GUIDEPOINT® SECURITY

Ransomware and Cyber Threat Insights:

The Rise of Ransomware's Middle Class

A GRIT Report

July-September 2024

Contents

Note From GRIT

After over two years of producing the Ransomware Report, change is in the air. GuidePoint Research and Intelligence Team's (GRIT) Q3 2024 Ransomware Report marks the beginning of our shift from monthly reports to quarterly and annual reports, which we believe will allow us to better focus on strategic shifts in the ransomware economy. Concurrent with this shift, we are beginning to expand our scope to the wider cybercrime landscape, which is often but not always inseparable from ransomware.

We've also included a new component in this Quarter's report – a "Field Report" based on our investigative observations and support to GuidePoint Security's Digital Forensics and Incident Response (DFIR) team over the course of countless incident response case engagements. As intelligence professionals we recognize that there are few more valuable sources of intelligence information than contemporary intrusions, and we look to continue mining live incidents for analysis and insight in for future reports.

Thank you for reading,

- GRIT

Methodology

Data collected for this report was obtained from publicly available resources, including threat groups themselves, and has not been validated by alleged victims. Collected data is reviewed for potential duplications or inaccuracies and is adjusted accordingly. Thus, the number of publicly observed attacks and the actual number of attacks conducted may not be equal. Some groups do not publicize all of their victims, and almost all groups offer an option to withhold announcement if the victim pays a ransom within a specified timeframe and/or remove the victims once a ransom has been paid. Additionally, some groups include incomplete information about their victim or claim an attack despite successfully attacking only a small subset of their target. For these reasons, the data in this report is useful in aggregate but should be evaluated as a report consisting of data sources that have variability. Despite the variability, this report is still an accurate representation of the total ransomware threat landscape.

We note that this report includes data and analysis of several groups that may be better described as "extortion" groups rather than "ransomware" groups. These groups may eschew encryption and instead focus only on data exfiltration and extortion or may not perform intrusion operations of any kind, instead extorting or re-extorting organizations based on historically compromised data. While these groups do not deploy ransomware, we are including them in our reporting due to their relationships with other ransomware groups and their impact on the extortion-based cybercrime environment.

Finally, we make efforts to exclude from our data those groups that self-identify as “hacktivists,” compromised data brokers and markets, or non-financially motivated data thieves and leakers. While these actors and venues doubtlessly have impacts, we distinguish them from financially motivated cybercrime and data extortion, which is the primary focus of this report. For this reason, our data may periodically reflect lower total numbers of incidents than other similar public reports.

Quarterly Ransomware Summary

While at the surface level, Q3 2024 appears to have remained stagnant relative to Q2, when looking beneath, we've observed continued changes in threat actor activity and behavior worthy of analysis in this report. Established groups such as Akira and RansomHub have continued consistent and prolific operations, enabled in part by edge device vulnerabilities as well as tried and true initial access techniques. For the second quarter in a row, growth in the total volume of ransomware victims has stalled and has even decreased year over year – from 1,308 observed victims in Q3 2023 to 1,024 in Q3 2024. While we've assessed the root causes of this contraction in the ransomware economy in recent reports, details continue to emerge.

Disruptions by law enforcement and the resulting fallout have scattered previously comfortable ransomware operators to the wind. Displaced from their former affiliate programs among the most prolific groups, these operators have had to expend time and effort finding a new home. The landing spots for displaced affiliates can be seen in the rise of groups, including RansomHub and Qilin.

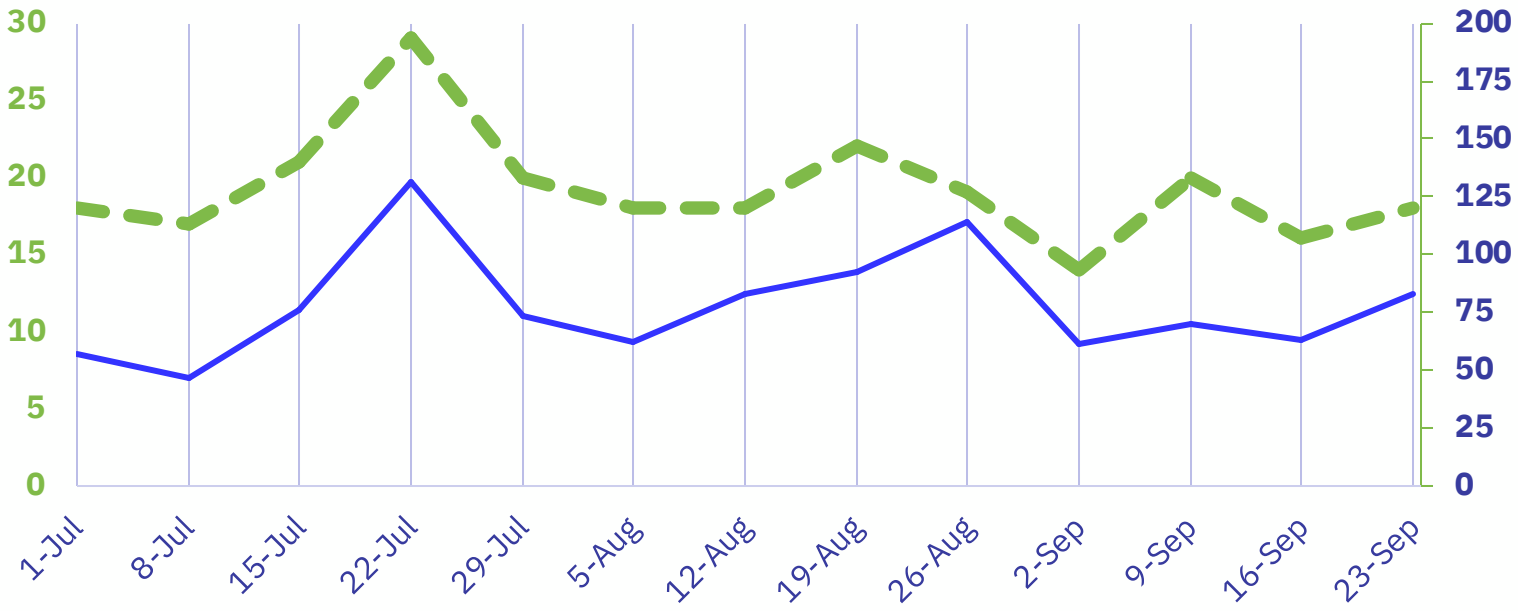
While other groups have moved to fill the shoes of former Ransomware-as-a-Service (RaaS) giants AlphV and LockBit, a noticeable gap remains. This may be a result of issues with growth, scale, or rote, boring operational minutia – it is too soon to tell. For now, we appear to be observing the emergence of a growing "middle class" in the ransomware ecosystem, less densely centralized than before but still driven by recognizable centers of gravity. That these "middle class" Established groups now claim dozens rather than hundreds of victims per month does not make them less dangerous, as we observe each day the compromises caused by their persistent operation.

While growth appears to have plateaued in recent months, ransomware has remained a profitable endeavor for cybercriminals and shows no indication of receding in the foreseeable future.

