RELIAQUEST®

Quarterly Cyber-threat Report:

Ransomware & Data-Leak Extortion

July 1, 2023—September 30, 2023

Make Security Possible

Table of Contents

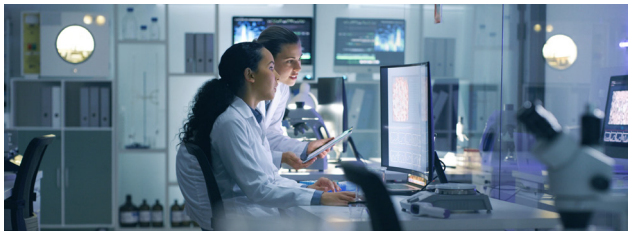
Executive Summary

LOCKBIT 3.0

CL0P^_-LEAKS

The **main active ransomware threats** to organizations, as revealed in analysis from the third quarter of 2023 (Q3 2023), came from established groups, such as "LockBit" and "Clop."

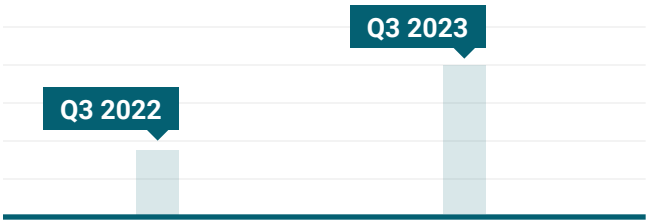
The latter was very busy concluding its MOVEit supply-chain attack, extorting companies by leaking data via torrent links, among other methods.



Unlike the many ransomware groups that "prohibit" targeting healthcare entities, "Rhysida" took the **unconventional approach of attacking the healthcare and social assistance sector**, causing system-wide outages for many US hospitals and clinics.

4.1% **A new group also made a sudden impact four days before the quarter ended:**

During that short time, "LostTrust" was responsible for 4.1% of all ransomware incidents in the quarter.



Overall, Q3 2023 saw **almost twice as much ransomware activity as a year ago**. There were slightly fewer compromised entities named on ransomware data-leak sites than in Q2 2023, but that quarter broke records in terms of ransomware activity.

The five sectors targeted the most remained the same since Q2 2023.

Professional, scientific, and technical services (PSTS) held the top position, with 21% of all ransomware incidents. Manufacturing came in a close second with 20%, followed by construction, healthcare and social services, and finance and insurance.

The five countries targeted the most remained the same since Q2 2023.

The US held the top position, by a wide margin: 48.5% of all companies named on data-leak sites were in the US. The UK, Germany, Canada, and France were the next most-targeted countries.

65% **Considerably fewer compromised entities were named on extortion-only data-leak sites this quarter:**

A 65% decrease occurred since Q2 2023. This was primarily because the "Karakurt Hacking Team"—typically the most active extortion-only group every quarter—was not very active.

Key recommendations for stopping ransomware attacks are:

- Enhance visibility across an environment.
- Implement security controls to catch and contain threat activity before it turns into a ransomware event.
- Apply a defense-in-depth strategy: Focus on defense measures that track threat actor tactics, techniques, and procedures (TTPs) instead of simply chasing indicators of compromise (IoCs).

Overview

ReliaQuest's Threat Research Team actively monitors the operations of ransomware activity. This report covers the most important ransomware-related events and trends we observed in Q3 2023. It describes the most impactful ransomware groups active in this quarter and provides detection and mitigation guidance.

Key Cyber Events

Rhysida Targets Healthcare, Education

The ransomware-as-a-service (RaaS) group Rhysida, which first emerged in May 2023, was highly active in Q3 2023. Rhysida targets organizations in various sectors but has shown a preference for educational services, accounting for 45.7% of all its incidents this quarter.

Many RaaS groups prohibit attacks against healthcare organizations, but in August 2023, Rhysida conducted a series of targeted attacks on the healthcare and social assistance sector, which included disrupting 17 hospitals and 166 clinics across the US. Rhysida auctioned off exfiltrated sensitive data to the highest bidder, including Social Security numbers (SSNs), passport details of clients and employees, driver's license details, patient files, and financial and legal documents. Information not sold via auction was subsequently exposed on the group's data-leak site for public download.

On August 04, 2023, the US Department of Health and Human Services (HHS) issued a warning about Rhysida's targeting of healthcare and public-sector organizations in Western Europe, North and South America, and Australia. HHS also cautioned that Rhysida had repeatedly targeted organizations in the educational services sector. These targeting patterns align with those of another ransomware group, "Vice Society," suggesting a connection between the two groups. HHS predicted that Rhysida will likely continue to be a significant threat to the healthcare and social services sector.

To protect against Rhysida, HHS recommends:

- **Virtual patching:** This will immediately protect against known vulnerabilities exploited by Rhysida when vendor-supplied patches are not available or cannot be immediately applied.

- **Proactive measures:** Conduct regular phishing awareness training, use endpoint security tools, employ immutable backups, implement network segmentation, use firewalls and intrusion detection systems, and have a well-defined incident response plan.

Clop Concludes MOVEit Campaign

On June 5, 2023, Clop claimed responsibility for a series of cyber attacks exploiting the zero-day vulnerability in the MOVEit Transfer software, tracked as CVE-2023- 34362. In Q3 2023, Clop continued to extort organizations in this campaign, naming most new compromised entities on its data-leak site in July 2023.

In August 2023, Clop initiated a multifaceted, extended initiative to extort these companies to pay a ransom, then seemed to conclude its MOVEit campaign in mid-September 2023, when it last updated its data-leak site.

Clop's Extortion Methods

Clop employed various tactics to pressure organizations to negotiate a ransom, if they had not yet contacted the group. These included:

- Slowly leaking compromised entities' data on the dark web in multiple parts.
- Exposing the data on the clear web using an impersonating domain—a strategy previously used by ALPHV.
- Naming the clients of targeted organizations, to imply data had been stolen from multiple companies in the compromise.
- Leaking excerpts of ransom negotiation conversations that identified compromised entities.
- Using torrents for peer-to-peer sharing of stolen data.

Clop's shift to leaking data on the clear web and through torrents made it easier for anyone to access the data without special dark-web software, increasing the pressure on compromised entities. Data is also easier to host and faster to download on the clear web, making it more likely stolen data will be downloaded.

Clop set deadlines for initiating negotiations and receiving payments. The group initially established a deadline of June 14, 2023 for any affected entity to make contact and begin negotiations. Failure to comply would result in the entities being named on the group's data-leak site. This demand was unique, placing the burden on companies to determine whether they were compromised and begin ransom negotiations.

The group reiterated a similar threat on August 10, 2023, warning that if companies failed to contact Clop by August 15, their data would be released via torrents on Clop's dark-web data-leak site and the clear web. Clop warned that it would also create the clear-web download URLs for large companies, which could be indexed by Google.

Next Moves for Clop

As Clop concludes its MOVEit campaign, the group will likely enter a temporary phase to plan its next move. Our monitoring indicates that Clop typically exhibits minimal or no activity for extended periods before launching large-scale attacks that impact numerous organizations (see Figure 1). Notable examples include its campaigns targeting vulnerabilities in MOVEit (beginning late May 2023), GoAnywhere (February–March 2023), and Accellion (December 2020) software.

