volume of Log4j threat activity throughout the year. Based on a review of our 44 Snort IDs (SIDs) that detect exploitation attempts against Log4j vulnerabilities, we found that the volume of alerts on these SIDs ballooned nearly 40 percent in January. Although it has since leveled

off from April onwards, the number of alerts still remains in the tens of millions. **(Figure 11).**

Beyond highlighting threat actors’ continued interest in scanning for vulnerable Log4j systems, the data is also largely representative of the volume of attacks Snort helped prevent. Any time a SID detects malicious activity, it drops the network traffic unless the user or organization changed the rule’s preset configuration.. All of the SIDs from this data set are rules that look for attempts to exploit a remote code execution vulnerability in Log4j’s “lookup” functionality, the Java Naming and Directory Interface (JNDI). This relates directly to the “Log4Shell” vulnerability (CVE-2021-44228). The top five SIDs accounting for the highest numbers of detections were 58722, 58723, 58742, 58737, and 58726. These SIDs accounted for 95 percent of the total hits—several million to tens of million per month.



Ransomware actors—already broadly known for being highly opportunistic—were also quick to attempt to monetize the Log4j flaws, and continue to do so today.

ACTORS OF VARYING SKILL, MOTIVATION LEVERAGE LOG4J IN THEIR OPERATIONS

The surge in Log4j activity was attributed to a variety of different actors throughout 2022, from basic cybercriminals to sophisticated APTs. In one instance during a CTIR engagement, we observed [Deep Panda](#), a suspected Chinese state-sponsored actor, exploiting Log4j to drop a custom backdoor on the victim’s system. The North Korean state-sponsored Lazarus Group is also targeting Log4j in its operations, as we detailed in another [blog](#). These findings are consistent with other reporting on many other advanced threat actors attempting to exploit Log4j vulnerabilities, including [Iran’s Islamic Revolutionary Guard Corps \(IRGC\)](#) and the China-linked APT41.

[Cryptocurrency mining groups](#) were among the first to start scanning for and exploiting Log4j—as they often are with new vulnerabilities—including unaffiliated actors and longstanding, well-known gangs like the [8220 Mining Group](#). Ransomware actors—already broadly known for being highly opportunistic—were also quick to attempt to monetize the Log4j flaws, and continue to do so today. We saw evidence of this in Q2 of this year, when [CTIR observed](#) a Conti ransomware affiliate exploiting Log4j on vulnerable VMware Horizon servers. This was consistent with earlier reporting that the adversary had been leveraging Log4j in their operations since December 2021—immediately after the vulnerabilities were made public—highlighting the speed at which actors begin exploiting newly disclosed security flaws as well as the long tail in adversary exploit attempts following initial surges after disclosure.



CONCLUSION

We assess that the threat of Log4j exploitation attempts will remain a challenge for organizations well into 2023 and beyond. Cyber threat actors are known to reuse the same tactics, tools, and techniques (TTPs) as long as they remain effective, and Log4j will likely be no exception. Log4j is still a highly viable infection vector for actors to exploit, and we expect that adversaries will attempt to continue to abuse vulnerable systems as long as possible. Although threat actors remain adaptable, there is little reason for them to spend more resources developing new methods if they can still successfully exploit known vulnerabilities.

This logic is supported by CISA’s annual findings on top exploited vulnerabilities. In its 2022 [report](#), CISA found that cyber actors continued to exploit publicly known, dated software vulnerabilities, some of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor.

Log4j’s pervasiveness in organizations’ environments makes patching challenging. Since the library is so widely used, Log4j may be deeply embedded within large systems, making it difficult to inventory where all software vulnerabilities may be in a particular environment. Moreover, there is no uniform patching system for Log4j, meaning it does not push software updates—including important security upgrades—regularly or automatically. As highlighted earlier, the number of CTIR engagements that exploited Log4j in 2022 underscores adversaries’ reliance on targeting unpatched and vulnerable public-facing applications. Actors’ successful targeting, organizations’ challenges around patching, Log4j’s pervasiveness, and adversaries’ historic propensity to exploit known vulnerabilities suggests that Log4j will remain a threat well into 2023.

 | TALOS

2022 **YEAR IN REVIEW**

GENERAL THREAT LANDSCAPE





REVIEW OF THE GENERAL THREAT LANDSCAPE IN 2022

While our ongoing support to Ukraine and response to the Log4j vulnerabilities were two of our most comprehensive and impactful efforts in 2022, we also dealt with a multitude of other threats as the security community faced an expanding set of adversaries and malware. In January, we identified several [emerging trends](#) that we expected would affect or dominate the threat landscape in 2022, many of which ultimately played out as significant events this year. In this section, we provide an overview of the general threat landscape throughout 2022 and major trends based on telemetry sets gathered across Talos, including behavioral indicators from Secure Malware Analytics, Snort and ClamAV alerts, Behavioral Protections (BPs) from Cisco Secure Endpoint, and case studies from CTIR engagements.

DUAL-USE TOOLS PROVIDE ACTORS A STEALTHY MEANS OF STAYING UNDETECTED IN AN ENVIRONMENT

Threat actors, including APTs, ransomware operators, and cybercrime groups, leverage offensive frameworks to support a range of actions across an attack lifecycle. These frameworks are referred to as dual-use tools because they are legitimately used by offensive security teams. These tools also provide an additional layer of protection through anonymity: cybersecurity professionals often have difficulty attributing use of these tools to any particular group since they can be observed across many different actors, and the TTPs observed in operations leveraging dual-use tools can vary greatly.

Cobalt Strike continues to remain a popular option for cyber threat actors. This legitimate network defense tool and threat emulation software has a range of capabilities, including reconnaissance, post-exploitation activity, and a range of attack simulations, making it a highly functional tool for adversaries. In early June, we observed an uptick in Snort ID (SID) 53658 for Cobalt Strike download attempts and Secure Malware Analytics behavioral indicator detections for Cobalt Strike-named pipe usage, as seen in **Figures 12 and 13**, respectively. This coincided with a 10 percent increase in Cobalt Strike sightings in CTIR engagements since January.

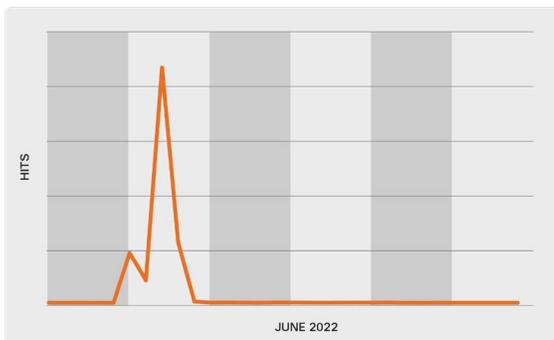


Figure 12. Detections for a Cobalt Strike Snort SID 53658.

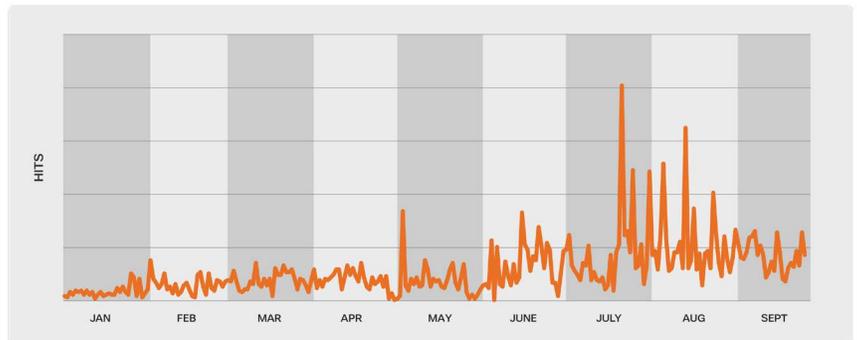


Figure 13. Behavioral indicators alerting on Cobalt Strike-named pipe usage.



In August, Talos [discovered](#) a campaign delivering Cobalt Strike beacons that could be used in future follow-on attacks. The discovered payload was a leaked version of a Cobalt Strike beacon containing commands to perform targeted process injection of arbitrary binaries. Cobalt Strike source code was leaked in late 2020, and the number of cracked and modified versions seen in the wild speaks to the tool’s success in operations. It also highlights malware operators’ willingness to continue to incorporate leaked versions of popular frameworks into their own operations.

Talos and the security community have been dealing with Cobalt Strike for years, continuously developing better and more robust [detections](#). We assess that threat actors may have adapted their behavior to these developments by turning to additional offensive frameworks such as Sliver and Brute Ratel.

Earlier this year, we began observing activity in our endpoint telemetry for the Sliver open-source red-teaming framework. This activity coincided with a CTIR engagement in March where Sliver was used to support a Conti ransomware attack exploiting Log4j for initial access.

The following is a case study from a CTIR engagement of a Conti affiliate incorporating Sliver which shows the adversary leveraging legitimate remote management tools as well:

The attackers gained initial access by exploiting Log4j on an unpatched, vulnerable VMware Horizon server. CTIR observed subsequent PowerShell commands attempting to download and silently execute a malicious Windows Installer file (“setup.msi”). This initiated the installation of Atera Agent, a legitimate remote management tool that provides a connection option for the ransomware affiliate to achieve persistence using a number of remote access tools, such as AnyDesk and Splashtop. PowerShell was used to install AnyDesk: “C:\Program Files (x86)\AnyDeskMSI\AnyDeskMSI.exe --service”. The adversary then used PowerShell commands to attempt to download and execute a payload masquerading as a VMware executable, identified as the Sliver implant. When executed, the sample connected to a C2 and appeared to sit dormant until additional commands were received.



At that time, Sliver’s presence in an IR engagement was notable as there were no publicly reported instances of Conti previously leveraging the implant in their operations. Sliver has since been publicly reported as a Cobalt Strike alternative and has been adopted into a variety of actors’ toolkits. In June, Talos identified [Avos](#) ransomware affiliate(s) gaining a foothold via VMware Horizon Unified Access Gateways vulnerable to Log4j and using Cobalt Strike and Sliver in post-exploitation activities.

Cobalt Strike

- A legitimate network defense tool and threat emulation software that has a range of capabilities, including reconnaissance, post-exploitation activity, and a range of attack packages, making it a highly functional tool for adversaries.
- Beacon is Cobalt Strike’s payload for generating attacks and creating outbound traffic over HTTP, HTTPS, or DNS. Cobalt Strike beacons can be compared with Meterpreter, which is part of the Metasploit framework, and used by penetration testers and offensive security researchers when delivering their services.

Brute Ratel

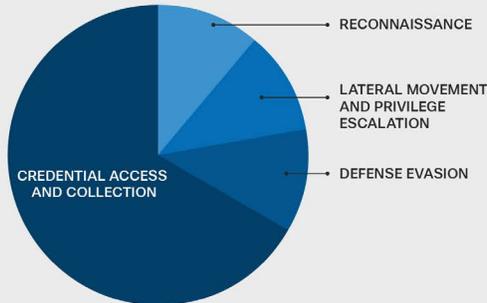
- A legitimate sophisticated red-teaming tool released in 2020 as an attack simulation tool. It has since been leveraged by threat actors to facilitate various stages of the attack lifecycle.
- Brute Ratel is specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV).

Sliver

- An open-source red-teaming framework and attack simulation tool that can be used to perform security testing. Sliver’s implants are dynamically compiled with asymmetric encryption keys per binary and supports C2 over a number of protocols (mTLS, HTTP, DNS).
- Sliver implants are supported on MacOS, Windows, and Linux . Sliver features multiple functionalities including staged and stageless payloads, dynamic code generation, named pipe pivots, in-memory .NET assembly execution, and much more.

Besides Sliver, adversaries have also been increasingly turning to the adversarial attack simulation tool Brute Ratel (BRc4). Actively being used to support attacks in the wild, Brute Ratel is of particular concern since the toolkit was cracked in late September and is being shared for free across several hacking forums and communities. This coincided with what Talos believes are the first reported instances of Qakbot operators using Brute Ratel. In June and September, two clusters of activity in our endpoint telemetry revealed an attack chain with Qakbot eventually dropping Brute Ratel. We assess that Brute Ratel’s rise in the threat landscape along with Qakbot operators’ recent adoption and the availability of the cracked version, will likely lead to more threat actors adopting the post-exploitation kit into their operations.

Talos discovered two new offensive frameworks called "[Manjusaka](#)" and "[Alchemist](#)." Although implemented in different ways, both follow the same design philosophy and virtually the same set of features, seemingly having the same list of requirements despite being created by different developers. They are designed and implemented to operate as standalone GoLang-based executables that can be distributed with relative ease, providing even amateur adversaries the capabilities to carry out operations. Alchemist is already being used in the wild, and although we haven’t observed widespread usage of Manjusaka as of this writing, it has the potential to be adopted by threat actors globally.



CREDENTIAL ACCESS AND COLLECTION

- DomainPasswordSpray** | Password spraying
- Hashcat** | An advanced password recovery utility that can help enable distributed password cracking
- Invoke** | NTLMExtract - PowerShell Empire script ("Invoke-NTLMExtract.ps1")
- NPPSpy** | Gathers credentials stored in plain text
- WebBrowserPassView** | Password recovery tool that reveals the passwords stored by commonly used Web browsers
- NinjaCopy** | PowerShell script ("NinjaCopy.ps1") part of the PowerSploit module used to dump "NTDS.dit", a database that stores Active Directory data

DEFENSE EVASION

- SharpUnhooker** | Provides antivirus evasion

LATERAL MOVEMENT AND PRIVILEGE ESCALATION

- SharpZeroLogon** | An exploit for Zerologon, CVE-2020-1472

RECONNAISSANCE

- Anonymous Fox** | A suite of automated hacking tools to exploit insecure admin panels or vulnerable platforms and websites

Figure 14. Range of tools observed across CTIR engagements in Q3 (July-September 2022).

Talos has observed additional dual-use tools as well. From July to September, CTIR saw a notable use of publicly available tools and scripts hosted on GitHub repositories or third-party websites to support operations across multiple stages of the attack lifecycle. From CTIR engagements in Q3 alone, over 50 percent of the tooling focused on accessing and collecting credentials, highlighting the role these tools play in potentially furthering an adversary’s objectives during that stage of an attack (**Figure 14**). CTIR commonly observes offensive security and red-team tools to support an adversary’s objectives; however, their increased presence indicates that adversaries are continuing to identify more flexible options to stay under the radar and achieve their objectives, highlighting their adaptability.

It is important to keep track of dual use tools so that enterprises can effectively monitor them in their environments. As the cybersecurity community continues to enhance detections, adversaries will likely continue to adapt and experiment with newer dual-use tools in their attacks.

CONSISTENT USAGE OF LOLBINS

As we look at threats consistently affecting enterprise environments throughout 2022, the usage of living-off-the-land binaries ([LoLBins](#)) and the techniques associated with them continue to be leveraged to support a variety of phases across an attack lifecycle. LoLBins are pre-installed on an operating system and are commonly abused by adversaries, combined with fileless malware and/or legitimate cloud services, to improve their chances of staying undetected within an organization. Due to an organization’s use of these tools as part of legitimate administrative functions, defenders may miss attacks leveraging LoLBins when monitoring for aberrant behavior.

