Ransomware Review: First Half of 2024

Executive Summary

Unit 42 monitors ransomware and extortion leak sites closely to keep tabs on threat activity. We reviewed compromise announcements from 53 dedicated leak sites in the first half of 2024 and found 1,762 new posts. This averages to approximately 294 posts a month and almost 68 posts a week. Of the 53 ransomware groups whose leak sites we monitored, six of the groups accounted for more than half of the compromises observed.

In February, we reported a 49% increase year-over-year in alleged victims posted on ransomware leak sites. So far, in 2024, comparing the first half of 2023 to the first half of 2024, we see an even further increase of 4.3%. The higher level of activity observed in 2023 was no fluke.

Activity from groups like Ambitious Scorpius (distributors of BlackCat) and Flighty Scorpius (distributors of LockBit) has largely fallen off due to law enforcement operations. However, other threat groups we track such as Spoiled Scorpius (distributors of RansomHub) and Slippery Scorpius (distributors of DragonForce) have joined the fray to fill the void.

Industries most impacted by ransomware were manufacturing (16.4% of observed posts), healthcare (9.6%) and construction (9.4%). Like with manufacturing, healthcare is extremely sensitive to disruptions and downtime.

The U.S. was home to the most victims by far in the first half of 2024. With 917 compromises, the US received 52% of total attacks. In order of impact, the remaining top 10 nations were: Canada, the U.K., Germany, Italy, France, Spain, Brazil, Australia and Belgium.

Newly disclosed vulnerabilities primarily drove ransomware activity as attackers moved to quickly exploit these opportunities. Threat actors regularly target vulnerabilities to access victim networks, elevate privileges and move laterally across breached environments. We'll list some of the most common vulnerabilities being exploited in 2024.

Palo Alto Networks customers are better protected from ransomware threats through our Network Security solutions, Prisma Cloud offerings and Cortex line of products.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Research	Cybercrime, Ransomware
Named Groups (Unit 42 Taxonomy)	Ambitious Scorpius, Anemic Scorpius, Bashful Scorpius, Burning Scorpius, Chubby Scorpius, Dark Scorpius, Drowsy Scorpius, Flighty Scorpius, Muddled Libra, Mushy Scorpius, Screaming Scorpius, Shifty Scorpius, Slippery Scorpius, Spicy Scorpius, Spikey Scorpius, Spoiled Scorpius, Stumped Scorpius, Wandering Scorpius, Whiny Scorpius
Named Groups	Alpha, ALPHV, AvosLocker, Black Basta, BlackCat, Blackout, BreachForums, CL0P, DoNex, DragonForce, GhostSec, Hunters International, Karakurt, KelvinSecurity, LockBit, Losttrust, LukaLocker, MyData, NoEscape, Nokoyawa, Qilin, Quilong, RansomHub, Scattered Spider, SocGholish, Trisec, Volcano Demon
CVEs Mentioned	CVE-2018-13379, CVE-2020-1472, CVE-2020-1472, CVE-2024-1708, CVE-2024-1709, CVE-2024-26169, CVE-2024-27198, CVE-2024-4577
Top Industries Mentioned	Healthcare, Manufacturing, Construction

Leak Site Trends in the First Half of 2024

Our team monitors data from dedicated leak sites (DLS) that are often only accessible through the dark web. Throughout our analysis, we compare the first half of 2024 (1H24) to the first half of 2023 (1H23) so that we are accounting for any seasonal fluctuations that can occur due to annual holidays, travel seasons and other recurring events that may impact threat activity.

Key Findings:

- 4.3% year-over-year increase in compromise announcements
    - 1H24: 1,762 compromise announcements from 53 sites – with the top six groups responsible for more than half of the compromises
    - 1H23: 1,688 compromise announcements
- 1H24 averaged 68 leak site posts per week
- Ransomware announcements continue to increase, despite multiple notable law enforcement disruptions and arrests
- The LockBit leak site remains the most active, posting misleading information and old data
- In February, we reported a 49% YoY increase in victims posted on leak sites. Our analysis of 2024 so far shows that ransomware groups are maintaining that higher level of activity, even further increasing activity relative to last year.

