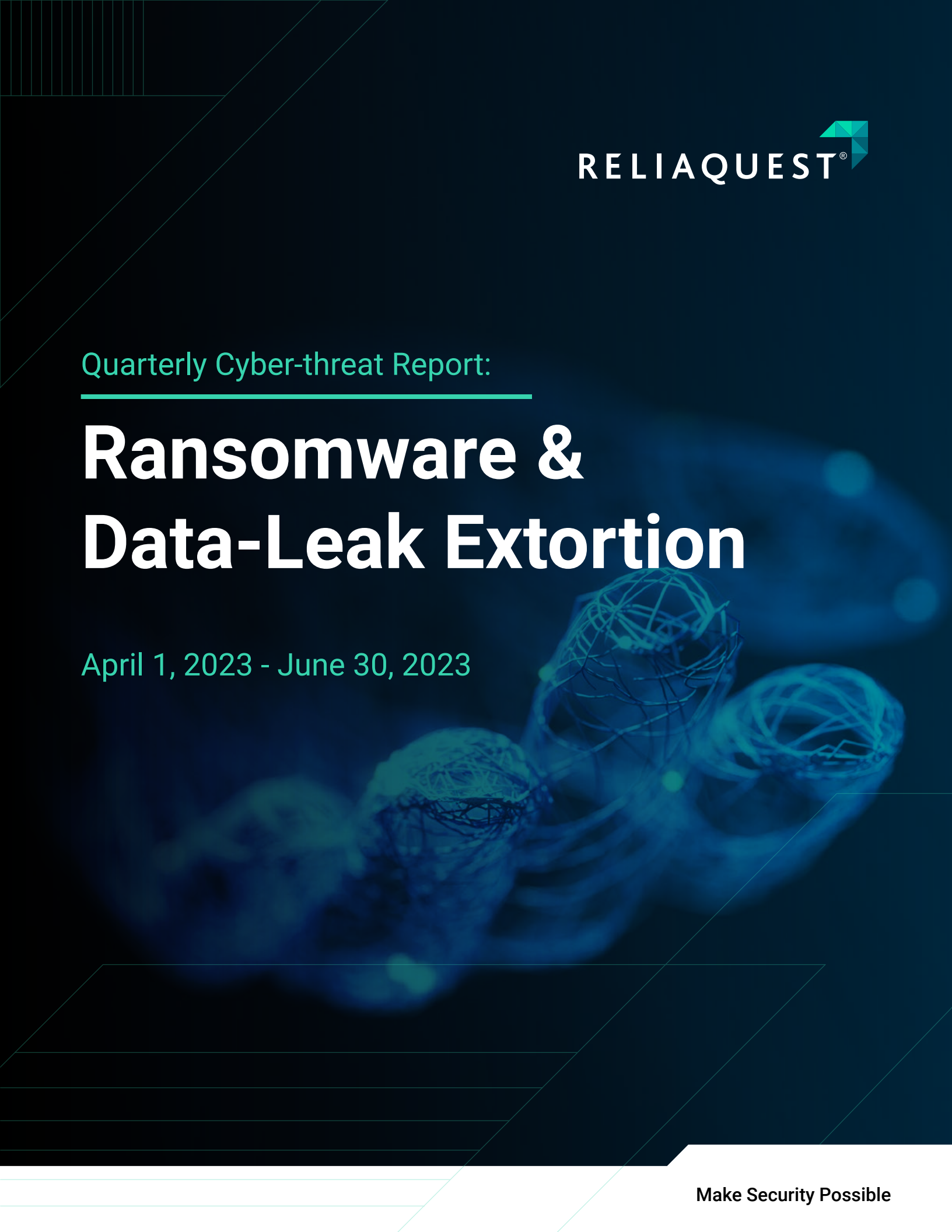
RELIAQUEST®

Quarterly Cyber-threat Report:

Ransomware & Data-Leak Extortion

April 1, 2023 - June 30, 2023



Make Security Possible

Table of Contents

Executive Summary 1

Q2 2023 Overview 2

Key Cyber Events 2

- Clop's MOVEit Campaign 2
- MalasLocker Targets Zimbra Servers 3

Ransomware and Extortion Metrics 3

Key Threats 5

- Clop 6
- LockBit 7
- ALPHV 8

Most Targeted Sectors 9

Most Affected Countries 10

Common MITRE ATT&CK Techniques 11

Detection Recommendations 11

- PSEXEC Pivoting 11
- PowerShell Obfuscated Script 12
- Default RDP Port Changed 12
- Shadow Copies Deleted 12

General Recommendations and Best Practices 13

Annex A: Research Methodology 14

Executive Summary

64.4%

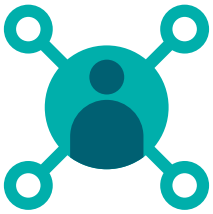
ReliaQuest's Threat Research Team observed 1,378 organizations named as victims on ransomware data-leak websites in the second quarter of 2023 (Q2 2023). This was a 64.4% increase from the record-breaking number of victims named in Q1 2023 (838 organizations).

49.4%

The US remained the most targeted country, representing 49.4% of all reported ransomware incidents, with the UK, Germany, Canada, and France following.

CL0P^_-LEAKS

This surge was linked to many new ransomware groups emerging and naming many victims, as well as a large-scale "Clop" ransomware supply-chain attack campaign. In addition, "LockBit" remained highly active, naming 246 victims.



The professional, scientific, and technical services sector emerged as the most targeted sector, affected by 20.2% of all reported attacks, and followed by manufacturing, finance and insurance, healthcare and social assistance, and construction.

MOVEit

In Q2 2023, Clop exploited a zero-day vulnerability in the MOVEit Transfer file transfer software, following its GoAnywhere exploitation attack. This new campaign allegedly led to hundreds of organizations being compromised. Clop named 89 victims on its data-leak site since June 14, 2023, likely all victims of the MOVEit exploitation.