	Q3 2024	Q2 2024	Q3 2023
Total Publicly Posted Ransomware Victims	1,024	1,117	1,308
Active Ransomware Groups	49	49	45
Average Daily Victims	11.1	12.3	14.2

Threat Actor Trends

Rate of Publicly Posted Ransomware Victims, Q3 2024



Calendar Weeks: July – September

Total Posts	Total Groups	Average Posts per Week	Average Groups Posting per Week
1,024	**49**	**73**	**18**

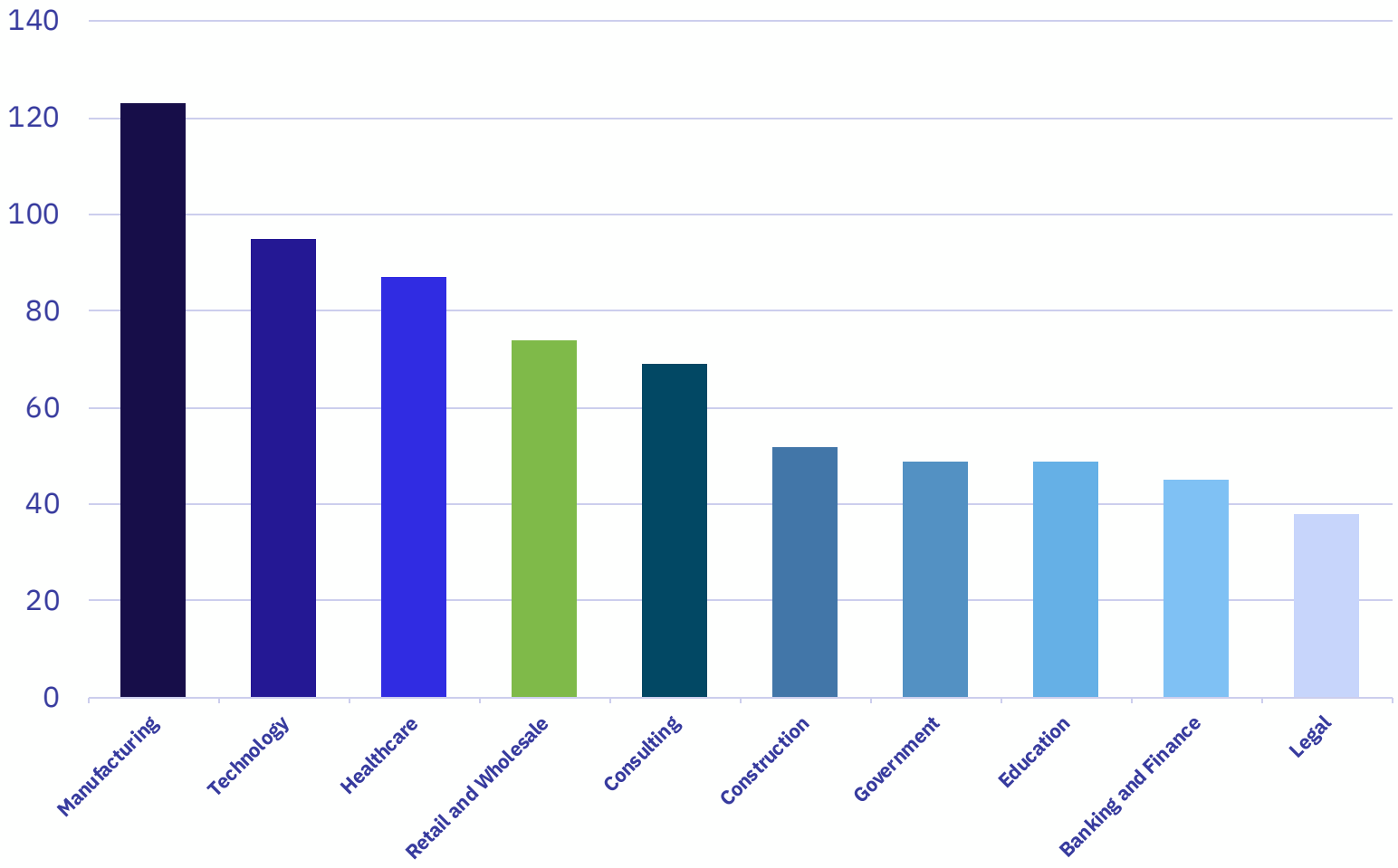
In Q3 2024, we observed 1,024 victims claimed by 49 distinct groups. During the same period in 2023, we witnessed 1,308 victims attributed to 45 unique groups, a decrease of 22% in total victim volume concurrent with an increase of 8% in discrete active groups.

Throughout Q3 2024, the daily rate of publicly posted ransomware victims stayed mostly steady, with the notable exception of one spike in mid-July, which was attributable to a high volume of posts (131) from multiple groups, including ElDorado, RansomHub, and DragonForce—nearly doubling the weekly average through the remainder of the quarter. A similar spike in late August can be attributed primarily to a singular drop of 14 victims by RansomHub on 30 August, more than quadrupling the group's daily average in what could be the clearance of a "backlog of victims."

We continue to observe a correlation between the number of distinct active groups and the total volume of observed victims, reflecting the continued impacts of even smaller Emerging groups on the ransomware economy.

Most Impacted Industries, Q3 2024

From Q2 to Q3 2024, the industries most impacted by ransomware have remained largely consistent, apart from a notable 24% decline in the number of observed victims from the Banking and Finance sector. Manufacturing, Technology, Healthcare, and Retail & Wholesale remain the most impacted industries by victim volume. Manufacturing remains the most impacted industry by a substantial margin, even with a slight decrease in total victims this quarter.