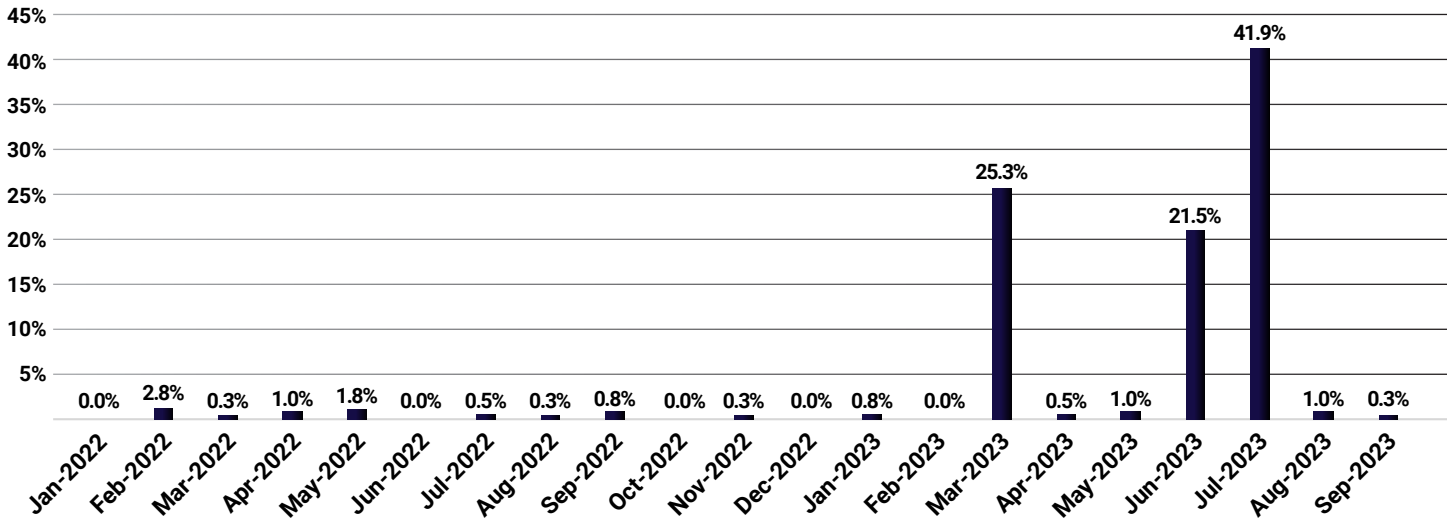


Figure 1: Percentage of companies named to Clop's leak site, January 2022–September 2023

The group has demonstrated a particular interest in targeting enterprise managed file transfer (MFT) solutions. It has engaged in extortion-only attacks in which it did not deploy ransomware, including the group's major campaigns (MOVEit, GoAnywhere, and Accellion). Extortion-only attacks primarily result in reputational and legal damages, but ransomware attacks can also lead to operational disruption.

ReliaQuest has observed numerous Clop attempts to exploit MOVEit vulnerabilities in our customers' environments. Our analysis led us to develop mitigation steps for organizations to protect against similar campaigns:

- **Minimize exposure on MFT sites:** Remove content from MFT sites after a short period (e.g., five to ten business days) to minimize exposure, as MFT services are primarily meant for file transfer and not long-term storage.

- **Strengthen on-premises application deployments:** Ensure that on-premises application deployments have robust logging and comprehensive tool coverage. These applications have a higher chance of being exposed to the internet and exploited before vulnerabilities are detected by the intelligence community. Implement strict access control lists (ACLs) to limit access to the applications, and consider implementing geofencing measures. In the case of MOVEit, be aware that most exploitation incidents originated from IP addresses in Slovakia.

- **Maximize application-specific log files and enable dedicated Windows logs (for MOVEit):** Most applications generate native log files that are stored on disk with limited retention and may not be forwarded to a security information and event management (SIEM) team or data lake. Application-specific log files are crucial for triage and incident response. If central logging is not feasible, consider increasing the maximum file size before logs start rolling over, or increasing the retention period on disk. At least 30 days of log retention should be sufficient for effective analysis. Additionally, verify if the MOVEit software has a dedicated Windows log, which, if available, should be enabled; this log may not be enabled by default and may have size limitations (e.g., 8MB).

Ransomware and Extortion Metrics

During Q3 2023, we observed a 6.9% decrease in the number of organizations being named on data-leak websites by ransomware gangs, compared with Q2 2023. Despite this slight decline, which likely reflects expected variation between quarters, ransomware activity remained high and groups' success seems to continue: 97.8% more entities were named on data-leak sites than in the same quarter last year (Q3 2022). This increase was likely driven by more ransomware groups operating in 2023; there were 50% more active groups than in the past year.

From Q2 2023 to Q3 2023, there was a 65% decrease in the number of organizations named on extortion-only data-leak sites[1]. The decline can be attributed to the reduced activity of the most active extortion group, the Karakurt Hacking Team, whose activity fluctuates between quarters. Although Clop's MOVEit campaign and others used an effective extortion-only model, most ransomware groups still heavily rely on encryption and double extortion, creating operational disruption that can pressure companies into paying ransoms.

Despite the relative scarcity of data-leak sites run by extortion-only threat actors, as compared to ransomware groups, extortion-only attacks are frequent. Some extortion-only attackers leak data on underground cybercriminal forums if a compromised entity fails to pay the ransom. Alternatively, they may offer to sell the stolen data to other threat actors; we have frequently observed this on prominent cybercriminal forums (see Figure 2).

[1] These sites are associated with groups that steal data and name their targets on data-leak sites, but do not deploy ransomware or carry out encryption. Although Clop's MOVEit campaign was extortion only, we classify Clop as a double-extortion ransomware group for its history of using the Clop ransomware to encrypt data.

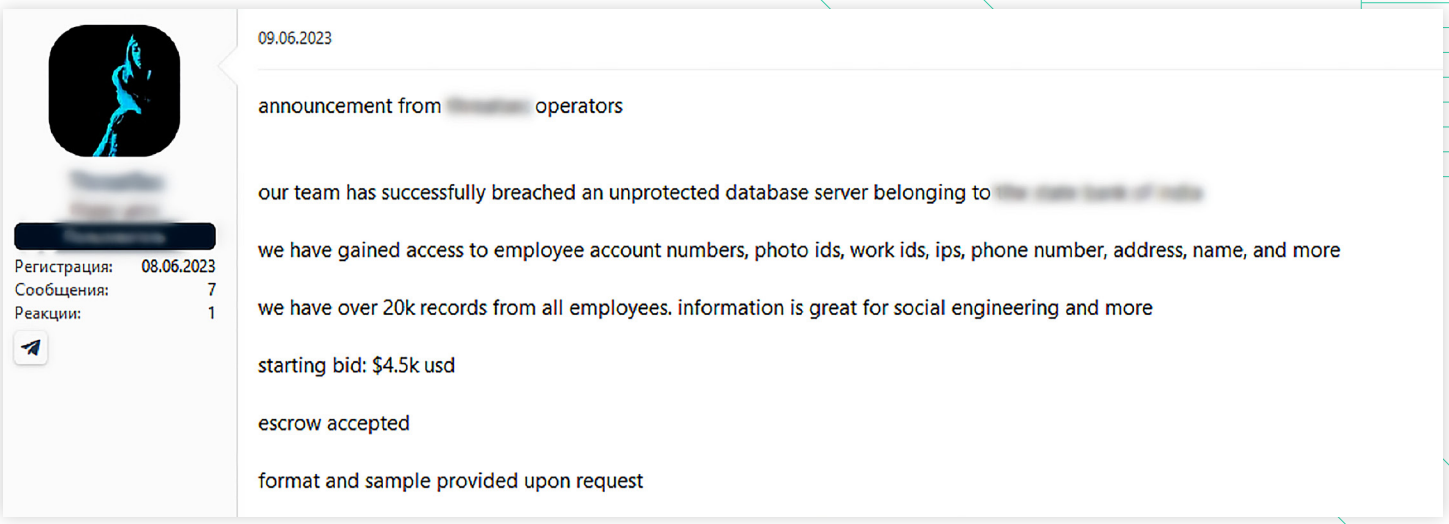


Figure 2: Cybercriminal forum user offering to sell stolen data

In Q3 2023, although there were no record-breaking monthly numbers, the overall ransomware activity level remained high, compared to activity in late 2022 and early 2023. September 2023 saw 71% more compromised entities than in September 2022, evidencing a rise in ransomware incidents throughout the past year.

