RELIAQUEST®

Quarterly Cyber-threat Report:

Ransomware & Data-Leak Extortion

April 2023

Make Security Possible

Table of Contents

Executive Summary

- In the first quarter of 2023 (Q1 2023), the ReliaQuest Threat Research Team observed 838 organizations falling victim to ransomware attacks and being named on dark-web data-leak sites. This is a 29.9% increase from the previous quarter.
- Q1 2023 was the most active quarter we have ever observed for ransomware since the start of double extortion in 2020. This rise was primarily driven by the most active month ever recorded for ransomware double extortion. In March 2023, 409 organizations were named on ransomware data-leak sites; this is 35% higher than the previous record of 303.
- High activity in March 2023 stemmed from a large-scale supply-chain attack by the "Clop" ransomware gang. Clop exploited a zero-day vulnerability in GoAnywhere managed file transfer (MFT), allegedly leading to the compromise of more than 130 organizations.
- The United States remained the country most targeted by ransomware groups, by a wide margin, making up 45.6% of all reported attacks. The United Kingdom, Canada, France, and Germany made up the remaining top five most-targeted countries.
- Ransomware groups focused on the industrial and manufacturing sectors, which accounted for 21.1% of all reported attacks. Technology was the second most-targeted sector, followed by construction and materials, healthcare, and education, respectively.
- Despite the rise in ransomware activity, we observed a 90.7% decrease in extortion-only attacks. This shift demonstrates that threat actors placed a high focus on ransomware and double extortion in Q1 2023.

Q1 2023 Overview

ReliaQuest's Threat Research Team monitors the activity of ransomware groups on the dark web and keeps track of all victims named on ransomware data-leak websites. We also keep track of major developments and trends in the ransomware-threat landscape. This report looks at the most important ransomware-related events during Q1 2023: key events, metrics of ransomware groups, and what steps organizations can take to protect themselves from these threats.

Noteworthy Q1 2023 observations included:

- An alarming surge in ransomware activity over the past few months: Q1 2023 set the record for being the quarter with the most ransomware victims ever recorded since the start of double extortion; 838 organizations were named on ransomware data-leak sites.
- A large-scale supply-chain attack by the Clop ransomware gang drove this rise in activity: In February, Clop claimed to have breached more than 130 organizations by exploiting a GoAnywhere MFT zero-day vulnerability (CVE-2023-0669). Clop listed 99 victims on its data-leak site in March 2023, likely linked to the GoAnywhere campaign.
- The US, UK, and Canada were targeted the most, and the top sectors were industrial-goods-and-services, technology, and healthcare: The number of victims in the healthcare sector was the highest ever recorded in a quarter since 2020.

Key Events

Clop exploited a GoAnywhere MFT zero-day vulnerability (CVE-2023-0669) in an attack campaign that resulted in more than 130 organizations being breached. This was not Clop's first large-scale supply-chain attack. In February 2021, Clop exploited an Accellion file transfer application (FTA) zero-day vulnerability to breach 100-plus organizations. There were many similarities between the two campaigns. Both exploited zero-day vulnerabilities in file-transfer platforms, and in both campaigns, Clop simply chose to steal data from victims and not drop ransomware. By skipping encryption, Clop was able to conduct the attacks at lightning speeds; reportedly, it took Clop only ten days to steal data from the 130 organizations using GoAnywhere MFT.

The Clop ransomware group has been active since February 2019 and has undergone many challenges, such as when Ukrainian affiliates were arrested in June 2021, and some of its infrastructure was shut down by law-enforcement officials. Many ransomware groups will cease operations after arrests or interference from law- enforcement bodies; however, Clop remained operational, and is now one of the oldest active ransomware groups practicing double extortion.

By skipping encryption, Clop was able to conduct these attacks at lightning speeds; reportedly **it took Clop only 10 days to steal the data from the 130 organizations** using GoAnywhere MFT.

Another important story this quarter was the FBI's seizure of servers of the Hive ransomware gang. On January 26, 2023, the US Department of Justice announced a months-long disruption campaign targeting Hive. The FBI reportedly infiltrated the group's infrastructure in late-July 2022, accessing decryption keys and preventing the payment of a $130 million ransom demanded by Hive. US and international law-enforcement officials also confiscated the servers of Hive's dark-web and internal sites. The servers were allegedly accessed through search warrants targeting email addresses associated with Hive members.

The seizure of Hive was a significant event, demonstrating the danger of ransomware groups remaining active for long periods. Hive first appeared in June 2021, and named more than 200 victims on its data-leak site before being shut down.

Ransomware and Extortion

We observed 842 organizations being named on ransomware and data-extortion websites on the dark web. This was a 22.4% increase compared to the previous quarter, where the total number was 688. While there was a noticeable increase in the number of ransomware attacks, we observed a large decrease in the number of extortion-only attacks (i.e., threat groups that steal data and use data-leak sites but do not encrypt files.) Activity by extortion-only groups decreased by 90.7% during the past quarter, likely due to the extortion group "Karakurt" having a quiet quarter.

	Q4 2022	Q1 2023	Change %
Victims in Ransomware Data-Leak Sites	645	838	29.9
Victims in Extortion Data-Leak Sites	43	4	-90.7

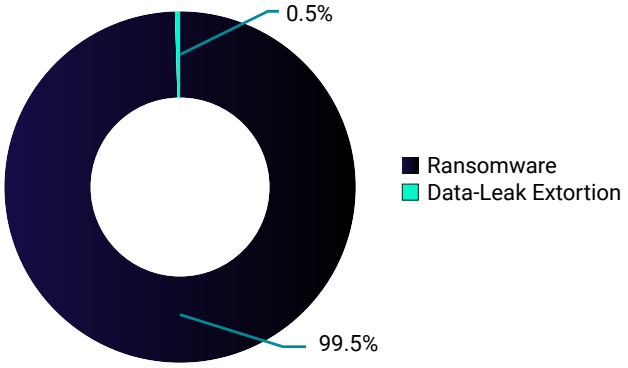

Figure 1: Breakdown of data-leak activity in Q1 2023

The numbers we analyzed in Q1 2023 were noticeably higher than in any other quarter we have observed previously. March 2023 has set the record for the most active month we have ever recorded in the history of double extortion ransomware. In March alone, there were more than 409 organizations named on ransomware data-leak sites, which is 35% higher than the previous record in April 2022.

March 2023 has **set the record for the most active month** we have ever recorded in the history of double extortion ransomware.