Manufacturing

- RansomHub
- LockBit
- Play

Technology

- RansomHub
- KillSecurity
- Play

Healthcare

- RansomHub
- Qilin
- Hunters International

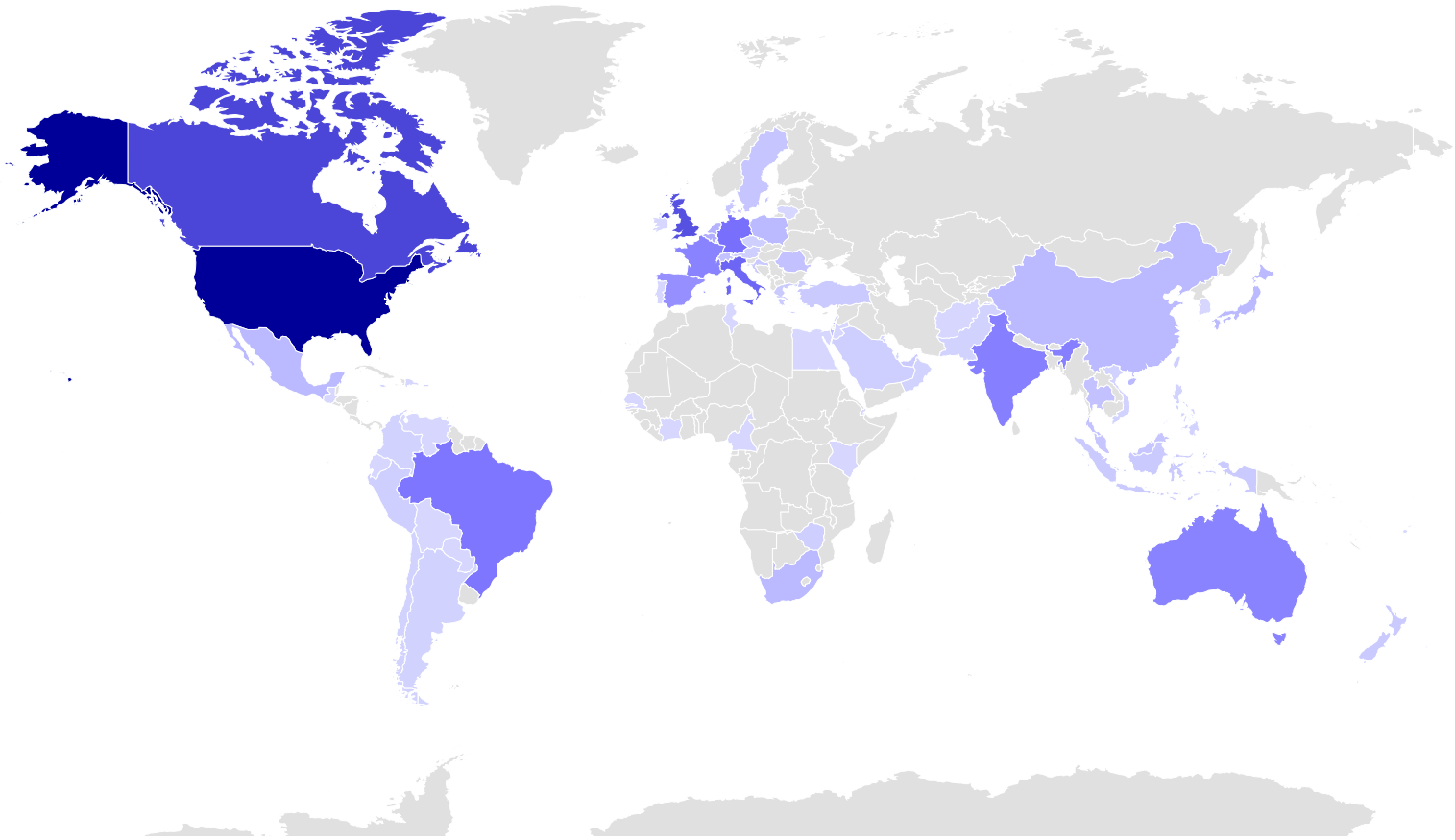
Retail & Wholesale

- RansomHub
- Play
- LockBit

Consulting

- RansomHub
- Play
- Lynx

Geographic Breakdown of Ransomware Victims, Q3 2024



Top 10:

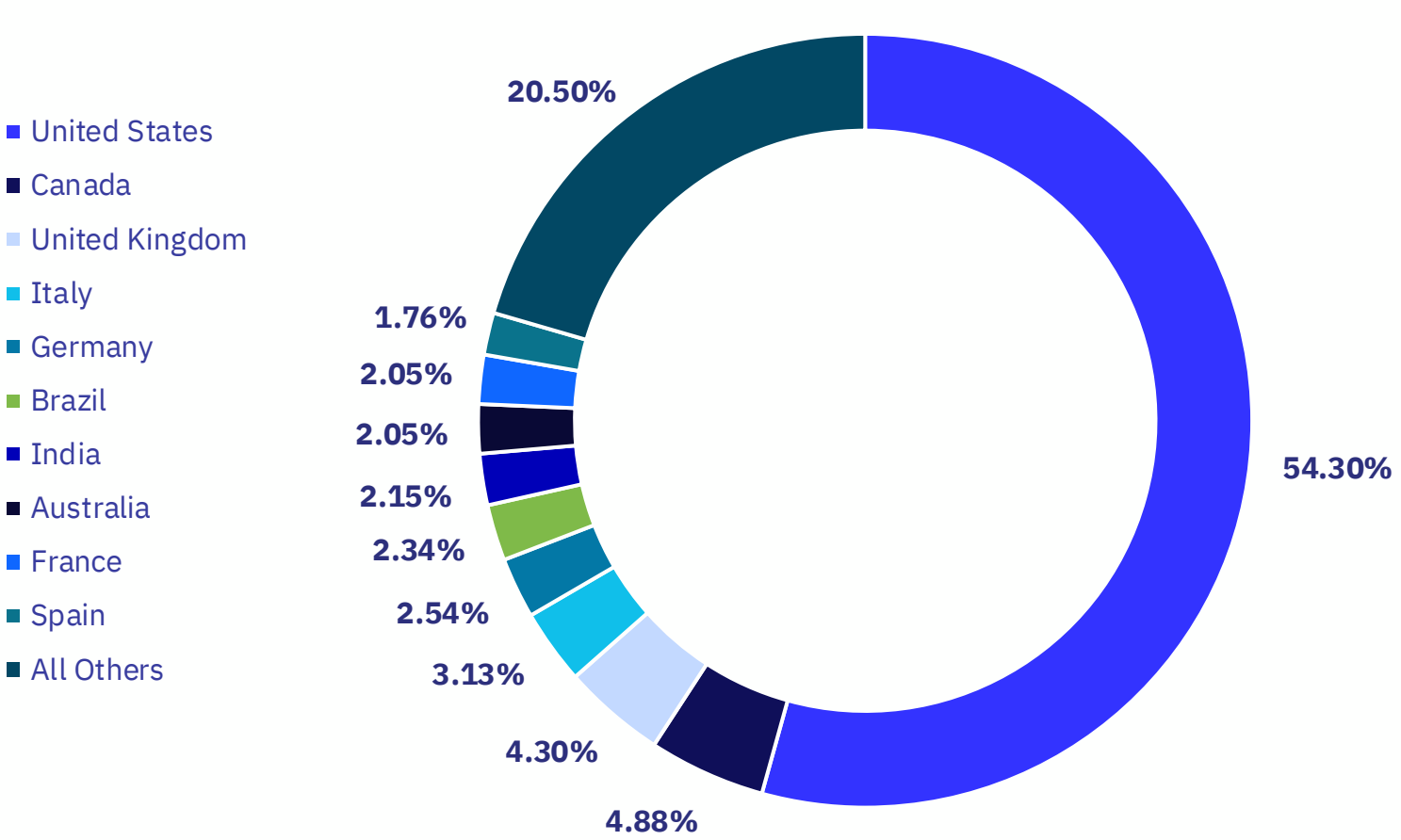
1. United States
2. United Kingdom
3. Canada
4. Germany
5. Italy
6. Brazil
7. France
8. Spain
9. India
10. Australia