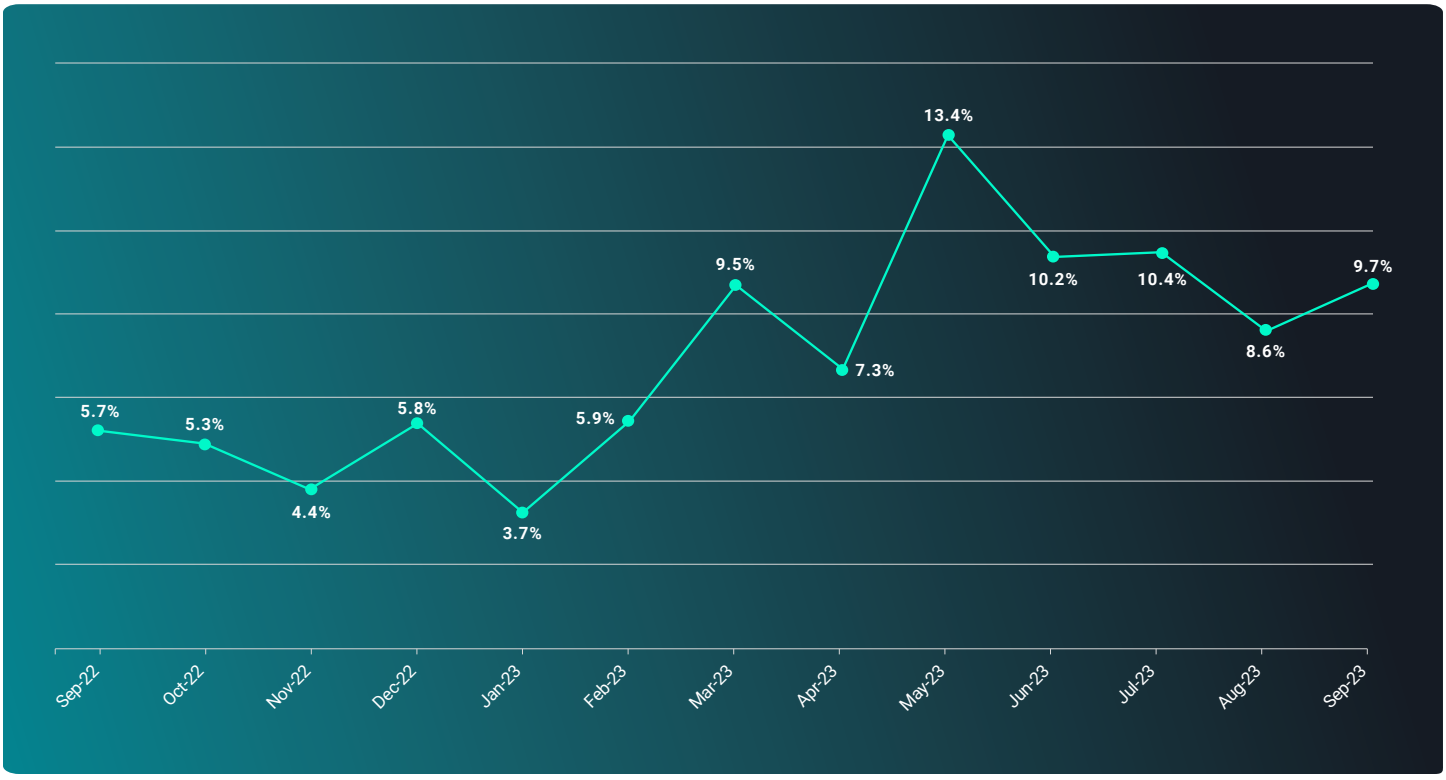


Figure 3: The percentage of ransomware attacks that occurred each month, September 2022–23, out of all ransomware attacks throughout the year

During Q3 2023, more than 50 ransomware groups named companies on their data-leak sites. ReliaQuest tracked all active ransomware groups and ranked them by the number of compromised entities named on each group's data-leak site.

If a ransomware group did not name many (or any) compromised entities, that group was not necessarily inactive. **If there were successful ransom negotiations with compromised companies**, their names would not be publicized on a data-leak site.

Key Threats

The ransomware groups LockBit, Clop, and "ALPHV" targeted the most organizations this quarter, according to posts on the groups' data-leak sites. Clop regained its position as the second most-active ransomware group, overtaking "Malas" from Q2 2023. Malas has not named any new entities on its data-leak site since May 2023, indicating that the group may no longer be operating.

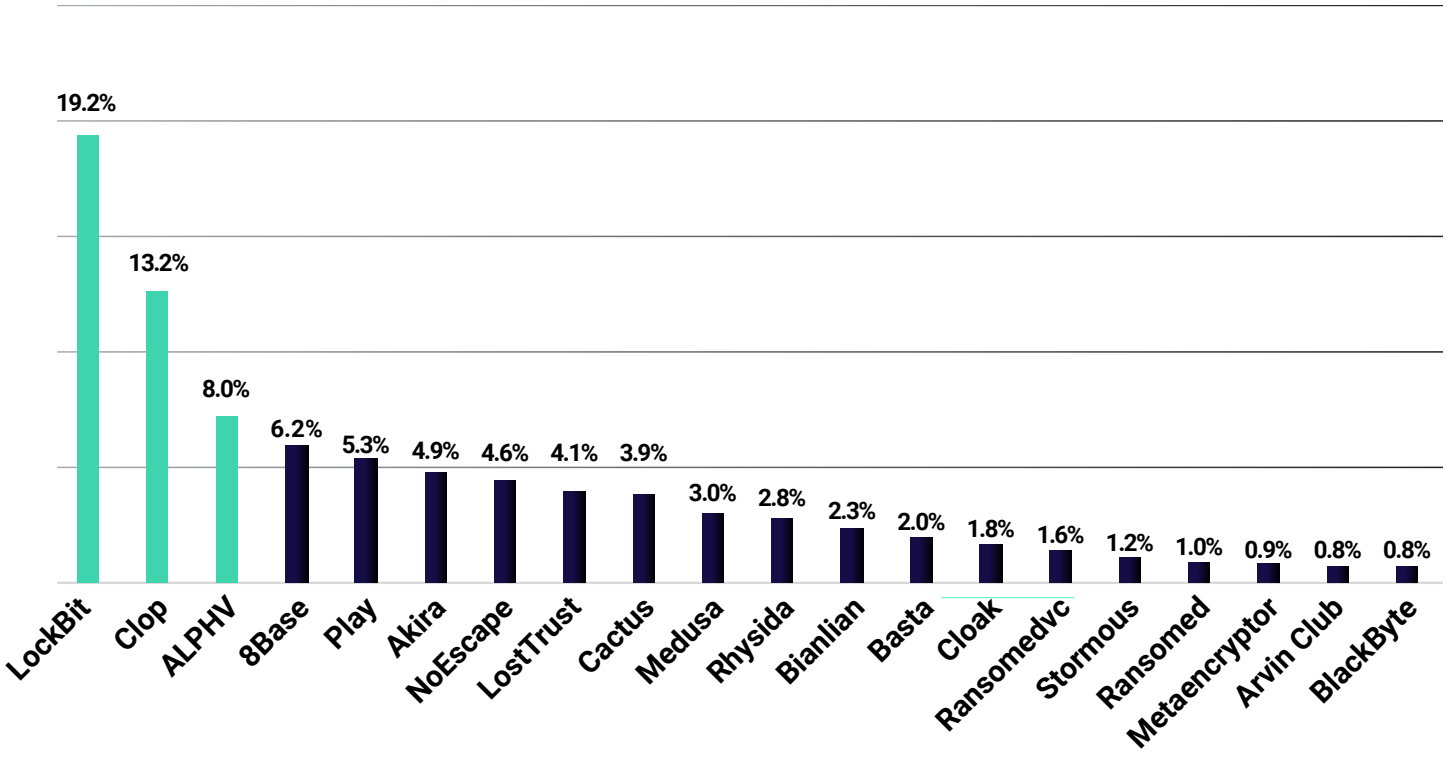


Figure 4: Top 20 active ransomware groups, as ranked by percentage of all compromised companies named on data-leak sites