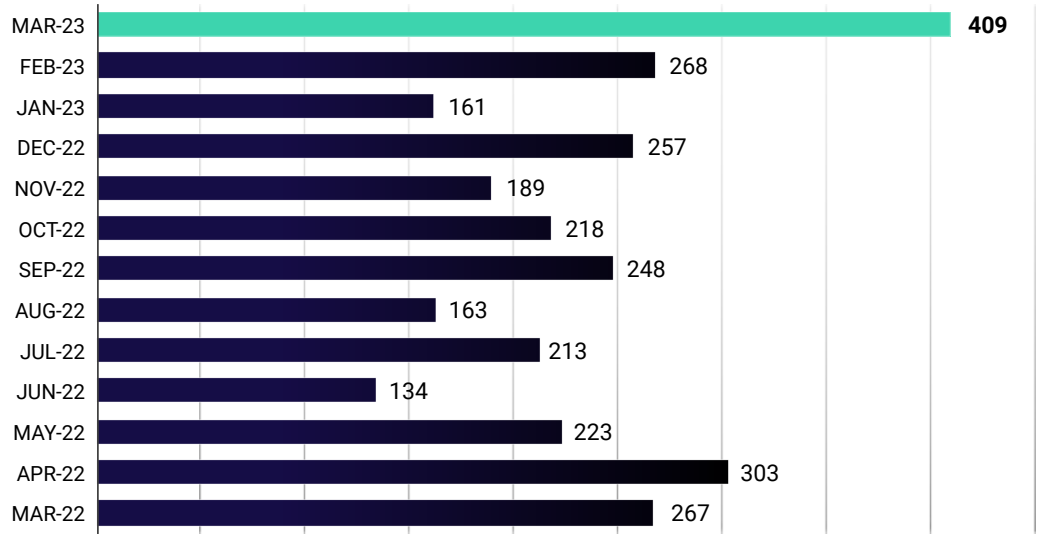

Figure 2: Ransomware activity by month since March 2022

The Threat Research Team monitors 109 ransomware data-leak sites daily; 46 are active at the time of writing. It is common for data-leak sites to become inactive within a few months of being opened. The graph below shows the number of victims named on ransomware data-leak sites throughout Q1 2023. Hive was shut down in late-January 2023, although the group was still able to target four victims before this seizure.

The most active group remained "LockBit" by a wide margin. "Clop" and "ALPHV" were the next most active ransomware groups. Most of Clop's activity occurred in March 2023, when the group leaked 99 victims on its data-leak site ">_CLOP^_-LEAKS". Clop's large wave of victims was likely associated with the exploitation of the GoAnywhere vulnerability in February 2023.

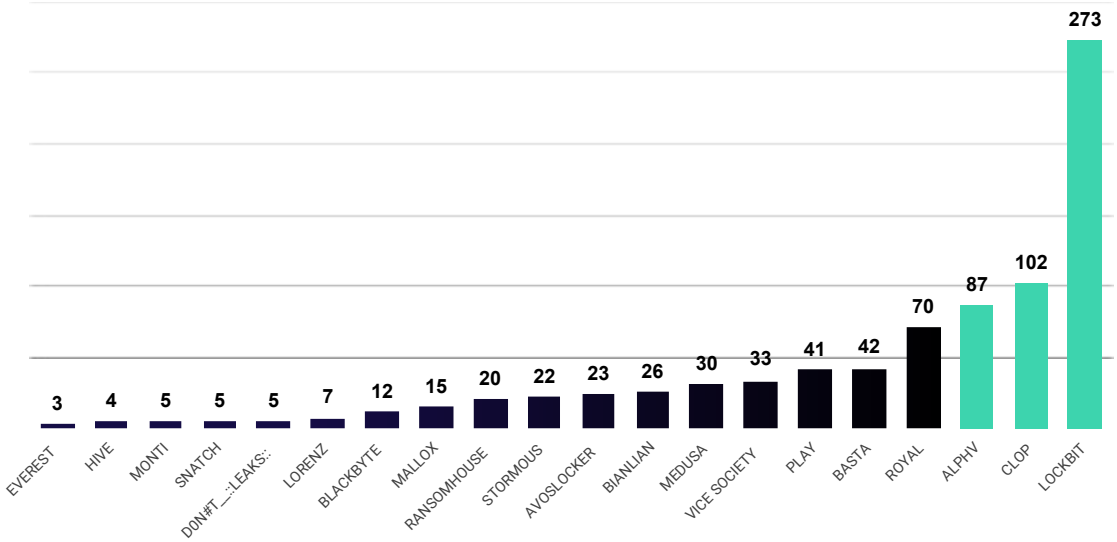

Figure 3: Number of victims named on top 20 ransomware data-leak sites, Q1 2023

The remainder of this report will focus on the three most active ransomware groups during this quarter, plus provide insight into the general ransomware-threat landscape.

LockBit

LockBit Ransomware Background:

- "LockBit" was first discovered in September 2019.
- LockBit was previously known as "ABCD" ransomware because of the ".abcd virus" extension when it was first observed.
- It operates as ransomware-as-a-service (RaaS), whereby affiliates are given access to the LockBit tool in exchange for a percentage of ransom payments (at least 25%).
    - As the tool is operated by affiliates, the tactics, techniques, and procedures (TTPs) often vary in LockBit attacks.
- LockBit operators do not work with English speakers and prohibit the targeting of Russia or any Commonwealth of Independent States (CIS) countries.

LockBit TTPs:

- LockBit affiliates use the "LockBit 3.0" ransomware (aka LockBit Black), which was released in June 2022.
    - LockBit 3.0 encrypts files saved to any local or remote device, but it skips any files that are associated with core system functionality.
    - LockBit 3.0 drops a ransom note with the filename "<Ransomware ID>.README.txt" and changes the victim's wallpaper and icons to the LockBit 3.0 logo.
- To exfiltrate data, LockBit affiliates use an information stealer and exfiltration tool known as "StealBit," a cloud-storage manager named "rclone," and public file-sharing services such as Mega[.]nz.
- Initial attack methods include social engineering, exploiting public-facing applications, drive-by compromise, hiring initial access brokers (IABs), and using stolen credentials to access valid accounts, such as remote desktop protocol (RDP), as well as brute-force cracking attacks.
- LockBit is known to delete log files and shadow copies to make recovery harder.
- The group weaponizes legitimate Living Off the Land Binaries and Scripts (LOLBAS) and uses tools such as Process Hacker, PowerShell, and PC Hunter.

LockBit 3.0 Ransom Note Snippet

~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Figure 4: A LockBit ransom note example

Victimology:

- The group targets a wide variety of sectors, but most of its victims were in industrial goods and services, construction and materials, and technology.
- LockBit practices a technique commonly referred to as big game hunting— focusing on a small number of high-value targets to maximize profit.
- The majority of LockBit victims are US organizations. North American and European organizations face a high threat from the group.
- LockBit's operators do not target any victims in Russia or other CIS countries.