Cyber threat actors are known to reuse TTPs as long as they remain effective, with LoLBins being no exception. Since Talos’ [publication](#) on hunting for LoLBins in 2019, we continue to see legitimate utilities leveraged by adversaries in all stages of an

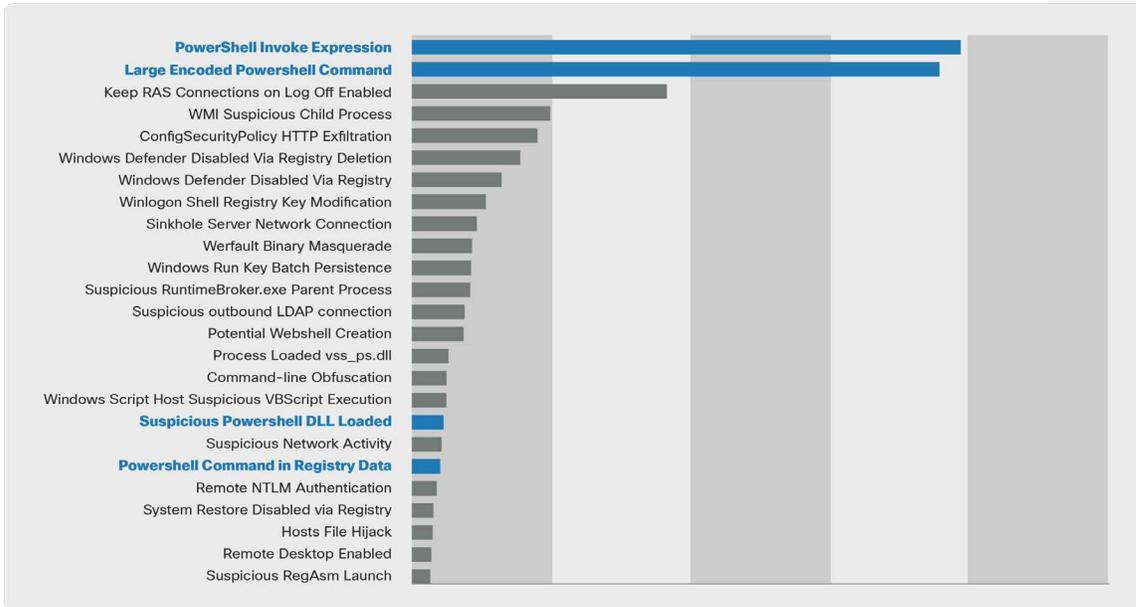


Figure 15. Top 25 most alerted Behavioral Protection signatures, Jan.-Sept. 2022.

attack to support their operations. Looking at 2022 behavioral protection (BP) data from Cisco Secure Endpoint, four of the 25 most alerted on BP signatures are PowerShell-related, highlighting threat actors’ consistent reliance on the malicious potential of PowerShell (**Figure 15**). Malicious use of PowerShell is pervasive, and is leveraged to support a broad range of operations including installing adware like ChromeLoader, downloading cryptocurrency miners, or exploiting vulnerabilities in software such as Elasticsearch.

Microsoft’s PsExec is another native utility that adversaries commonly abuse. With the ability to execute programs or processes remotely, PsExec has played a large role in executing ransomware in 75 percent of ransomware engagements CTIR [observed](#) in Q3 (July-September).

In a Black Basta ransomware engagement, CTIR identified another commonly abused LoLBin, "vssadmin.exe," that displays the volume shadow copy backups being used to delete local shadow copies, a common technique associated with ransomware adversaries. Shortly after, PsExec launched the malicious ransomware DLL and deleted local backups with VSSadmin. Files with the extension ".basta" started appearing on the affected endpoints.

Given the unique challenges LoLBins present to defenders, from appearing as legitimate to obscuring attribution, we expect them to remain popular among a wide variety of threat actors.



WHAT WAS OLD IS NEW AGAIN: USB ATTACKS INCREASE IN 2022

We are reminded that beyond the emerging threats and evolving actor TTPs, threat actors will continually look to rely on techniques that remain successful against older, unpatched legacy enterprise systems, only adapting if these former techniques should stop working. Since January, CTIR has responded to a growing number of engagements in which removable USB drives infected organizations with malware. We have observed several malware families delivered in this way, including Sality and PlugX, which target Windows systems and are known to spread through removable drives. Although adversaries have been leveraging USB drives for initial access for years, the activity

illustrates that the threat has not abated and highlights that organizations should continue to stress the importance of USB hygiene.

This also coincides with a general uptick in detections in Cisco Secure Malware Analytics for various behaviors associated with USBs and external drives. Those behaviors include executables being written to a USB drive or setting hidden attributes for files on a USB drive to stay undetected, as seen in **Figures 16 and 17**, respectively. While we cannot explain the spike in July as shown in **Figure 17**, in what will be covered in more detail below, the number of threats now leveraging USBs throughout the year likely contributes to the general uptick in behaviors associated with their use.

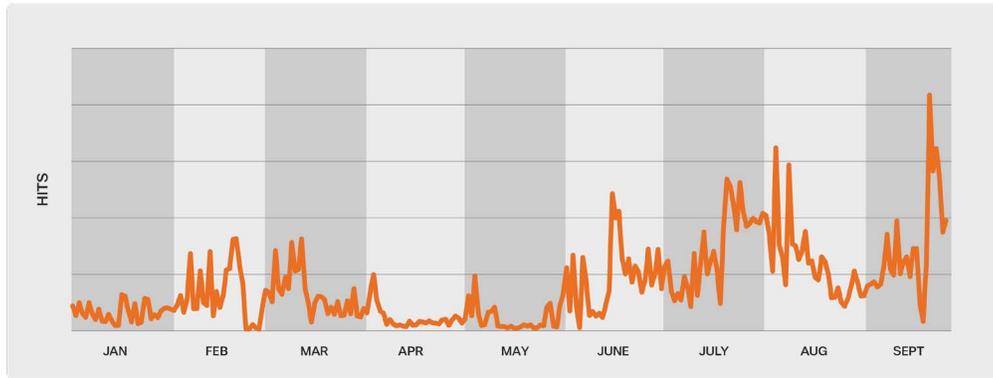


Figure 16. Behavioral indicators for executables written to USB.

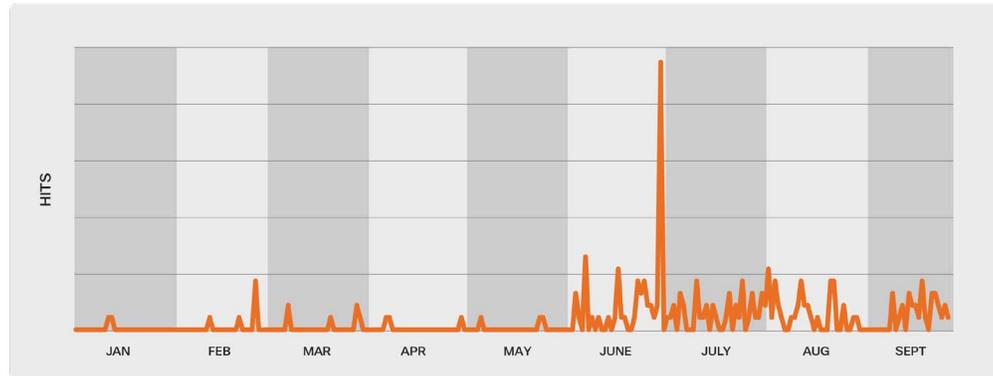


Figure 17. Behavioral indicators for setting hidden attributes for files on a USB.



We have continued to observe ongoing activity associated with a malware called [Raspberry Robin](#), which leverages a number of LoLBins and exhibits worm-like capabilities allowing it to spread via external drives, such as USB devices. In a distinguishing pattern of command line activity associated with the legitimate Windows Installer “msiexec.exe,” we observed activity in our endpoint telemetry which revealed obfuscated command line arguments that seemed to take the name of an infected external drive with values including “USB,” “USB DISK,” or “USB Drive.” After initial infection, it downloads its payload through “msiexec.exe” from compromised QNAP Network Attached Storage (NAS) devices, executes its code using the legitimate Windows utility “rundll32.exe,” and establishes a C2 channel through The Onion Router (Tor) connections (**Figure 18**).

While we consistently observe this activity in our Talos Threat Hunting telemetry based on automated hunting rules, we observed a spike in automated hunts searching for Raspberry Robin activities in April when it remained consistently high for several months, as seen in **Figure 19**.

As we continued our analysis into this threat, we also observed attempts to bypass Microsoft’s user access control (UAC) feature, commonly abused by cyber threat actors to operate on compromised devices with advanced or administrator-level permissions. Raspberry Robin attempts to remain undetected through its use of system binaries, Tor-based command and controls (C2s), and abuse of compromised QNAP accounts. It remains very prolific across customer endpoints globally, although the adversary’s ultimate goal remains largely unknown.

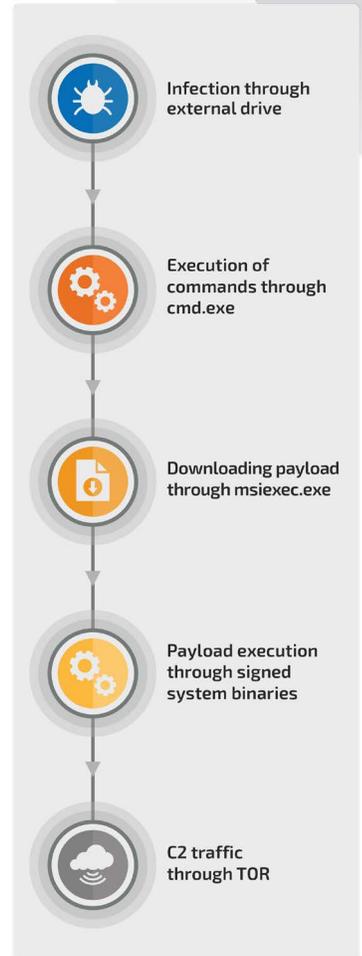


Figure 18. Execution chain of Raspberry Robin.

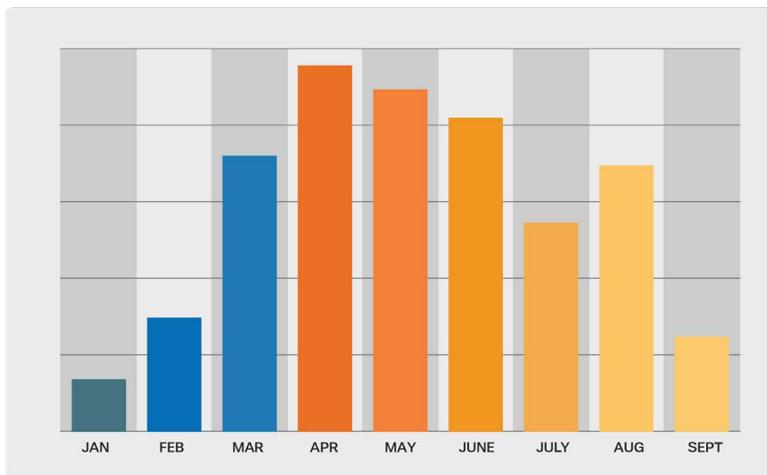


Figure 19. Raspberry Robin activity identified from automated hunts over time.



We have continued to observe this USB trend outside of CTIR engagements and endpoint telemetry as well. We have observed several APT groups update their campaigns and malware in 2022 to leverage USB drives. This includes the suspected Pakistan-linked [Transparent Tribe](#), who have incorporated USB modules, and North Korea-based [Lazarus Group](#), who have performed USB dumping to copy files and folders from USB drives.

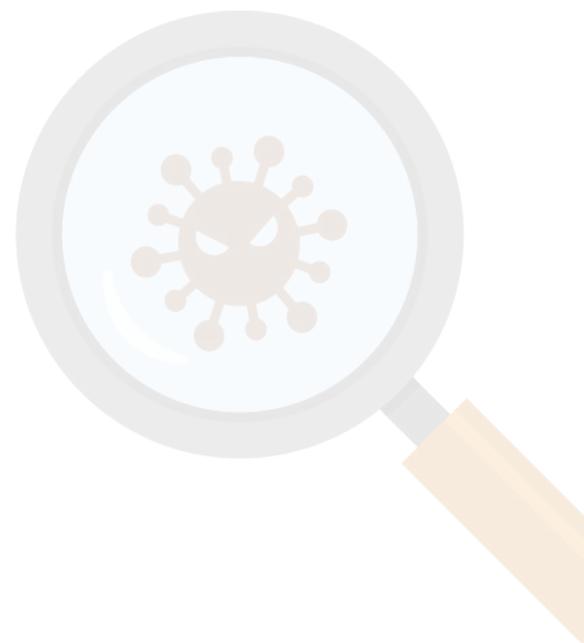
In addition, in January 2022, the Federal Bureau of Investigation (FBI) [warned](#) organizations about malicious USB drives purporting to contain COVID-19 information sent in the mail impersonating the U.S. Department of Health and Human Services. Once connected, the USB would register itself as a keyboard and send automated keystrokes to the user's machine, subsequently running malicious PowerShell commands that downloaded and executed malware. In some cases, ransomware was deployed on the compromised networks.

CONCLUSION

We assess that as the security community continues publishing playbooks and guidance to help track and detect rogue dual-use tools and LoLBins, attackers will likely feel compelled to adapt and update their TTPs to thwart analysis. We can see this as threat actors turn to newer offensive frameworks that are less familiar to security teams like Sliver and Brute Ratel. Additionally, they will likely continue to incorporate cracked/leaked versions of popular red-teaming tools into their operations, sidestepping the steep costs associated with distribution licenses and further widening the pool of actors who rely on them.

Organizations can increase their resilience and help to reduce the risk of adversaries abusing these dual-use tools and/or LoLBins by monitoring command line invocations of tools capable of carrying out actions such as modifying services and executing files that don't correspond to normal usage patterns. Monitoring for changes to executables and other files associated with Windows services reflected in the Registry will also minimize the risk of an adversary attempting to establish persistence.

In addition, 2022 has shown us that USB attacks are back and that adversaries will adapt their tactics to take advantage of enterprises shifting their attention away from older attack vectors. We urge all organizations who may use USBs or removable drives for legitimate business operations to limit and if possible, restrict USB usage in the environment. We also recommend that organizations provide user awareness training about the risks associated with connecting known and unknown USBs to corporate systems or personal devices.





 | TALOS

2022 **YEAR IN REVIEW**

RANSOMWARE THREAT LANDSCAPE



Ransomware affiliates are no longer structured in silos and are now working across multiple ransomware groups, where the more unique an actor's skill set is, the more opportunities they have to support multiple campaigns and organizations.

RANSOMWARE THREAT LANDSCAPE

We continue to see an evolving ransomware threat landscape as new ransomware-as-a-service (RaaS) groups emerge and existing groups re-brand or shut down operations. As we moved into 2022, we continued monitoring the potential impact of the United States' [whole-of-government approach](#) to countering the ransomware threat, which included initiatives enacted by the Departments of Treasury, Justice, State, and other agencies to disrupt ransomware actors' ability to operate. This crackdown, which coincided with similar targeted efforts by global law enforcement and private industry, occurred against the backdrop of Russia's war against Ukraine, which itself has contributed to significant changes in the landscape. However, ransomware remains a pervasive threat, particularly for education organizations which was the top targeted vertical in 2022.

Talos tracks over a dozen RaaS groups by monitoring when victim information is posted to ransomware data leak sites (**Figure 20**). We note that in **Figure 20**, some groups do not timestamp their posts so this list may not be representative of all the posts made from January to October. Based on our findings, LockBit was the most active RaaS group this year, accounting for over 20 percent of the total number of dark web victim posts, closely followed by Hive and Black Basta. The LockBit findings align with our overall tracking and understanding of the group's activities this year, as we mention in more detail below, in which the group has continued to announce new capabilities and updates amidst facing mounting setbacks.

These findings also support a [trend](#) toward a greater democratization of ransomware adversaries that Talos began highlighting in CTIR engagements since at least Q1 2022. We see this play out across several telemetry sources, such as Cisco's malware analysis platform, Secure Malware Analytics, and internal dark web monitoring efforts, where we are seeing the emergence of a multitude of ransomware groups, an overall change from previous years in which a select few ransomware groups monopolized the landscape. Ransomware affiliates are no longer structured in silos and are now working across multiple ransomware groups, where the more unique an actor's skill set is, the more opportunities they have to support multiple campaigns and organizations. This diversification in the RaaS space is also reflected in different initial access TTPs from leveraging high-profile vulnerabilities to buying access on forums through initial access brokers (IABs).