Extortion-only attacks remained relatively few in Q2 2023, although there were 20 victims named on extortion-only data-leak sites: a notable increase from the 4-victim count in Q1 2023.

Q2 2023 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 Q2 2023. It describes the most impactful ransomware groups active in this quarter, and provides detection and mitigation guidance.

Key Observations of Q2 2023 Included:

- In Q2 2023, we observed yet another large surge in ransomware activity. This quarter once again set the record for the most victims ever recorded being named to ransomware data-leak sites. There was an increase of 540 victims compared to the previous quarter.

- May 2023 set a new record for the number of ransomware victims posted to data-leak sites, totaling 600 victims. This figure represented a 46.7% increase compared to the previous record observed in March 2023, where we reported 409 victims. Notable events in May 2023 included the ransomware group "Malas" naming 172 victims and the group "8Base" naming 69 victims.

- The most targeted countries were the US, UK, and Germany. The most targeted sectors were professional, scientific, and technical services, manufacturing, and finance and insurance. Targeting of the healthcare sector remained prevalent, with a 50.9% increase from the previous quarter.

Key Cyber Events

Clop's MOVEit Campaign

The most significant and impactful ransomware-related event in Q2 2023 was the exploitation of a zero-day vulnerability in the MOVEit Transfer software (CVE-2023-34362). On June 5, 2023, the Clop ransomware gang took responsibility for a series of cyber attacks exploiting this vulnerability. The group claimed to have stolen the data of hundreds of companies in the process.

Clop demanded that victims make contact to initiate ransom negotiations by June 14, 2023, or risk being named on the group's data-leak site, >_CLOP^_-LEAKS. This unique approach placed the responsibility on victims to determine whether they had been compromised and to begin negotiations.

Clop began gradually naming victims on June 14, 2023, with 89 organizations named by the end of June. The group continues to name new victims, making the victim count over 240 at the time of writing, and likely to continue in July and August.

This MOVEit campaign was the third time that Clop has exploited major vulnerabilities in enterprise managed file transfer (MFT) software for large-scale extortion:

- In February 2023, the group claimed responsibility for breaching more than 130 companies in just ten days, by exploiting a zero-day vulnerability in Fortra GoAnywhere MFT (CVE-2023-0669).

- In December 2020, Clop exploited zero-day vulnerabilities in Accellion's legacy file-transfer application (FTA) software, stealing data from more than 100 companies.

Uniquely, Clop did not deploy ransomware in these campaigns but instead focused on stealing data, efficiently targeting more than 100 companies in less than a week at one stage.

Clop will probably continue to exploit vulnerabilities in enterprise file transfer software. The group has demonstrated potential of such campaigns with its MOVEit breach, having extorted multiple companies whose revenue exceeds 1 billion dollars. Clop's success will likely inspire other ransomware groups.

MalasLocker Targets Zimbra Servers

A new ransomware gang, known as Malas, initiated attacks in March 2023 by encrypting the email messages of users with its "MalasLocker" ransomware and deploying a suspicious JSP file onto Zimbra servers. The ransomware note, named "README.txt," made an unconventional demand: Instead of asking victims for money, the group demanded donations to a nonprofit organization with Malas' approval. Malas promised to provide a decryptor and not leak data if victims made the donation.

In mid-May 2023, Malas launched a data-leak site on the dark web and immediately named and leaked the data of 169 victims. This large leak made Malas the second most-active ransomware group during Q2 2023. However, the group only exposed the configuration files of Zimbra servers belonging to victims, which likely created a low impact. In comparison, Clop placed fifth in terms of victim numbers in Q2 2023 but made the greatest impact with its MOVEit campaign and the breach of multiple large organizations.

Malas' motives and tactics diverge from those of typical ransomware groups. Its distinctive approach aligns more closely with hacktivism than traditional ransomware operations. Most hacktivist groups rely on distributed denial of service (DDoS) attacks to cause disruption and make statements; Malas demonstrated that ransomware can also be a potent tool for causing disruption and drawing attention to a cause.

Ransomware and Extortion Metrics

In Q2 2023, we observed 1,398 organizations named on the data-leak websites of ransomware and extortion gangs. This number was a substantial increase of 66% since Q1 2023, which saw 842 victims named. The number of ransomware attacks has more than doubled over the past two quarters, highlighting the growth and success of ransomware operations.

There was a 400% increase in the number of extortion-only attacks that posted victim names on data-leak sites; the perpetrators steal data and name victims but do not use encryption. The prevalence of such attacks was primarily attributed to the "Karakurt Hacking Team" extortion group, which had a relatively active quarter, claiming 19 victims. The spike in attacks was likely caused by natural deviations in quarterly numbers. While the number of attacks rose by 400%, the 20-victim count of Q2 2023 is still relatively low.

Although Clop's recent campaign could be considered to have included only extortion, we have classified Clop as a double-extortion ransomware group for its history of using the Clop ransomware to encrypt data. Only dedicated extortion-only groups were counted in Table 1 and Figure 1 as extortion groups.

> The number of ransomware attacks **has more than doubled** over the past two quarters, highlighting the growth and success of ransomware operations.

	Q1 2023	Q2 2023	% change
Victims named on ransomware data-leak sites	838	1,378	64.4
Victims named on extortion-only data-leak sites	4	20	400

Table 1: Victims named on data-leak sites of ransomware and extortion groups

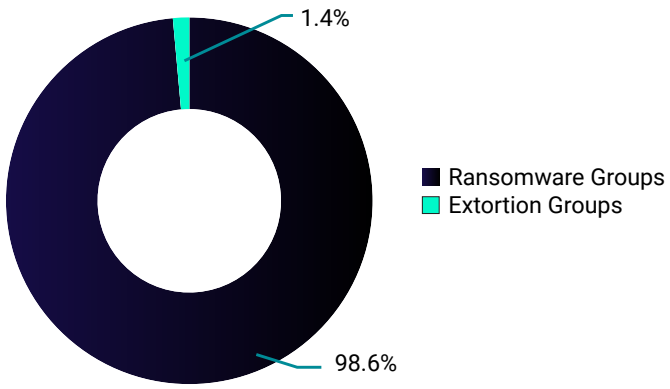


Figure 1: Types of data-leak activity

Q2 2023 marked another record-breaking quarter for double-extortion ransomware operators. The total number of ransomware victims surged by 64.4%. May became the most active month ever recorded, with 600 victims: a 46.7% increase over the previous record set in March 2023 (409).