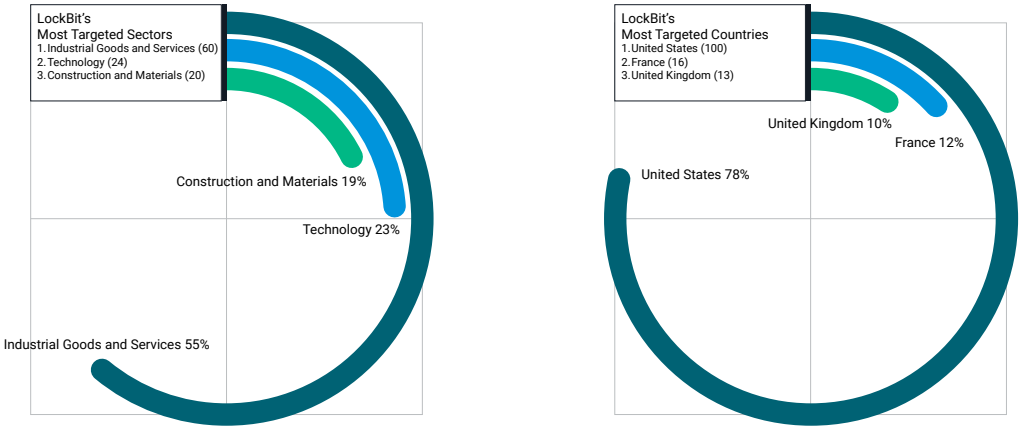

Figure 5: Breakdown of the top 3 sectors and geographies targeted by LockBit in Q1 2023
~~~

LockBit in Q1 2023:

- The United States was the most-targeted location by a wide margin, accounting for 36.6% of all LockBit's attacks.
- France, the UK, Canada, and India combined made up 19.1% of LockBit victims in Q1 2023.

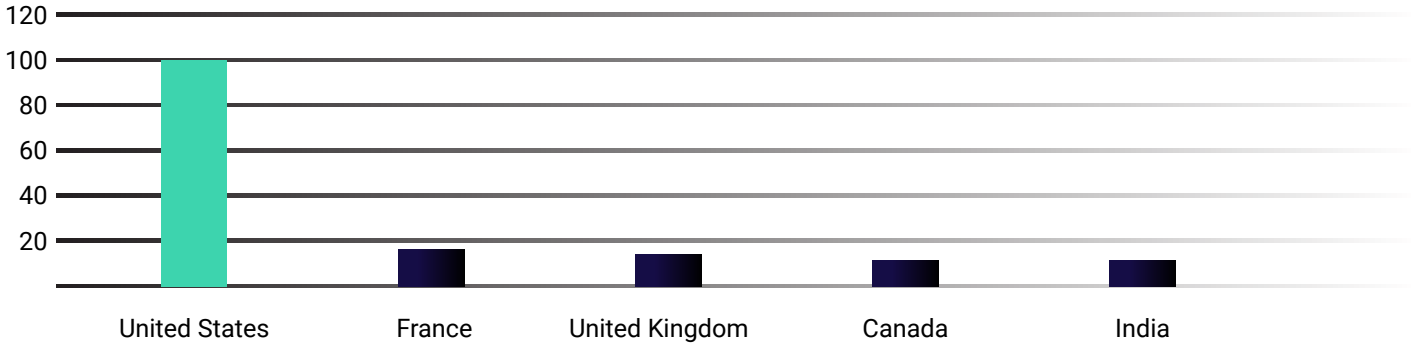

Figure 6: Most targeted countries by LockBit in Q1 2023

- The most-targeted sector was industrial goods and services, accounting for 22% of all LockBit's victims.
- Technology, construction and materials, healthcare, and financial services made up 27.8% of LockBit events combined.
    - The targeting of healthcare is interesting because LockBit previously claimed to not attack healthcare, educational, and charity organizations

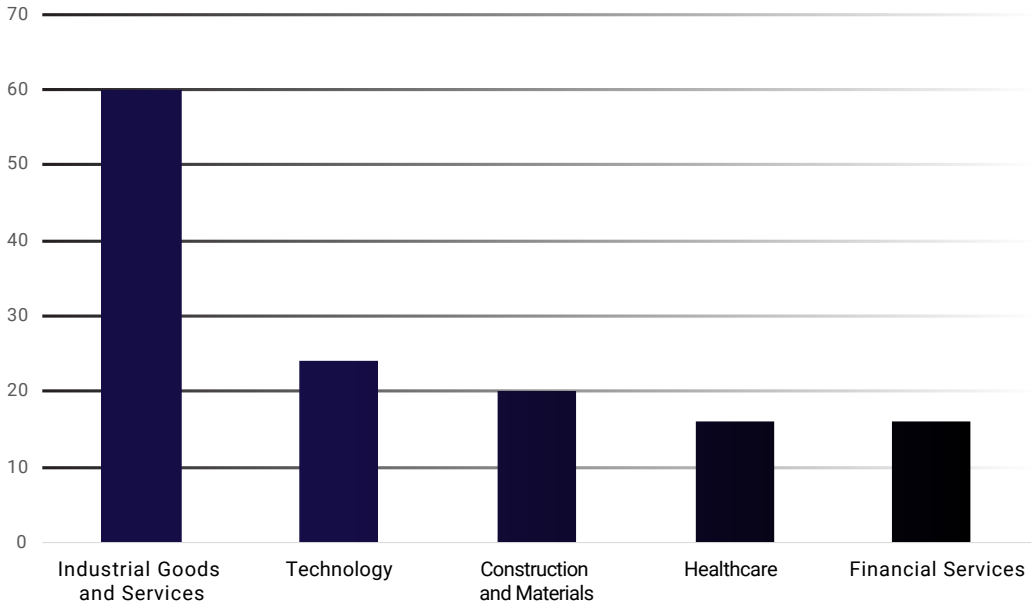

Figure 7: Distribution of attacks affecting the top 5 most targeted sectors by LockBit in Q1 2023

Clop

Clop Ransomware Background:

- The Clop ransomware was first discovered in February 2019.
- It is one of the oldest double extortion ransomware groups active today; it opened its data-leak site “CL0P^_- LEAKS” in March 2020.
- The ransomware used by the group is an updated version of the “CryptoMix” ransomware, first discovered in March 2016.
- Clop is deployed by a subgroup of “FIN11” called TA505, the same group behind the “Dridex” banking trojan and the “Locky” ransomware.
- The group developed a Linux encryptor in December 2022, but it was flawed and researchers were able to create a decryptor for the Linux version.

Clop TTPs:

- Initial attack methods include spam email messages with malicious links or attachments, exploit kits, malicious advertisements, and fraudulent websites.
- Clop uses the AES cipher to encrypt files and appends a “.Clop” file extension, or variations of the word Clop, to encrypted files.
- Clop’s operators use a remote-access tool named “SDBBot,” which is considered a precursor to Clop ransomware.
- The ransomware attempts to disable Windows Defenders and remove Microsoft Security Essentials.
- Clop has been known to exploit zero-day vulnerabilities and conduct supply-chain attacks. The group has been linked to two large supply-chain attacks.
    - Attack exploiting a zero-day in GoAnywhere MFT (CVE-2023-0669) that allegedly affected over 130 organizations.
    - Attack exploiting zero-day vulnerabilities in Accellion FTA (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104) that allegedly affected over 100 organizations.