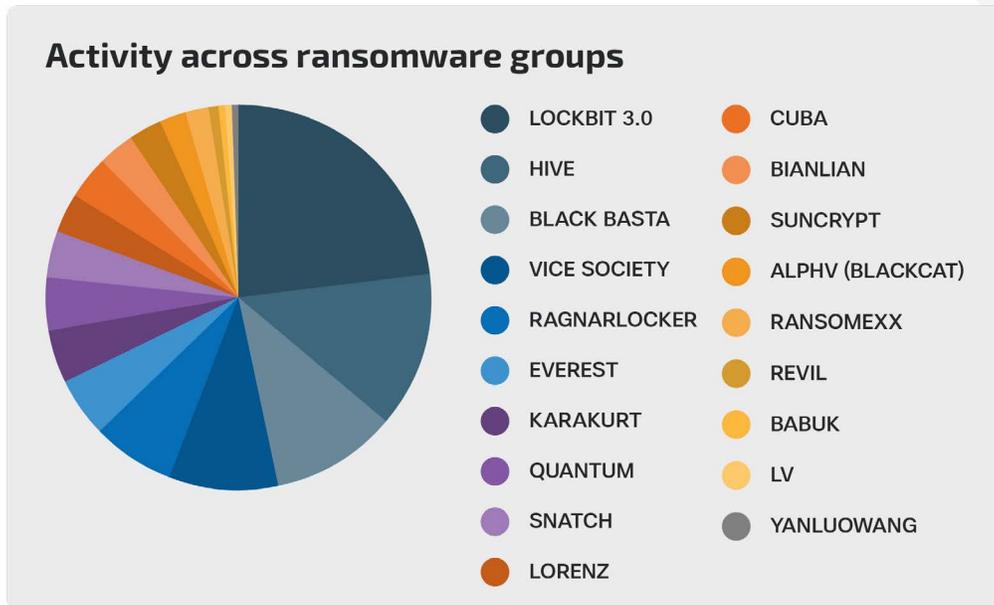


Figure 20. Number of posts made to ransomware data leak sites tracked by Talos, January–October.

Throughout 2022, Hive was the primary ransomware family observed throughout several CTIR engagements, followed by Vice Society and Conti. As the year went on, however, Conti [announced](#) it was ceasing operations, and by June had taken much of its infrastructure offline, discussed in greater detail below. Soon after Conti shut down, a relatively new family and suspected Conti re-brand dubbed Black Basta emerged. While Black Basta entered the scene later in the year, the group quickly became incredibly active as evidenced by the number of posts made to their data leak site (**Figure 20**).

In looking at ransomware as a percentage of total IRs in 2022 (**Figure 21**), with the exception of false positives and acknowledging the lack of data from Q4, we see ransomware making up slightly over 20 percent of threats seen in CTIR engagements so far this year. The number of ransomware CTIR engagements were highest in Q1, dropped in Q2, and picked up again by the end of Q3. This follows a trend noted earlier in the report where we saw a dip in CTIR-observed threats such as ransomware between February and June, suggesting that threat actors may have been focused on the Russia-Ukraine attack space since the start of the war.

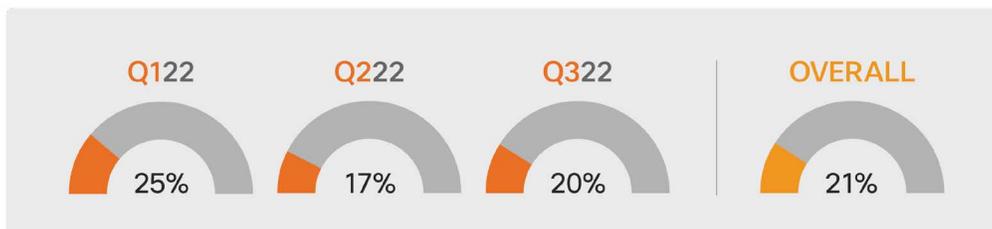


Figure 21. Ransomware as a percentage of IRs, 2022.



EDUCATION IS TOP TARGETED VERTICAL OF 2022

The education sector, as one of the nation’s critical infrastructure subsectors, has been most affected by ransomware attacks in CTIR engagements since January. While not an unusual targeted vertical for threat actors in general, this is part of an ongoing trend of ransomware groups disproportionately targeting the education sector, consistent with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) [reporting](#). Ransomware affiliates will likely continue to view organizations in the education vertical as high-value targets, especially during times when those entities have exceptionally low downtime tolerance, such as during back-to-school season. Additionally, by disrupting core university services, such as financial aid and student loans, this likely incentivizes victims to pay the ransom in order to return to normal operations as quickly as possible.

In one Vice Society ransomware incident affecting an education institution, analysis revealed numerous outbound remote desktop protocol (RDP) connection attempts from an infected host to other systems, indicating an attempt to move laterally. We identified two remote access software tools, AnyDesk and TeamViewer, with over 50 systems observed reaching out to TeamViewer. An exception was also added to the Windows Defender firewall for “AnyDesk.exe” executions by the SYSTEM account. The likely trigger for ransomware was PsExec execution followed by deployment of ransomware which was written to the Windows Roaming profile of the compromised user.

While the education sector was the most targeted sector since January, the local government and municipality sector was the next most affected sector in CTIR engagements since the start of the year (**Figure 22**).

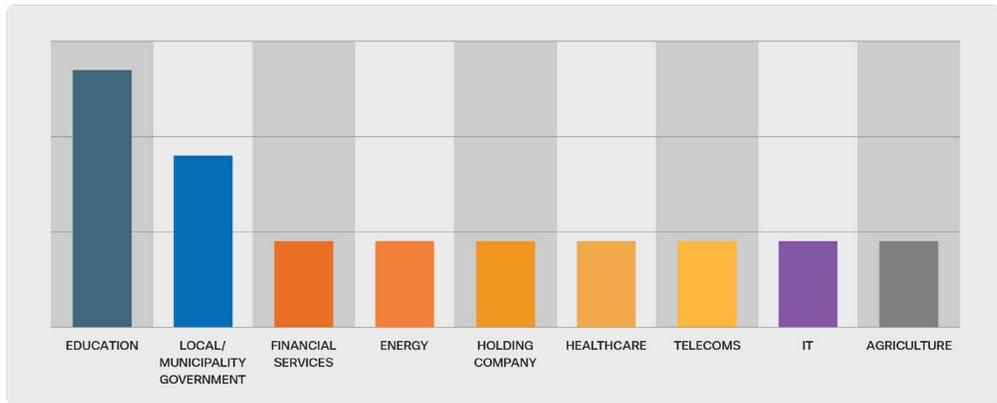


Figure 22. Confirmed CTIR ransomware incidents per sector, Jan.-Sept. 2022.



RANSOMWARE GROUPS TAKE SIDES IN THE RUSSIA-UKRAINE WAR

As previously mentioned in the Ukraine section of this report, the war in Ukraine compelled many threat actors to choose sides in the conflict and direct their operations against pro-Russia or pro-Ukraine targets. We saw early indications of this as ransomware groups and other cybercriminals started issuing statements in support of or opposition to the Russian government. At the onset of the invasion, [crowd-sourced attacks](#) presented a real threat to organizations as unpredictable adversaries emerged. Open-source reports indicated announcements from dark web forum administrators stating they would close their doors on users connecting from Russia, in clear opposition to the Kremlin's actions.

The Conti RaaS group was among the most vocal to have claimed sides at the beginning of the war, warning they would attack anyone who attempted to interfere with Russia's invasion of Ukraine. This claim, and others made by similar groups, caused internal strife and infighting among many members of the ransomware community. After Conti members publicly supported Russia's invasion of Ukraine, an individual with ties to Conti took revenge against the ransomware gang by leaking information about the group, including the malware's source code and internal chats between affiliates. Conti is a group whose TTPs continue [to be leaked](#) in a series of playbooks by reportedly disgruntled affiliate(s) starting in 2021. Talos was able to obtain these leaks, which exposed interesting operational information such as internal messages between Conti operators, various roles within the organization, and their process for hiring new affiliates. Open source reporting confirms that Conti continues to deal with fallout from their decision. In one such cluster of activity, [Cobalt Strike servers](#) previously operated by former Conti members were flooded with anti-Russian messages.

After Russia's invasion of Ukraine, high-profile and emerging cybercriminal groups took sides, highlighting the impact of the invasion across all levels of cybercriminal enterprises. Following in Conti's footsteps, less familiar ransomware adversaries such as the Stormous ransomware gang and the CoomingProject also publicly pledged support for Russia and began claiming politically motivated attacks against Ukraine and its allies.

At the onset of the invasion, crowd-sourced attacks presented a real threat to organizations as unpredictable adversaries emerged.



FRICION IN THE RAAS COMMUNITY LEADS TO AN EVOLVING LANDSCAPE

The ransomware space is dynamic, continually adapting to changes in the geopolitical environment, actions by defenders, and efforts by law enforcement, which increased in scope and intensity in 2022. This leads groups to rebrand under different names, shut down operations, and form new strategic partnerships.

As we continue to monitor changes in this space, we constantly look to dark web forums to shine light on operational changes and RaaS members' growing distrust of certain groups. These changes often create ripple effects in the ransomware landscape and change how RaaS groups attract and recruit talent and retain existing members, all of which can present challenges to open-source monitoring of these groups.

Following the aforementioned Conti leaks in May 2022, Conti first announced it was ceasing operations, and by June had taken much of its infrastructure offline, including Tor servers used to leak data and negotiate ransom payments with victims. We saw this coincide with a general drop off in Conti detections in our telemetry, specifically in our Secure Malware Analytics' (SMA) behavioral indicator data set, as shown in **Figure 23**.

As the effects of Conti shutting down began to set in, by mid-year, a suspected re-brand of Conti dubbed "Black Basta" emerged. Public reporting indicates that the similarities between the two families are based on likenesses in the payment and leak websites as well as the communication styles from some of its members. Talos tackled the emergence of this threat by creating SMA behavioral indicators for Black Basta. In late May, we began to see detections for Black Basta registry modifications, which alerts when a victim's desktop is altered to display a wallpaper just prior to dropping the Black Basta ransom note (**Figure 24**).

In what appears to be a common theme this year regarding the release of leaked information in the community, Talos became aware of the disclosure of a leaked builder for the LockBit 3.0 ransomware

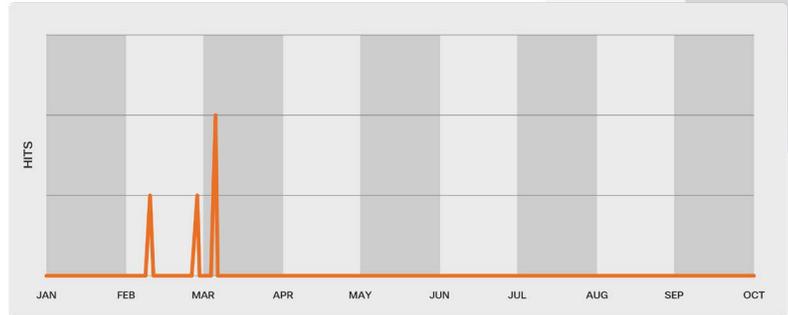


Figure 23. Behavioral indicator detections for Conti ransomware.

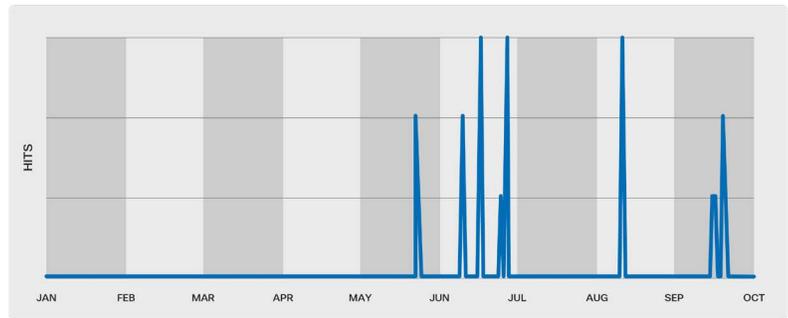
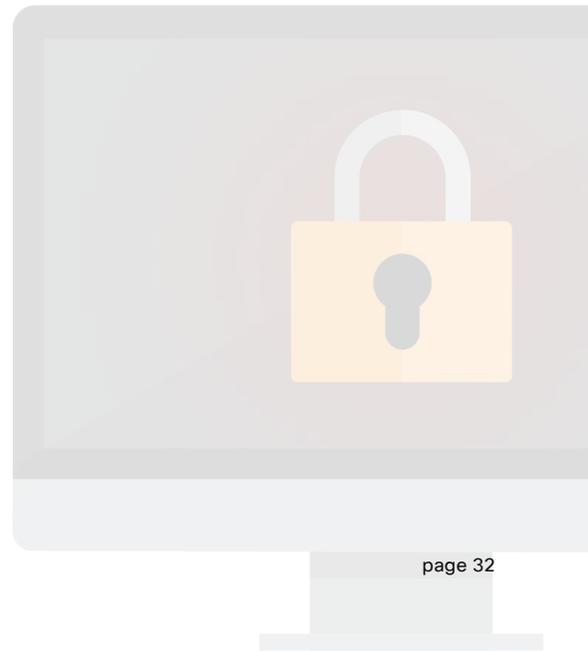


Figure 24. Behavioral indicator detections for Black Basta registry modifications.





encryptor dubbed “LockBitBlack.” The individual claiming responsibility for leaking the builder is an alleged LockBit developer who, according to LockBit, claimed they were disgruntled with the group’s payment structure. Based on our analysis of the leaked builder and alerts from the two new Snort rules (60622-60623) generated from it, we confirmed that it could allow anyone to build the executables required to launch their own ransomware operation, including an encryptor, decryptor, and specialized tools to launch the decryptor. The builder contains a configuration file that can be used to customize an encryptor, including modifying the ransom note per victim, changing configuration options, deciding what processes and services to terminate, and specifying the C2 server where the encryptor will send data. By modifying the configuration file, any threat actor can customize it to fit their own needs, as well as modify the created ransom note to link to their own C2 infrastructure.

In August, Talos became aware of several prominent ransomware operations, such as [ALPHV](#) (also referred to as BlackCat) and [LockBit](#), experiencing suspected DDoS [attacks](#) against their public data leak sites. These sites are typically hosted on Tor hidden services where, in a tactic known as double extortion, RaaS affiliates will post victim information if the ransom demand is not met. Shortly after, Talos began tracking at least seven more RaaS leak sites that became inaccessible and went offline intermittently. A handful of the RaaS leak sites continued to face intermittent outages for several weeks, suggesting that this activity was a concerted effort meant to disrupt and perhaps sow discord among RaaS operators and affiliates by interfering with and hindering the ability for these groups to post new victim information. While the motivation and source of this activity still remains unknown, the possibility that these disruptions may have come from a competitor to sow discord and bring about unwanted attention likely created tension among some of the affected groups.

The leaked LockBit 3.0 builder will likely present challenges for defenders and researchers going forward as attribution becomes more difficult in future suspected LockBit attacks. Groups have already started to adopt this builder into their operations, including a new ransomware group dubbed “BI00dy Gang” who already began using the leaked LockBit 3.0 builder in recent attacks. Consistent with the Conti playbook leaks, this could enable lower-skilled actors to save time and resources by relying on leaked builders and source code of other ransomware operations, as opposed to independently developing their own ransomware.

CROSS-PLATFORM RANSOMWARE PROVIDES MORE ADAPTABILITY

Ransomware operators are increasingly turning to cross-platform programming languages like Rust or Golang to develop more agile ransomware variants that may prove more difficult for researchers to analyze and reverse engineer.



...we gained insight into how the actors determine ransom amounts, their willingness to negotiate lower prices, sales tactics and coercive means to compel victims to pay...

In April 2022, the FBI [released](#) IOCs associated with ALPHV ransomware group that was uniquely recognized as the first group to commercialize ransomware based on the Rust coding language. Leveraging Rust allows ALPHV affiliates to tailor the initial infection vector to the individual targets as the ransomware can be used against both Windows and Linux operating systems.

In late March, Hive operators were seen making updates to convert their VMware ESXi Linux encryptor to Rust and adding new features to make it harder for security researchers to monitor their negotiations with victims. Based on Hive-victim [conversations](#) from March that we obtained, the ransomware operators also started to use an updated encryptor also written in Rust, and implied in conversations with victims that any other decryption tool would be useless. We note that these chats predated the research published by researchers from South Korea's Kookmin University detailing a method for decrypting files infected with Hive ransomware, with the Korean Internet and Security Agency (KISA) releasing a recovery tool about a month later. These updates indicate the Hive developers are intent on continuing their operations despite repeated setbacks by security researchers and government efforts to thwart their activities.

ADDITIONAL RAAS INSIGHTS FROM THE DARK WEB

Talos' ongoing analysis of the dark web and underground cybercrime forums provides us with leaked components of ransomware operations. These insights have led us to better support our customers by crafting detections and defensive playbooks based on any code and TTPs obtained, and more closely track the ransomware affiliates associated with these activities.