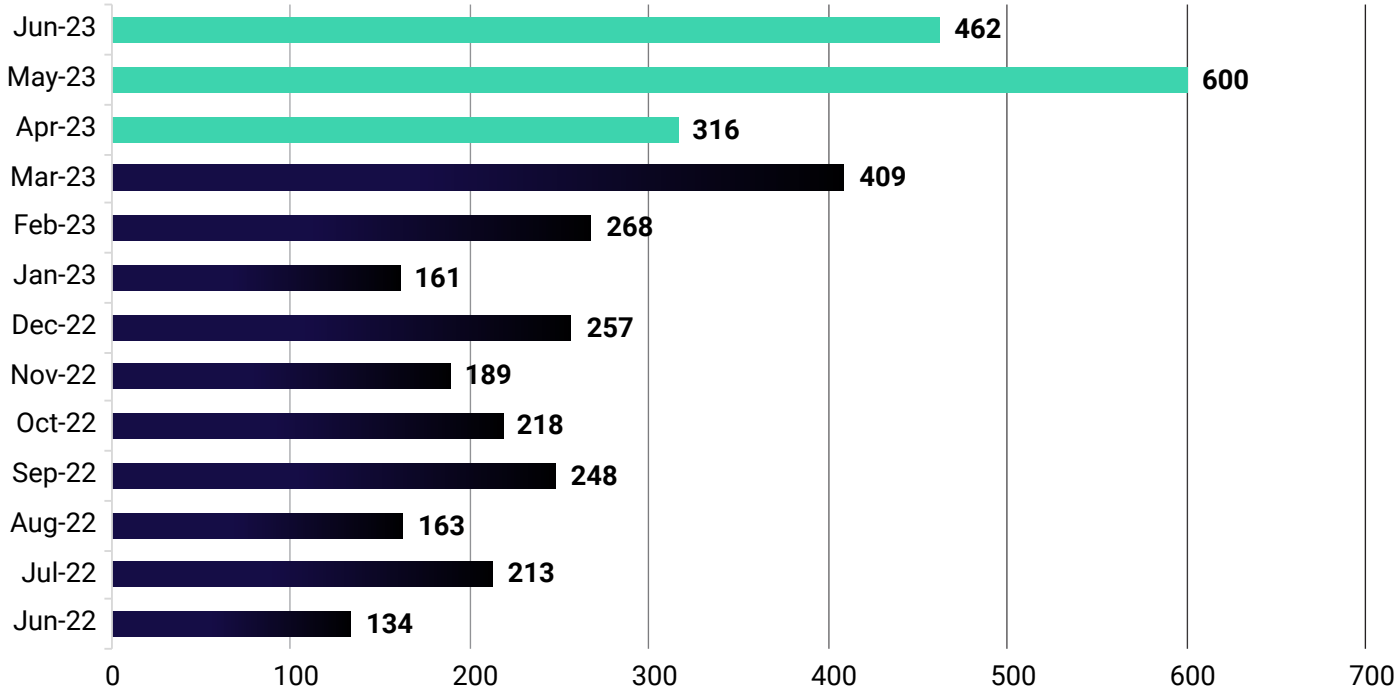


Figure 2: Number of ransomware victims named, by month, since June 2022

During Q2 2023, 43 ransomware groups named victims on their respective data-leak sites. ReliaQuest tracks the activity of these groups and records every victim posted on their data-leak sites, along with relevant details, such as the sector and location of each victim. The graph below shows the number of victims named on the 20 most-active data-leak sites.