- Clop does not always deploy ransomware in attacks. The group has been known to infiltrate organizations, steal data, and demand a ransom via email.
- Campaigns by Clop often start with “spray and pray” attacks, where the group sends phishing emails on a large scale, then chooses which victims they want to compromise further.

Clop Ransom Note Excerpt

[Victim Name]

===DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM ===

Here are some of the files we downloaded from your network:

[PII]

If you refuse to cooperate, all data will be published

For free download on our portal:

hxxp://santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad[.]onion/ -> TOR browser

CONTACT US BY EMAIL:

unlock@[email].com

or

unlock@[email2].com

OR WRITE TO THE CHAT AT ->

hxxp://6v4q5w7di74grj2vtmikzgx2tnq5eagyg2cubpcnqrvvee2ijpmprzqd[.]onion

(use TOR browser)

Figure 8: Example of a Clop ransomware note

Victimology:

- Clop targets large enterprises in a variety of sectors worldwide.
- The top sectors targeted by Clop are industrial goods and services, technology, and healthcare.
- The most-targeted countries are the United States, Canada, and the UK.
- The ransomware is built to terminate itself if the target organization's location is identified as Russia or another CIS country.
- The Clop ransomware's operators participate in big game hunting, in which they target large organizations to achieve large ransom payments.

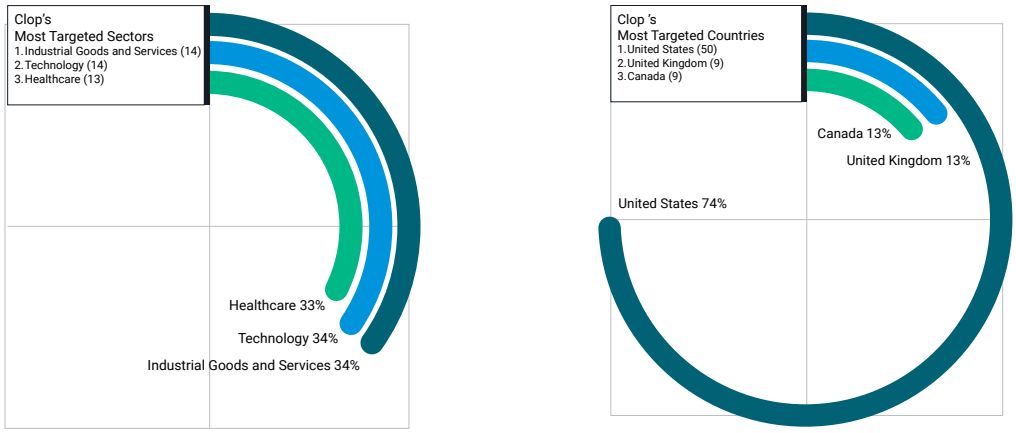

Figure 9: Breakdown of the top 3 sectors and geographies targeted by Clop in Q1 2023

Clop in Q1 2023:

- The US was the most-targeted country by a very wide margin, accounting for 49% of all Clop's attacks.
- The UK, Canada, Australia, and Colombia combined made up 23.5% of Clop victims in Q1 2023.

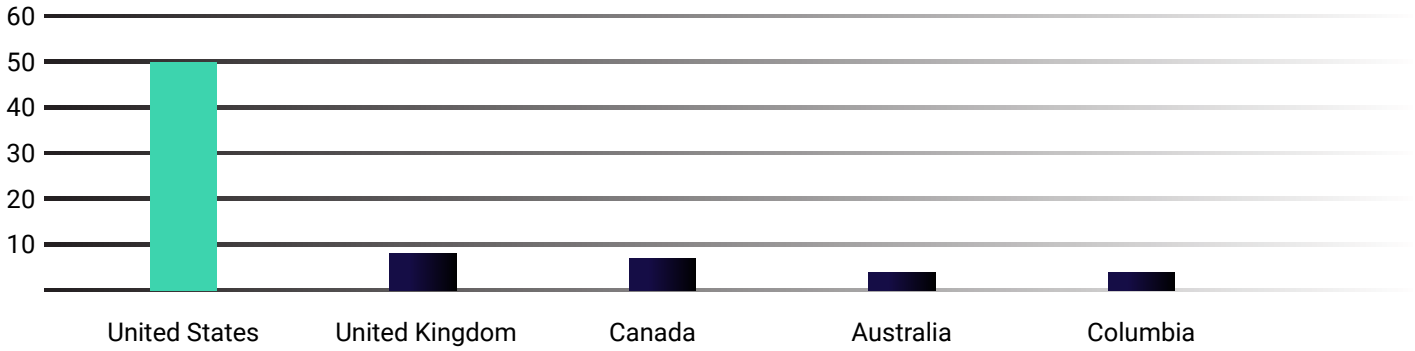

Figure 10: Most targeted countries by Clop in Q1 2023

- The most-targeted sector was a tie between industrial goods and services and technology, accounting for 27.5% of all Clop's victims combined.
- Healthcare, financial services, and construction and materials made up 25.5% of Clop events combined.

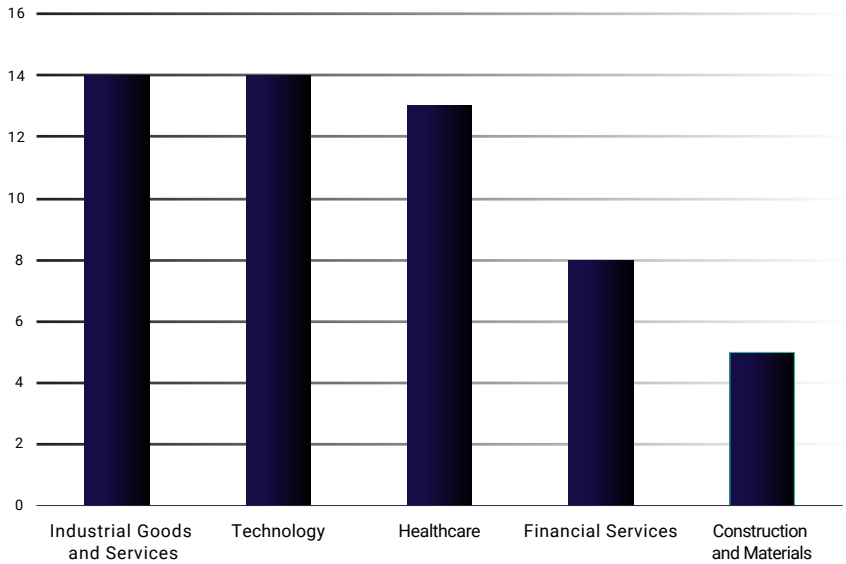

Figure 11: Distribution of attacks affecting the top 5 most targeted sectors by Clop in Q1 2023

ALPHV

ALPHV Ransomware Background:

- The ALPHV (aka BlackCat, AlphaV, AlphaVM) ransomware was first detected in November 2021 and is written in the Rust programming language.
- It is the first known ransomware group to successfully use Rust programming language-based ransomware to compromise victims.