Ransomware Impacts by Country, Q3 2024

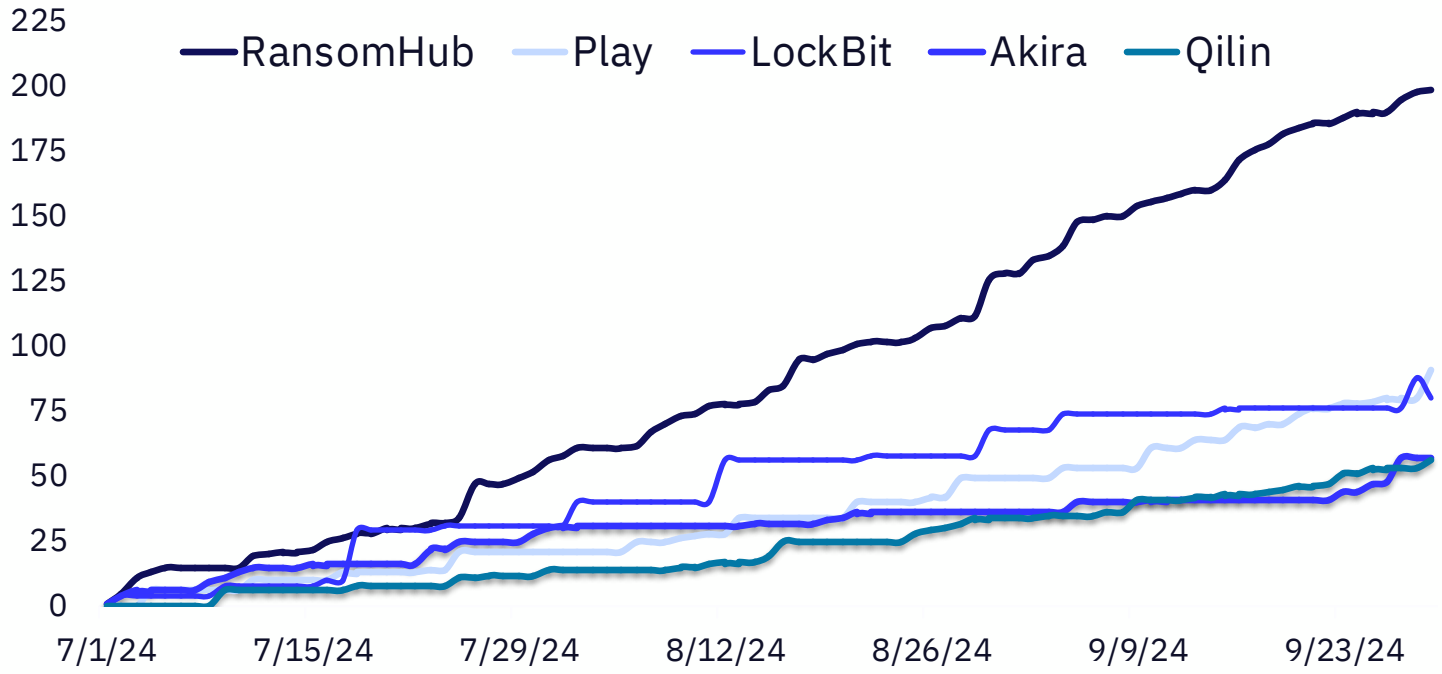
For the second consecutive quarter, the United States accounted for over 50% of observed ransomware victims, with at least 556 victims headquartered within its borders. The United Kingdom and Germany experienced a significant decline in observed attacks during the same period, benefitting from a quarter-over-quarter decrease of 34% and 42%, respectively.

Recent spikes in European activity in the preceding quarter may be attributable to increased attacks from LockBit, particularly as ransom payments from US-based organizations became nonviable in the wake of US sanctions. The UK has imposed similar sanctions, potentially resulting in a similar decremented payment viability in attacks attributed to LockBit affiliates.

Other countries that have experienced surges in observed ransomware victims, including Brazil and India, remained among the 10 most impacted this quarter, continuing to demonstrate ransomware's impacts on rising economies worldwide.



Cumulative Victims by Threat Group



RansomHub

In only its second quarter of operations, RansomHub continues to be at the highest operational tempo among its peers, accounting for 19% of Q3's total ransomware victim count. Their 199 victims claimed this quarter eclipses their Q2 victim count of 80 victims, marking a 149% increase quarter over quarter.

Play

Play persists as the second most prolific group in Q3, accounting for 9% of observed victims at 91. Play has remained persistent—though largely quiet—since appearing in late 2022 and has reached a consistent attack rate of approximately 1 victim per day for the past two quarters.

LockBit

Despite clear and lasting impacts from Operation Cronos' disruption, LockBit continues to claim a substantial number of victims quarter over quarter, albeit with shifting impacts by location and size of its apparent victims. LockBit remains the third most impactful group by victim volume, accounting for 9% of observed victims; however, GRIT notes a shift in LockBit's typical victim profile, marking a departure from "Big Game Hunting" and more significant impacts on Small-to-Medium sized Businesses (SMBs) and organizations outside of the United States.

Akira and Qilin

We shine a spotlight on these threat actor groups in subsequent sections.

Threat Actor Spotlight: Akira

Threat Actor Spotlight –Akira

Akira is a double-extortion RaaS operation that has been active since at least March 2023. The group has remained a mainstay and “middle of the pack” ransomware group that has been consistent but never a leader in the ransomware ecosystem.

Akira’s Data Leak Site

Based on victims sourced from Akira’s data leak site, Akira was the sixth most active group throughout Q3 2024. Despite Akira’s relatively middling victim count, GRIT has responded to a spate of ransomware attacks attributed to Akira throughout Q3 and has confirmed similar observations through industry peers; in multiple cases in which we have firsthand familiarity, Akira has delayed publishing of non-compliant victim data by several weeks. We assess that Akira’s actual impacts are far more wide-ranging than currently reflected in publicly available victim data, resulting in a “backlog” of victims pending negotiations and/or eventual posting to Akira’s data leak site.

Threat Actor Spotlight – Akira (Continued)

Along with GRIT communication efforts, GuidePoint Security's DFIR team responded to an increased number of Akira attacks in Q3. Although we lack conclusive evidence to convict with high confidence, available circumstantial forensic evidence supports the assessment that Akira continues to exploit the recent SonicWall improper access control vulnerability, CVE-2024-40766. This assessment is supported by open source and security vendor reporting, which has indicated the same since September 2024. Identifying the initial intrusion vector in these incidents consistently proved to be a difficult task, as the requisite logging for detecting compromise of edge devices is infrequently enabled.

Additionally, we have observed Akira affiliates' exploitation of CVE-2023-27532, a missing authentication vulnerability in Veeam's backup and replication component that has allowed attackers to retrieve encrypted credentials from the Veeam backup service for later lateral movement and privilege escalation; in open-source and vendor reporting, as well as our direct experience, Akira affiliates' exploitation of this vulnerability has closely followed exploitation or abuse of public-facing VPN services.

Alongside its fellow Conti descendent Black Basta, Akira affiliates are among the most frequently cited as exploiting vulnerabilities as part of their intrusion, suggesting the ability and willingness to rapidly adopt new tactics. Akira remains a prolific threat in the ransomware landscape, and we assess that their increased operational tempo is likely to become increasingly visible in the near term.