LockBit named the most entities, accounting for 19.2%. The group has consistently held this top position every quarter since the initial release of the "LockBit 2.0" ransomware in July 2021. With the introduction of "LockBit 3.0" in June 2022, the group continued to evolve and expand its operations.

LockBit's ongoing dominance is likely driven by the group's professionalism and reputation, and its easy-to-use ransomware builder, which have attracted new affiliates[2] and grown the LockBit brand.

The next most-active groups were Clop, ALPHV, "8Base," and "Play." "Akira," although only the sixth most-active group, demonstrated continued development and growth. The group extended its targeting to Linux servers and successfully exploited a zero-day vulnerability in Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) during attacks.

The new LostTrust took eighth position in the top ten most active groups, with 4.1% of all recorded incidents. LostTrust launched its data-leak site on September 26, 2023, with only four days left in the quarter, meaning its eighth-place position is a significant event.

At the time of writing, little is known about LostTrust, aside from it likely being a rebrand of MetaEncryptor—using a nearly identical encryptor and data-leak site. However, some of the entities named by LostTrust were targeted by other ransomware groups in the past; it is realistically possible that LostTrust was formed by ex-affiliates of those groups, or it targets vulnerabilities that have been exploited by other ransomware operations.

Despite not being one of the top ten groups to name the most compromised organizations, Rhysida had a very significant quarter targeting healthcare and education organizations, conducting multiple high-profile attacks. The group's ransomware is likely still in the early stages of development (its application program is named Rhysida-0.1), so it is realistically possible that Rhysida will evolve into a significant threat.

Clop's **Great Surge**

Despite its second-place position, Clop achieved a remarkable feat that few ransomware groups have accomplished. In July 2023, Clop's data-leak site featured more than three times the number of organizations named by LockBit that month. The MOVEit exploitation campaign accounted for the significant increase in named entities.

The following profiles describe three ransomware groups that created an impact in Q3 2023, including events, TTPs, and mitigation strategies. These groups may not have compromised the most entities, but their developments or campaigns were notable.

[2] Affiliates of ransomware developers receive customizable ransomware from the developers to conduct attacks, in exchange for a small cut of profits.

CL0P^_-LEAKS

Clop Background

Clop is one of the oldest double-extortion ransomware groups active today. The RaaS group has been encrypting and stealing data, as well as naming companies on its data-leak site, CL0P^_-LEAKS, since March 2020.

The Clop ransomware is an updated version of the "CryptoMix" ransomware, written in C++ and first discovered in March 2016. It was created to target Windows systems. Clop is built to terminate itself if the target organization's location is identified as Russia or another Commonwealth of Independent States (CIS) country. Clop is believed to have Russian origins.

Clop is deployed by a subgroup of the cybercrime group "FIN11" called TA505: the same group behind the "Dridex" banking trojan and the "Locky" ransomware.

Clop's operators' primary goal is financial gain. They have earned substantial payouts from ransoms: as much as $500 million.

Clop TTPs

Clop is known for exploiting zero-day vulnerabilities in MFT software to conduct mass ransomware attacks. In these campaigns, Clop typically does not deploy ransomware and simply exfiltrates data.

Initial attack methods include exploiting zero-day vulnerabilities, sending phishing emails with malicious links or attachments, using exploit kits, posting malicious advertisements, and creating fraudulent websites. Clop has also been known to buy access from initial access brokers (IABs).

Clop's toolkit includes many malware types, including the "FlawedAmmyy"/"FlawedGrace" remote-access trojan (RAT) and the "SDBot" backdoor. Other malware and tools include "Truebot," "DEWMODE," and "LEMURLOOT" for information collection, propagation, and network expansion.

Once inside a network, Clop operators use remote desktop protocol (RDP) and tools like Cobalt Strike for lateral movement, culminating in file encryption and ransom demands.

Clop does not always deploy ransomware. The group has been known to infiltrate organizations, steal data, and demand payments via email.

When deploying ransomware, Clop uses the AES (Advanced Encryption Standard) cipher to encrypt files and adds a ".Clop" (or similarly named) filename extension. Clop has anti-analysis capabilities and anti-virtual machine analysis to prevent investigations in emulated environments.

Clop is known to publish victims' data in parts, slowly over time, with each containing files in split ZIP archives (file.zip, file.z01, file.z02, etc). Files leaked by Clop are typically hosted on the dark web.

Active since: February 2019

Threat Level: **Very High**

Top 3 all-time targeted sectors (% of all sectors Clop targeted):

1) Professional, scientific, and technical services - 30.9%
2) Manufacturing - 17.9%
3) Finance and insurance - 16.5%

Top 3 all-time targeted regions (% of all regions Clop targeted):

1) US - 61.8%
2) Canada - 7.1%
3) UK - 5.7%

In Q3 2023, Clop mostly affected US organizations: 66.3%. The group is known for specifically targeting US organizations, possibly because of its success in receiving ransom payments there. According to HHS, the Clop ransomware group has allegedly received payouts amounting to $500 million since its creation[3].

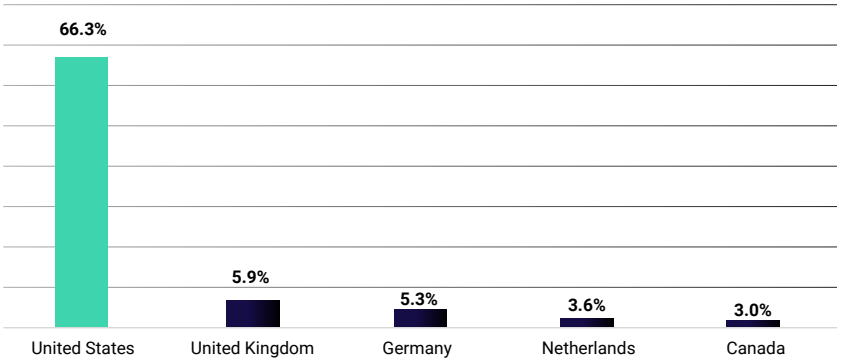


Figure 5: Countries targeted most by Clop in Q3 2023

The sector that Clop primarily targeted in Q3 2023 was PSTS, which handles and processes substantial amounts of customer data. Clop has threatened to leak customer data to pressure companies into meeting ransom demands.