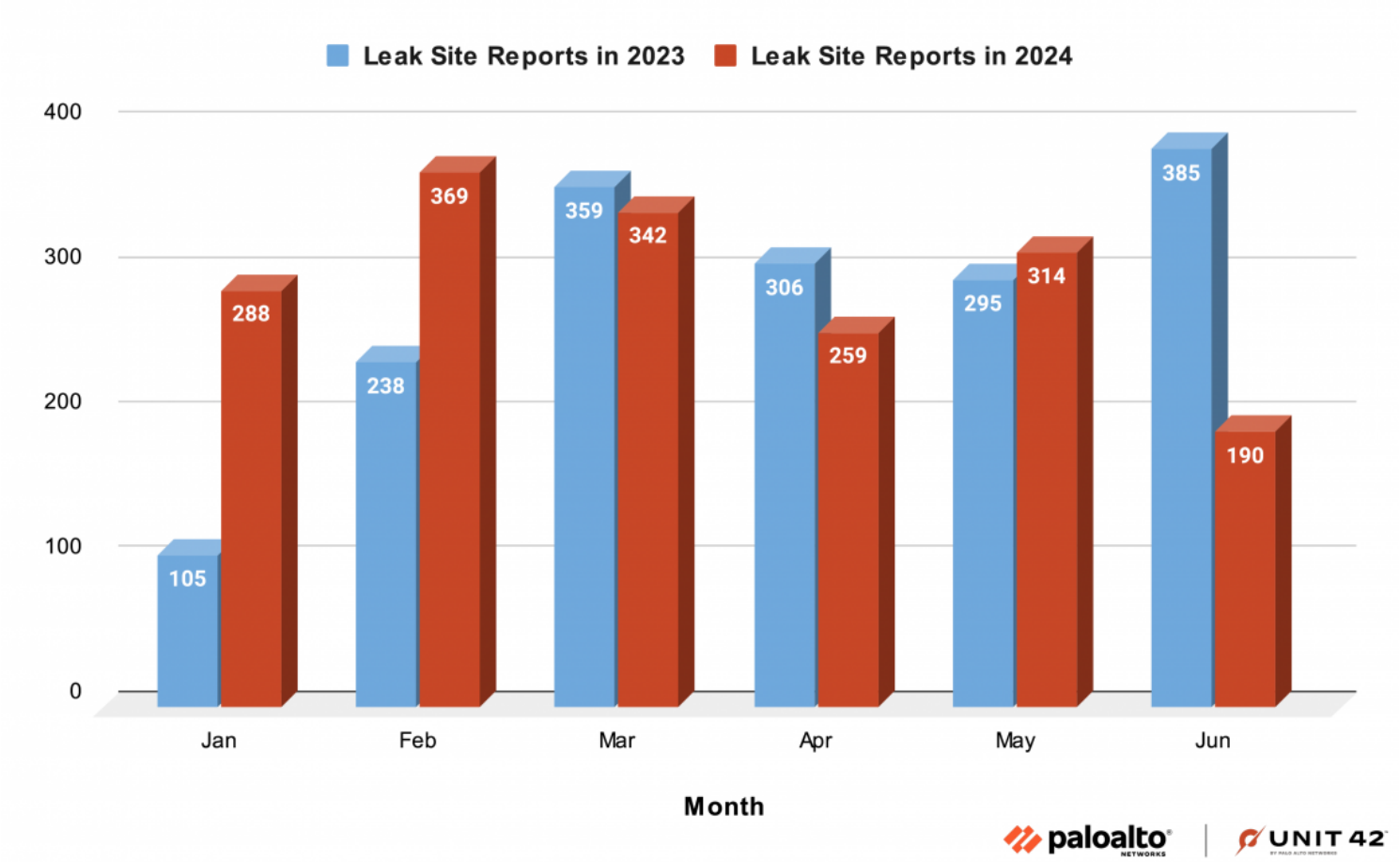

Figure 1. Month-by-month comparison of ransomware leak site reports.

Figure 1 shows a month-by-month breakout of the numbers, comparing each of the first six months in 2023 with each of the first six months in 2024.

We observed a notable decrease in ransomware leak site reports in June of 2024. Significant decreases in activity on the LockBit and 8Base leak sites largely accounted for this drop.

Threat Group Activity

Leak site data indicates 53 ransomware groups have been active so far in 2024, but the top six ransomware groups account for a little more than half of the total compromises.

Unit 42 tracks threat groups using a naming system that pairs a modifier with a designated constellation per group. Unit 42 maintains a master list of the threat actor groups we track, along with

common akas. More details on cybercrime groups are detailed in the below graphic.

As seen in Figure 2, four ransomware groups that were among the six most active in 2023 remained among the most active so far this year. During the first half of 2024, Ambitious Scorpius (distributors of ALPHV/BlackCat) and Chubby Scorpius (distributors of CL0P) dropped out of the top rankings. These groups were displaced by Dark Scorpius (distributors of BlackBasta) and Transforming Scorpius (distributors of Medusa).