Industry Spotlight: Retail & Wholesale

Industry Spotlight – Retail & Wholesale

Based on historical trends, we pay particular attention to the Retail & Wholesale industry as Q3 transitions to Q4. In recent years, GRIT has observed increased impacts on Retail & Wholesale victims during the latter half of the calendar year, which we have hypothesized may be linked to increased victim revenue during the holiday season or overworked and understaffed defenders during a frequent vacation period.

In Q3, the Retail & Wholesale industry was the fourth most impacted of the verticals tracked by GRIT, with 74 posted victims. This represents a year-over-year decrease of 10% from 82 victims in Q3 2023. Anecdotally, this decrease may be attributable to reduced "big game hunting" operations from recently disrupted ransomware groups such as AlphV/BlackCat or LockBit; or to increased defensive investments by large retailers, several of which maintain industry-leading cybersecurity capabilities. Notably, Sophos has reported consecutive drops in ransomware impacts against retail, with a decline from 77% to 45% of retail organizations acknowledging having suffered a ransomware attack between 2022 and 2024, respectively.

Despite this good news, the Retail & Wholesale sector faces unique challenges. Its component businesses are often multinational in nature and dependent on extensive supply chains, potentially increasing victim attack surface volume and the impacts of disruptive encryption by a successful ransomware attack. These risks align with hypothesized increased impacts during the holiday season, during which operational downtime would generate outsized impacts on revenue and attract unwanted public attention from direct customers.

As the year comes to a close, GRIT continues to monitor the Retail & Wholesale sector for public compromises and attacks to further refine our understanding of possible cycles in attack volume impacting the industry.

The Retail & Wholesale Industry faces unique ransomware challenges

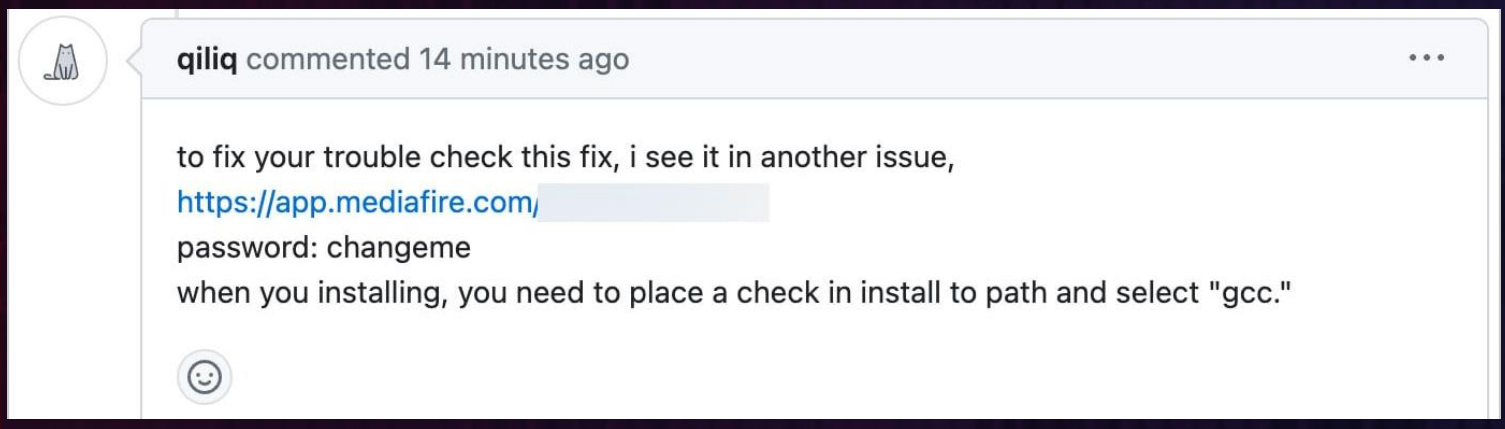
Other Reporting and Events

Legitimate Services Abused to Push Malware

Throughout Q3, GRIT has tracked an uptick in the use of integrated messaging services in known and trusted platforms, which threat actors have exploited to deliver targeted phishing messages. One such example was a widely reported campaign focused on the distribution of Lumma Stealer to GitHub users via the "issues" feature. To perform this social engineering technique, the actor opens an issue on a GitHub repository owned by the target. This issue purports to be from a security researcher who has found a vulnerability in the project and requests that the maintainer of the repository visit a malicious external website for more details.

Every issue that is opened on an open-source project triggers an email notification to its maintainers, which originates from the legitimate address notifications@github.com; this process allows the email to elude email filters, and often arrives in the target mailbox containing the full text and hyperlinks of the attacker in the issue they had opened. This mechanism has the effect of delivering attacker-controlled malicious content via an otherwise trusted source, increasing the chances of a target falling victim to the phishing attempt.

In the case of the Lumma Staler campaign, if a target visits the malicious site, they are greeted by a fake captcha test that asks a user to perform a series of steps to confirm their humanity. These steps involve the user executing a series of keyboard shortcuts that result in the execution of an attacker-created PowerShell command and ultimately the installation of Lumma Stealer, a common piece of info stealing malware.

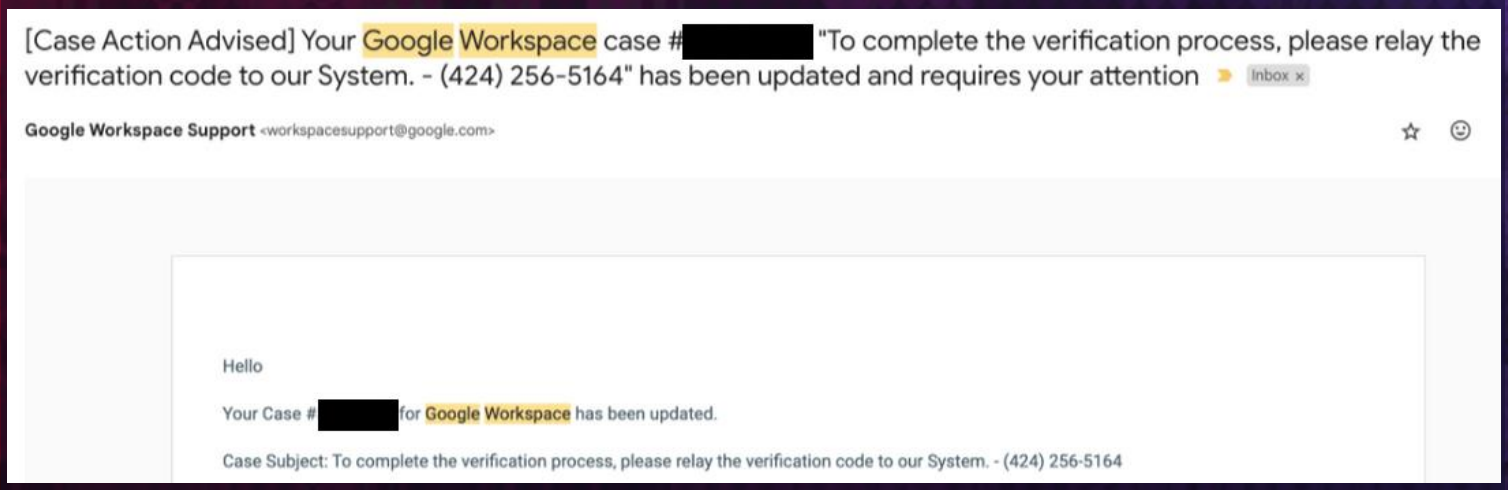


An example malicious issue request; Source: Bleeping Computer

Legitimate Services Abused to Push Malware

Another example of this technique in the wild is much more targeted and sinister. GRIT observed a threat actor targeting individuals with a public presence in the cryptocurrency community by using a sophisticated social engineering campaign. This campaign was designed to result in the takeover of the target's Google account, with the end goal of compromising the target's crypto wallets via password resets.