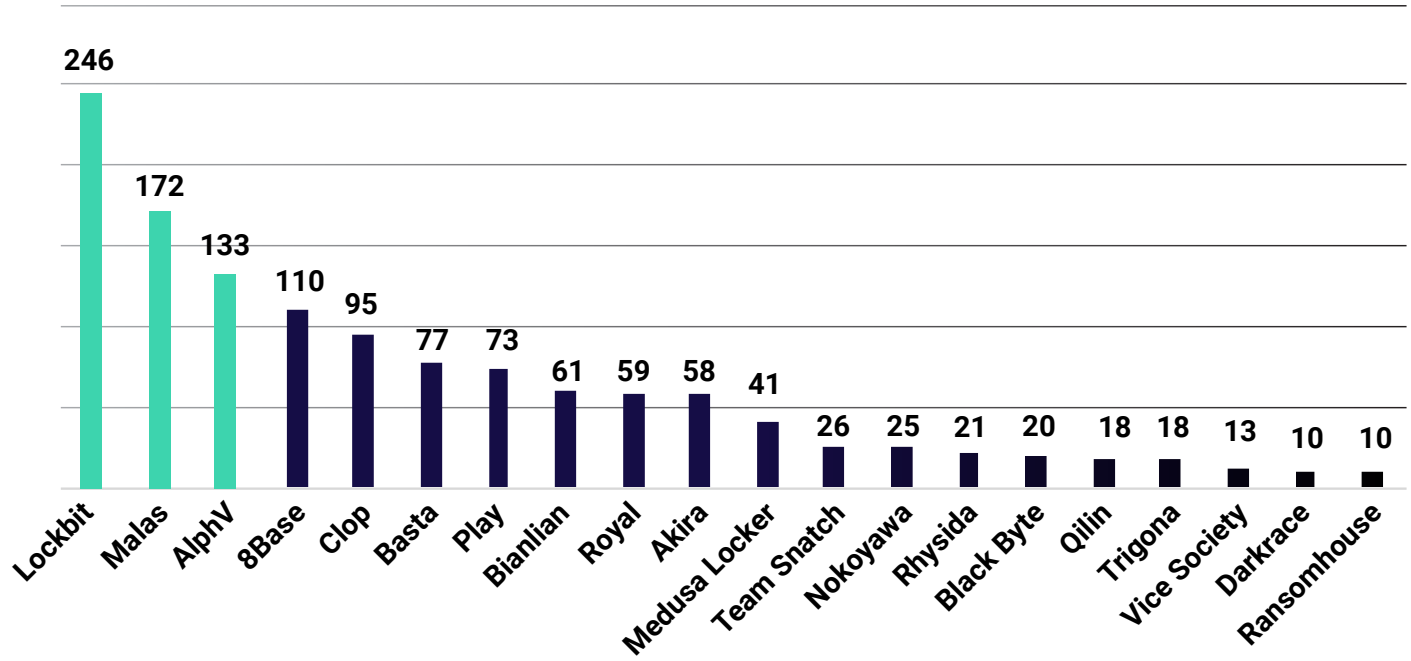


Figure 3: Number of victims named on top 20 ransomware data-leak sites

Key Threats

LockBit remained the most active ransomware group, by a significant margin. Two unexpected newcomers were also among the top five most active groups: Malas and "8Base" created data-leak sites and quickly gained attention by naming many victims at once. Those large victim counts probably include organizations the groups breached before the creation of their data-leak sites.

Clop ranked fifth in terms of victim numbers, but had the greatest impact with its breach of multiple billion-dollar organizations by exploiting the MOVEit vulnerability. Clop demonstrated that the impact of attacks and groups is influenced by a variety of factors, including not just victim numbers but the size of victims, nature of the data stolen, and broader threat posed to the security of organizations.

The following section of the report highlights the three most impactful ransomware groups active in Q2 2023. These segments will provide an overview of each group, detail their TTPs, and highlight notable events during the quarter.

CL0P^_-LEAKS

Clop Background

Clop is one of the oldest double-extortion ransomware groups active today; the group established CL0P^_- LEAKS in 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 deployed by a subgroup of the cybercrime group "FIN11" called TA505: the same group behind the "Dridex" banking trojan and the "Locky" ransomware.

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 remote-access trojan (RAT) "FlawedAmmyy" and the "SDBot" backdoor. Other malware and tools include "Truebot", Cobalt Strike, "DEWMODE," and "LEMURLOOT."

In deploying ransomware, Clop uses the AES (Advanced Encryption Standard) cipher to encrypt files and adds a ".Clop" (or similarly named) filename extension.

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

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, 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
Victims named on data-leak sites as of June 30, 2023: 371

Top 3 targeted sectors:
1) Professional, scientific, and technical services - 123
2) Manufacturing - 92
3) Finance and insurance - 68

Top 3 targeted regions:
1) US - 243
2) Canada - 34
3) Germany - 25

Victims named in Q2 2023: 95

In Q2 2023, 61.1% of Clop victims were based in the US, and 17.9% were in Germany, Canada and France.

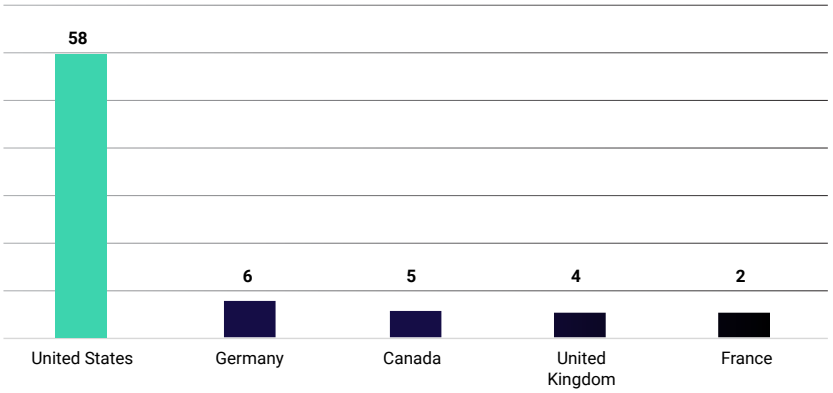


Figure 4: Countries targeted most by Clop in Q2 2023

The sector Clop targeted the most in Q2 2023 was finance and insurance, accounting for 30.5% of victims. The professional, scientific, and technical services sector followed closely, with 27.4% of victims.

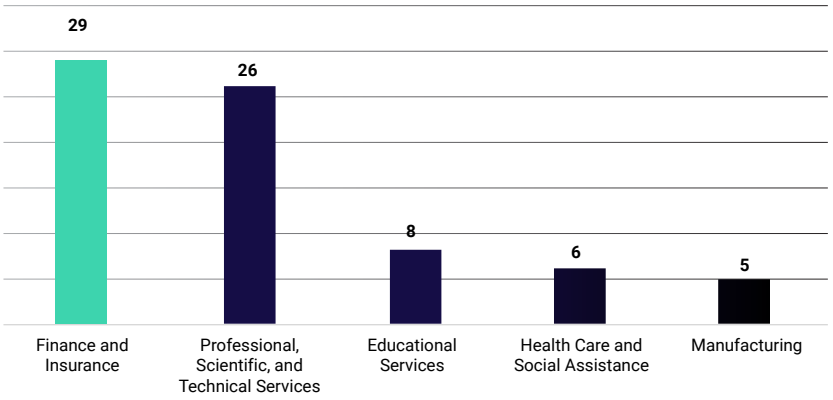


Figure 5: Sectors targeted most by Clop in Q2 2023

Notable developments/events in 2023:

- In June 2023, Clop exploited a zero-day vulnerability in the MOVEit Transfer software (CVE-2023-34362) to breach hundreds of companies.
- In February 2023, Clop claimed responsibility for more than 130 attacks exploiting a zero-day vulnerability in the GoAnywhere MFT (CVE-2023-0669).
- In February 2023, the first Linux-targeting Clop variant was reported. A flaw in its encryption allowed researchers to publish a decryption key.