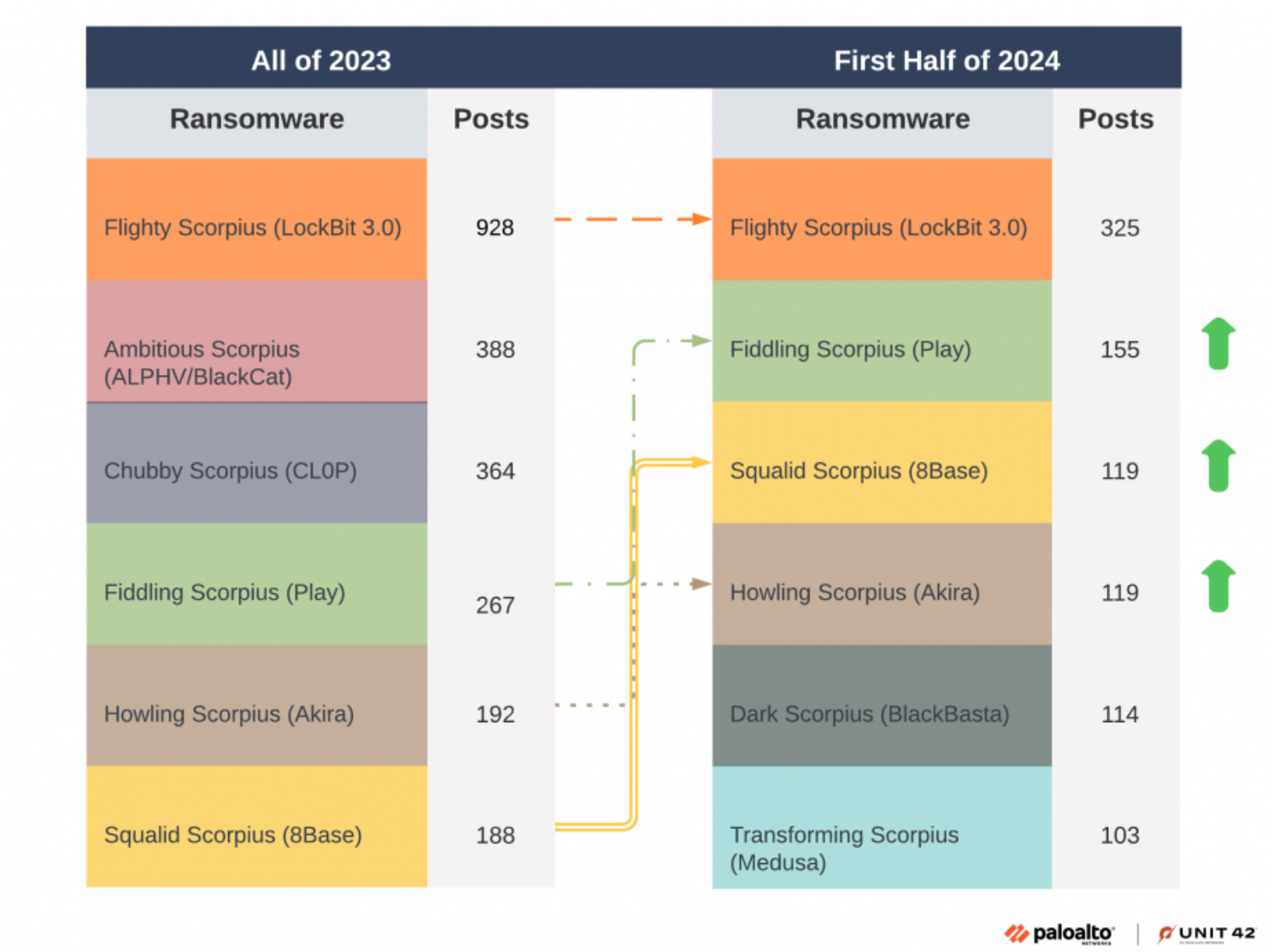

Figure 2. Comparing the top six ransomware groups from all of 2023 with the first half of 2024.

Threat actors regularly target vulnerabilities to access victim networks, elevate privileges and move laterally across breached environments. Our threat landscape has been inundated with zero-day and other serious vulnerabilities, giving threat actors a large menu to choose from. According to our most recent Unit 42 Incident Response Report, vulnerabilities became the leading cause of initial access in our cases in 2023, overtaking other common methods such as phishing for the first time.

That trend continues in 2024. Below, we provide some of the more prolific vulnerabilities exploited by ransomware groups in the first half of 2024. We encourage organizations to implement a robust vulnerability management program that accounts for known exploited vulnerabilities, such as those included below.

- CVE-2018-13379 - Fortinet SSL VPN
- CVE-2024-1709 - ConnectWise ScreenConnect
- CVE-2024-1708 - ConnectWise ScreenConnect
- CVE-2024-27198 - TeamCity
- CVE-2024-4577 - PHP-CGI script engine
- CVE-2020-1472 - Netlogon Remote Protocol
- CVE-2024-26169 - Microsoft Windows Error Reporting Service

Law Enforcement Takedowns and Disruptions

In the dynamic ransomware landscape, some threat actors have quietly scaled down or completely ceased operations in the first half of 2024. However, some high-profile ransomware groups have disappeared in very public ways.

Law enforcement activity continues to have a wide-reaching impact on the ransomware threat landscape in 2024. Takedowns of prominent ransomware groups, forums and individuals in the first half of the year have created ripples throughout the criminal ecosystem.

Law enforcement highlights from the first half of 2024 include:

- January 2024: U.S. law enforcement arrested a prominent member of Muddled Libra on charges that include wire fraud, identity fraud and cryptocurrency theft.
- February 2024: Law enforcement takedown of the LockBit 3.0 Tor site disrupted its ransomware operations.
- March 2024: Affected by a December 2023 law enforcement takedown, the Ambitious Scorpius group finalized an exit scam by selling its ALPHV/BlackCat source code and pretending the FBI seized their site and infrastructure.
- May 2024: The U.K., U.S. and Australia unmasked and sanctioned the leader of Flighty Scorpius, the group behind LockBit ransomware.
- May 2024: The group behind GhostLocker ransomware, GhostSec, announced its exit from ransomware and return to hacktivism.
- May 2024: Law enforcement agencies seized control of BreachForums and a Telegram channel by BreachForums administrator nicknamed Baphomet, leading to speculation that Baphomet had been arrested.
- June 2024: Law enforcement arrested the leader of a cybercrime group we track as Muddled Libra (aka Scattered Spider). Law enforcement agencies have identified this group as an affiliate of the ALPHV/BlackCat ransomware program.

- June 2024: The administrator behind the ShinyHunters handle on BreachForums retired and turned over the site to a new administrator account named Anastasia.
- July 2024: Law enforcement arrested another leader of the Muddled Libra group.