- ALPHV operates as RaaS, whereby its developers lease ransomware to affiliates interested in conducting cyber extortion.
    - The affiliate program does not tolerate inactivity. Affiliates who do not perform any activity in two weeks have their accounts frozen or deleted.
    - Affiliates make between 80 to 90% of their final ransom, depending on the value of the payment.
- The affiliate program was advertised on the RAMP cybercriminal forum on December 9, 2021; it was described as the next generation of ransomware.
- ALPHV provided its affiliates with a “built-in mixer” that provided a break in tracking blockchain transactions.
- ALPHV has been associated with two other ransomware groups—“DarkSide” and “BlackMatter”—due to design overlaps.

ALPHV TTPs:

- ALPHV can target all versions from Windows 7 and above, and various versions of Linux (ESXI, Debian, Ubuntu, and ReadyNas).
- To gain initial access, the group has exploited vulnerabilities, used social engineering, and leveraged IABs to provide access to compromised organizations.
    - As the RaaS program relies on affiliates to distribute its ransomware, these techniques are expected to differentiate depending on the affiliate.
- ALPHV operators have been known to leverage compromised user credentials to gain initial access, and once that access has been established, it compromised Active Directory user and admin accounts.

- The operators then used Windows Task Scheduler to deploy the ALPHV ransomware via malicious Group Policy Objects (GPOs).
- ALPHV leveraged PowerShell scripts and Cobalt Strike in its initial deployment, and it also leveraged Windows admin tools and Sysinternals during compromise.
- To maintain persistent access in a victim's environment, ALPHV carefully avoids shutting down critical processes and application folders.
- ALPHV affiliates conducted reconnaissance within the compromised networks. This included identifying sensitive data for exfiltration and high-value systems to encrypt. The ransomware then attempted to exfiltrate the victim's information, including data stored by cloud providers, prior to encrypting data.
- The malware has four encryption modes: full, fast, DotPattern, and Auto. It uses the two encryption algorithms ChaCha20 and AES.
- Following successful exfiltration and encryption of files and data, ALPHV leaves a customized ransom note behind. Files are appended with a random extension, such as ".wpzlbji".
- Once infected, ALPHV generates a unique onion domain for each new victim, which can be used to negotiate ransom payments.

ALPHV Ransom Note