Through open-source research, we obtained and analyzed over four months of chat logs that include more than 40 separate [conversations](#) between Conti and Hive ransomware operators and their victims. The obtained chats highlight nuances in communication styles and ransom negotiations between the threat actor and victims. By analyzing their chats, we gained insight into how the actors determine ransom amounts, their willingness to negotiate lower prices, sales tactics and coercive means to compel victims to pay, and many other details about their operations.

We have also identified techniques to help discover ransomware operators' infrastructure, allowing us to [uncover](#) previously unknown infrastructure for several groups including the DarkAngels, Snatch, Quantum, and Nokoyawa ransomware groups. Ransomware operators typically limit their activities to the dark web to conceal their activities and victim communication portals are accessible only on Tor network via specific URL(s). Although they use Tor to conceal their activities, we have been able to identify configuration mistakes that expose



some of their infrastructure, which leads to a better understanding of a group’s operations and resources.

By the end of 2021 and beginning of 2022, popular dark web forums like XSS and Exploit had been tightening their restrictions on ransomware-related sales and discussions, threatening to ban members if ransomware discussions took place, even removing ransomware advertisements and offerings. Other forums such as RAMP (Russian Anonymous Marketplace), explicitly stated that they welcomed ransomware marketplace activity. However, by mid-late 2022 even RAMP started tamping down on content as new administrators were rotated in. Talos Russian linguists have noted that RAMP’s reputation among the Russian hacker community is worse under the current RAMP administrator, citing that the general chat room is very quiet with total participation in single-digits, with the majority of the chatter coming from RAMP administrators or moderators. Meanwhile XSS has nearly 40k members, and while ransomware chats are still strictly limited, participation has not wavered as significantly as it has on RAMP.

CONCLUSION

This year, we faced a growing set of ransomware families and adversaries against the backdrop of the Russia-Ukraine war and an ever evolving RaaS community. We can likely date the accelerated landscape changes back to at least mid-2021, when the Colonial Pipeline DarkSide ransomware [attack](#) and subsequent law enforcement takedown of [REvil](#) led to the dispersal of several ransomware partnerships. Fast forward to this year, when the ransomware scene seems as dynamic as ever, with various groups adapting to increased disruptive efforts by law enforcement and private industry, infighting and insider threats, and a competitive market that has developers and operators shifting their affiliation continuously in search of the most lucrative ransomware operation.

As the year has shown us, these narratives will likely continue to play out into 2023, as organizations are on heightened alert, continually creating new detections and mitigations against the ransomware threat. In a trend observed in [CTIR Q3](#) data, we saw an equal number of pre-ransomware and ransomware engagements, making up nearly 40 percent of threats that quarter. This finding is notable and could be reflective of the increase in specialization and outsourcing in the ransomware community. In addition, it highlights how defenders’ detection methodologies have evolved to focus more on alerting on suspicious behavior before the final payload is dropped.

However, the end of the great ransomware monopolies has presented challenges to threat intelligence analysts. As we see in [Figure 20](#) above, at least eight groups make up 75 percent of the posts to data leak sites that Talos actively monitors. The emergence of new groups makes attribution difficult as adversaries work across multiple RaaS groups.

In what could likely be a trend we observe in 2023, groups such as LockBit have started to feature additional methods of data extortion, such as threatening to conduct DDoS attacks against victim organizations if a ransom demand is not met. As defenders continue to detect the behaviors associated with pre-ransomware TTPs, we may see a shift in groups relying on inventive and ever-evolving extortion tactics prior to ransomware deployment as a way to bypass detection efforts and still receive a financial pay out.

 | TALOS

2022 **YEAR IN REVIEW**

COMMODITY LOADERS





The four most active commodity loaders in 2022 were Qakbot, Emotet, IcedID, and Trickbot.

COMMODITY LOADERS

Commodity loaders—commercial trojans that deploy second-stage malware—are a constant threat that continue to have a global impact across all industry sectors. As such, Talos regularly tracks these malware families and the threat they pose to customers’ networks. This section examines Talos’ observations of commodity loaders in 2022 based on a full review of multiple data sources.

The four most active commodity loaders in 2022 were Qakbot, Emotet, IcedID, and Trickbot, according to our analysis of several network and endpoint telemetry sets (**Figure 25**). These four threats were initially developed as banking trojans, designed to compromise entities for monetary gain. Over time, adapting to greater security controls in the banking sector, they developed into much more sophisticated threats, leveraging multi-phase attack chains, evolving Tactics, Techniques, and Procedures (TTPs), and deploying additional malware. This evolution continues to impact the threat landscape, drawing the attention and resources of global law enforcement and forcing organizations and network defenders to constantly be on the lookout for changing techniques. Despite best efforts to detect and stop these threats, the malware operators continue to adjust their TTPs to keep up with changes in victims’ security environments. This is reflected in the malware’s evolution, as they now operate primarily as loaders with modular functions, allowing cybercriminals the flexibility and agility to quickly adapt to a wide variety of security environments, and the flexibility to use these loaders in conjunction with a range of open-source tools and newly developed malware.

In one overarching trend we observed, operators more frequently delivered Qakbot, Emotet, and IcedID using ISO, ZIP, and LNK file types, likely to circumvent Microsoft’s efforts to block macros-enabled documents. In another trend, Talos observed Qakbot, Emotet, and IcedID operators downloading and launching malicious payloads using living-off-the-land binaries (LoLBins) found on victim environments. In some cases, the Qakbot and Emotet affiliates refined their attack sequence by experimenting with different LoLBins to improve chances of staying undetected within an organization.

The geopolitical environment has also had an influence on cybercriminal’s operations. The war in Ukraine sparked infighting and internal leaks, and international law enforcement efforts have dismantled criminal botnets, causing many cybercriminal organizations to fracture. These shifts are reflected in the data we collected. For example, notably absent from any significant trend findings is Trickbot, whose developers are suspected to have joined the Conti ransomware gang, a group that suffered an internal data breach this year in response to its leadership declaring support for Russia. Although our telemetry detected activity associated with Trickbot, we assess



much of this activity was likely detecting old, infected endpoints, as the malware operators have been inactive since early 2022. Similarly, Emotet, although still operational, remains significantly less

active than it was before the botnet was dismantled in early January 2021 by law enforcement. Other malware has filled the void by becoming more popular, such as Qakbot and IcedID.

Commodity Loaders				
	Qakbot	IcedID	Emotet	Trickbot
Aliases	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo, Heodo	N/A
Affiliations	Commodity malware likely developed by Eurasian cybercriminals	Unknown	Commodity malware developed by Mummy Spider, a Russian-aligned cybercrime group	Commodity malware developed by Wizard Spider, a Russian-aligned cybercrime group
Active since	2007	2014	2017	2016
Goals				
<ul style="list-style-type: none"> Gain initial access and establish persistence to facilitate further intrusion activities. Deploy next-stage malware, including ransomware. 				
Victimology				
<ul style="list-style-type: none"> Targets all sectors worldwide. Since the Russia-Ukraine war, Trickbot has threatened to retaliate against perceived attacks against the Russian people. 				
Notable TTPs				
<ul style="list-style-type: none"> Phishing, malspam, social engineering, vulnerability exploitation, data theft—such as financial data and credentials—and worm-like propagation. Highly modular, allowing operators to conduct a wide range of attacks. 				
Malware & tooling				
<ul style="list-style-type: none"> The malware variants both deploy, and are deployed by, various other malware families, including one another. Use commercial tools, such as Cobalt Strike, as well as LoLbins in various stages of the attack lifecycle. 				

Figure 25. Commodity loaders threat matrix.



QAKBOT

[Qakbot](#) (aka Qbot, Quackbot, and Pinkslipbot) is one of the most widely used and actively developed threats in the global cybercrime scene. Qakbot was initially discovered in 2007 as a banking trojan but, since then, its features have been continuously updated, allowing affiliates to form botnets, deliver secondary payloads, exfiltrate data, and use the malware in tandem with a wide range of modules.

In 2022, Qakbot was one of the most active commodity loaders seen in Talos' endpoint telemetry. In line with previous years, Qakbot affiliates continue using familiar TTPs, such as phishing emails containing malicious links or attachments as the initial infection vector. However, the operators are highly aware of, and responsive to, defenders' security detection protocols and are known to change their tactics accordingly. In 2022, Talos observed affiliates varying their use of previously observed tools and TTPs, such as social engineering lures, links, and file attachments, likely to evade detection. Additionally, for the first time this year, we observed

Qakbot incorporating new payloads, such as Black Basta ransomware and the legitimate red-teaming tool Brute Ratel.

Qakbot among most active commodity loaders impacting Cisco customers

Since late January 2022, Talos has observed increasingly high activity associated with Qakbot, as well as spikes in activity around May/June and August/September, according to telemetry from Cisco Secure Endpoint (**Figure 26**). This increased Qakbot activity is in line with a broader resurgence of the malware, as competing email-based botnets like Emotet and Trickbot have suffered continued setbacks from law enforcement and tech companies.

Two Snort SIDs (58280 and 58279) accounted for almost 90 percent of Qakbot detections. Both SIDs detect attempts to download SquirrelWaffle from a Qakbot-affiliated botnet, which could then be used to facilitate deploying the Qakbot payload. [SquirrelWaffle](#) is a malware loader known for providing threat actors an initial foothold onto compromised systems.

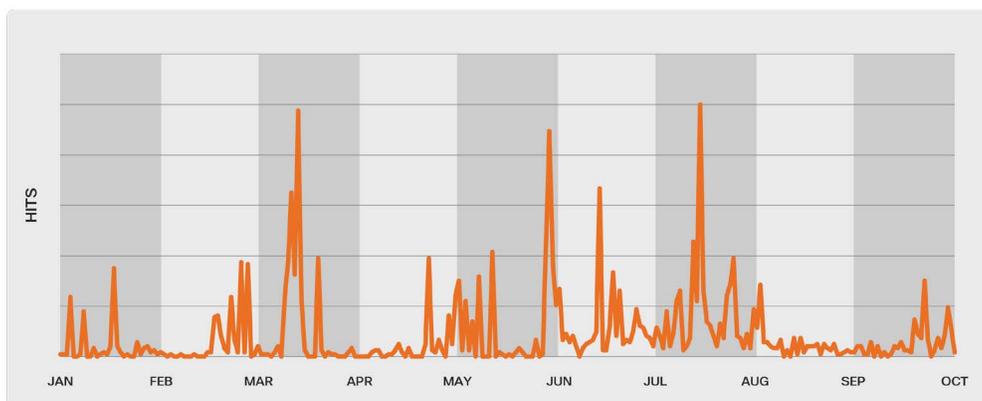


Figure 26. Qakbot mutex detections by Secure Malware Analytics.

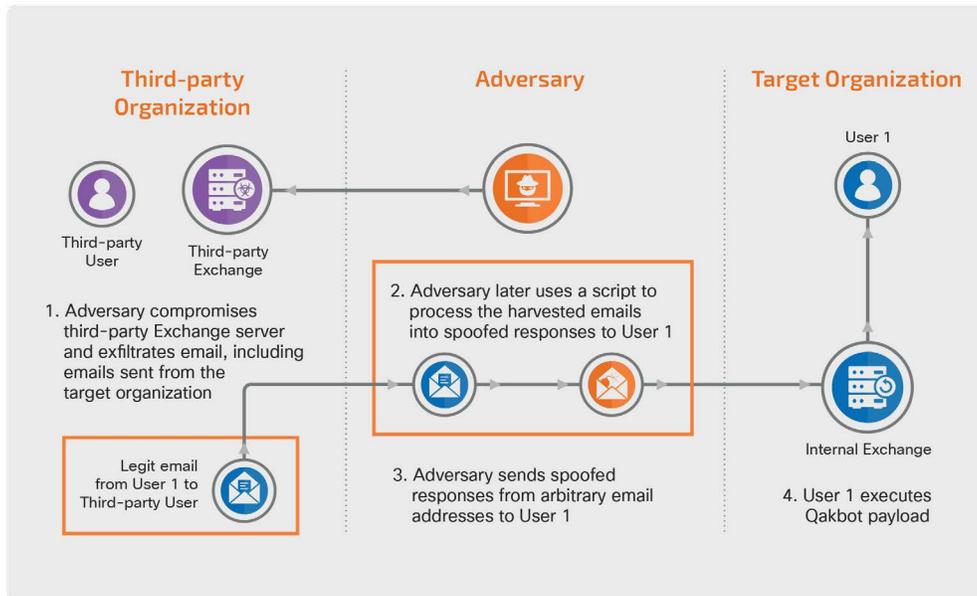


Figure 27. External thread hijacking.

Qakbot begins using external thread hijacking

Since at least March 2022, affiliates have delivered Qakbot via [external thread hijacking](#), whereby attackers use compromised email threads between the targeted organization and a trusted third party to send phishing emails, purportedly as a reply from the third party (**Figure 27**). This method is more likely to garner trust with the victim than a new email from an unfamiliar sender. Furthermore, thread hijacking does not necessitate compromising an email account that is internal to the victim’s organization, which would risk detection. In one CTIR engagement involving Qakbot, responders assessed the email threads were harvested months to years ago during the 2021 ProxyLogon campaign, tracked as CVE-2021-26855, targeting vulnerable Microsoft Exchange servers.

Affiliates move away from the XLSB files in favor of ISO files containing a LNK file

We observed Qakbot affiliates using hijacked email threads to deliver ZIP files containing an ISO file, which contain a LNK shortcut file and other files needed to execute the malware. The activity uses “mshta.exe” to execute remote Microsoft HTML applications (HTA) files, which download a dropper DLL that injects Qakbot into “wermgr.exe”, the Windows error reporting process (**Figure 28a**). Threat actors deploying Qakbot also use hijacked email threads to deliver ZIP files but switched from using “mshta.exe” to executing initial stages using “wscript.exe”, the Windows script host. This process launches a dropper DLL and finally injects Qakbot into “wermgr.exe”.

Qakbot transitioned to using LNK files from XLSB files, likely due to Microsoft’s announcement in mid-2022 that they would begin blocking document macros by default on downloaded content.

The macros are blocked based on a “mark of the web” (MOTW) attribute, which flags files that were downloaded from the web. However, delivering a LNK file—and other files like ZIP and ISO—only places a MOTW marking on the attachment itself. The contents do not have a MOTW marking, allowing operators to deliver macros-enabled documents undetected. Furthermore, the attached file itself could initiate downloading the payload if it contained for example a LNK file and a DLL. While these are not new TTPs for Qakbot, their episodic and opportunistic use indicates that Qakbot actors likely change their TTPs in response to victims’ dynamic security environments.

Operators leverage LoLBins, likely to evade detection

We observed Qakbot malware operators switching from using “rundll32.exe” to “regsvr32.exe” for both downloading and launching the Qakbot DLL. When “rundll32.exe” was used, the Windows binary had a command line parameter that contained a known PowerShell function name, which was easily detected and blocked. Switching to “regsvr32.exe” changed the Windows binary command line parameter to a Windows ActiveX Control file (OCX) in XML format, which avoided PowerShell detections. We also observed affiliates refining their execution methods by moving away from the Windows command line tool “curl.exe” and toward Microsoft’s calculator application, “calc.exe,” likely because it is vulnerable to a DLL side-loading attack. “Calc.exe” will load a DLL from its current folder instead of loading the original one from the System32 directory, so Qakbot operators can use a legitimate application to load their malicious DLL, further enhancing the legitimacy of their operations.

Operators continue to incorporate new and advanced open-source tools

For the first time, in June 2022, we observed Qakbot operators incorporating Black Basta ransomware and Brute Ratel, a legitimate red-teaming tool into their infection chain, alongside previously observed tools such as the red-teaming

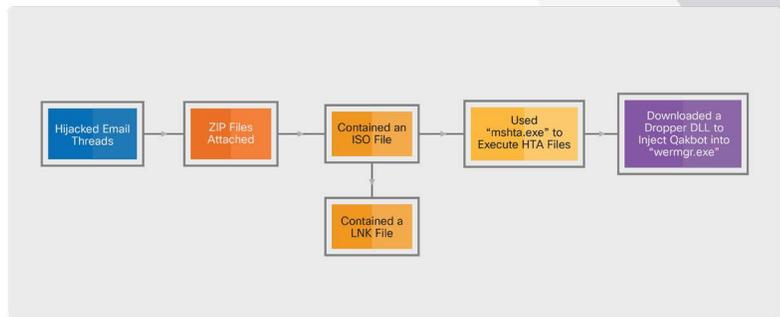


Figure 28a. Qakbot infection chain using LNK files and “mshta.exe”.