While infrastructure seizures by law enforcement are not new, they appear to have been more impactful than previous takedowns. Law enforcement agencies have continued seizing infrastructure and making arrests in 2024, but they have also started targeting organizations affiliated with these ransomware groups. These actions have impacted ransomware groups in different ways.

Takedown, Recovery and Exit Scam: Ambitious Scorpius

Known for its ALPHV/BlackCat ransomware, Ambitious Scorpius was the second-most prolific group according to our 2023 leak site data. After the FBI disrupted this group's operations in December 2023, many predicted this group could shut down or rebrand their creation as new ransomware.

By March 2024, Ambitious Scorpius finalized an exit scam by selling its ALPHV/BlackCat source code and pretending the FBI seized their site and infrastructure.

From Takedown to Fraudulent Claims and Possible New Group: Flighty Scorpius

After its February 2024 law enforcement takedown, Flighty Scorpius stood up new infrastructure and began targeting more victims with LockBit 3.0 ransomware.

After restoring its operations, this threat actor posted dubious claims of new victims to its leak site that appeared to be old compromises, exaggerations or outright fabrications. For example, in June 2024, the group claimed to have compromised the US Federal Reserve, but further investigation revealed it was a US-based bank.

On May 7, the National Crime Agency announced a joint international effort had unmasked the leader of Flighty Scorpius and imposed various sanctions on his travel and finances. Known as LockBitSupp, the leader is alleged to be Russian national Dmitry Khoroshev. They also issued arrest warrants for additional affiliates of the group.

Seizures, Arrests, Retirements and Transitions: BreachForums

BreachForums, a criminal forum where threat actors buy and sell stolen data and access to compromised networks, has a history of name changes and takedowns. In May 2024, law enforcement seized BreachForums and arrested its administrator known as Baphomet.

The site came back weeks after the May 2024 takedown under an administrator named ShinyHunters. This ShinyHunters account might be related to the ShinyHunters hacking collective, a group we track as Bling Libra. In June 2024, the user behind the BreachForums' ShinyHunters account reportedly retired and moved the forum to a new administrator.

Arrest of Affiliate's Key Member and Leaders: Muddled Libra

In January 2024, US law enforcement arrested a prominent member of Muddled Libra, named Noah Michael Urban, on charges that include wire fraud, identity fraud and cryptocurrency theft. In June 2024, a joint law enforcement effort resulted in the arrest of a 22-year-old UK citizen in Spain believed to be the leader of Muddled Libra. Law enforcement arrested another leader in July. It is too early to tell if these arrests will impact the group's capabilities.

An Apparent Exit From Ransomware: GhostSec

In a May 2024 interview, GhostSec announced it was ending its ransomware operations and returning to hacktivism. GhostSec will reportedly hand off its GhostLocker RaaS operations to the Stormous ransomware group.

This group started nearly a decade ago, with the stated aim of targeting and disrupting terrorist organizations like ISIS. They developed GhostLocker RaaS in October 2023 as a means to fund their hacktivism activities.

The group had strict stipulations against targeting healthcare and education. If its ransomware hit victims in those sectors, GhostSec said it stepped in to mitigate the damage. The group's leader Sebastian Dante Alexander noted it favored "...higher scale corporations, which I believe — to an extent — are all greedy."

A member of the Five Families, GhostSec previously coordinated attacks with the Stormous ransomware group, another member of the Five Families. To exit the ransomware scene, GhostSec stated it will transfer GhostLocker's source code (version 3) and the rest of its ransomware operations to Stormous. The group stated that its purpose for the transfer is a clean break without an exit scam. Of note, however, the claimed break involves handing off the ransomware used to extort victims rather than ending its use.

Other Ransomware Groups

Chubby Scorpius, which distributes CL0P ransomware, was the third most active ransomware group in 2023, but its activity fell dramatically in 2024. As of June, this group accounts for less than 0.75% of the total posts in our leak site data.

Other ransomware groups that have not been active on leak sites in 2024 are Bashful Scorpius (distributors of Nokoyawa ransomware), KelvinSecurity, Losttrust, Mushy Scorpius (distributors of Karakurt), Spicy Scorpius (distributors of AvosLocker) and Stumped Scorpius (distributors of NoEscape).

While these groups might have stopped due to the economics of a constantly evolving cybercrime market, additional factors could have influenced these apparent departures. Recent high-profile takedowns of ransomware groups by law enforcement and the legal pursuit of ransomware affiliates and criminal marketplaces like BreachForums could have created an air of mistrust and fear among cybercrime threat actors.

New Kids on the Block

With the departure of various ransomware threat actors, other groups have moved to fill in the void so far in 2024. Here’s a quick look at some of the emerging ransomware groups Unit 42 has been tracking in 2024 that may have hit your radar based on recent events.

Groups discussed in this section include:

- Spoiled Scorpius (Distributors of RansomHub)

- Slippery Scorpius (Distributors of DragonForce)
- Burning Scorpius (Distributors of LukaLocker)
- Alpha/MyData ransomware
- Trisec ransomware
- DoNex ransomware
- Quilong ransomware
- Blackout ransomware

Spoiled Scorpius (Distributors of RansomHub)

Spoiled Scorpius is the name we use for the group behind RansomHub, a RaaS first announced in February 2024 on the Russian Anonymous Market Place (RAMP) cybercrime forum from an account named koley. This group is largely opportunistic, but it prohibits attacks on entities in Cuba, China, North Korea and Russian territories. It also prohibits targeting non-profit organizations. Spoiled Scorpius is known to recruit affiliates from RAMP Forum and advertises a payout of 90% to affiliates with the group claiming the remaining 10%.