The campaign begins with a phone call to the target. Spoofing a number associated with Google headquarters, the threat actor poses as a member of account support staff. The threat actor, who communicates as a native English speaker, states that there is an issue with the target's account and directs the target to check their email for a message from the legitimate address workspacesupport@google.com. This message, which looks legitimate, asks the target to forward their two-factor verification code to a specific phone number.



An example of this sophisticated social engineering campaign using Google Workspace

In reality, all of the steps are controlled by the threat actor who, if successful, utilizes the stolen two-factor code to complete their takeover of the target's Google account. The actor takes multiple steps to add to the legitimacy of their request and build trust throughout the process. The email is in fact a legitimate notification from Google's Workspace support, but its content is generated by the threat actor through a complicated series of maneuvering. To generate this seemingly legitimate notification the actor sets up their own Google Workspace account and opens a support case with the target's email as an involved party. They include the body of their phishing message in the subject and comments of this case which is passed along by the support system to all associated email addresses including the target.

Legitimate Services Abused to Push Malware

While the abuse of trusted notification services is not a new approach, these two cases have provided evidence that threat actors are still seeking novel delivery techniques for their social engineering campaigns.

Especially when targeting tech-savvy users, threat actors know that they face an uphill battle in establishing trust with their victims. Leveraging trusted services serves to increase the trust factor while also reducing the need for threat actor-controlled infrastructure.

GRIT assesses that threat actors will continue to abuse trusted services and infrastructure for delivery and will continue to explore other services for new and novel techniques to strengthen their social engineering campaigns further, overcoming increased defenses and awareness.

Law Enforcement Affecting Adversary Confidence in Tooling

In 2024, law enforcement agencies worldwide have adopted a new approach to combating cybercrime. Rather than solely disrupting the use of cybercriminal tools, authorities are now targeting the trust between cybercriminals and the operators of these tools. Much like other organized crimes, cybercrime relies heavily on trust and relationships. Even solo threat actors depend on specific tools and infrastructure to carry out and profit from their operations, placing their faith in the operators of these platforms to avoid detection. By undermining this trust, law enforcement aims to complicate and stress the operations of cybercriminals.

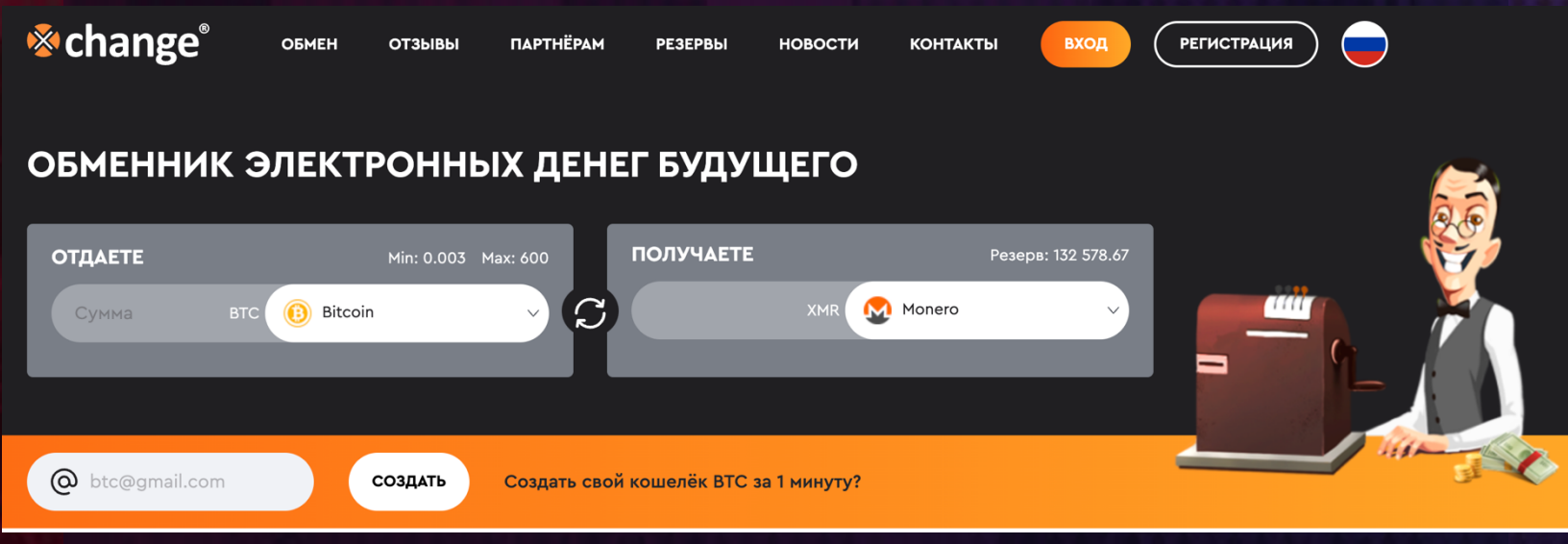
One significant example of this new strategy is the August 24th arrest of Pavel Durov, founder and CEO of Telegram, by French authorities. Durov is accused of knowingly allowing Telegram to be used for money laundering, drug trafficking, and other criminal activities. Telegram, a platform with minimal moderation, has become a hub for cybercriminals, where users can connect, share tutorials, and buy tools for their operations.

Following Durov's arrest, Telegram announced a change to its privacy policy, now pledging to cooperate with law enforcement when valid court orders are issued for users involved in criminal activities, expanding beyond its previous focus on terrorism-related cases. This move has sparked fear and uncertainty among Telegram’s criminal users, prompting discussions about migrating to other platforms—an action likely to sow distrust and increase operational friction.

Law Enforcement Affecting Adversary Confidence in Tooling

Another key development occurred in Germany, where federal police seized 47 cryptocurrency exchanges, including the popular Xchange.cash, in September. These platforms allegedly helped cybercriminals convert stolen cryptocurrency into fiat currency, crucial for ransomware and other illegal operations. By shutting down these services, German authorities have not only disrupted the financial lifelines of criminals but also raised the threat of further indictments based on the data collected from these exchanges. As a result, cybercriminals are left to scramble for alternatives, adding risk and uncertainty to their operations.