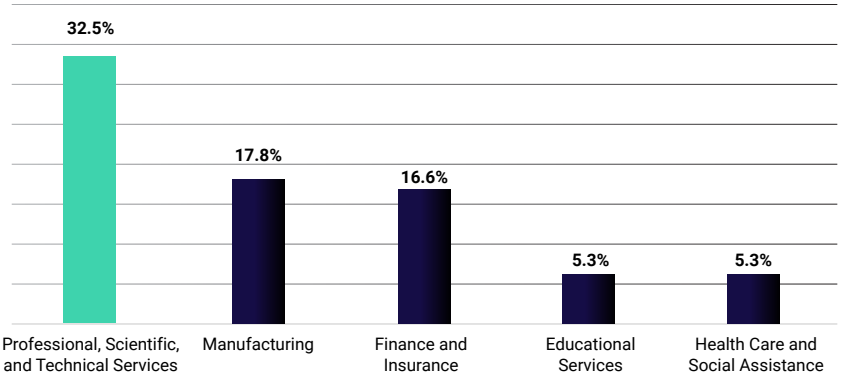


Figure 6: Sectors targeted most by Clop in Q3

Notable developments/events in Q3 2023:

- Clop used unique extortion tactics to pressure MOVEit compromised companies into ransom negotiations. These tactics have included posting breached data on clear-web domains and using torrents for the peer-to-peer sharing of stolen data.
- The group only named four new compromised entities in August and one in mid-September. No torrent leaks were involved in these attacks. It is unknown whether the attacks were a part of the MOVEit campaign.

[3] hxxps://www.aha[.]org/system/files/media/file/2023/01/hc3-tlp-clear-analyst-report-clop-ransomware-1-4-23.pdf

Rhysida Background

The Rhysida double-extortion RaaS group operates a data-leak site to leak and auction off breached data. Researchers have linked Rhysida to the "Vice Society" ransomware group.

Rhysida portrays itself as a "cybersecurity team" that highlights security problems in organizations' systems, claiming to be doing them a favor.

The group primarily targets the education sector. Unlike many other RaaS groups, Rhysida attacks have also involved the healthcare sector.

Analysis of Rhysida ransomware samples suggests an early stage of development; they lack some common features found in mature ransomware.

Rhysida TTPs

Rhysida typically initially accesses targeted networks through phishing attacks, then uses Cobalt Strike for lateral movement.

Rhysida uses ChaCha20 to encrypt files, but its ransomware could easily switch to another algorithm in future.

Rhysida uses a 4096-bit RSA key and AES-CTR for file encryption, appending the .rhysida extension to encrypted files. Its ransom note is a PDF document named CriticalBreachDetected.pdf, which is placed in affected folders.

To execute the Rhysida ransomware, the group employs the use of PsExec and a PowerShell script called SILENTKILL. This script carries out various actions, such as terminating antivirus-related processes, deleting Volume Shadow Copies, modifying RDP configurations, and changing the user's Active Directory (AD) password.

Rhysida operators have used RDP, Windows Remote Management, and Cobalt Strike for lateral movement in a compromised system.

Rhysida has leaked stolen data on the dark web, enabling visitors to browse through directories of stolen files and download them.

Threat Level: **High**

Active since: May 2023

Top 3 targeted sectors (% of all sectors Rhysida targeted):

1) Educational services – 41.1%
2) Professional, scientific, and technical services – 16.1%
3) Healthcare and social assistance – 12.5%

Top 3 targeted regions (% of all regions Rhysida targeted):

1) US – 23.2%
2) Italy – 10.7%
3) UK – 8.9%

Although targeting the US the most, Rhysida did not seem to have a significant preference for any region (unlike other ransomware groups); targets were spread across Europe and North America.

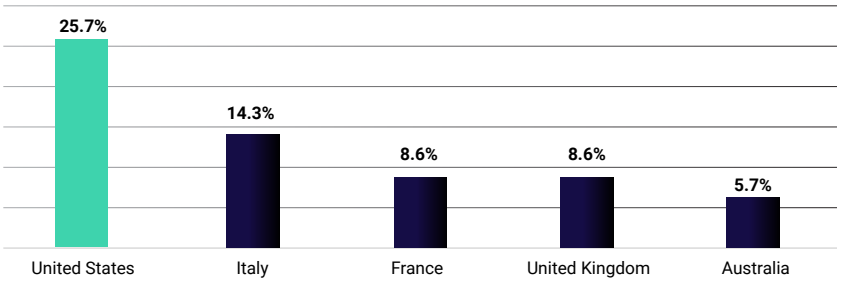


Figure 7: Countries targeted most by Rhysida in Q3 2023

Rhysida significantly focused on the educational services sector. This notable strategy is similar to that of Vice Society, which was notorious for targeting education entities.

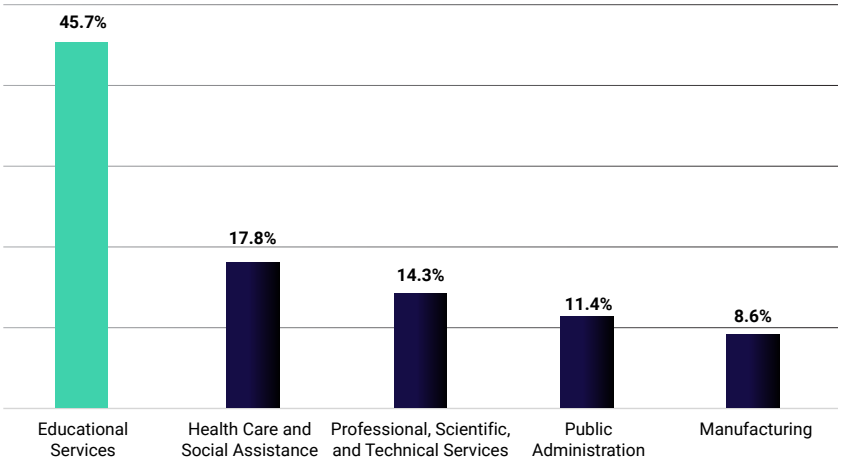


Figure 8: Sectors targeted most by Rhysida in Q3 2023

Notable developments/events in Q3 2023:

- The group began a wave of attacks against the healthcare sector in Q3 2023.
- In August, Rhysida conducted a high-profile attack against an organization in the healthcare sector in California. This attack allegedly resulted in more than 500,000 SSNs and patient files being stolen, and more than five company subsidiaries being affected, leading to lengthy downtimes and data theft.

Akira Background

The Akira double-extortion ransomware group targets large- to mid-sized enterprises, primarily in the US.

The group gained attention for its retro-looking data-leak website, where users enter commands to see names of compromised entities and download leaked data through a command-line interface.

Akira demands exorbitant ransom amounts, sometimes reaching hundreds of millions of dollars.

The group is unlikely to be connected to a 2017 ransomware group named Akira.

Akira TTPs

Initial delivery of Akira ransomware often involves exploiting vulnerabilities in public-facing services or applications. The group has targeted flaws in multi-factor authentication (MFA) and VPN software.

Akira attempts credential dumping through Local Security Authority Subsystem Service (LSASS) dumps. This enables the group to obtain credentials for lateral movement and privilege escalation within the compromised network.

Akira uses the Windows Restart Manager application programming interface (API) to close processes or shut down Windows services that may interfere with the encryption process.

Akira has also been associated with Living Off the Land Binaries (LOLBins) or commercial off-the-shelf tools, like PCHunter64. The group also uses minidumps[4] to gather intelligence on targeted networks.

When executed, Akira deletes Windows Volume Shadow Copies using a PowerShell command.

The group drops a ransom note named akira_readme.txt in each encrypted folder, and appends encrypted files with the .akira extension.

The group leaks breached data through torrent magnet links and TORRENT files. It instructs visitors to use torrent clients to download the leaked data.

[4] Diagnostic files that contains essential information about a crashed process or application.