Through Unit 42 Incident Response engagements, we have observed a chain of events that indicates this group achieves initial victim access via SocGholish malware delivered through search engine optimization (SEO) poisoning. We assess the group behind SocGholish sold victim access from their infections to Spoiled Scorpius affiliates who deployed the ransomware. We also found evidence that Spoiled Scorpius used its access to victim systems to delete backups from both on-premises and cloud storage.

RansomHub ransomware is written in Golang and C++. Spoiled Scorpius has used distributed denial of service (DDoS) attacks or exploited vulnerabilities such as CVE-2020-1472 to breach its victims. The group also cold calls victims to further exert pressure on them to pay the ransom.

A June 2024 article states a connection between RansomHub and a previous RaaS first observed in 2023 called Knight (Cyclops). Spoiled Scorpius also appears to have links to Ambitious Scorpius.

Slippery Scorpius (Distributors of DragonForce)

Slippery Scorpius is our name for the group behind DragonForce ransomware. This group was first detected in November 2023. Slippery Scorpius gained notoriety in 2024, when this group started extorting victims directly through phone calls and then leaking recorded audio of the conversations.

Like many ransomware groups, Slippery Scorpius performs double-extortion, using its leak site to post the stolen data of its victims who fail to pay. Due to similarities in their code, DragonForce ransomware appears to be based on the leaked source code of LockBit 3.0.

Slippery Scorpius should not be confused with the Malaysian-based hacktivist group named DragonForce that first appeared as early as 2021. This DragonForce hacktivist group does not appear to be related to DragonForce ransomware.

Burning Scorpius (Distributors of LukaLocker)

Originally nicknamed Volcano Demon, the group we track as Burning Scorpius is behind new ransomware named LukaLocker. This ransomware has encrypted both Windows and Linux systems since June 2024.

Unlike other ransomware groups, Burning Scorpius does not host a leak site. Instead, this group contacts executives and IT leadership repeatedly through phone calls with threatening messages to directly extort its victims.

Other New Groups

Alpha ransomware, not to be confused with the ALPHV/BlackCat ransomware group, was active as early as May 2023 and its leak site first appeared in January 2024. Since their site uses MYDATA as its title, some have used MyData as its ransomware name or threat actor identifier. The leak site is reportedly unstable and frequently offline, indicating this group is relatively new, inexperienced and loosely managed. Our leak site data reveals this group has reported nine victims in the first six months of 2024.

The Trisec ransomware group emerged in February 2024 and claims to be affiliated with the Tunisian government. They specifically stated that they "only hires Tunisian blackhats," and this group has advertised for various positions through its leak site and Telegram channel. The group claims to be

both financially motivated and state-sponsored, dabbling in a variety of cybercrime. So far, its victimology appears opportunistic in both industry and region.

DoNex ransomware first appeared in March 2024 and its earliest file samples date back to February. It is a new, financially motivated group that has targeted victims in the US and Europe. Avast has developed a decryptor for victims to restore their files.

The Quilong ransomware group claimed to have compromised three plastic surgery centers in Brazil earlier in 2024, as well as a car dealership. The posted some of the alleged stolen data on their leak site, taunting medical providers with claims that they had failed to protect their patients.

The Blackout ransomware group was first active in late February 2024 and initially claimed on their leak site to have attacked healthcare entities in Canada, France and Germany. Leak site posts from this group show subsequent attacks on a Mexico-based telecommunications company and Croatian targets in the manufacturing industry.

Rebrands

After the exit scam by Ambitious Scorpius, we are keeping an eye out for indicators that this group might be returning by rebranding with a different name. If so, this group will need a strategy to gain back its affiliates, since many have been recruited by other ransomware groups.

Law enforcement actions we previously mentioned against Flighty Scorpius have led to its decline in 2024. Government agencies took down the ransomware's infrastructure and sanctioned its alleged leader in May 2024. We saw only seven verified compromises from its leak site in June, a dramatic drop compared to previous months.

As a way to revive its operations, this group could rebrand as new ransomware. While rebranding remains a possibility for Flighty Scorpius, the previous success of LockBit ransomware has already led other groups to create their own ransomware based on its codebase.

For example, new ransomware named Brain Cipher emerged in June 2024, and research has shown it is based on LockBit 3.0 code. We analyzed a Brain Cypher sample used in an attack against an

Indonesian target, and our existing LockBit 3.0 prevention and detection signatures also worked on this sample.

Industries and Regions Impacted

While ransomware targeting remains largely opportunistic, industries like manufacturing remain highly susceptible to these types of attacks. As in 2023, manufacturing continues to be the sector most impacted by ransomware. At 289 compromises, 16.4% of all ransomware attacks during 1H24 affected manufacturing organizations.

Healthcare was the second most impacted industry in 1H24, rising from sixth place in 2023. Like with manufacturing, healthcare is very sensitive to disruptions. It is also riddled with a plethora of technologies and devices that can be hard to catalog and protect.