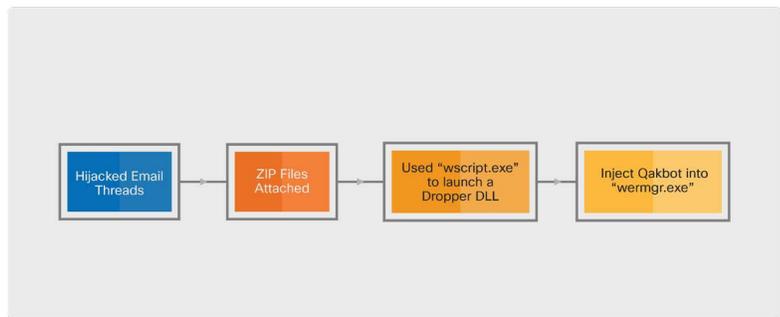


Figure 28b. Qakbot infection chain using “wscript.exe”.



tool Cobalt Strike and the hacking tool DarkVNC. Qakbot operators' deployment of Black Basta, a relatively new ransomware variant, highlights their intent to continue to partner with other adversaries, as well as other adversaries' perceived value of incorporating Qakbot into their own operations. This is consistent with behavior from other modular threats like Emotet and Trickbot, where we have seen collaboration between email-based threat actors and other ransomware groups. Qakbot operators' use of Brute Ratel suggests the tool is likely rising in prominence, as Qakbot actors continue to incorporate new threats and techniques into their operations that will help them remain effective. Furthermore, the new incorporation of Brute Ratel bolsters our previous assessment that Qakbot developers continue to make improvements to the malware's overall infection chain to make it more difficult to detect.

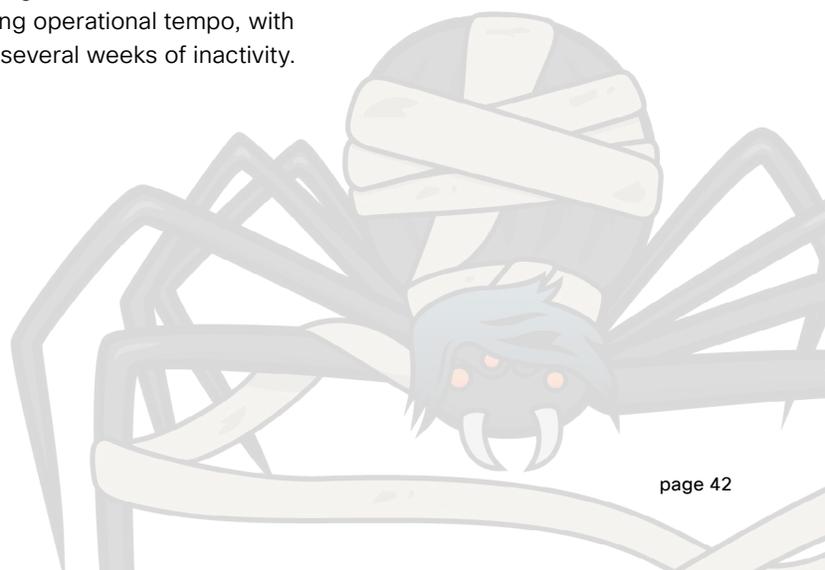
EMOTET

[Emotet](#) is a modular trojan first discovered in 2014 that has become one of the most widely distributed malware threats in recent years. Originally developed as a banking trojan, it is now often used to obtain an initial foothold in new environments from which the adversary can launch additional malware. [In early 2021](#), international law enforcement announced a takedown campaign to disrupt Emotet, effectively removing the botnet from the threat landscape. In November 2021, Emotet re-emerged and used Trickbot infrastructure to begin rebuilding its botnets. While Emotet's current campaigns have not returned to the same levels seen prior to the 2021 takedown, it has once again become a serious threat that continues to amplify.

Emotet activity likely not fully recovered from being dismantled in 2021

Emotet activity is traditionally characterized by episodic [spikes in activity](#) and periods of dormancy that can range from weeks to months. While these periods of inactivity correspond to lack of spam distribution, the botnets are typically still operational and, as such, previously infected systems can still be leveraged for intrusions. Emotet activity in 2022 maintained this varying operational tempo, with several large spikes in activity broken up by several weeks of inactivity.

While Emotet's current campaigns have not returned to the same levels seen prior to the 2021 takedown, it has once again become a serious threat that continues to amplify.



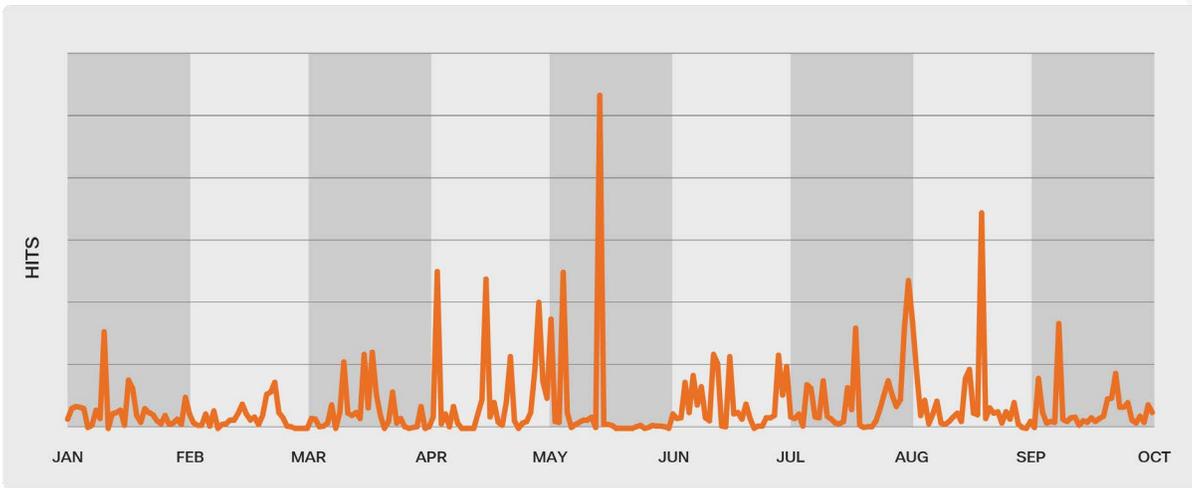


Figure 29. Emotet mutex detections by Secure Malware Analytics.

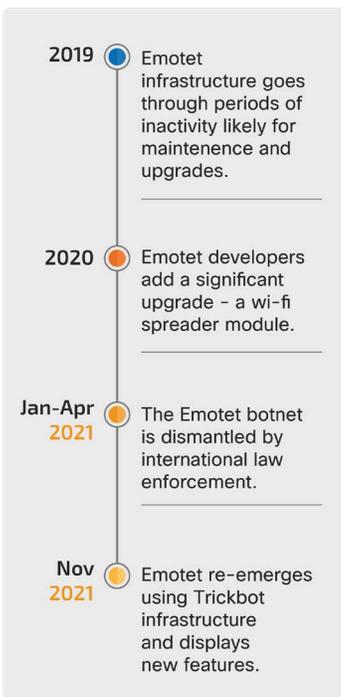


Figure 30. Timeline of Emotet activity.

This is also reflected in **Figure 29** tracking mutex detections by Secure Malware Analytics.

Out of 26 Snort SIDs that detect Emotet exploitation attempts, we found the top SID (48402) that accounted for 99 percent of detections is triggered by an infected host attempting to make outbound C2 connections with the Emotet botnet. At least some of this activity is likely accounted for by devices that were previously infected by Emotet when its botnet was operating at full strength and are still attempting to connect to the older infrastructure that was dismantled by law enforcement (**Figure 30**).

Operators move away from using PowerShell to obfuscate activity

While most Emotet activity observed in 2022 involved PowerShell, some actors tried different tactics in response to defenders’ close monitoring of the scripting language. For example, in one campaign, Emotet was downloaded using the Windows download and data transfer utility “curl.exe” instead of PowerShell. Additional LoLBins were used as well, including “regsvr32.exe”, to both download and launch payloads. When run with an OCX file parameter, “regsvr32.exe” can download an executable using HTTP and run it, a tactic similarly used by Qakbot as described above.

Operators launch payloads via LNK and Excel files

In 2022, many TTPs traditionally associated with Emotet remained consistent, such as reliance on phishing as the initial infection vector and social engineering to manipulate users into clicking on a link or



attachment. However, similar to Qakbot and other malware families, in 2022, Emotet adopted a new infection chain that incorporates LNK files, moving away from using Microsoft Word attachments to Microsoft Excel attachments with embedded macros. When Emotet reemerged in November 2021 after a short hiatus, it operated on two separate botnets called epochs that delivered spam messages containing password-protected ZIP archives, Word documents, or Excel spreadsheets with embedded VBA macros. In 2022, we observed these epochs each using a different method to deploy Emotet. One sent phishing messages containing XLS attachments with embedded macros, and the other sent emails with malicious links or malicious attachments that were either password-protected ZIP files, Excel documents without macros, or LNK files.

ICEDID

[IcedID](#) (aka BokBot) is a modular commodity loader initially created in 2017 to steal financial data. It has since expanded its functionality to also deliver subsequent payloads, such as ransomware. It primarily targets U.S. organizations in the financial services sector and has a wide range of malicious capabilities, such as browser hooking, credential theft, establishing an adversary-in-the-middle (AiTM) proxy, and establishing remote control using a virtual network computing (VNC) module.

Operators use new TTPs to deploy IcedID and enhance obfuscation

Prior to 2022, IcedID affiliates most commonly sent phishing emails with a password-protected ZIP file attachment that contained a Word document embedded with macros that when executed would launch the IcedID payload. In 2022, Talos observed affiliates conducting phishing campaigns using different TTPs to deploy IcedID. In some cases, the emails had an ISO file attachment that contained a ZIP file, which contained a LNK and DLL. In other cases, emails had ISO file attachments that contained a LNK and DLL, omitting the ZIP file. Finally, we saw emails with HTML attachments containing JavaScript and a DLL. In each case, “rundll32.exe” was used to run and execute the DLL. Often, the IcedID executables were digitally signed, possibly to feign legitimacy in order to bypass security applications.

Talos also observed campaigns in which threat actors used evasive measures while deploying IcedID. In one case, the phishing emails contained a Word document with embedded VBA macros instead of a LNK file. During execution, the malicious VBA macros created a renamed copy of “rundll32.exe” in an attempt to evade security applications that look for malicious activity by identifying pattern matching on “rundll32.exe”. In another case, the IcedID installer

Often, the IcedID executables were digitally signed, possibly to feign legitimacy in order to bypass security applications.



script was obfuscated by inserting the caret symbol in between letters to try and evade pattern matching.

```
cmd.exe /c "start 73gLujjt.png && start r^un^d^l^l3^2 T^YnvUcnF.d^l^l, #1"
```

Operators may be adopting Bumblebee in place of IcedID

Since its initial discovery, IcedID activity has shifted away from primarily functioning as a banking trojan, toward more commonly being used as a dropper for other malware. Though it seemed it was poised to fill the void left by Emotet after the botnet was dismantled in January 2021, IcedID has not been as active in 2022 as other commodity loaders, such as Qakbot. Around March a new loader called Bumblebee was first observed and believed by several security researchers to be in the process of replacing IcedID. This is based on observed threat activity dropping Bumblebee, by operators who are known to have previously used IcedID. While we cannot assess at this time whether adversaries are using Bumblebee instead of IcedID, our telemetry does reflect a sharp drop in IcedID hits on Snort rules between March and April, around the time Bumblebee was first observed (**Figure 31**). We do note, however, that at the time of writing, Bumblebee has not appeared in any CTIR engagements, and our telemetry has detected much fewer Bumblebee events compared to IcedID throughout 2022.

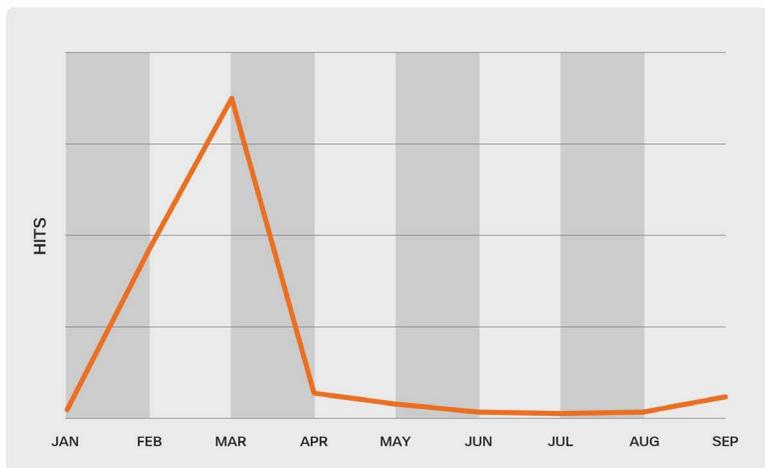


Figure 31. Snort activity tracking IcedID.

IcedID used to target Ukrainian entities, likely in support of Russia’s war against Ukraine

Talos’ internal Ukraine task unit monitors daily threat activity across nearly 40 Ukraine-based Cisco customers from various critical



infrastructure sectors, including energy and utilities, banking, healthcare, transportation, and defense. In April 2022, the task unit observed IcedID on several Ukrainian customers’ environments in the energy and government sectors around the same time that open-source reporting indicated that Conti, a prolific pro-Russia ransomware group, deployed IcedID in several campaigns against Ukrainian entities in response to the Russia-Ukraine war. In one operation, Cisco Secure Endpoint detected the creation of scheduled tasks to execute malicious DLLs using “rundll32.exe” or “regsvr32.exe” on a compromised endpoint. This led to the discovery of multiple additional Cisco Secure Endpoint detections involving IcedID deployed on the system. In a second operation, IcedID was likely deployed via a malicious file. The file appeared with different names, one of which was in Russian language, across several endpoints. Additionally, the file used HTTP traffic for command-and-control (C2) and downloaded subsequent files affiliated with IcedID. There is no indication these events are connected but they are all likely in support of the Russian war effort in Ukraine.

TRICKBOT

[Trickbot](#) was originally discovered in 2016 as a banking trojan, but over the years, its functionality expanded to drop other malware, leading to highly lucrative ransomware attacks. The malware was also constantly updated to grow the botnet, improve functionality, and work congruently with a wide range of modules that allowed threat actors to tailor attacks to the victim’s environment.

Trickbot remains a concern despite significantly decreased activity

At the close of 2021, Trickbot was [one of the most widely used malware strains](#) in the cybercrime scene, and even showed signs of expanding, as the [FBI](#) officially linked Trickbot to the Diavol ransomware, first discovered in October 2021 (**Figure 32**). However, between December 2021 and February 2022, Trickbot activity inexplicably began plummeting. Although we have since seen some minor developments, many believe the operators have abandoned the botnet. Several theories have circulated, speculating that Trickbot operators moved on to work for Conti, an aforementioned ransomware group with whom Trickbot had a longstanding close relationship, or the operators abandoned Trickbot in favor of another email-based botnet, like Emotet. While the exact cause is unknown, it is unlikely the operators were forced to stop due to external setbacks such as international law enforcement disruptions or a competing cybercriminal group.

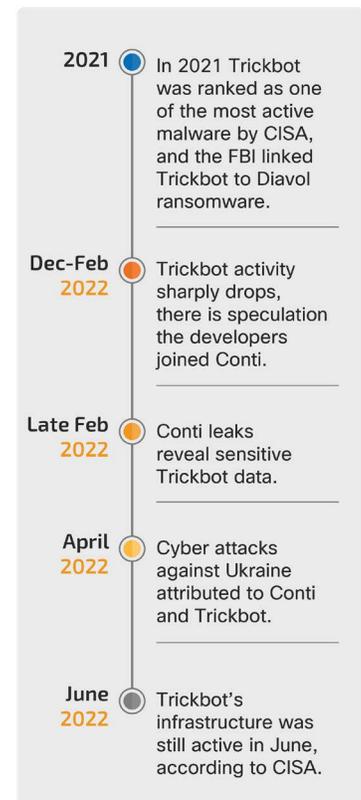


Figure 32. Timeline of Trickbot activity.