-->> Introduction

Important files on your system was ENCRYPTED and now they have "wpzlbji" extension.

>> Sensitive Data

Sensitive data on your system was downloaded and it will be PUBLISHED if you refuse to cooperate.

Data includes:
[Description of data stolen]

>> CAUTION

DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure

Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: hxxps://torproject.org/
2) Navigate to:
[Onion URL]

Figure 12: One of ALPHV's many ransomware notes

Victimology:

- ALPHV has primarily targeted entities in the industrial goods and services sector, followed by the legal services and construction and materials sectors.
- The most-targeted countries by ALPHV were the US, Germany, Australia, Canada, and the UK.
- The ransomware has also been used to target entities in Asia and the Middle East.
- Targeting of countries in the CIS region was strictly prohibited, also including China, Taiwan, Hong Kong, and Turkey.

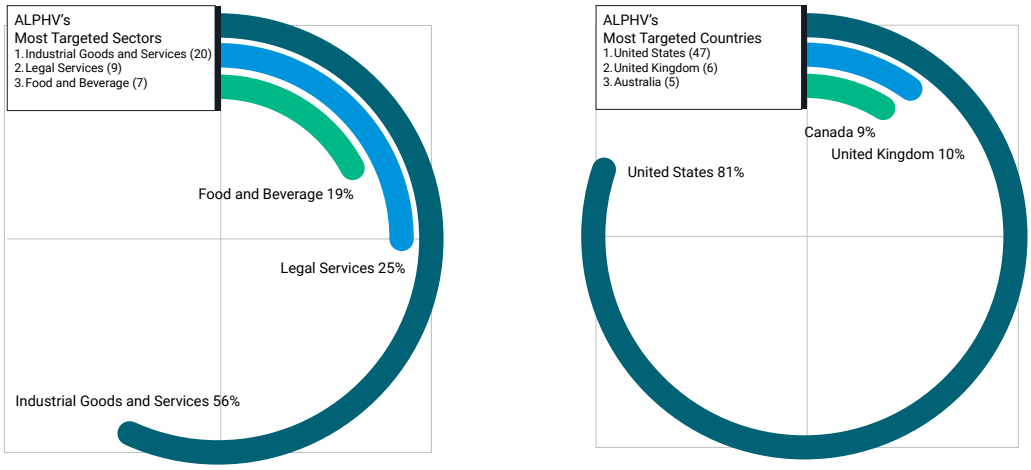

Figure 13: Breakdown of the top 3 sectors and geographies targeted by ALPHV in Q1 2023

ALPHV in Q1 2023:

- The United States was the most targeted country, accounting for more than half of all ALPHV's attacks (54%).
- The UK, Australia, Italy, and Canada combined made up 12.6% of ALPHV victims in Q1 2023.

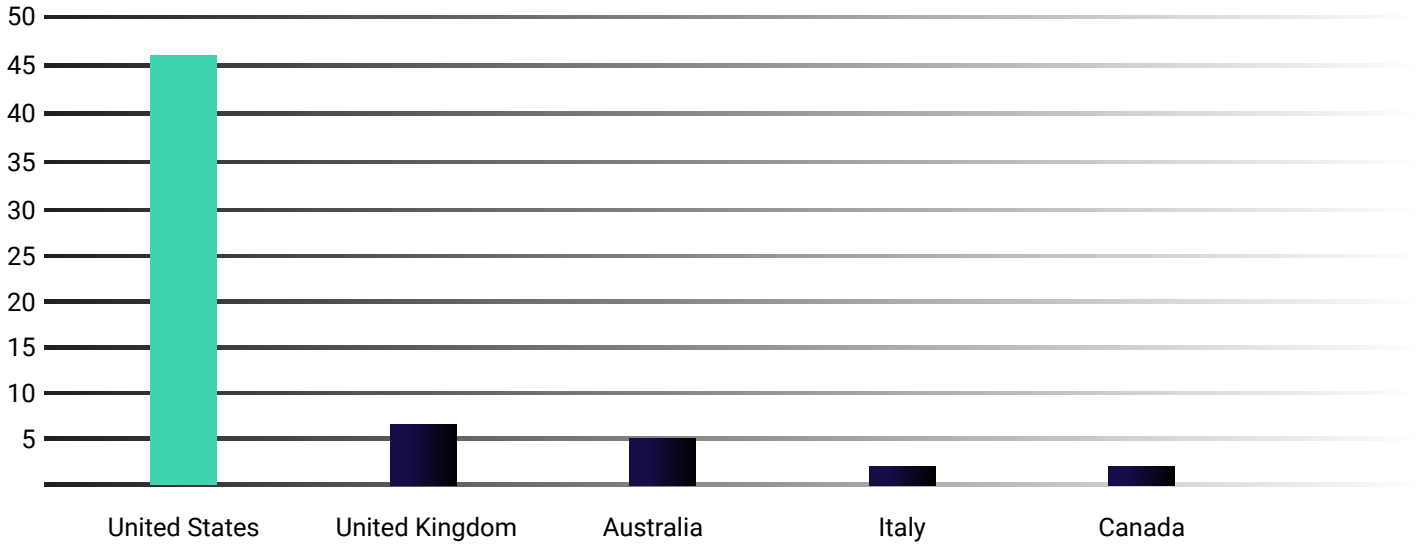

Figure 14: Most targeted countries by ALPHV in Q1 2023

- The most-targeted sector was industrial goods and services, accounting for 23% of all ALPHV's victims.
- Legal services, food and beverage, healthcare, and education made up 20.7% of ALPHV events.

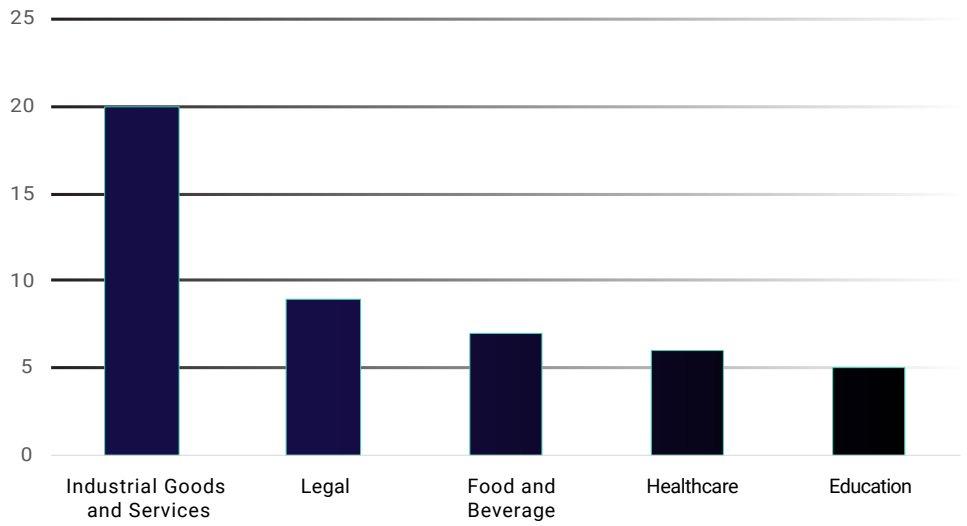

Figure 15: Distribution of attacks affecting the top 5 most targeted sectors by ALPHV in Q1 2023

Common Mitre ATT&CK Techniques Between These 3 Groups

We analyzed Mitre techniques for each of the top three groups to determine commonalities between their offensive approaches. While these Mitre techniques are intended to provide insight into the TTPs used by these groups, it is important to be aware that many large ransomware groups work in affiliate programs. As these programs include a large variety of threat actors, TTPs are likely to differ between attacks.

The most common Mitre techniques associated with the top three ransomware groups are.

- Account Discover (T1087)
- Data Encryption for Impact (T1486)
- Inhibit System Recovery (T1490)
- Process Discovery (T1057)
- Data Obfuscation (T1001)
- Windows Management Instrumentation (T1047)
- Steal or Forge Kerberos Ticket (T1558)

Most Targeted Sectors in Q1 2023