Construction is the third most impacted industry in 1H24. About 9.4% of all compromises affected organizations involved in construction.

Figure 3 shows a bar graph representing the industries most affected by ransomware attacks in the first half of 2024.

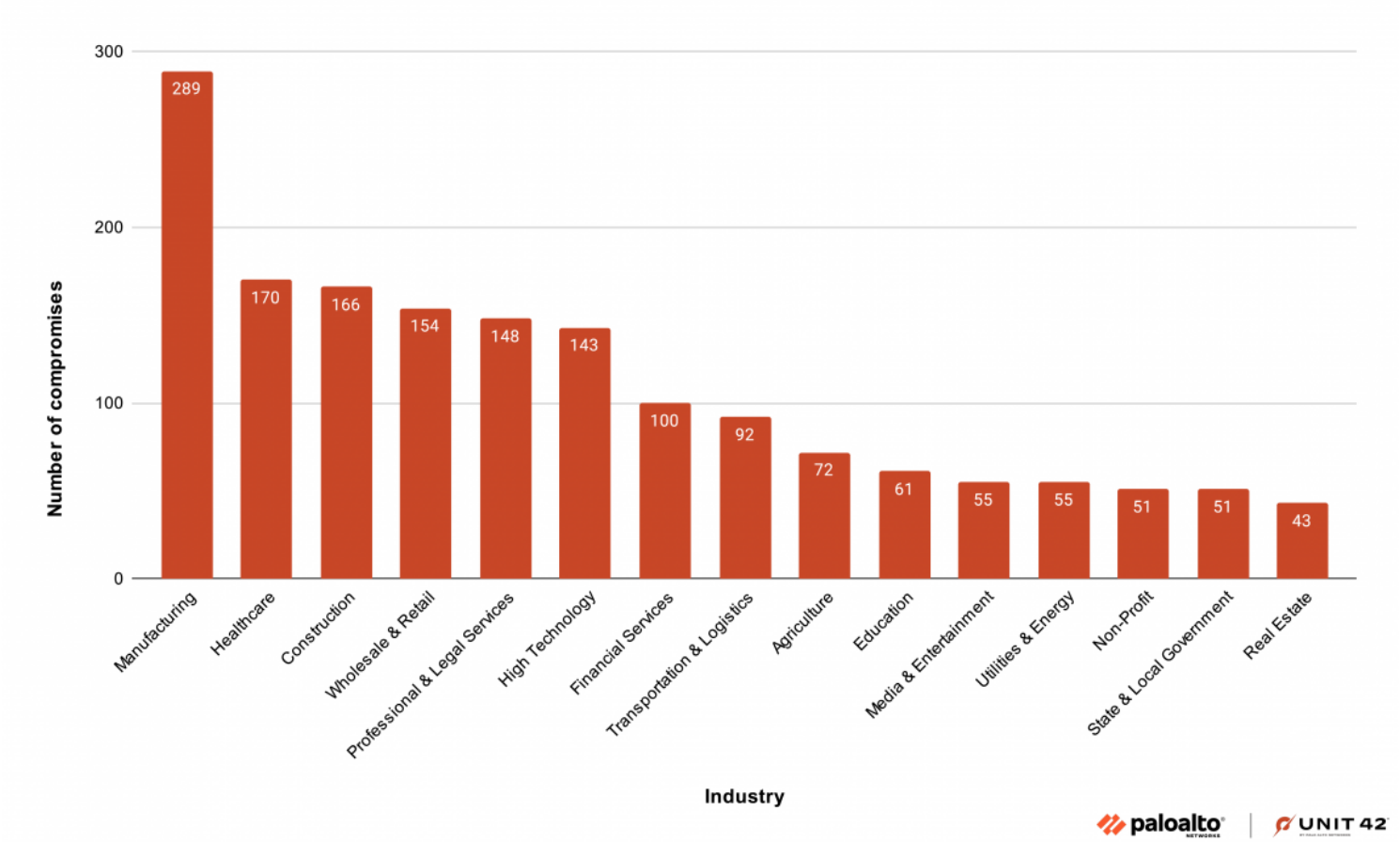

Figure 3. Industries affected by ransomware in the first half of 2024.

Unsurprisingly, the U.S. was home to the most victims by far in the first half of 2024. With 917 compromises, organizations in the U.S. received 52% of total attacks. The remaining top 10 nations where organizations were affected, in order of impact, were Canada, the U.K., Germany, Italy, France, Spain, Brazil, Australia and Belgium. Below, Figure 4 shows the breakdown.