LockBit Background

LockBit's ransomware is formerly known as "ABCD" because of the ".abcd virus" extension used in early deployments.

The LockBit group operates a ransomware-as-a-service (RaaS) model, whereby affiliates make a deposit to use the tool for custom attacks, then split at least 25% of the ransom payout with LockBit .

LockBit does not collaborate with English speakers and it prohibits the targeting of Russia or any CIS countries.

The group practices double extortion, exfiltrating data before encryption and threatening to publish the victim's data on its data-leak website, LockBit Blog, if ransom demands are not met.

LockBit TTPs

LockBit affiliates use the "LockBit 3.0" ransomware (aka LockBit Black), which was released in June 2022.

Initial attack methods include performing social engineering; exploiting public-facing applications; conducting drive-by compromise[1] ; hiring IABs; using stolen credentials to access valid accounts, such as remote desktop protocol (RDP) accounts; and conducting brute-force attacks targeting administrator accounts.

LockBit 3.0 delivers a ransom note named <Ransomware ID>.README.txt and changes the victim's device wallpaper and icons to the LockBit 3.0 logo.

To exfiltrate data, LockBit affiliates use an information stealer and exfiltration tool named StealBit, a cloud-storage manager named rclone, and public file-sharing services, such as Mega[.]nz.

The group weaponizes legitimate Living off the Land binaries and scripts (LOLBAS), and uses such tools as "Process Hacker", PowerShell, and "PC Hunter."

LockBit is known to delete log files and shadow volume copies to complicate recovery.

LockBit has a timer on its data-leak site, indicating when victims' data will be exposed. The group often provides options to delete or download the data. Once the timer runs out, data is leaked, sometimes using public file-sharing sites, such as sendbig[.]com.

Active since: September 2019
Victims named on data-leak sites as of June 30, 2023: 1,796

Top 3 targeted sectors:
1) Manufacturing - 555
2) Professional, scientific, and technical services - 351
3) Construction - 161

Top 3 targeted regions:
1) US - 602
2) France - 101
3) Italy - 90

Victims named in Q2 2023: 246

The US accounted for 37.8% of all LockBit's victims in Q2 2023, followed by France, Canada, Germany and Italy with 15% in total.

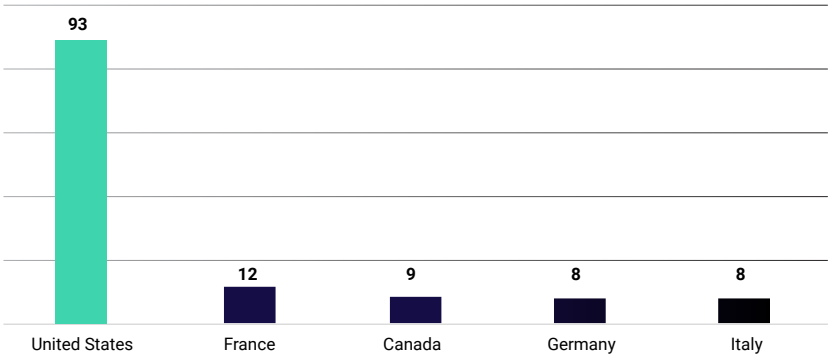


Figure 6: Countries targeted most by LockBit in Q2 2023

In this quarter, LockBIt's most-targeted sector was manufacturing, accounting for 22.4% of all LockBit victims, and the next most-targeted sectors accounted for 39.8% of victims.

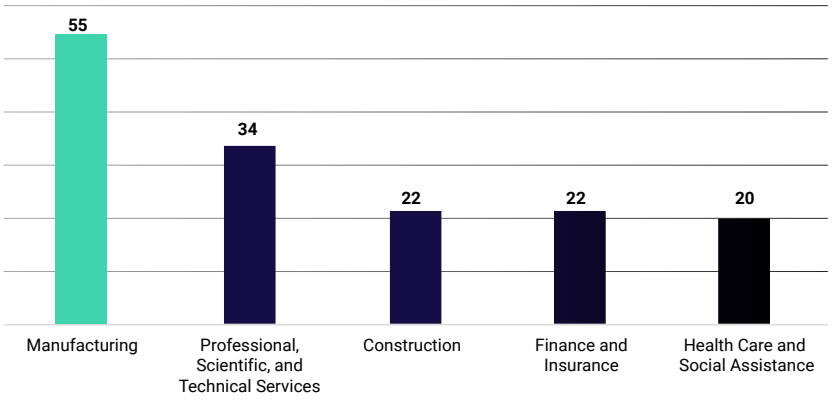


Figure 7: Sectors targeted most by LockBit in Q2 2023

Notable developments/events in 2023:

- In February 2023, LockBit released a new version of its ransomware, named LockBit Green, which is designed to target cloud-based services.
- In April 2023, new samples of ransomware that target Mac operating systems from the LockBit gang were discovered.
- In April 2023, LockBit was reportedly delivered using the "SocGholish" malware loader, dropping "BLISTER" as a second-stage loader.

[1] These are attacks where users visit websites infected by threat actors, which are aimed to target vulnerable web browsers.

ALPHV

ALPHV Background

"ALPHV" is the first ransomware group known to successfully use Rust programming language-based ransomware.

The group operates a RaaS model and affiliates typically make between 80% to 90% of the final ransom amount.

The group has claimed to not attack medical institutions, ambulances, or hospitals. That rule does not apply to private clinics and pharmaceutical companies.

ALPHV is associated with two other ransomware groups—"DarkSide" and "BlackMatter"—owing to design overlaps.

ALPHV TTPs

The group has been known to practice triple extortion, which includes ransomware, data theft and extortion, and DDoS attacks.

ALPHV uses the AES and ChaCha20 encryption algorithm and is reportedly capable of targeting many operating systems, including Windows, ESXi, Debian, Ubuntu, Synology, and ReadyNAS.

To gain initial access, the group has exploited vulnerabilities, abused compromised passwords, or relied on IABs.