Figure 16 shows sectors targeted by ransomware data-leak site operators throughout Q1 2023. The most-targeted sector was industrial goods and services, accounting for 21.1% of ransomware victims this quarter. The remaining sectors that made up the top five most-targeted included technology, construction and materials, healthcare, and education.

The most targeted sector was industrial goods and services accounting for **21.1% of ransomware victims** this quarter

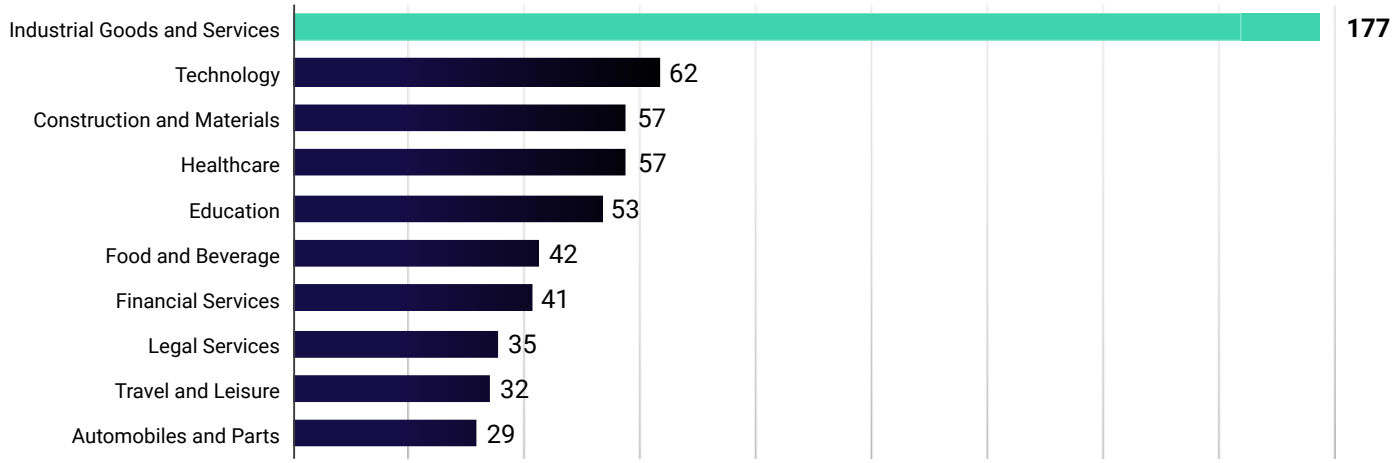

Figure 16: Most targeted sectors by ransomware groups in Q1 2023

The rise in targeting of the healthcare industry was a key finding this quarter. More than 30 healthcare organizations were named on ransomware data-leak sites in March 2023. This number is the highest we have observed over the past year.

Figure 17: Ransomware attacks targeting the healthcare industry since April 2021

Over the past 12 months, the most consistently targeted sector was industrial goods and services. There were natural deviations for other sectors between different months; however, the sectors that frequently made the top three most-targeted sectors each month were technology and construction and materials. It is likely that these sectors will remain the most targeted throughout 2023.

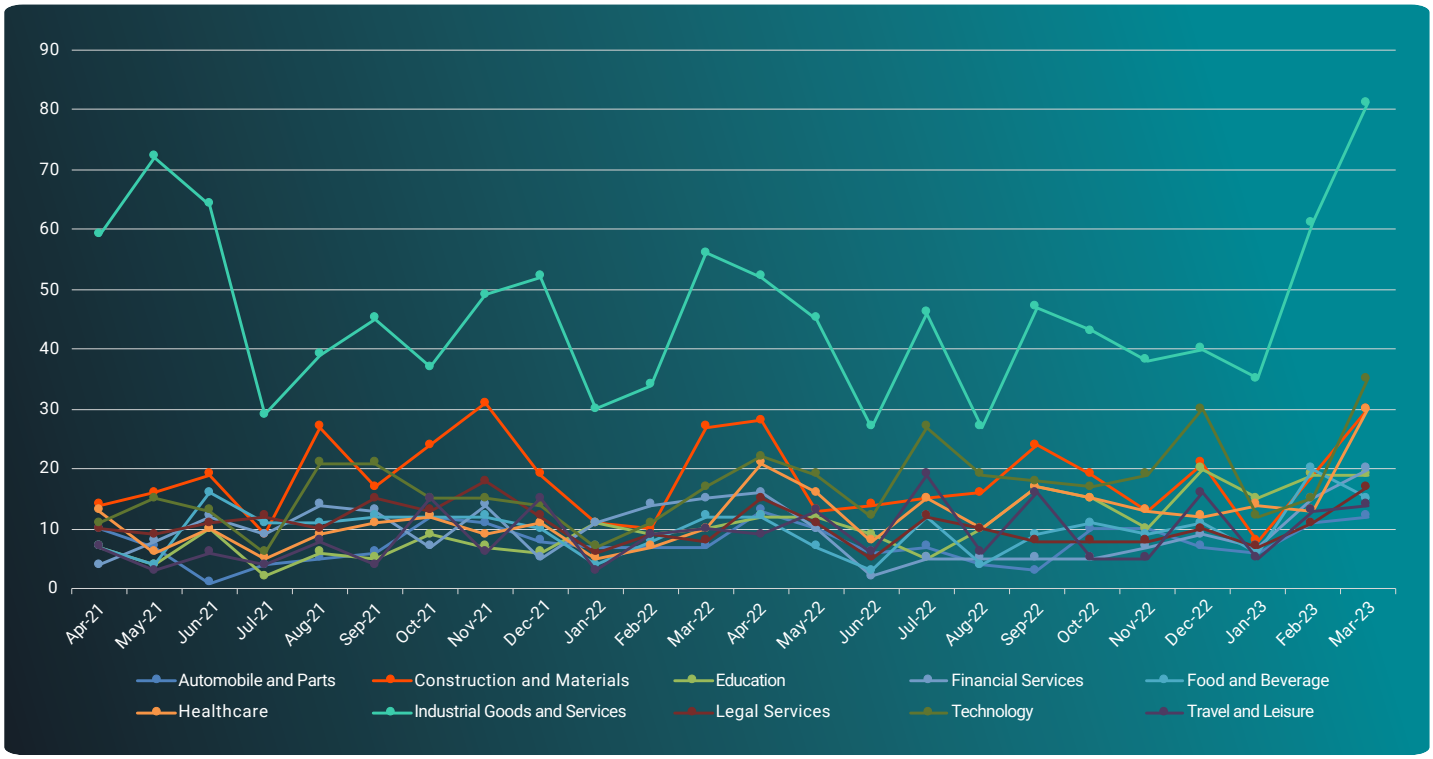

Figure 18: Ransomware attacks targeting top sectors since April 2021

Affected Countries in Q1 2023

The table below shows the ten most-targeted countries (and number of victims) for each of the five most active ransomware data-leak sites. The most-targeted country was the United States, followed by the United Kingdom, and Canada. The United States is a popular target due to the success of threat actors in receiving ransom payments from organizations in the United States.

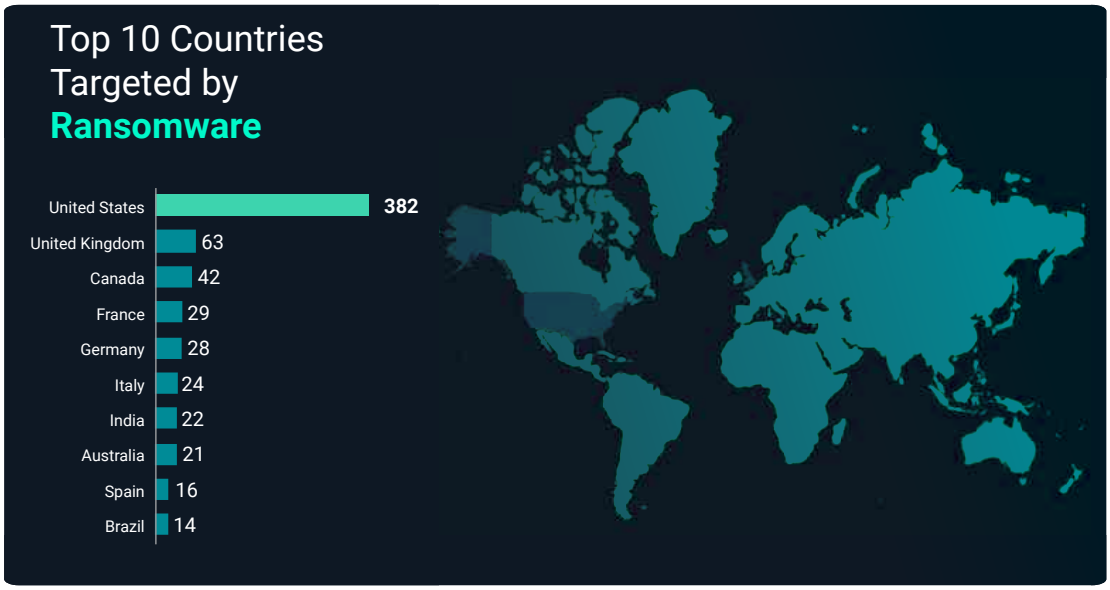

Figure 19: Most targeted countries by ransomware attacks in Q1 2023

Most double extortion ransomware groups prohibit the targeting of organizations operating in the CIS region, in countries such as Russia. This limitation can protect ransomware operators from legal repercussions for their attacks, since extradition of cybercriminals is not always possible from the region.

Over the past 12 months, the target region of ransomware groups remained consistent. Slight deviations were often observed from month to month. However, the US remained the most active region by a wide margin. This is a trend that is expected to continue over the next year.