Threat Level: **High**

Active since: March 2023

Top 3 targeted sectors (% of all sectors Akira targeted):
1) Professional, scientific, and technical services – 23.1%
2) Manufacturing – 17.4%
3) Construction – 12.4%

Top 3 targeted regions (% of all regions Akira targeted):
1) US – 83.5%
2) Canada – 5.8%
3) UK – 2.5%

Akira primarily targets the US (in 90.5% of its Q3 2023 attacks). The group very likely tailors its targeting specifically to US organizations, perceiving them as more likely to pay ransoms.

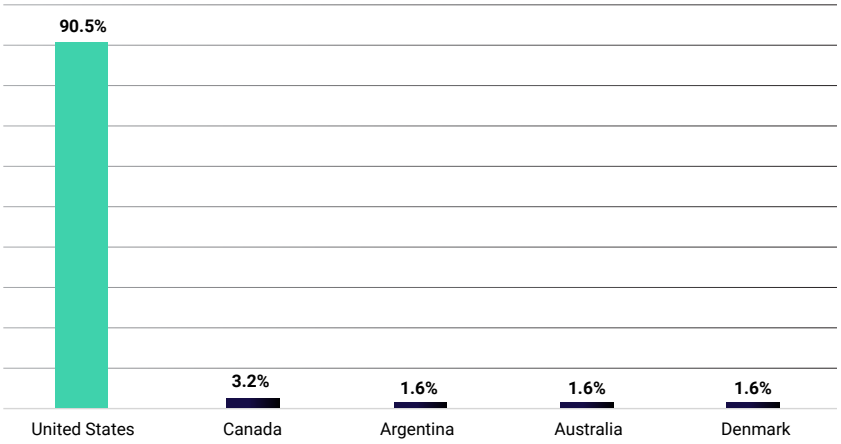


Figure 9: Countries targeted most by Akira in Q3 2023

A significant portion of Akira attacks have focused on the manufacturing and PSTS sectors: sectors with high revenues. As an added incentive for ransomware operators, many companies in those sectors cannot afford lengthy periods of downtime.

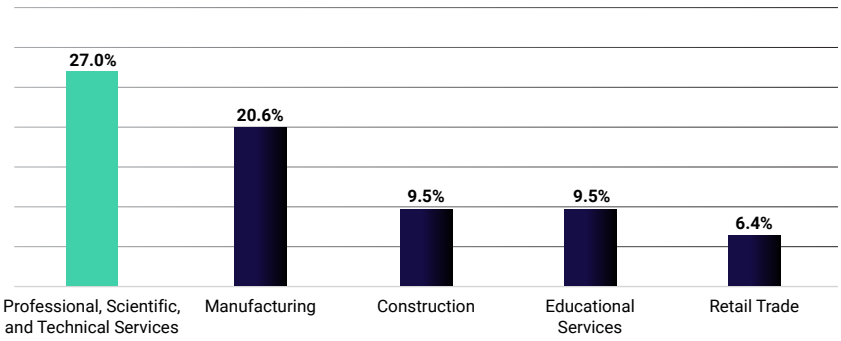


Figure 10: Sectors targeted most by Akira in Q3 2023

Notable developments/events in Q3 2023:

- In September 2023, it was reported that Akira expanded its capabilities to target Linux servers, specifically focusing on VMware ESXi virtual machines.
- Also in September, reports surfaced regarding Akira's targeting of Cisco VPNs that lacked MFA. This campaign exploited a zero-day vulnerability known as CVE-2023-20269, enabling brute-force attacks on existing VPN accounts.

Most Targeted Sectors

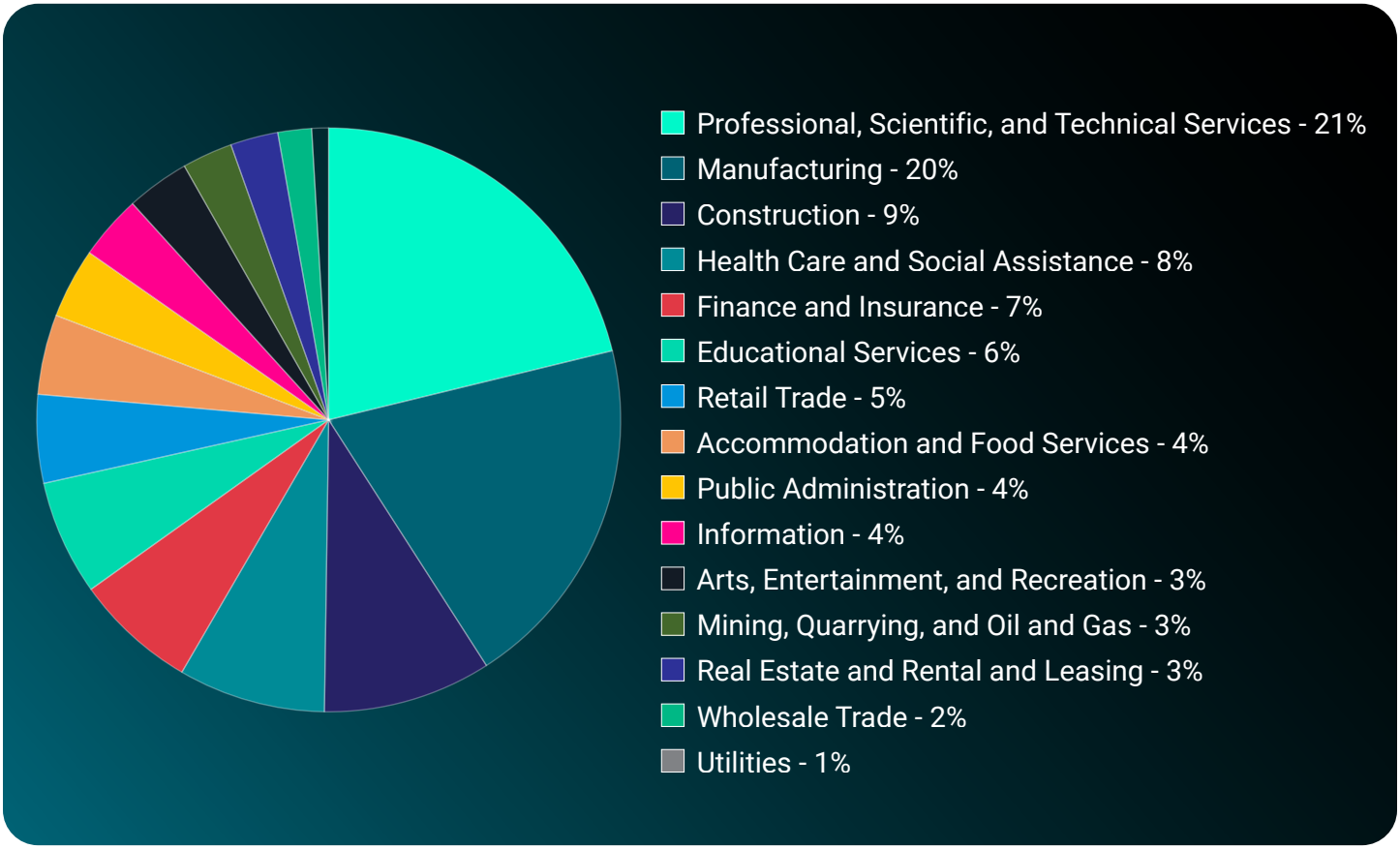


Figure 11: Sectors most targeted by ransomware groups

There were no significant shifts in sectoral targeting patterns. A few factors help explain why organizations in the PSTS, manufacturing, and construction sectors were targeted the most:

- Many heavily rely on technology, and several use outdated systems that are vulnerable to cyber attacks. Others are vulnerable because their network infrastructure is not entirely visible.
- They play a critical role in supply chains, which appeals to ransomware operators.
- Many provide services, often sharing data and infrastructure that could be compromised to simultaneously target multiple companies.