ALPHV has been observed using additional tools, like WebBrowserPassView, Cobalt Strike, AdRecon, PsExec, Nirsoft, "Emotet," "Mimikatz," and "LaZagne" to obtain passwords, gain initial access, and/or escalate privileges.

ALPHV often uses PowerShell scripts and Cobalt Strike in its initial deployment, plus Windows administrator tools and Sysinternals during compromise.

ALPHV exfiltrates data using a customized tool named Fendr (aka ExMatter), which was previously used by BlackMatter and the "Conti" ransomware groups.

ALPHV is known to share images of sensitive documents, such as passports, on its data leak site to pressure victims. The group has been known to leak files using file sharing sites such as sendspace[.]com and dropmefiles[.]com, as well as its own dark web data-leak site.

Active since: November 2021
Victims named on data-leak sites as of June 30, 2023: 466

Top 3 targeted sectors:
1) Manufacturing - 140
2) Professional, scientific, and technical services - 105
3) Finance and insurance- 47

Top 3 targeted regions:
1) US - 239
2) Canada - 19
3) Australia - 18

Victims named in Q2 2023: 133

ALPHV primarily targets organizations in the US, accounting for 53.4% of all its victims in Q2 2023. Canada, France, Australia and Brazil represented 11.3% of all ALPHV victims.

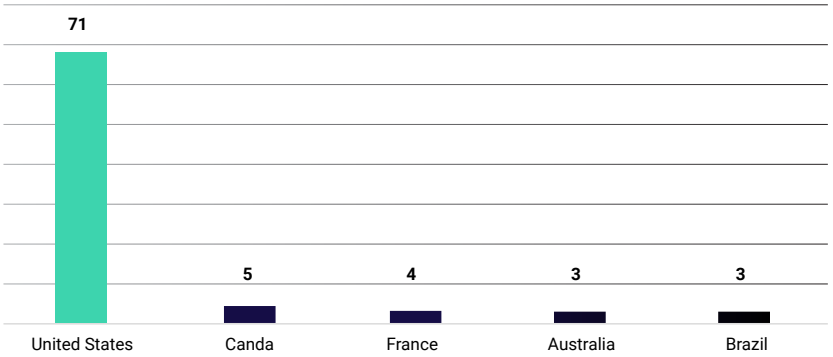


Figure 8: Countries targeted most by ALPHV in Q2 2023

ALPHV's targeting covered several sectors; the top five represented 70% of all victims. Professional, scientific, and technical services was targeted the most, with 21.1% of incidents. Healthcare and social assistance made it into the top five, despite ALPHV's rule against targeting medical organizations.

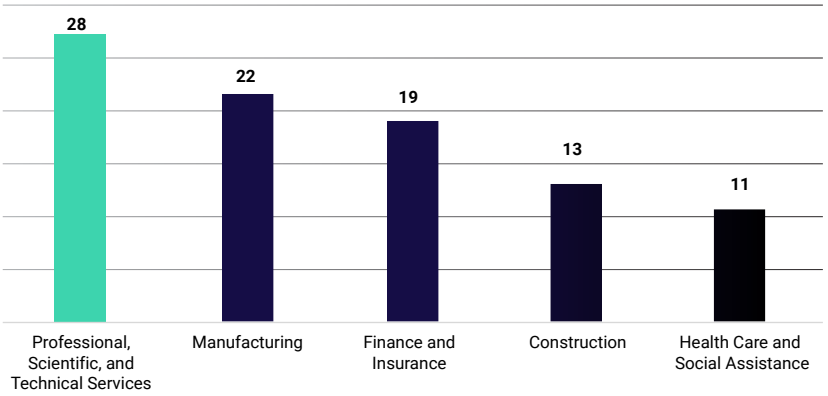


Figure 9: Sectors targeted most by ALPHV in Q2 2023

Notable developments/events in 2023:

- In June 2023, ALPHV claimed to have stolen 7TB of data from a healthcare company in the UK and called it the largest "leak from [a] healthcare system in the UK."
- On May 22, 2023, ALPHV began using malicious signed Windows kernel drivers, including "POORTRY," during attacks to terminate security applications.
- In January 2023, ALPHV used a novel tactic to leak the data that it had stolen from a victim. ALPHV created a clear-website that was a replica of the victim's legitimate domain.

Most Targeted Sectors

Figure 10 shows the sectors targeted most by ransomware groups in Q2 2023. The professional, scientific, and technical services sector was the top target, accounting for 20.2% of all victims. The manufacturing sector closely followed, with 19.6% of victims. The remaining sectors in the top five were finance and insurance, healthcare and social assistance, and construction.