Talos continues to monitor for Trickbot activity as the group has historically reemerged after significant setbacks and long periods of inactivity.

While some believe Trickbot is no longer actively used by its original operators, its botnet is still showing activity in our endpoint telemetry, and [CISA](#) confirmed that the group’s infrastructure was still active as of July 2022. Considering the numerous public reports on Trickbot’s inactivity, there are several possible explanations that could account for at least some of the Trickbot activity our telemetry detected this year.

Firstly, dismantling the botnet would not automatically remediate previously infected systems. Those systems can remain infected and continuously attempt to connect to Trickbot C2 servers that have been disabled, which would trigger detection systems, such as Snort. Out of 75 Snort IDs (SIDs) that detect Trickbot exploitation attempts, we found the top SIDs that accounted for over 95 percent of detections were 50714, 57893, and 54212. The first SID is triggered when it detects a Trickbot self-signed certificate and the latter two SIDs are triggered when a Trickbot-infected device beacons out to a Trickbot C2. These lingering detections do not necessarily correspond to active Trickbot events or indicate any kind of response from the C2 server or that a connection was established.

Secondly, Cisco’s malware analysis sandbox, Secure Malware Analytics, allows individuals to manually upload malware samples in addition to automatically collecting currently active samples. It’s possible that researchers are analyzing older Trickbot samples, which would skew the number of Trickbot detections.

Thirdly, other threat actors could be leveraging previously infected Trickbot devices and older Trickbot infrastructure to conduct their own operations, which would then be detected in our telemetry as Trickbot. For example, if Trickbot has moved on to work for Conti or adopted Emotet as some security researchers have suggested, those malware families may be using old Trickbot infrastructure. Furthermore, cybercriminals are known to have purchased access to systems compromised by Trickbot to conduct operations.

Talos continues to monitor for Trickbot activity as the group has historically reemerged after significant setbacks and long periods of inactivity. Furthermore, since there is no indication of external factors forcing the group to halt operations, it is conceivable they may choose to start investing in Trickbot again at some point in the future.

Tracking metrics using automated hunts

One of Talos’ internal teams is responsible for developing automated searches called “hunts” for Secure Endpoint Premier customers. These hunts search for behaviors that are commonly associated with various malware, including Qakbot, Emotet, IcedId, and Trickbot. The hunts help identify previously unknown, or ongoing non-remediated



threats, within a customer’s environment. Each time a hunt detects the particular behavior it was programmed to search for, a report is generated. While the results cover a limited set of Cisco customers, it provides another data set for us to analyze about threat activity throughout 2022.

In 2022, we created two new automated hunts searching for Qakbot behaviors; specifically, the use of the “curl.exe” command and “rundll32.exe” to call the “DllInstall” function, allowing Qakbot to inject itself into “wormgr.exe”. We also created one new hunt for Emotet behavior searching for Invoke-Expression (IEX) commandlet execution without calling “powershell.exe”. Older hunts created prior to 2022 also generated reports. They detected Emotet behavior using Microsoft Office products to execute malicious files via “regsvr32.exe” and IcedID behavior using “rundll32.exe” to execute suspicious DLLs and call their functions by ordinal number instead of function name.

CONCLUSION

We assess that victims’ security environments will likely continue to influence the TTPs of affiliates who use Qakbot, Emotet, and IcedID. These groups have continuously evolved their malware since they were first active to include updated features, such as modules that give affiliates the flexibility to use these threats in a variety of ways, and to carry out tasks other than the initial intended function of stealing financial data. There is no reason to suspect this will stop. Notably, according to CTIR data commodity malware was the top threat in Q2, comprising 20 percent of threats observed, displacing ransomware which had held that position for over a year.

We further assess the overall threat of commodity loaders will likely remain high in the foreseeable future as they are reliably successful tools for financially motivated cybercriminals and have proven to be resilient to botnet disruptions and security solutions. Furthermore, new malware families are continuously being released, reflecting a desire among cybercriminals to use this type of malware.

Finally, we assess the Trickbot botnet will remain active due to the malware’s global impact and the sale of access to Trickbot compromised networks to cybercriminals. This activity does not necessarily mean the malware is being actively used by the developers, but it does mean that Trickbot remains a potentially serious threat that we continue to track closely.



 | TALOS

2022 **YEAR IN REVIEW**

ADVANCED PERSISTENT THREATS



Across most APT activity observed this year, there was a greater trend towards the incorporation of customized malware and the deployment of newer variants of previously known malware.

ADVANCED PERSISTENT THREATS

The geopolitical environment became even more complex and tense in 2022. This led to changes in the threat landscape as has been described in other sections of the report. Advanced persistent threats (APTs), especially those that are state-sponsored or state-aligned, also adapted to these geopolitical challenges, particularly Russian APTs in response to the war in Ukraine. In addition, Talos observed several offensive cyber campaigns linked to a number of groups stemming from Iran, China, North Korea, and countries in the Indian subcontinent engaging in a variety of operations ranging from espionage and intellectual property theft to destructive malware. Across most APT activity observed this year, there was a greater trend towards the incorporation of customized malware and the deployment of newer variants of previously known malware. Moreover, APT groups continue using publicly known exploits, such as in Log4j utilities, to compromise organizations with weak patching protocols.

As befits their name, APT groups are very difficult to eradicate from a network once they find their way in, they often achieve multiple means of access. In addition, our research shows that these groups are continuing to adapt to defenders as well, consistently updating their tooling and evolving their behavior to achieve their goals.

One interesting trend to note is that this year we observed more APT activity in our Cisco Talos Incident Response (CTIR) engagements than usual. This includes the Iran state-sponsored MuddyWater group and several China-affiliated APTs. These engagements allowed us to gain deeper insights into their operations, enhancing our general understanding of them.

RUSSIA

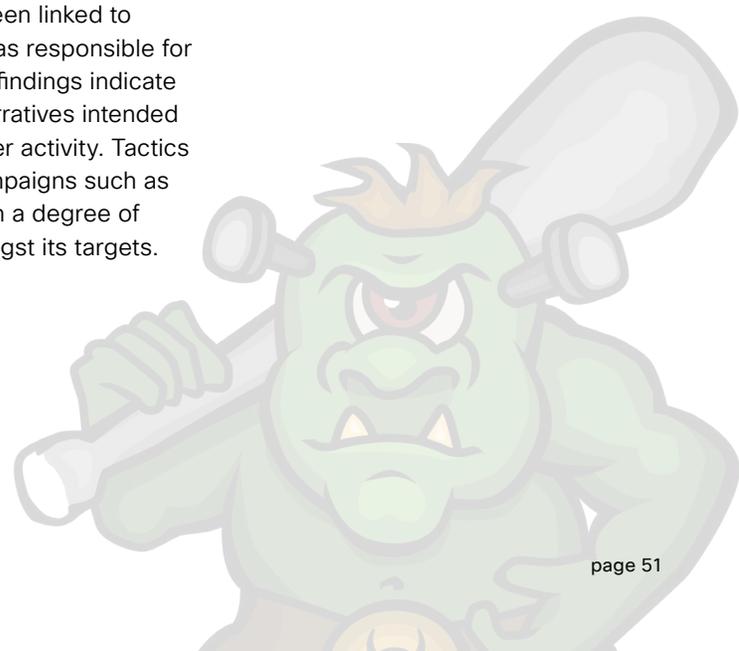
Russia-linked and state-sponsored groups were some of the most active APTs Talos observed in 2022, and these groups became especially high-interest for us as we positioned ourselves to support Ukrainian entities during the war. Moscow continues to support a broad range of offensive cyber activities to achieve state interests, which include ensuring internal political security, controlling the information environment, and advancing regional and international objectives. Talos tracks numerous APTs engaged in cyber espionage, cyber influence, and/or destructive attacks, and those efforts intensified leading up to and coinciding with Russia's invasion of Ukraine in February. This section's assessment of Russian APTs observed this year does not include the various cybercriminal and ransomware groups likely operating in Russia with the tacit approval of the government.



Threat actors engaged in destructive attacks, further enabling cyber influence operations

Talos assesses that prior to Russia’s military operations in Ukraine, suspected state-sponsored actors engaged in a campaign to disrupt Ukrainian computer networks, and then leveraged the campaign in an influence operation casting blame on Ukrainian forces. Labeled “[WhisperGate](#),” the destructive attacks shared similarities with the [NotPetya](#) wiper malware that affected Ukrainian and global entities in 2017. Like NotPetya, WhisperGate’s payload was a malware executable designed to wipe the entire master boot record (MBR) and leave behind a ransom note. However, ransomware and extortion were clearly not the final objective, since the overwritten MBR could not be recovered. Talos estimates that the actor behind this attack likely had access to victim networks for many months. They may have exploited supply chains or vulnerabilities in Log4j and OctoberCMS, according to [CERT-UA](#), and we believe they used stolen credentials. Ukrainian victims were subsequently infected with at least four other wiper families including [HermeticWiper](#), [CaddyWiper](#), [DoubleZero](#), and [CyclopsBlink](#), indicating what likely required an advanced level of technical sophistication, planning, and persistence highly characteristic of state-sponsored actors.

In particular, characteristics of the WhisperGate attack appeared similar to campaigns previously linked to the APT group Fancy Bear (aka APT28, Tsar Team, STRONTIUM), a suspected unit of Russia’s Military Intelligence Directorate of the General Staff (GRU). Beyond WhisperGate’s destructive effects, we observed actors associated with Fancy Bear who likely used the attacks as a pretext for disinformation operations against the Ukrainian public. We found [evidence](#) in the WhisperGate attack—which attempted to disguise itself as a nationwide ransomware campaign—that could be traced to a previous Russian disinformation operation. The actor’s contact email in the fake WhisperGate ransom note was used in a previous disinformation campaign. By tracing the email, we discovered that a known Russia-aligned propagandist—who has been linked to previous Fancy Bear disinformation campaigns—was responsible for fabricating the content used in the operation. Our findings indicate that APT actors have attempted to create false narratives intended to complicate attribution of Russian malicious cyber activity. Tactics such as inserting “false flags” into destructive campaigns such as WhisperGate provide the Russian government with a degree of plausible deniability and further sow discord amongst its targets.





ACTOR PROFILE

Gamaredon

Aliases
 Primitive Bear, Armageddon, Shuckworm, Winterflounder, BlueAlpha, BlueOtso, IronTiden, SectorC08, Callisto, Trident Ursa

Affiliations
 Russia

Active since
 2013

Goals
 Espionage, data theft, establishing long-term access

Victimology
 Actively targets Ukrainian entities, specifically government organizations, critical infrastructure and entities affiliated with Ukraine’s defense, security and law enforcement apparatus. Secondary operations include broad targeting of entities in Europe and globally, including, government, military, humanitarian and non-profit organizations.

Notable TTPs
 Social engineering techniques, spear-phishing, compromised domains and dynamic DNS, long-term access, data exfiltration, custom script-based malware.

Malware & tooling
 Gamaredon employs a variety of custom, self-developed implants that are used exclusively by the adversary ranging from customized script-based malware to infostealers and backdoors. Notable malware families include GammaLoad, GammaSteel, Giddome, Powerpunch and Pterodo.

Figure 33. Gamaredon threat actor profile.

Persistent cyberespionage campaigns enabled Russian military operations

Russia state-sponsored APTs have long engaged in cyberespionage operations against Ukraine, but the importance of spycraft became even more pronounced in the lead up to Russia’s invasion of the country in February. Threat actors very likely used their persistent access for intelligence-gathering operations in support of preliminary military objectives, which included destabilizing the Ukrainian government’s command and control, dominating the information environment, supporting invading forces, and creating pathways for disruptive cyber attacks. Talos monitored several APT groups engaged in cyberespionage against Ukrainian targets, including Gamaredon and Turla.

Cisco Talos closely tracks activities associated with the Gamaredon Group, an APT which is broadly suspected to be a team of Russian government-supported actors in Crimea **(Figure 33)**. Gamaredon has historically primarily targeted Ukrainian political, military, and other government and non-government organizations in support of the Kremlin’s strategic interests.

Earlier this year, Gamaredon actors [launched](#) a massive spear phishing campaign designed to infect Ukrainian government users with information-stealing malware. The APT actors sent emails containing malicious documents (maldocs) designed to retrieve a remote template containing malicious VBS macros. Upon user execution of the document, the macros downloaded RAR archives containing Windows shortcuts (LNK) with filenames related to Russia’s invasion of Ukraine **(Figure 34)**. Upon opening the LNK, a series of PowerShell scripts retrieve payloads from remote Gamaredon infrastructure. The multistage infection process ultimately delivers a customized information-stealer that searches victim endpoints and exfiltrates sensitive data. If directed by the operators, the implant can also deliver additional malicious payloads. Our analysis of the victims, infrastructure, TTPs, and malicious samples in these attacks is consistent with [reporting](#) from CERT-UA attributing similar activity to Gamaredon.



LNK Filename	Translation
Розвідувальне зведення від 08 серпня 2022 року щодо різких змін в оперативної обстановці.lnk	Intelligence summary from August 8, 2022 regarding drastic changes in the operational environment.lnk
Щодо надання пропозицій до наради Про стан протидії злочинності на території проведення ООС.lnk	Regarding the proposals submission for the meeting on the state of combating crime in the territory of the OOC.lnk (Talos Note: OOC stands for Joint Forces Operation)
Інформація щодо злочинів, пов'язаних зі збройним конфліктом, вчинених стосовно дітей та у сфері охорони дитинства станом на 10.08.2022.lnk	Information on crimes related to the armed conflict committed against children and in the field of childhood protection as of 10.08.2022.lnk
Щодо порушення кримінального провадження (ЄРДР 2201605000000123 від 09.08.2022 ч.1 ст.111).lnk	Regarding the initiation of criminal proceedings (ERDR 2201605000000123 dated 09.08.2022, part 1, article 111).lnk

Figure 34. Gamaredon LNK filenames containing geopolitical lures, found in spear phishing emails.

ACTOR PROFILE

Turla

Aliases
Venomous Bear, Waterbug, Snake, Uroburos, WhiteBear, Iron Hunter, ITG12, KRYPTON

Affiliations
Russian origin, attributed by some security researchers to the Russian FSB

Active since
2004

Goals
Long-term, persistent cyber espionage in support of Russian state intelligence objectives

Victimology
Targeted operations against high-value military, government, diplomatic, and private sector entities, primarily in countries aligned with NATO and post-Soviet countries. Targets can vary based on geopolitical events that align with Russian intelligence objectives.

Notable TTPs
Turla employs watering holes, sends spear phishing emails leveraging social engineering techniques, deploys custom malware, and exploits known vulnerabilities to conduct cyber espionage and exfiltrate data. Turla is adept at defense evasion, and uses techniques such as custom decryption routines and modified uncommon encryption methods.

Malware & tooling
Turla employs a wide range of custom malware, modified open-source malware, and publicly available tools. Notable custom tools include Tiny Turla, Uroburos, and Mosquito.

Another indication of the high level of Russian APT activity comes from evidence of cyber operations linked to the Turla group (**Figure 35**). Based on an internal, comprehensive review of Turla threat activity, we found that the group remains engaged in highly targeted operations against military, government, diplomatic, and private sector entities in countries aligned with NATO as well as in post-Soviet states. This APT continues using watering holes, spear phishing campaigns, social engineering techniques, exploitation of known vulnerabilities, and custom backdoors such as Crutch and Gazer to gain access and exfiltrate data. Turla actors have also hijacked satellite communications for command-and-control (C2) infrastructure, a technique consistent with our [reporting](#) last year.

Figure 35. Turla threat actor profile.



Talos estimates that Gamaredon, Turla, and several other Russian APT groups will continue to conduct cyberespionage campaigns globally, but with a much greater emphasis on Ukraine and NATO allies as the war proceeds. They will continue to collect intelligence of military value to support Russia’s war efforts and political intelligence that may support Russia’s influence operations and strategic objectives. We can reasonably expect that as Russian strategic interests evolve, so too will the operational priorities of these groups. We also expect this activity to continue past any kinetic ceasefire on the battlefield.