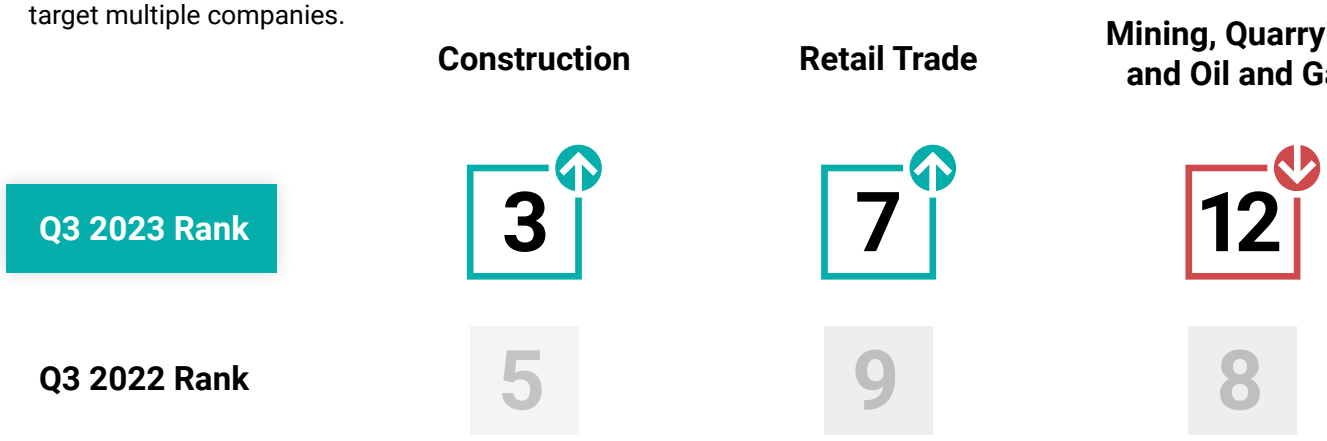


Figure 12: Minor shifts in sector ranking from Q2 to Q3 2023, as measured by number of ransomware incidents

Most Affected Countries

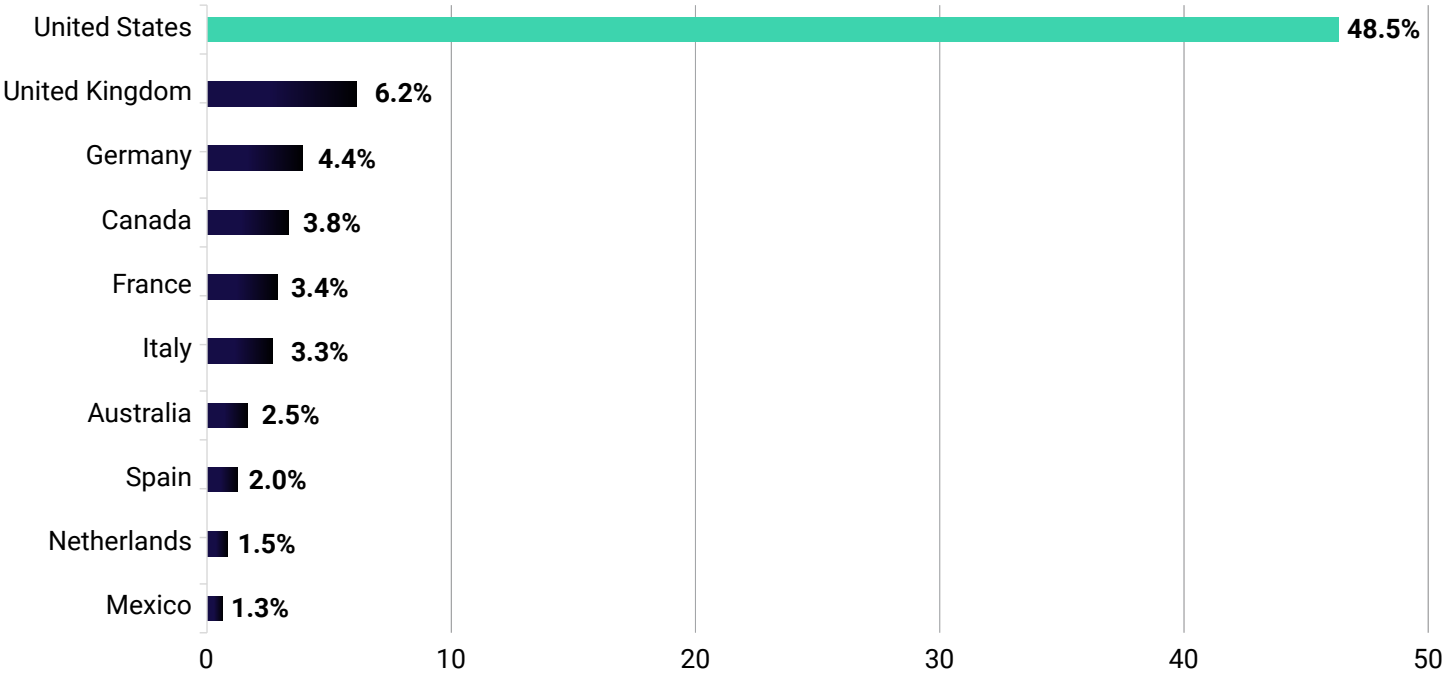


Figure 13: Top ten countries most targeted by ransomware groups

The US being the most targeted country by a wide margin—accounting for close to half of all entities named on ransomware data-leak sites—was unsurprising; the US is typically the country most targeted by ransomware groups every quarter, owing to multiple factors:

- An abundance of potential targets
- Previous success of ransomware groups in receiving ransom payments from the US
- Attackers' nationalistic motives
- A perception of US entities offering a higher potential to pay ransoms

After the US, the remaining countries in the top five most targeted were the same as in Q2 2023: the UK, Germany, Canada, and France.

The UK experienced a 37.9% increase in targeting since the previous quarter, and Australia and Italy each saw significant increases: of 60% and 55.5%, respectively. These significant increases may seem alarming, but may not necessarily indicate new trends or heightened threats against these countries. Instead, the higher number of compromised companies can often be attributed to smaller-scale ransomware operations, such as attacks by Rhysida on Italy and Australia.

In contrast, Brazil was targeted 43.5% less, dropping to 13th place. Switzerland was targeted 25% less and Canada 3.9% less. These countries are not targeted as often as the US, and percentages can fluctuate between quarters, based on small variations in the number of compromised companies.

Common MITRE ATT&CK Techniques in Q3 2023

We analyzed the techniques of the ten most active ransomware groups as classified by the MITRE ATT&CK framework, to determine commonalities and provide appropriate detection rules. However, many large ransomware groups have affiliate programs that employ a large variety of threat actors, so TTPs are likely to differ among attacks.