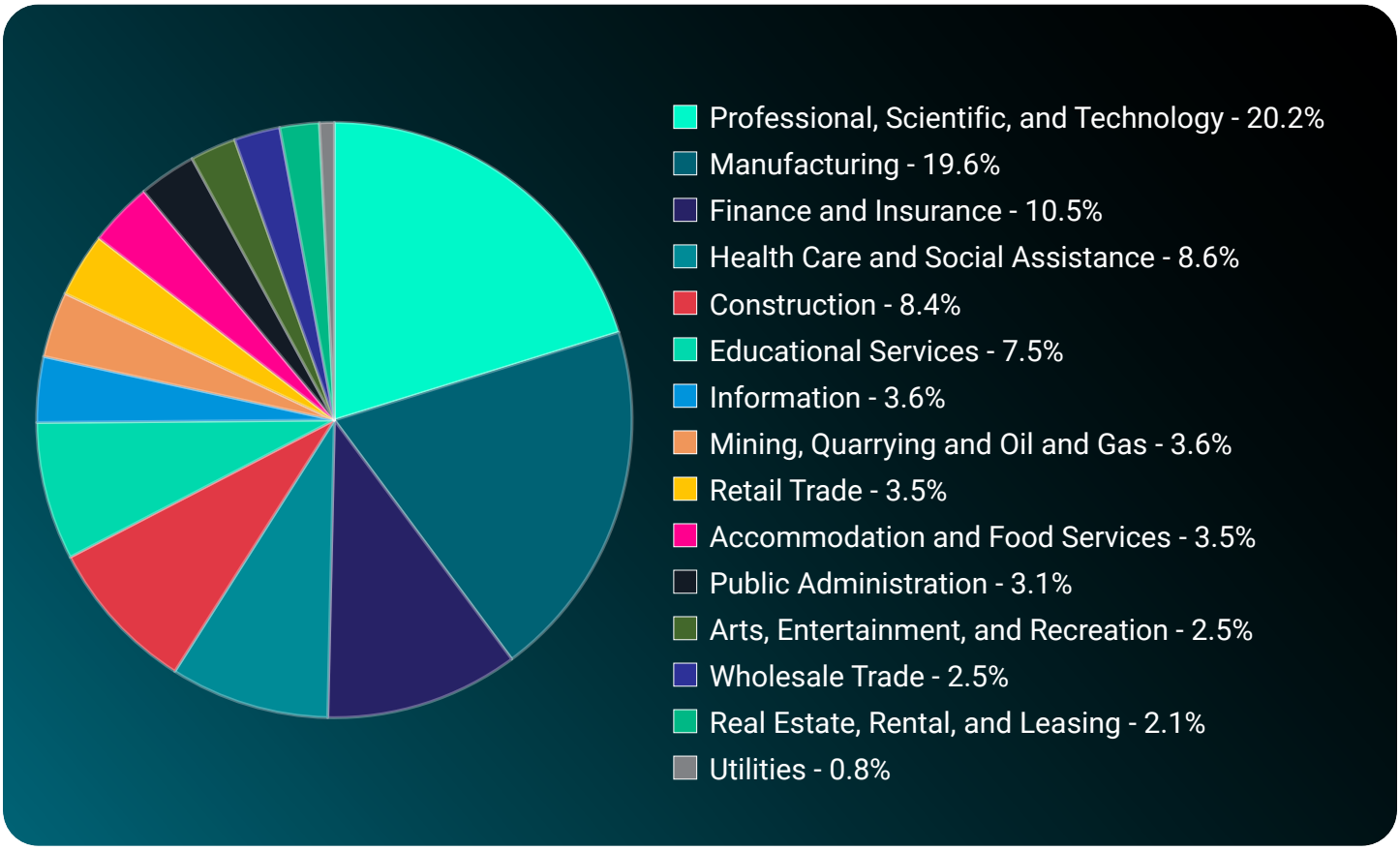


Figure 10: Most-targeted sectors by ransomware groups

In previous quarters, the manufacturing sector was overwhelmingly targeted the most, but it has moved to second position as ransomware groups focused heavily on organizations that provide services to other companies. Professional, scientific, or technical services entities often store the data of multiple clients, making them attractive targets for ransomware. Breaching even one such company can lead to the exposure of numerous clients' data, amplifying the impact. The professional, scientific, and technical services sector will likely continue to be a prominent target.

Healthcare remained a popular target, despite many ransomware groups claiming to avoid targeting that sector; this trend has persisted since Q1 2023. In Q2 2023, 86 healthcare organizations were named on ransomware data-leak sites: a 50.9% increase since the previous quarter.

> Professional, scientific, or technical services entities often **store the data of multiple clients**, making them attractive targets for ransomware.

Most Affected Countries

Figure 11 shows the ten countries targeted most by ransomware groups in Q2 2023. The US took the lead by a wide margin, representing an elevated threat to entities there. The number of victims in the US rose by 47.6% from Q1 2023, when 382 US organizations were named on ransomware data-leak sites.

Following the US were the UK, Germany, Canada, and France. The UK remained in second place, but with five fewer victims in Q2 2023. The other countries demonstrated slight shifts, as commonly seen with quarterly metrics.

The appeal of US targets is likely driven by the presence of numerous wealthy organizations and the **success of ransomware groups in securing payments** from US victims.