IRAN

Talos made several significant discoveries in 2022 related to Iran state-sponsored APTs, indicating that these groups remain highly engaged in cyberespionage to achieve Iranian political, economic, and national security objectives. Iran state-sponsored groups continue to conduct pervasive, malicious cyber attacks against entities in North America, Europe, the Middle East and Asia with the primary goal of stealing intellectual property and collecting intelligence. However, we also believe that Iranian APTs retain the technical means to deploy ransomware and other destructive malware, and—as the damaging July attacks against the Albanian government suggest—are willing to disrupt public services and critical infrastructure.

Iran state-sponsored APT likely a conglomerate of regionally focused subgroups

The APT known as MuddyWater, a group of threat actors [attributed](#) to Iran’s Ministry of Intelligence and Security (MOIS), was especially active in 2022, using persistent access to target global energy and telecommunications firms, the defense industrial base, and local and national governments **(Figure 36)**. Earlier this year, we conducted a comprehensive review of multiple MuddyWater campaigns and [concluded](#) that the actor is likely a conglomerate of multiple independent teams using different tactics against targets in specific regions of the world. This finding is contrary to

ACTOR PROFILE

MuddyWater



Aliases

Static Kitten, MERCURY, Seedworm, TEMP.Zagros, Earth Vetala

Affiliations

Iran, Ministry of Intelligence and Security (MOIS)

Active since

2017

Goals

Espionage and intellectual property theft in support of Iranian national security and economic objectives; ransomware for disruptive operations.

Victimology

MuddyWater predominantly focuses on high-value targets in the Middle East, Asia, North America, Africa, and Europe. The group has conducted cyber operations against both public and private organizations and has targeted numerous industry verticals including telecommunications, oil and gas, information technology, academia, local and national governments, and NGOs.

Notable TTPs

MuddyWater uses spear phishing emails to deliver ZIP files that contain additional malicious components. The actors exploit known vulnerabilities and use open-source tools to gain access to and exfiltrate sensitive data, move laterally, and deploy follow-on malware. MuddyWater also uses side-loading DLLs to trick legitimate programs into running malware and obfuscates PowerShell scripts to hide C2 functions.

Malware & tooling

MuddyWater uses multiple malware threats, including the POWERSTATS, Small Sieve, and Mori backdoors, PowGoop loader, and Canopy/SloughRAT remote access trojans. The actors use publicly available tools, such as PowerShell, VBScript, and JavaScript, as well as living-off-the-land binaries (LoLBins). Additional post-exploitation and remote access tools include Mimikatz, ConnectWise, and RemoteUtilities.

Figure 36. MuddyWater threat actor profile.



the prevailing view that MuddyWater operates as a single actor.

Based on a comprehensive review of MuddyWater activity from 2021 to 2022, we found both unique and shared TTPs in campaigns against entities in the Middle East, Pakistan, Armenia, Turkey, and the Arabian Peninsula. We uncovered a pattern in which artifacts such as maldocs, infection tokens, downloaders and various persistent access tools—uniquely used in previous campaigns against specific geographic targets—were later reused and combined with additional techniques in separate

campaigns against other geographic targets. Talos also found that in each geographically distinct campaign, at least one completely new TTP was introduced in each operation (**Figure 37**).

These observations strongly support our belief that MuddyWater consists of multiple groups charged with targeting a specific country or region. While it appears that each group develops independent TTPs, tools, and malware, they borrow others from different MuddyWater teams, those that have been proven effective in separate geographic campaigns.

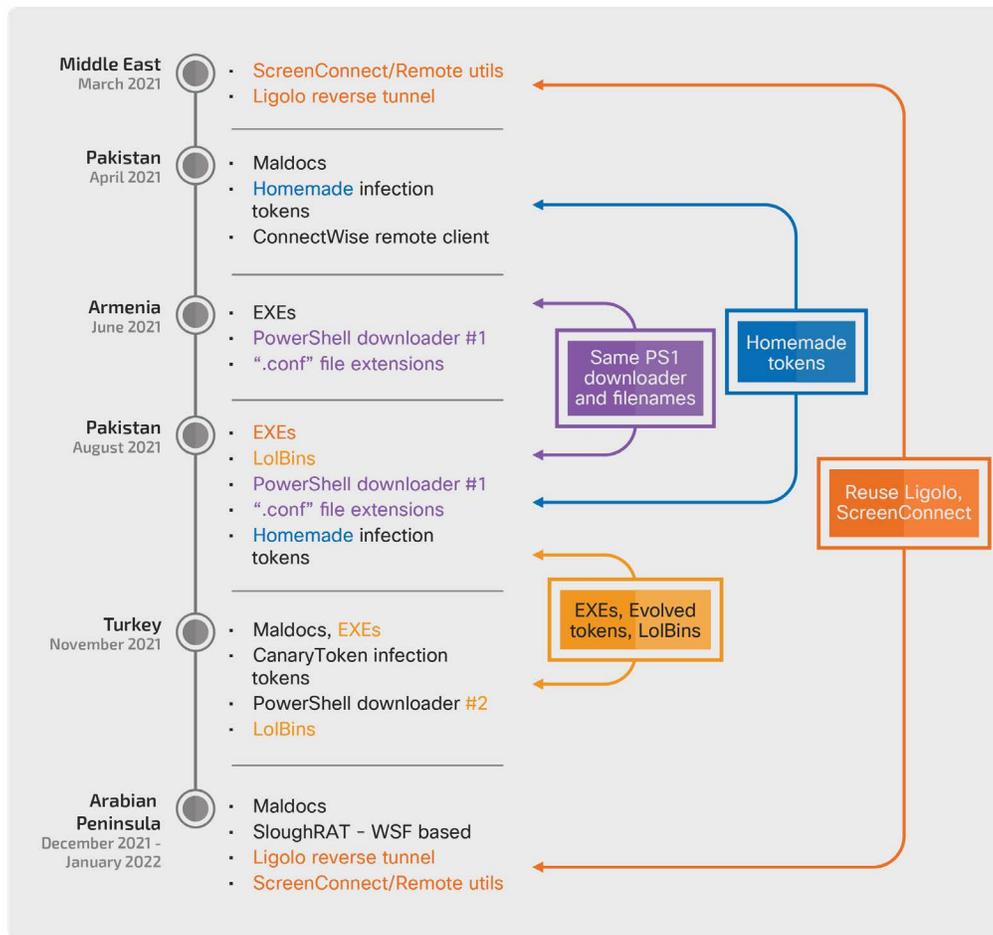


Figure 37. MuddyWater campaigns and overlaps in TTPs.



In line with previous activity, MuddyWater employed phishing emails, PDFs with embedded links, and weaponized Microsoft office documents to gain initial target access in 2022.

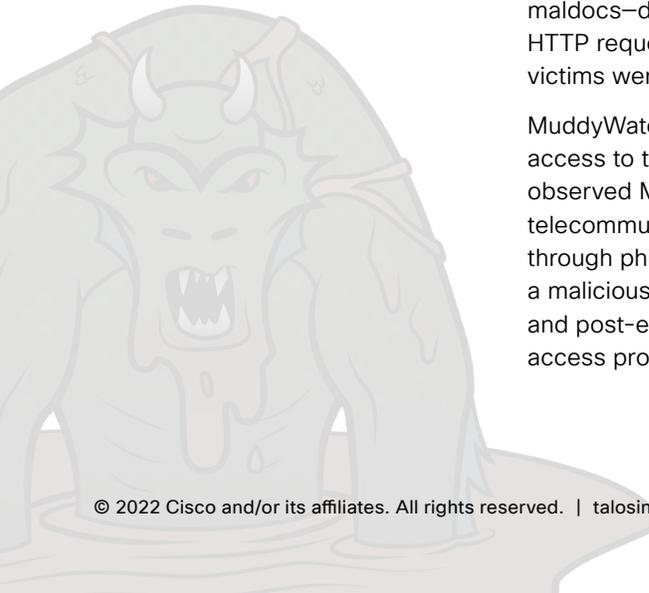
MuddyWater leverages diverse techniques for cyberespionage

In 2022, MuddyWater used diverse techniques for initial infection and intelligence collection which, based on our findings, is consistent with the group’s historic ability to update its attack lifecycle. In line with previous MuddyWater activity, the threat actors employed phishing emails, PDFs with embedded links, and weaponized Microsoft office documents to gain initial target access. For example, earlier this year, Talos [reported](#) on MuddyWater attempts to compromise Turkish government entities using malicious PDFs and Microsoft Excel (XLS) files masquerading as real documents from the Turkish Health and Interior ministries. The PDF files contained embedded links that downloaded XLS files containing malicious macros. In other variants, we observed that clicking a malicious URL would deliver a Windows executable file. In both cases, the attack culminated with the execution of VBS or PowerShell-based scripts which ultimately retrieved the final payload.

This year, MuddyWater deployed a new implant named [SloughRAT](#), also known as [Canopy](#). The actors sent phishing emails containing malicious Excel files to Middle Eastern targets, according to CTIR findings. Upon user execution, the file’s malicious macros dropped two scripts, one of which was the Windows Script File (WSF)-based remote access trojan SloughRAT. SloughRAT collects system information, including the IP address of the infected endpoint, and user and system names. The implant receives commands from a C2 server, and any data collected from the network as a result of the command execution is sent via an HTTP POST request to another MuddyWater server. We also observed MuddyWater deploy the open-source reverse-tunneling tool Ligolo for even greater attacker control.

This APT has also employed tracking tokens in its espionage operations. In the aforementioned campaign targeting Turkey, MuddyWater actors used Canary Tokens ([canarytokens\[.\]com](#)), a service for tracking embedded tokens in objects like documents, web pages, and emails, to alert the sender when the receiver opened an object. In addition to dropping scripts, some VBA macros in the maldocs—delivered in phishing emails to Turkish recipients—sent HTTP requests to [canarytokens\[.\]com](#), alerting MuddyWater when victims were infected.

MuddyWater is sophisticated in the way it achieves persistent access to target environments. In a CTIR emergency response, we observed MuddyWater activity in the network of a Middle East-based telecommunications company. The APT gained its initial foothold through phishing emails sent to the company’s employees containing a malicious attachment. The operator dropped a plethora of backdoor and post-exploitation tools, including Mimikatz, and legitimate remote access programs such as ConnectWise and RemoteUtilities. However,





even after remediation, the company was again compromised earlier this year. We found the presence of additional MuddyWater backdoors on server infrastructure and the use of Impacket for remote service execution and execution of attack tools. We assess that MuddyWater is adept at diversifying its hidden accesses.

CHINA

In 2022, China-linked APT actors targeted entities across a wide variety of industry verticals, predominantly those that correspond to Beijing’s foreign and domestic policy goals. Based on Talos intelligence, our findings are consistent with U.S. government [reporting](#) that Chinese malicious cyber operations aim to steal intellectual property and sensitive data from key industries and critical infrastructure. Typically, the most targeted verticals are those determined to be national priorities in China’s five-year plans. Relatedly, our research indicates that Chinese APTs attempted or successfully gained access to telecommunications firms, software and managed service providers, healthcare and public health entities, defense companies, government agencies, and nonprofits, among other sectors that may involve China’s national interests. Talos estimates that these actors’ goals were to maintain persistent access to enterprise networks for intelligence collection and data theft.

We also tracked Chinese APT activity as it adapted to emerging regional and global geopolitical events. In the lead up to and following the Russia-Ukraine war, Talos researchers observed targeted espionage campaigns against European entities, attributed to known Chinese APT groups. Later in the year, amid heightened tensions between China, the United States, and Taiwan, we monitored for APT activity coinciding with DDoS attacks against several Taiwanese government websites.

Mustang Panda exploits the Russia-Ukraine war to target European entities

Earlier this year, the Chinese APT group Mustang Panda [leveraged](#) the Russia-Ukraine war to target European organizations, including Russian entities, in a widespread espionage campaign. Beginning around January 2022, Mustang Panda began sending European victims phishing attachments consisting of themes related to EU political activities. These included lures related to the European Commission report on state aid to Greece, and later, the EU’s 2022 human rights priorities. Corresponding with Russia’s invasion of Ukraine in February, Mustang Panda changed the themes to include documents concerning military activities along Russia’s borders with Ukraine and Belarus. In all cases, the emails were the first stage in the delivery of a multi-stage infection chain meant to download tools and





ACTOR PROFILE

Mustang Panda



Aliases
RedDelta, Bronze President, TA416

Affiliations
China

Active since
2012

Goals
Espionage

Victimology
Mustang Panda victims are geographically dispersed. The group has targeted governments, NGOs, religious institutions, think tanks, telecommunications companies, internet service providers, and activist groups in the United States, Europe, Taiwan, Hong Kong, Tibet, Myanmar, Mongolia, Vietnam, Afghanistan, Pakistan, India, and many others.

Notable TTPs
Mustang Panda commonly sends socially engineered phishing emails for initial access. Attachments are often disguised as official documents from legitimate governments or organizations. Initial deployment of the PlugX RAT enables Mustang Panda to download and install additional malware.

Malware & tooling
Mustang Panda relies on the use of popularly available attack frameworks such as Cobalt Strike and Meterpreter as well as custom made malware. The group also develops DLL based loaders, customized stagers and reverse shells to deploy their bespoke implants such as PlugX (Korplug) and Poison Ivy, and open source tools such as NBTScan.

Figure 38. Mustang Panda threat actor profile.

malware primarily used for persistent access. This espionage activity is consistent with what we know about this threat actor (**Figure 38**).

While this activity marks a shift in the group's traditional targeting of entities located predominantly in the U.S. and Asia, it is consistent with their opportunistic approach of exploiting current events to compromise victims. Mustang Panda has been known to use themed lures relating to various current-day events and issues, including the COVID-19 pandemic, international summits, and various political topics.

Mustang Panda has continued using loaders as a payload delivery mechanism, an evolving approach that has previously included maldocs, shortcut files and malicious archives. These loaders are used to fetch and deploy three components on infected systems: a legitimate EU report (a PDF serving as a decoy distraction); a benign executable used to load a malicious DLL loader; and the DLL loader used to decode, load and finally activate the final DLL payload. In most cases, Talos observed that the ultimate malicious payload was the remote access trojan PlugX, a post-exploitation RAT commonly associated with Mustang Panda and other China-linked APTs. PlugX capabilities generally include system and process enumeration, file management and modification, keylogging, screenshot capture, and remote shell execution. Mustang Panda has also been known to deploy multiple variations of infection chains to deploy PlugX, bespoke stagers, and meterpreter-based and custom reverse shells. These infection chains consist of LNK files and maldocs used to deploy various malicious components.

China-linked APTs targeted usual victims, exploit known flaws

While the Russia-Ukraine war presented new opportunities to exploit a vulnerable victim base, Chinese APTs also continued relentless campaigns against their usual targets, which commonly include entities in Asia, such as the Taiwanese government, Hong Kong activists, Mongolian and Tibetan NGOs, Japan, Myanmar, and telecommunications companies in Afghanistan and India.



In 2022, we observed Mustang Panda targeting its typical victims, as we saw the adversary [deploy](#) bespoke intermediary stagers against Asian targets with the ultimate goal of downloading additional malware on infected endpoints. In February, Mustang Panda operators sent archive files—masquerading as Association of Southeast Asian Nations (ASEAN) Summit documents—to users in Southeast Asia. We observed that when the user clicked the accompanying executable, a malicious DLL implant loaded and subsequently decoded shellcode acting as a stager for additional malicious artifacts that could be downloaded from an actor-controlled C2.

Publicly known exploits used for initial infection continue enabling Chinese APT cyber attacks. For example, a separate China-linked cyber espionage group known as Deep Panda [attempted](#) to exploit flaws in the Log4j logging utility, judging from CTIR data. The attacker successfully used a custom backdoor in a healthcare organization’s network to establish persistence. After an initial access foothold was gained, we found evidence that the actor used a PowerShell script to download and execute files from a Deep Panda-linked C2 server.