The most common MITRE techniques associated with the most active ransomware groups were:

MITRE ATT&CK Stage	Technique ID	Description
Initial Access	T1566.001	Spearphishing Attachment
Initial Access	T1566	Phishing
Execution	T1569.002	Service Execution
Execution	T1059.003	Windows Command Shell
Execution	T1059.001	PowerShell
Execution	T1129	Shared Modules
Persistence	T1547.001	Registry Run Keys / Startup Folder
Privilege Escalation	T1055	Process Injection
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Privilege Escalation	T1620	Reflective Code Loading
Defense Evasion	T1070.01	Clear Windows Event Logs
Defense Evasion	T1490	Inhibit System Recovery
Defense Evasion	T1562.04	Disable or Modify System Firewall
Defense Evasion	T1562.001	Disable or Modify Tools

MITRE ATT&CK Stage	Technique ID	Description
Defense Evasion	T1070.004	File Deletion
Credential Access	T1003.003	OS Credential Dumping: NTDS
Discovery	T1018	Remote System Discovery
Discovery	T1518.001	Security Software Discovery
Discovery	T1082	System Information Discovery
Discovery	T1057	Process Discovery
Discovery	T1087.002	Domain Account
Discovery	T1018	Remote System Discovery
Discovery	T1135	Network Share Discovery
Discovery	T1083	File and Directory Discovery
Lateral Movement	T1021.001	Remote Desktop Protocol
Lateral Movement	T1021.002	SMB/Windows Admin Shares
Collection	T1005	Data from Local System
Collection	T1114.001	Local Email Collection
Command and Control	T1105	Ingress Tool Transfer
Exfiltration	T1041	Exfiltration Over C2 Channel
Impact	T1486	Data Encrypted for Impact

Detection Recommendations

ReliaQuest helps customers ensure a focus on comprehensive coverage and a defense-in-depth strategy, and the ReliaQuest GreyMatter® Detect library covers all phases of the attack lifecycle. To identify valuable opportunities for detecting ransomware activity, robust endpoint logs are required; visibility limitations should be pre-emptively addressed, rather than in response to a breach. Customers should review GreyMatter Detect to identify areas for improvement.

Analysis of post-exploitation activity suggests that **threat actors favor the techniques listed below**; defenders can use this list to identify coverage gaps in environments.

PsExec Pivoting

Remote administration tools, such as PsExec, are lightweight programs that allow users to connect to and remotely execute processes on other systems. An attacker will connect to a share of an internal host and upload the PsExec program, where they can execute it and begin sending remote commands to fully compromise the host. Programs executed on remote systems connected to by PsExec will run under the PSEXECSVC.exe process. Attackers will often use PsExec to pivot throughout environments because of the tool's versatility and signed status.

Relevant MITRE ATT&CK techniques:

- T1021.002 – SMB/Windows Admin Shares
- T1569.002 – Service Execution

Phishing - Allowed Attachments with Suspicious Extension

Sending phishing emails is the most common delivery method for malware. Email gateways have significantly improved at identifying and blocking known file extensions often used in phishing attacks, but some extensions may still bypass security checks and land in the user's inbox. In the case of emails with attachments, monitor incoming emails for file extensions that are commonly associated with phishing and are not blocked by the email gateway, such as .img or .iso.

Relevant MITRE ATT&CK techniques:

- T1566.001 – Spearphishing Attachment
- T1204.002 – Malicious File

Active Directory Enumeration

AD enumeration is a technique used by adversaries to gather more information about an environment. Tools like Adfind and Sysinternals AD Explorer facilitate easy searching of AD through the command line. Using this information, the threat actor can escalate privileges and pivot throughout the environment, potentially ending in ransomware deployment. Detection rules can be implemented on the endpoint to monitor for the use of these tools.

Relevant MITRE ATT&CK techniques:

- T1482 – Domain Trust Discovery
- T1016 – System Network Configuration Discovery
- T1087.002 – Domain Account

Cobalt Strike

Cobalt Strike provides command-and-control beacon functionality that enables communication between the attacker and the compromised systems. This enables the attacker to stealthily issue commands, exfiltrate data, and maintain control over the infected systems. Once sufficient control has been established over the network, the attacker deploys and executes the ransomware, encrypting valuable data and removing any Volume Shadow Copies or backups within the target environment. Detections can be put in place at the endpoint or network level to determine whether Cobalt Strike is being used in an environment.

Relevant MITRE ATT&CK techniques:

- T1055 – Process Injection
- T1059.001 – PowerShell

General Recommendations and Best Practices

Network

- **Implement MFA:** Enable code-based MFA for all user accounts, especially for remote access and privileged accounts. This adds an extra layer of security and makes it harder for attackers to gain unauthorized access. See our blog covering this topic here.
- **Implement canary tokens:** Canary tokens, such as Thinkst Canary, provide high-fidelity, low-cost, and easy-to-implement security measures.
- **Segment networks:** Ensure proper network segmentation of devices so they can only communicate with other devices needed to support their specific business functions.
- **Monitor external-facing assets:** Threat actors frequently scan the internet for public-facing assets that have exploitable vulnerabilities, to gain initial access. Remedy any accidental exposure and patch out-of-date services, prioritizing services that have known vulnerabilities.

Internal System

- **Apply a defense-in-depth strategy:** Focus on defense measures that track threat actor TTPs, ensure visibility into your environment, and implement multiple security controls to detect and prevent ransomware activity.
- **Restrict PowerShell use:** Use group policy objects to restrict PowerShell use to only specific users or administrators who manage a network or Windows operating system. Refer to the "Keeping PowerShell: Security Measure to Use and Embrace" cybersecurity information guide[5] for implementation.

[5] hxxps://media.defense[.]gov/2022/jun/22/2003021689/-1/-1/1/csi_keeping_powershell_security_measures_to_use_and_embrace_20220622.pdf

- **Implement a recovery plan and maintain offline backups:** Maintain and retain multiple copies of sensitive data and servers in a physically separate, segmented, and secure location. Regularly maintain offline backups of data and restoration capabilities.

- **Use application control:** Because weaponized script files are used heavily by initial-access malware, only permit the execution of signed scripts (wherever appropriate and possible). Consider redirecting the default application for JavaScript, Visual Basic, and other executable script formats to open by default in notepad.exe instead of wscript.exe.

- **Ensure comprehensive coverage:** Prioritize visibility and validation of visibility. Endpoint logging and visibility play a key role in detecting and addressing exploit or threat activity. Make sure to enable coverage for antivirus or endpoint detection and response tools in your environment. Additionally, send logs to a central location like a SIEM for comprehensive visibility. This proactive approach enables earlier detection and remediation of intrusions, preventing them from reaching ransomware or extortion levels of severity.

- **Keep all operating systems, software, and firmware up to date:** Regularly update and patch operating systems, software, and firmware. Prioritize patching known exploited vulnerabilities in internet-facing systems.

Threat Actor Tracking

- **Use threat intelligence:** Threat intelligence is crucial for enhancing defenses against threats. Begin by understanding your organization's industry and identifying the threat actors or ransomware groups targeting it. Track the associated TTPs or indicators of compromise (IoCs) to gain valuable insights. Prioritize mitigation actions based on the potential impact and likelihood of these threats. Implement specific controls tailored to the identified TTPs or IoCs, to reduce the likelihood and impact of relevant threats, thereby strengthening your overall security posture.

- **Use GreyMatter Digital Risk Protection (GMDRP):** Threat actors often buy credentials to gain initial access to, and a strong foothold in, the compromised environment. Use GMDRP to continuously monitor for compromised credentials posted on the dark web.

Please take a few minutes to complete the survey located here,
to provide feedback on the quality of the report.

Annex A: Research Methodology

This report is based solely on reporting that has aligned with the ReliaQuest Threat Research Team's intelligence requirements and thresholds, and additional open-source reporting; there may have been exposures and vulnerabilities falling outside these parameters that are not included.

Our sources were:

- hxxps://www.hhs[.]gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf
- hxxps://www.hhs[.]gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf
- hxxps://www.trendmicro[.]com/en_vn/research/23/h/an-overview-of-the-new-rhysida-ransomware.html
- hxxps://www.sentinelone[.]com/anthology/rhysida/
- hxxps://www.sentinelone[.]com/anthology/akira/