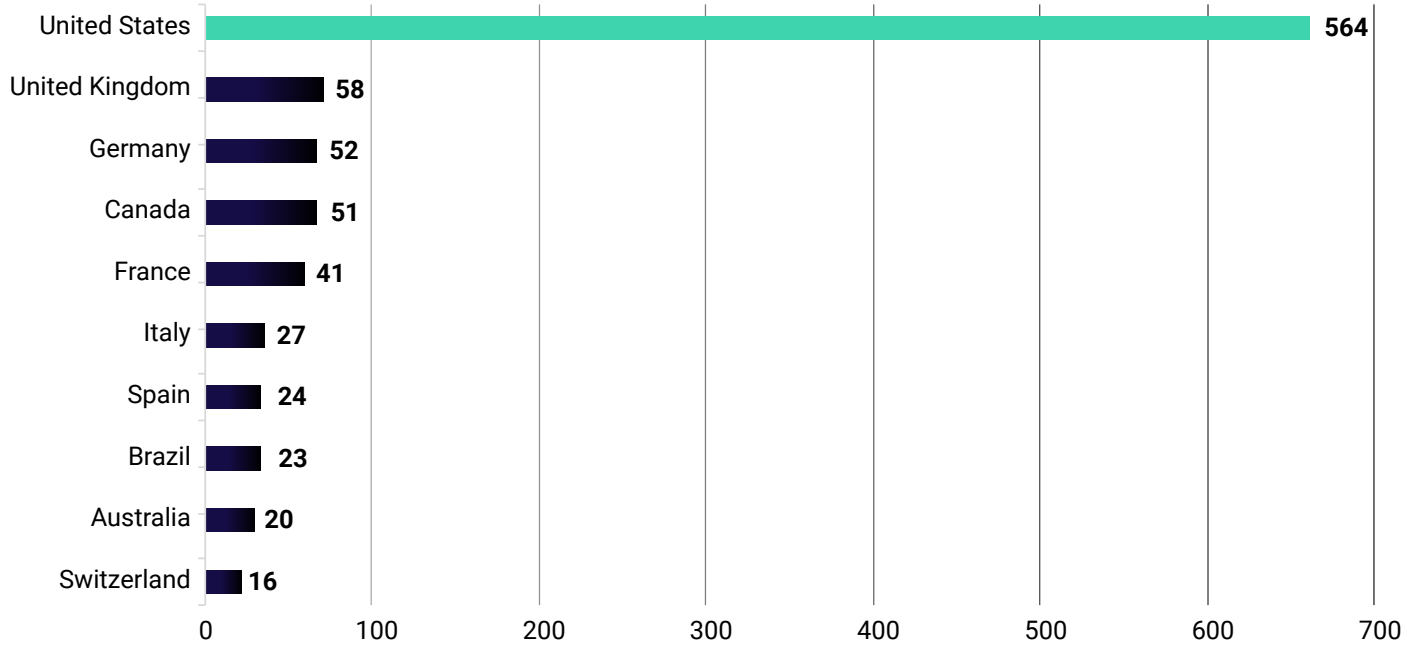


Figure 11: Top ten countries most targeted by ransomware groups

The appeal of US targets is likely driven by the presence of numerous wealthy organizations and the success of ransomware groups in securing payments from US victims. Targeting of other countries is typically opportunistic, depending on a victim's size, revenue, and brand recognition, among other factors. Ransomware groups tend to prioritize targets with large organizational structures and high revenue. This "big game hunting" enables threat actors to maximize financial gain and reputational impact.

No organizations in Russia or the greater CIS region were named on ransomware data-leak sites during Q2 2023. Typically, ransomware groups prohibit the targeting of countries operating within that region to avoid the scrutiny of Russian law-enforcement agencies. This strategic avoidance helps maintain the operational security of ransomware groups and will likely continue.

Common MITRE ATT&CK Techniques

We analyzed the techniques of top ransomware groups as classified by the MITRE ATT&CK framework, to determine commonalities and provide insight into TTPs. However, many large ransomware groups work in 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 top ransomware groups are:

- Command and Scripting Interpreter: Windows Command Shell (T1059.003)
- Ingress Tool Transfer (T1105)
- External Remote Services (T1133)
- Impair Defenses: Disable or Modify Tools (T1562.001)
- Data Encrypted for Impact (T1486)
- Windows Management Instrumentation (T1047)
- Exploit Public-Facing Application (T1190)

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. Valuable detection use cases require endpoint logging or visibility; visibility limitations should be proactively addressed rather than in response to a breach. Clients should review GreyMatter Detect to identify areas for room 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 customer environments.

PSEXEC Pivoting

Remote-administration tools, such as PsExec, are programs that allow users to connect to and remotely execute processes on other systems. An attacker can 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. Attackers often use PsExec to pivot throughout environments because of the tool's versatility and signed status. Programs executed on remote systems connected via PsExec run under the PsExecSvc process.

Relevant MITRE ATT&CK techniques:

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

PowerShell Obfuscated Script

Attackers attempt to obfuscate their PowerShell scripts to avoid detection from signature-based monitoring tools. One method is to insert escape characters between every other character in the function calls; PowerShell interprets the script in the same way while the actual string text triggers an alert, which hinders pattern matching. Detecting the use of escape characters within PowerShell commands may indicate potentially malicious obfuscated commands.

Relevant MITRE ATT&CK techniques:

- T1059.001 - PowerShell
- T1027.010 - Command Obfuscation

Default RDP Port Changed

RDP enables remote connections to other computers in a network, typically using TCP Port 3389. The Conti ransomware group has used the technique of changing the RDP listening port, allowing incoming RDP connections on an uncommon port to evade defenses. Look for any changes to the listening port number through a change to the registry.

Relevant MITRE ATT&CK technique:

- T1021.001 - Remote Desktop Protocol

Shadow Copies Deleted

Ransomware's deletion of all shadow volume copies is common; the program encrypts the host and deletes backups to remove the possibility of restoring the computer and avoiding a ransom payment. Monitor for the deletion of all shadow volume copies on a Windows host through the command line.

Relevant MITRE ATT&CK techniques:

- T1059.003 - Windows Command Shell
- T1070.004 - File Deletion
- T1490 - Inhibit System Recovery

General Recommendations and Best Practices

Network

- Disable Server Message Block (SMB): Because attackers use SMB to propagate malware and move laterally through networks, disable SMB V1 and V2 and upgrade to version 3. In addition, harden SMB by limiting or blocking traffic to systems.
- Disable unnecessary RDP: Remote desktops and similar services, often left exposed, can be used for initial attack access. Audit for the use of these services, ensure proper configuration, and log RDP login attempts.
- 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: Remove any accidental exposure and patch any out-of-date services, prioritizing services that have known vulnerabilities. Threat actors frequently scan the internet for public-facing assets that have an exploitable vulnerability, to gain initial access.

Internal System

- 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 for implementation.
- 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: Valuable detection use cases require endpoint logging or visibility. Enable coverage for antivirus (AV) or endpoint detection and response (EDR) tools within your environment for maximum visibility of exploit or threat activity.
- Use automatic updates: Use the software update feature on your computer, and mobile or other connected devices, wherever possible and pragmatic.

Threat Actor Tracking

- Use threat intelligence: A threat intelligence platform can provide valuable insights by identifying indicators of compromise (IoCs) and TTPs. Use it to determine what tools will enhance preparedness and defenses.
- Use GreyMatter Digital Risk Protection (GMDRP): Threat actors often buy credentials for initial target access and a strong foothold in the compromised environment. Use GMDRP for continuous monitoring for compromised credentials posted on the dark web.
- Stay up to date: Remain informed about the latest cyber news and understand the current cybercrime landscape, trends, and potential threats to your specific sector or country, to proactively prepare for upcoming attacks.

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:

- ReliaQuest's primary-source intelligence
- hxxps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-165a
- hxxps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-158a
- hxxps://www.bleepingcomputer[.]com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/