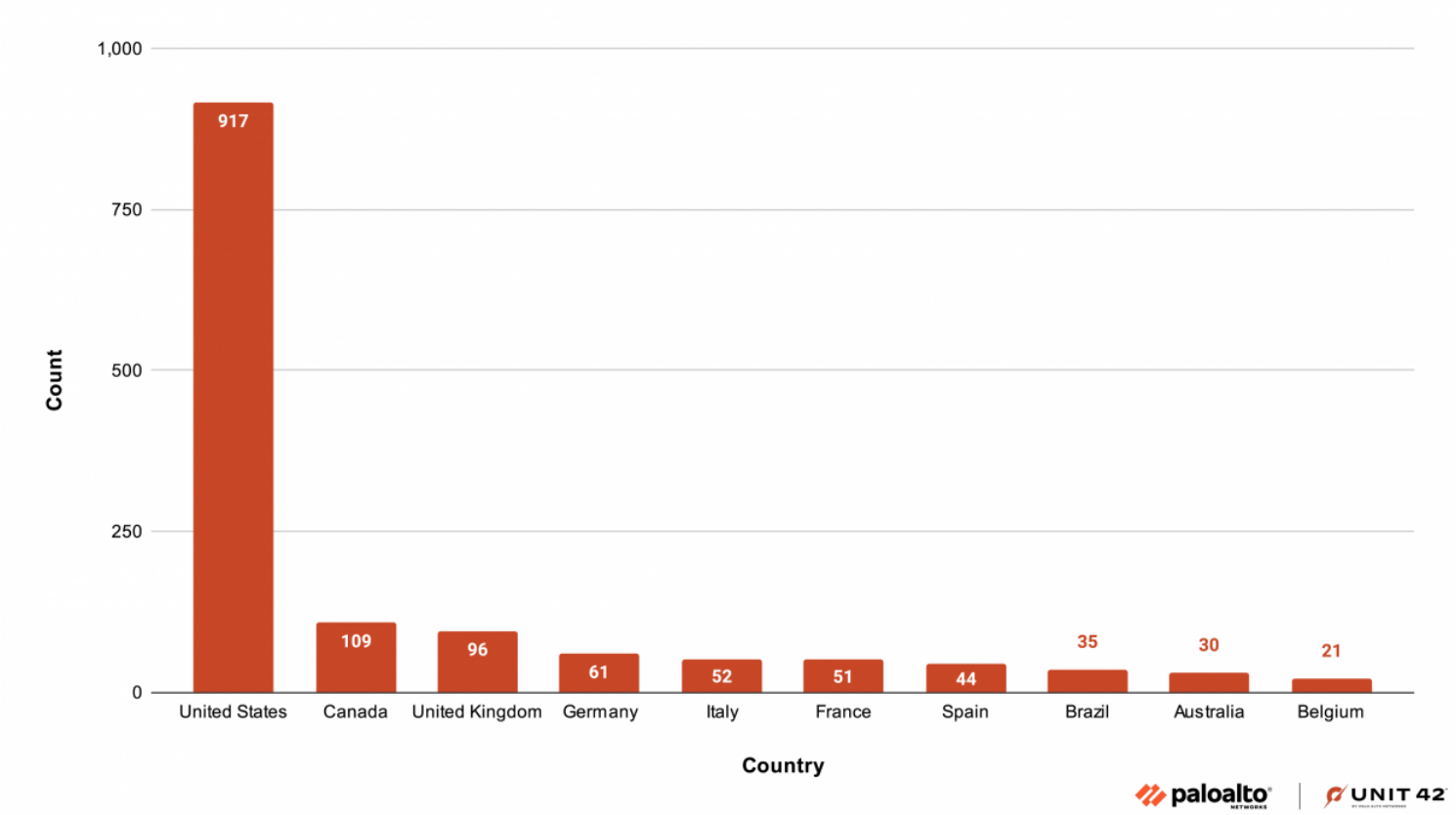

Figure 4. Nations where organizations were affected by ransomware in the first half of 2024.

The Data and Where It Comes From

Analysis and information for this article is primarily based on publicly reported information and data from ransomware leak sites.

Our team monitors data from these sites that are often accessible through the dark web. We reviewed and compiled compromise announcements from 53 sites in the first half of 2024 to identify trends in the ransomware landscape. We also leveraged our firsthand experience with these groups through Unit 42 Incident Response engagements to develop our understanding of their tools and techniques within victim networks.

Since most ransomware groups now commonly use leak sites to pressure victims, researchers often use this data to identify trends and levels of ransomware activity for threat actors. However, defenders and researchers should use leak site data with caution as it might not always provide an accurate picture.

Threat actors will often omit victims who pay quickly from a group's leak site. Additionally, threat actors will frequently misrepresent the source of the data on the group's leak site.

Despite these drawbacks, this data provides valuable information on trends, newcomers and threat groups that have disappeared from the threat landscape.

Conclusion

This article reviewed trends and significant events for ransomware in the first half of 2024. We reported trends from compromises reported by ransomware leak site posts.

While leak site data indicates that manufacturing remained the most affected sector, healthcare jumped to second place, with high-profile attacks grabbing headlines during the first six months of 2024. Overall, the majority of organizations impacted by ransomware were based in the U.S.

Even with law enforcement's best efforts to dismantle and stamp out the most prolific ransomware threat actors, plenty of highly skilled and motivated groups are waiting, willing to step in and fill the void. The success and subsequent explosion of ransomware in the past few years have led to an ever-increasing pool of individuals and groups gambling for their chance at fame and fortune.

Palo Alto Networks customers are better protected from ransomware threats through Network Security solutions, Prisma Cloud offerings and Cortex line of products.

In particular, our Next-Generation Firewall with Cloud-Delivered Security Services like:

- Advanced URL Filtering and Advanced DNS Security can block malicious URLs and domains associated with ransomware.
- Advanced Threat Prevention can block ransomware threats at both the network and application layers, including port scans, buffer overflows and remote code execution.