While it remains unclear whether these actions are part of a coordinated law enforcement strategy, the effect is evident: distrust and uncertainty are undermining the cybercrime ecosystem. A prime example is Operation Cronos, which significantly weakened the notorious LockBit ransomware group. While LockBit wasn't completely eliminated, the damage caused by sowing distrust has caused affiliates to abandon the group, reducing its once significant threat. Law enforcement's new tactic may not guarantee complete victories, but by fostering distrust and raising the costs for cybercriminals, it is proving to be an effective tool in disrupting their activities.



Screenshot of the Xchange.cash cryptocurrency exchange website
Source: Internet Archive

Field Report: Qilin Ransomware

Field Report: Qilin Ransomware

In late Q3, GuidePoint's Digital Forensics and Incident Response team responded to a ransomware incident involving a successful attack by the financially motivated RaaS group, Qilin. Over the course of under 2 hours, a Qilin affiliate gained access, moved laterally, and executed the Qilin ransomware against a small enterprise environment.

Qilin's first victims were observed in August 2022, though the group did not begin consistent operations until May 2023. Qilin has impacted at least 161 organizations, with global impacts across multiple industries. Although the bulk of Qilin's observed victims are based in Western countries, we have observed Qilin victims from diverse locales, including Argentina, Brazil, China, Japan, Saudi Arabia, and Thailand. In Q3 2024, Qilin accounted for 56 observed attacks or 5% of the observed total across all tracked groups.

Over the next several pages, we'll explore several of the observed tactics, techniques, tools, and procedures demonstrated by the Qilin affiliate. Appropriate security best practices which could have complicated many of these behaviors include:

- Vulnerability Management, including prioritization of vulnerabilities known to be under active exploitation "in the wild" or with publicly available Proof-of-Concept (PoC) exploit code
- Application whitelisting, blacklisting, and/or sandboxing
- Least privilege access control, preventing non-privileged workers from accessing or executing scripts via PowerShell or cmd.exe

Qilin: Initial Access

- A dearth of available logs complicated a determination of the Qilin affiliate's initial access vector. Qilin has been reported to use phishing and spearphishing to gain initial access in past cases.
- In the course of reviewing available logs, we noted the affiliate's compromise of a SonicWall Active Directory account, though we are unclear what - if any - actions the affiliate may have taken with this account.
- It is possible that the Qilin affiliate obtained initial access through the victim's SonicWall SSL VPN appliance, though the available logs were insufficient to make this determination. The victim's SonicWall appliance was vulnerable to CVE-2024-40766, an improper access control vulnerability impacting the underlying SonicOSand reportedly under exploitation by ransomware actors"in the wild." We are not aware of previous reporting indicating exploitation of this vulnerability by Qilinaffiliates.
- MITRE ATT&CK TTPs:
  - TA0001, Initial Access
  - T1133, External Remote Services
  - T1190, Exploit Public-Facing Application

Qilin: Defense Evasion

- The Qilin affiliate was observed using a 32-bit version of the ScreenConnect RMM tool, potentially to evade defenses. Attackers may use 32-bit applications to avoid detection by security software or in virtualized environments specifically designed for 64-bit applications.
- The affiliate also successfully cleared security event logs in an attempt to obfuscate their actions on-network and frustrate response efforts.
- MITRE ATT&CK TTPs:
  - T1027, Obfuscated Files or Information

Qilin: Credential Access

- The Qilin affiliate was observed dropping multiple credential dumping tools and have used at least two as part of their intrusion:
    - **secretsdump.exe:** a tool that is part of the Impacket suite that can be used to dump NTDS.DIT or dump hashed credentials from LSASS process memory. *The Qilin affiliate executed this tool.*
    - **Mimikatz:** a widely known tool used for dumping plaintext and hashed credentials from memory, among other tasks. *The Qilin affiliate executed this tool.*
    - **Pwdump:** a collection of tools used to extract hashed credentials from Windows systems.
    - **Fgexec.exe:** a component of fgdump, an enhanced version of **Pwdump**.
    - **Cachedump.exe:** a tool used to extract cached domain credentials from Windows systems.
- Each of these tools was seemingly executed out of a Documents sub-folder created for the ConnectWise RMM tool which had been installed, i.e., C:\Users\Administrator\Documents\ConnectWiseControl\Files\secretsdump.exe
- MITRE ATT&CK TTPs:
    - T1003, OS Credential Dumping
    - T1003.005, OS Credential Dumping: Cached Domain Credentials
    - T1555, Credentials from Password Stores

Qilin: Execution, Command & Control

- The Qilin affiliate was observed abusing the legitimate Total Software Deployment tool used for software deployment. Specifically, the affiliate used the tool's Inventory Service and Audit Service to install the ConnectWise and ScreenConnect Remote Monitoring and Management (RMM) tools on enterprise systems for later execution.
- Notably, in historical open-source reporting, the abuse of Total Software Deployment has been attributed to other now-defunct ransomware groups, including Conti and AlphV/BlackCat; the combined use of Total Software Deployment with ScreenConnect has been attributed to AlphV/BlackCat and Medusa.
- MITRE ATT&CK TTPs:
  - T1072, Software Deployment Tools
  - T1210, Exploitation of Remote Services
  - T1219, Remote Access Software

Qilin: Lateral Movement

- The Qilin affiliate was observed deploying a 32-bit version of the ScreenConnect RMM tool to connect and move laterally over Port 8041 within the victim's environment.
- The Qilin affiliate was observed deploying the ConnectWise RMM, which was executed from the Documents folder.
- MITRE ATT&CK TTPs:
  - T1210, Exploitation of Remote Services
  - T1219, Remote Access Software