NORTH KOREA

Talos observed prolific activity from malicious cyber threat actors tied to the government of North Korea. The Lazarus Group is one such adversary, which we observed deploying new malware against targets **(Figure 39)**. Lazarus continues to support North Korean political and national security objectives through malicious cyber activities designed for espionage, data theft (including intellectual property), and disruptive attacks. The group has broadly targeted government organizations, healthcare, the defense industry, media, and critical infrastructure entities. Lazarus has also conducted widespread monetary theft primarily against financial institutions including cryptocurrency exchanges. According to the U.S. Intelligence Community’s (USIC) annual threat assessment, the global theft has potentially [resulted](#) in the loss of hundreds of millions of dollars, probably to support North Korea’s military research and development including its nuclear and missile programs.

ACTOR PROFILE

Lazarus Group

Aliases
Hidden Cobra, APT38

Affiliations
North Korea

Active since
2010

Goals
Espionage, data theft, disruptive attacks and financial gain to support state objectives, including political and national security, military research and development and evasion of international sanctions.

Victimology
Broad targeting of entities globally, including government, defense, finance, media and critical infrastructure entities.

Notable TTPs
Exploitation of known vulnerabilities, social engineering techniques, spear-phishing, data exfiltration, custom malware and pseudo-ransomware/wipers.

Malware & tooling
Lazarus employs a variety of custom, self-developed malware families it uses exclusively, including RATs, wipers, backdoors and DDoS botnets. Notable threats include WannaCry, MagicRAT, TigerRAT, YamaBot, VSingle and CRAT.

Figure 39. Lazarus Group threat actor profile.



Talos discovered Lazarus Group deploying a new remote access trojan, which we named MagicRAT, as well as other custom implants for internal reconnaissance and data theft.

Lazarus exploits Log4j to distribute new and previously known implants

Between February and July 2022, Lazarus Group actors [exploited](#) flaws in VMware Horizon public-facing servers to gain initial footholds into enterprise networks. Lazarus Group used the Log4Shell vulnerability to target energy companies located in Canada, the United States, and Japan. Talos [discovered](#) Lazarus Group deploying a new remote access trojan, which we named MagicRAT, as well as other custom implants for internal reconnaissance and data theft.

The Lazarus Group’s new MagicRAT is written in C++ and, in a novel development, is programmed with the Qt Framework. Qt software is designed for developing graphical user interfaces, of which MagicRAT has none. While MagicRAT’s capabilities are relatively standard compared to other RAT families, we believe the integration of the Qt Framework is unique since the increased complexity of the code makes reversing more difficult. Furthermore, this combination likely makes machine learning and heuristic analysis detection less reliable since there are fewer known samples of malware programmed with Qt.

MagicRAT is a fairly simple remote access trojan, providing Lazarus Group with system information, and supplying a remote shell for arbitrary command execution, file exfiltration, file deletion, and RAT self-removal. However, we also found that once MagicRAT achieved persistence, it could launch additional payloads from its C2 infrastructure, including a lightweight port scanner and another known Lazarus Group remote access trojan called TigerRAT. We observed two new features of TigerRAT variants this year—a USB dump capability, and preparation for web camera capture. These features supplement the implant’s traditional capabilities which include gathering system information, arbitrary command execution, screen capture, keylogging, socks tunneling, file management, and self-deletion.

Lazarus actors continue to distribute other known customized malware families, such as the VSingle and YamaBot RATs, consistent with previous group activity. In one cluster of activity in the aforementioned campaign targeting energy providers in Canada, the United States, and Japan, we [observed](#) the VSingle implant act as a loader for YamaBot. The standard RAT capabilities included enumerating files and directories, sending process information to C2s, downloading files from remote locations, executing arbitrary commands, and self-uninstallation.





ACTOR PROFILE

Transparent Tribe



Aliases

APT36, Mythic Leopard, COPPER FIELDSTONE

Affiliations

Pakistan

Active since

2016

Goals

Espionage, intellectual property theft

Victimology

Transparent Tribe's targeting is generally limited to the Central, Southern, and Eastern regions of Asia, including military and governmental organizations and officials in Afghanistan and India. The APT has also spied on Pakistani-based activists. Additional victims are in the defense industry and the education sector, including universities and students.

Notable TTPs

Transparent Tribe often uses maldocs with malicious VBA macros or links to remote infrastructure for the initial infection. Documents sent in spear phishing emails often contain geopolitical themes relevant to regional issues. To further lure victims, the group also uses honeytrap-disguised stagers located in Google Drive folders, and registers domains with names that would appear relevant to victims.

Malware & tooling

Transparent Tribe deploys customized malware including CrimsonRAT and ObliqueRAT, and additional .NET-based implants.

OTHER NOTABLE APT ACTIVITY

In 2022, Cisco Talos observed significant cyber threat activity emanating from threat actors operating in the South Asia region. In particular, we tracked numerous APT campaigns that primarily targeted entities in India. The majority of cyber attacks targeting India appear to come from state-linked actors in Pakistan, a longtime regional adversary. Amidst ongoing geopolitical concerns over territorial disputes, insurgent activities, and Chinese influence, high-profile confrontations have increasingly played out in the cyberspace arena. Pakistan-linked APTs have targeted Indian critical infrastructure, military personnel, security and political think tanks, telecommunications firms, and educational entities. These operations have typically been motivated by espionage.

Pakistan-linked APT targets multiple industries for espionage, pivots particularly to the education sector

Much of the malicious cyber activity we observed in this theater is attributed to the Pakistan-linked group Transparent Tribe. The group's operations, which we have monitored since at least 2016, predominantly target government and military entities and affiliated organizations in Afghanistan and India. This includes pseudo-government entities and individuals belonging to think tanks, universities, and the defense industrial base (Figure 40).

In what appears to be an expansion of Transparent Tribe's standard victimology, the group began targeting students and educational institutions in the Indian subcontinent. In a campaign that began earlier this year, the APT started delivering maldocs with malicious VBA macros to students at Indian universities and colleges via spear phishing emails. Once executed, the macros extract an embedded archive file, which ultimately contains CrimsonRAT, Transparent Tribe's malware of choice. CrimsonRAT includes numerous capabilities for spying on endpoints and sending information back to Transparent Tribe-operated C2 infrastructure. Many of the maldocs

Figure 40. Transparent Tribe threat actor profile.



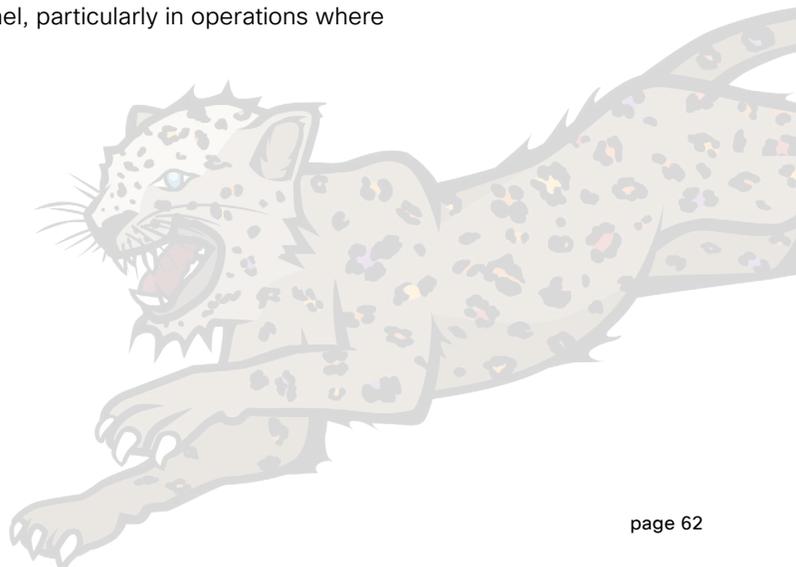
Transparent Tribe continues using a number of well-known implants such as CrimsonRAT and ObliqueRAT to maintain persistent access, indicating that this actor still considers these tools to be highly effective.

were hosted on attacker-registered domains that masqueraded as legitimate education-related sites such as “studentsportal[.]live” and “studentsportal[.]website”. The APT also uses media-themed domains, such as “cloud-drive[.]store”, as well as websites with embedded Google Drive folders containing pictures of women. These tactics and themes are consistent with file-sharing domain and honeytrap-based attacks observed in [previous Transparent Tribe campaigns](#) and similarly used by a Pakistan-based group Talos has [tracked](#) as the APT SideCopy.

While the education campaign diverted from Transparent Tribe’s typical focus on government officials and organizations, we believe that the goal may have been to steal valuable and restricted research from premier institutions supporting the Indian government, an objective that would be consistent with Pakistani strategic interests. Transparent Tribe’s continued use of signature RATs in its campaigns very likely indicates that long-term access and espionage remain this actor’s objectives.

Transparent Tribe continues deploying well-known RATs and introduces new custom malware

Transparent Tribe continues using a number of well-known implants such as CrimsonRAT and ObliqueRAT to maintain persistent access, indicating that this actor still considers these tools to be highly effective. Across most campaigns we studied in 2022, the group delivered maldocs to recipients which, upon user execution, deployed CrimsonRAT, a .NET-based implant serving as the group’s preferred malware since at least 2020. CrimsonRAT contains numerous capabilities for collecting host information such as listing files, folders and drives on a system, process IDs and names running on the endpoint, and file metadata and content, all as specified by the C2. CrimsonRAT also exfiltrated information from keyloggers and screenshots. Transparent Tribe has continued its use of ObliqueRAT, a C/C++ based implant discovered by Talos in [2020](#). Transparent Tribe appears to mostly reserve this malware for targeted attacks on Indian government personnel, particularly in operations where stealth is a priority.





Bitter APT began using a new tool we identified as ZxxZ, indicating the group is becoming more technically sophisticated.



This year, Transparent Tribe also incorporated new custom malware, suggesting the APT is attempting to diversify its tooling portfolio to compromise more targets. This malware consists of easily and quickly deployable downloaders, droppers, and lightweight RATs. In one [campaign](#) targeting Indian government officials, a lightweight, .NET-based implant was observed in several infection chains. Relative to CrimsonRAT and ObliqueRAT, this implant had limited capabilities but enough functionality to monitor and control infected devices.

Lesser-known Bitter APT increases its presence, targets South Asian governments with new implant

In addition to uncovering campaigns by well-known actors, we also discovered operations by the lesser-known South Asian threat actor Bitter (aka T-APT-17), shedding light on a group that has developed new malware and attacked a number of high-level targets. In a campaign beginning in August 2021 and continuing into this year, the Bitter APT has [targeted](#) South and East Asian governments and entities in the energy and engineering sectors. Espionage appears to be this group’s main objective, having engaged in a long history of social engineering, as well as vulnerability exploitation and RAT deployment.

This year, Bitter threat actors began using a new tool which Talos identified as the ZxxZ implant, a development indicating that the group’s attack chain is becoming more technically sophisticated. In one campaign, Bitter distributed themed lure documents to individuals in Bangladeshi government agencies including high-ranking officials in the police force. When the victims opened the maldocs—often malicious RTF documents or Excel spreadsheets containing shellcode designed to exploit known Microsoft vulnerabilities—the ZxxZ trojan, disguised as a legitimate program, was downloaded from Bitter’s hosting server and executed on victim endpoints. This new implant is capable of remote file execution and can deploy other malicious Bitter tools including BitterRAT, Artra downloader, SlideRAT and AndroRAT. As the group is a lesser-known actor, our discovery of this implant contributes to the cybersecurity community’s understanding of Bitter’s operations and rapidly evolving suite of malware.

Code-sharing between South Asia-linked threat actors

Earlier this year, Talos [published](#) research suggesting that, in an unusual trend, several APT actors operating in South Asia were possibly unintentionally reusing VBA code written by different threat groups. We found surprising evidence that malicious artifacts associated with the Donot Team (aka APT-C-35)—an APT that has historically targeted Chinese organizations and Pakistani government and military entities—shared VBA code similarities with the Pakistan-



based Transparent Tribe. While we believe it is unlikely that there was any deliberate or direct code sharing between the groups, particularly given the oppositional nature of each other's targets, it's possible that these APTs visited publicly available libraries to access and develop code which they judged to have been successful in other threat group campaigns. Moreover, it is possible that they adopted TTPs and malware used in each other's attacks to increase the chance of false attribution.

CONCLUSION

The risk of APT attacks against public and private entities persists in this heightened threat environment. While the cybersecurity community focused its attention this year on tracking the impacts of the Russia-Ukraine war, the spread of ransomware and other modular threats, and the proliferation of cybercriminal groups, state-linked and government-sponsored APT groups have continued and expanded their operations in response to major shifts in the 2022 geopolitical landscape. Threat actors remain committed to achieving objectives commonly in line with their national interests. Motivations such as espionage, intellectual property and financial theft, and network disruption were most commonly seen across APT attacks, and Talos assesses that the risk of these events will carry well into 2023.

Across most of the APT groups described herein, Talos observed a greater trend towards the introduction of newly customized malware and tools, or the development of variants for those which were previously known. Along with the incorporation of open-source tools, such as remote access software and post-exploitation frameworks, the diversification of APT malware and the sophistication of the infection chains indicate that state-linked threat actors are not giving up even when they are detected and blocked by security systems or when their TTPs are publicly revealed. The sophistication inherent by virtue of APT groups means that defenders should always assume that there is a possible risk of an attack. Nevertheless, better security hygiene can help mitigate APT activity. A layered security apparatus which includes segmenting networks, implementing multi-factor authentication, and limiting user access to tools for which there isn't a legitimate business function (e.g. remote access software), combined with smarter organizational policies such as patching and end-user education, is the optimal approach for preventing APT attacks.

Finally, Talos assesses that tracking geopolitical conditions can help defenders understand APT goals and targets. As demonstrated in the cases of Russia, Iran, China, North Korea and countries in the Indian subcontinent, trends involving national interests such as defense, the economy, borders, sanctions, and diplomacy tend to influence or drive APTs' offensive operations. Closely monitoring these nations' goals and aspirations can help direct defenders' efforts.



CONCLUSION

While the threats facing enterprises and individuals remain as serious as ever in 2022, the geopolitical environment in which adversaries operate has become significantly more complex. Where adversaries once forced change in the threat landscape, whether through updating tooling or infrastructure, creating new levers to pressure enterprises into complying with their demands, or developing new exploits, we now see this complex geopolitical environment forcing change in the threat actors themselves.

This shift manifests itself throughout the sections of this report. The fallout from the war in Ukraine has not only resulted in Russia-based APTs being deployed to attack Ukrainian targets, but has led to chaos in the Eastern European ransomware economy as groups splinter and take sides. The former ransomware landscape which saw monopolies composed of dominant groups has transformed into a diverse group of threat actors, responding to increased attention from law enforcement as well as infighting and internal leaks. Similarly, as law enforcement actions prohibitively affect former mainstay commodity loaders such as Emotet and Trickbot, other families, like Qakbot, find room to expand their operations, always staying on top of security researchers' detection methods and updating their tactics, techniques, and procedures (TTPs) as needed. Relatedly, as the security community refines their detection and tracking for Cobalt Strike to a greater degree, 2022 has seen an explosion in new offensive frameworks, which may present more challenges for defenders. All the while, highly sophisticated and well-resourced state-sponsored groups continue to launch attacks that support the shifting geopolitical goals of their affiliated governments.

What does this shift mean for defenders? First, the flexibility and adaptability of major threat actors means that context matters more than ever. Defenders must grasp the

geopolitical trends driving threat activity and have thorough actor tracking methodologies and threat intelligence processes in place to document the evolving behavior of these mercurial adversaries. Second, as adversaries adapt their behavior and tooling in response to detections, defenders need to think about building a robust security ecosystem and must make sure security products are difficult to uninstall and are fully deployed. Third, with the amount of threats facing enterprises, security alerts must be designed to provide essential context about the threat including assessments of severity and recommendations for remediation to avoid alert fatigue. Finally, as threat actors increase in sophistication, in order to create resilience enterprises must implement a “not if, but when” mindset in regards to compromise, and think about ways to make it more difficult for the adversary once they are inside a victim network, developing incident response plans and gaming out different threat scenarios.

Although the story of 2022 reveals a number of significant challenges, it also shows the resolve and capability of defenders. The work Cisco Talos has done in Ukraine demonstrates the power defenders can wield when working together on a common mission for good. We will continue to obstruct adversaries that threaten our customers, our partners, and our communities. We look forward to thwarting as many of them as possible in 2023.