Our Cortex protections include Cortex Xpanse, which detects vulnerable services exposed directly to the internet that might be exploitable and infected by ransomware. Through Cortex XDR and XSIAM, all known ransomware samples are prevented by the XDR agent out of the box using the following endpoint protection modules:

- The Anti-Ransomware module to prevent encryption behaviors on systems running Microsoft Windows or macOS.
- The Local Analysis module will detect ransomware binaries on Windows, macOS and Linux.
- XDR also includes protection capabilities like Behavioral Threat Protection (BTP) which helps prevent ransomware activity on Windows, macOS and Linux.
- Palo Alto Networks' Cloud Security Agent (CSA) leverages XSIAM to provide cloud based detection and monitoring capabilities to both Cortex and Prisma Cloud cloud agents.

Our cloud-based security solutions also help protect virtual machines running in cloud environments.

We frequently update machine learning models and analysis techniques in Advanced WildFire with information discovered from our day-to-day research on ransomware.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- RansomHub. Because every abandoned affiliate needs a home - Barracuda
- GhostLocker: The New Ransomware On The Block - Cyberint
- LOCKBIT Black's Legacy: Unraveling the DragonForce Ransomware Connection - Cyble
- DragonForce Ransomware Group Posts Audio of Conversations with Victims - Datarecovery.com
- Decrypted: DoNex Ransomware and its Predecessors - Avast
- Assessing the Disruptions of Ransomware Gangs - Intel471

- Fla. Man Charged in SIM-Swapping Spree is Key Suspect in Hacker Groups Oktapus, Scattered Spider - Krebs on Security
- Exposing Alpha Ransomware: A Deep Dive into Its Operations - Netenrich
- Ransomware Attackers May Have Used Privilege Escalation Vulnerability as Zero-day - Symantec Threat Intelligence
- RansomHub: New Ransomware has Origins in Older Knight - Symantec Threat Intelligence
- BreachForums Down, Official Telegram Channels Deleted and Database Potentially Leaked - The Cyber Express
- BreachForums Returns With a New Owner After ShinyHunters Retires - The Cyber Express
- FBI Seizes BreachForums Again, Urges Users to Report Criminal Activity - The Hacker News
- U.K. Hacker Linked to Notorious Scattered Spider Group Arrested in Spain - The Hacker News
- Road to redemption: GhostSec's hacktivists went to the dark side. Now they want to come back. - The Record
- Threat Brief: ConnectWise ScreenConnect Vulnerabilities (CVE-2024-1708 and CVE-2024-1709) - Palo Alto Networks Unit 42
- Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evade Detection and Law Enforcement Takedowns - Palo Alto Networks Unit 42
- Ransomware Retrospective 2024: Unit 42 Leak Site Analysis - Palo Alto Networks Unit 42
- BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs - Bleeping Computer
- BlackCat ransomware shuts down in exit scam, blames the "feds" - Bleeping Computer
- LockBit ransomware now poaching BlackCat, NoEscape affiliates - Bleeping Computer
- New Hunters International ransomware possible rebrand of Hive - Bleeping Computer
- Cybersecurity Advisory: Scattered Spider - US Cybersecurity Infrastructure Security Agency (CISA)
- Trisec: A New Ransomware Actor - Clipeus Intelligence
- LockBit’s Claimed Hack on US Federal Reserve Turns Out to Be a Publicity Stunt; Stolen Data Came From Just One US Bank - CPO Magazine
- BreachForums seized by law enforcement, admin Baphomet arrested - CSO Online
- Triangulating Trisec, a newly emerged ransomware gang - CyberDaily.au
- The Rise and Fall of BreachForums... For Now? - DarkOwl
- Hunters International Cyberattackers Take Over Hive Ransomware - DarkReading
- Leak Site BreachForums Springs Back to Life Weeks After FBI Takedown - DarkReading
- RansomHub Actors Exploit ZeroLogon Vuln in Recent Ransomware Attacks - DarkReading
- Out-of-bound Write in sslvpnd - FortiGuard Labs

- Ransomware Roundup - KageNoHitobito and DoNex - FortiGuard Labs Threat Research
- GRIT Ransomware Report: February 2024 - GuidePoint Security
- Halcyon Identifies New Ransomware Operator Volcano Demon Serving Up LukaLocker - Halcyon
- HC3: Threat Profile: Black Basta< [PDF]/a> - US Department of Health and Human Services
- HC3: Threat Profile: Qilin, aka Agenda Ransomware [PDF] - US Department of Health and Human Services
- Update: CVE-2024-4577 quickly weaponized to distribute "TellYouThePass" Ransomware - Impervia
- LockBit Scrambles After Takedown, Repopulates Leak Site with Old Breaches - Infosecurity Magazine
- Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant - US Department of Justice
- U.S. and U.K. Disrupt LockBit Ransomware Variant - US Department of Justice
- The Looming Shadow: Ransomware Threats in the Manufacturing Sector - L2L
- LockBit leader unmasked and sanctioned - UK National Crime Agency (NKA)
- Brain Cipher Ransomware: In-Depth Analysis, Detection, and Mitigation - SentinelOne
- Lockbit Ransomware Administrator Dmitry Yuryevich Khoroshev - US State Department
- Cops cuff 22-year-old Brit suspected of being Scattered Spider leader - The Register

Updated August 13, 2024, at 8:40 a.m. PT to update Figure 2 image and caption.