Qilin: Impact

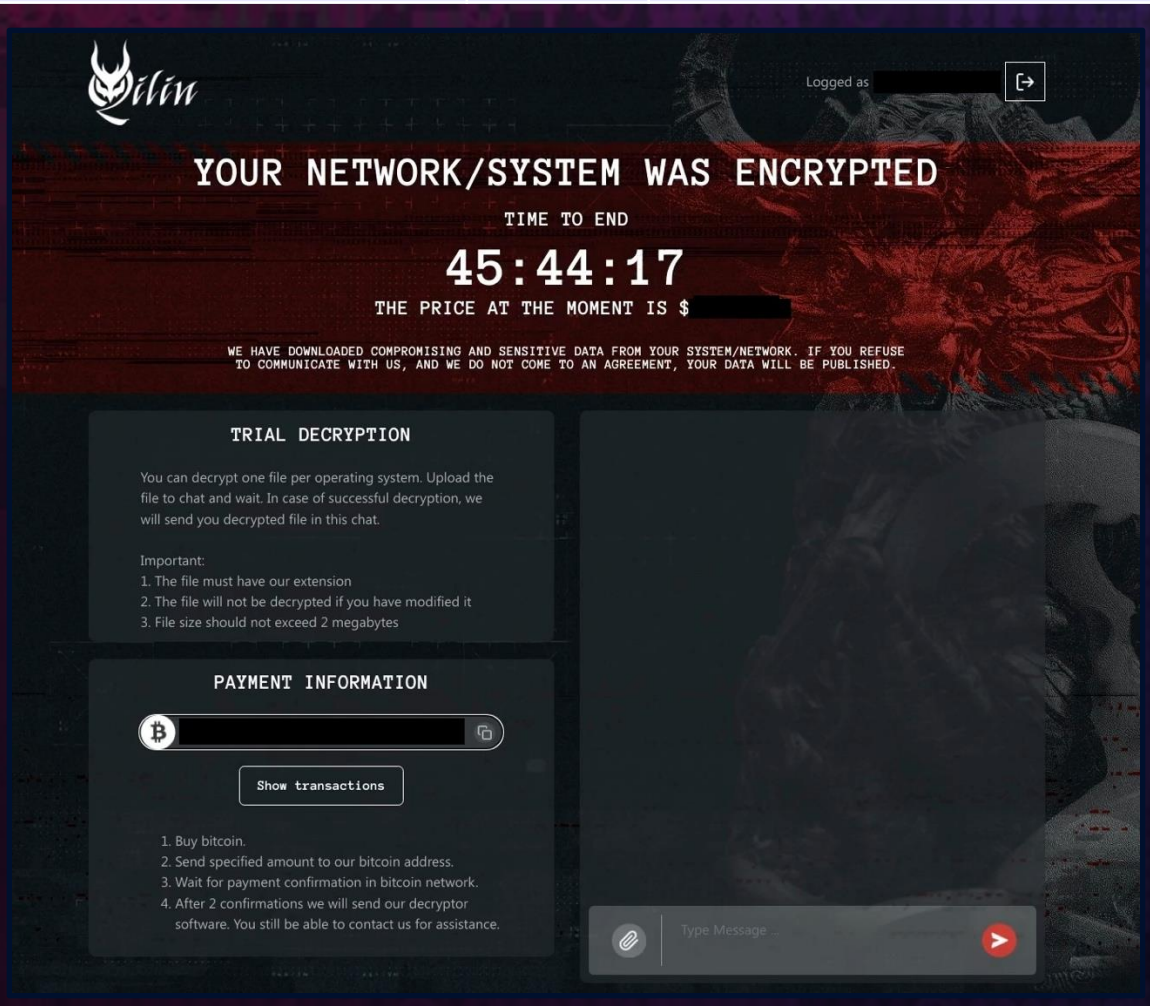
- We observed the Qilin affiliate's transfer of the Qilin ransomware encryptor, named "Wm.exe", first to the root C:\ directory and later to the Documents folder. The affiliate later executed the encryptor from the C:\ directory, with resulting logs saved to C:\Users\Administrator\AppData\Local\Temp\QLOG\
- The affiliate deployed the encryptor by creating a new entry, bmcntq, within the HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry, setting the encryptor to execute upon user login.
- The encryptor observed the following whitelist and blacklist in determining which file types should and should not be encrypted:

extension_white_list: ["mdf", "ldf", "bak", "vib", "vbk", "vbm", "vrb", "vmdk", "abk", "bkz", "sqb", "trn", "backup", "bkup", "old", "tibx", "pfi", "pvhd", "pbf", "dim", "gho", "vpcbackup", "arc", "mtf", "bkf", "dr"] [08:49:44|+0.01408710] <ThreadId(1)>: filename_black_list: ["desktop.ini", "autorun.ini", "ntldr", "bootsect.bak", "thumbs.db", "boot.ini", "ntuser.dat", "iconcache.db", "bootfont.bin", "ntuser.ini", "ntuser.dat.log", "autorun.inf", "bootmgr", "bootmgr.efi", "bootmgfw.efi", "#recycle", "autorun.inf", "boot.ini", "bootfont.bin", "bootmgr", "bootmgr.efi", "bootmgfw.efi", "desktop.ini", "iconcache.db", "ntldr", "ntuser.dat", "ntuser.dat.log", "ntuser.ini", "thumbs.db", "#recycle", "bootsect.bak"] [08:49:44|+0.01624920] <ThreadId(1)>: directory_black_list: ["windows", "system volume information", "intel", "admin$", "ipc$", "sysvol", "netlogon", "$windows.~ws", "application data", "mozilla", "program files (x86)", "program files", "$windows.~bt", "msocache", "tor browser", "programdata", "boot", "config.msi", "google", "perflogs", "appdata", "windows.old", "appdata", "..", ".", "boot", "windows", "windows.old", "$recycle.bin", "admin$"]

extension_black_list: ["themepack", "nls", "diapkg", "msi", "lnk", "exe", "scr", "bat", "drv", "rtp", "msp", "prf", "msc", "ico", "key", "ocx", "diagcab", "diagcfg", "pdb", "wpx", "hlp", "icns", "rom", "dll", "msstyles", "mod", "ps1", "ics", "hta", "bin", "cmd", "ani", "386", "lock", "cur", "idx", "sys", "com", "deskthemepack", "shs", "theme", "mpa", "nomedia", "spl", "cpl", "adv", "icl", "msu"]

Qilin: Indicators of Compromise

Value	Type	Notes
f218a09174ccbc0765f40640200ff81c9a37e5f584845df8d60e61872baba427	SHA256	Qilin Encryptor
cf58ca5bf8c4f87bb67e6a4e1fb9e8bada50157dacbd08a92a4a779e40d569c4	SHA256	Cachedump.exe
f83b5d1cfb691c94844d9a9c2a385f2f1aae144ee69bee7577438f252fc102dc	SHA256	TotalSoftwareDeployment.exe
147.124.219[.]81 : 64444	IPv4	Affiliate ConnectWise Infrastructure



Qilin's chat infrastructure
Source: GRIT

Quarterly Wrap Up

At a macro level, Q3 2024 reflects a calming of the waters following the myriad shakeups that occurred earlier this year. While some affiliates and operators are still in flux, many may have found new homes for their continued work. The rapid normalization of the posting rates of top groups evidences this. RansomHub continues to impress with their burgeoning affiliate program. However, the group still has a long way to go before they reach the operational maturity and tempo of their most prolific predecessors. As we discussed in this report, a strong “middle class” has emerged in the ransomware ecosystem, distributing ransomware victims across a greater number of distinct groups.

As we look to Q4 in the months ahead, we will be alert to whether this new balance of power retains its status quo or whether Established groups such as RansomHub emerge more dominantly over their peers. In previous years, Q3 almost always represented the busiest time in the ransomware ecosystem, but after multiple quarters disrupting the trend of exponential growth, it remains to be seen if Q4 will return to baseline or continue bucking expectations. We assess that continued reductions in ransomware victim volume will be largely dependent on the extent to which individual disrupted affiliates have resumed operations at their former tempo.

Based on activity observed year to date, GRIT assesses that the most likely course of action through the remainder of 2024 and into 2025 is a continued pace of ransomware operations similar to those observed in Q2 and Q3 2024, with victim volume neither substantially increasing nor decreasing overall. Without a major centralized force pushing victimization to new heights, we may not again see numbers rivaling 2023’s peaks for some time. That being said, we acknowledge that the ransomware ecosystem has been anything but predictable in recent years and that the greed of individual cybercriminals will always introduce the potential for strategic surprises. GRIT will continue to analyze the macro and micro trends to help shed some light on the multifaceted and dynamic systems at play in the ransomware space.