The **US remained the most active region** by a wide margin. This is a trend that is expected to continue over the next year.

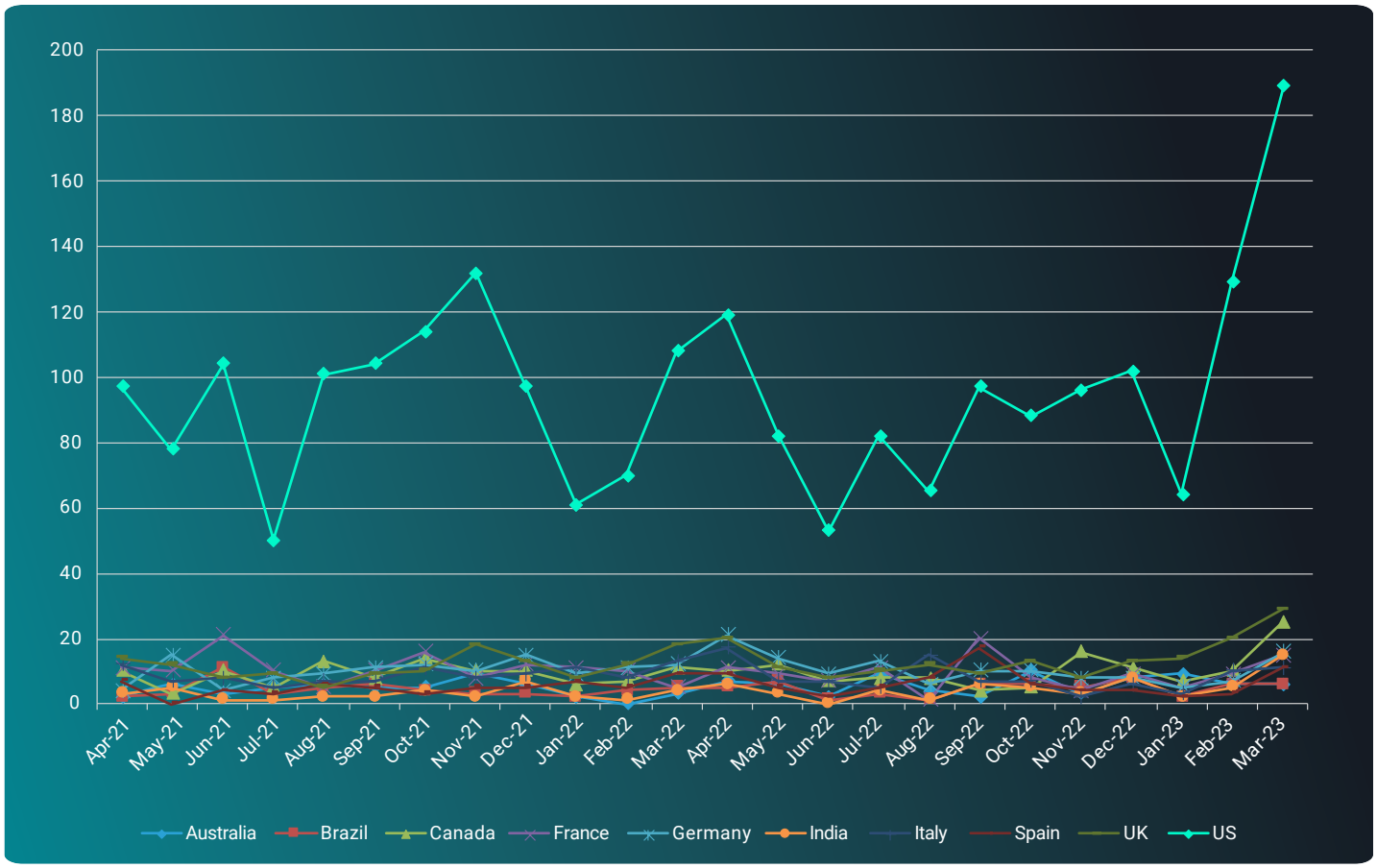

Figure 20: Ransomware attacks targeting top countries since April 2021

Detections Recommended

ReliaQuest GreyMatter® Detect is a robust library that covers all phases of the attack lifecycle. ReliaQuest works with customers to ensure that focus is placed on working towards comprehensive coverage following the strategy of defense in depth. Valuable detection use-cases require endpoint logging or visibility. GreyMatter Detect may be reviewed to identify areas for room for improvement. Visibility limitations should be proactively addressed and not the action item of a recent breach.

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

Suspicious Service Installation

Detects a service installed that has a suspicious name. Most legitimate services have descriptive names that make it easy to identify their function.

- T1543 - Windows Service
- T1569 - Service Execution

Service Installation in Suspicious Directory

Typically, legitimate services are installed in their respective program folders. Alerting on services executing files from anomalous directories such as high-level directory or temp directory can help detect potential lateral movement or persistence.

- T1543 - Windows Service
- T1569 - Service Execution
- T1569.002 - System Services: Service Execution

PowerShell Scheduled Task Creation

Threat actors can use PowerShell Scheduled Task Creation to execute malicious commands on a victim's computer as a persistence mechanism.

- T1053 – Scheduled Task/Job
- T1059 – PowerShell

Impacket Lateral Movement

Impacket is favored by many threat actors due to leveraging Windows management protocols to execute remote commands from a compromised user account. This creates a unique detection opportunity during the lateral movement phase of an attack.

- T1021 – Remote Services
- T1047 – Windows Management Instrumentation
- T1053 – Scheduled Task/Job
- T1059 – Command and Scripting Interpreter

General Recommendations and Best Practices

Network Recommendations

- **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:** For accidental exposure and out-of-date services. Remove any accidental exposure and patch any out-of-date services, with priority for services that have known vulnerabilities. Threat actors will frequently scan the internet for public-facing assets that have an exploitable vulnerability and gain initial access via this method.

Internal System Recommendations

- **Use application control:** Where appropriate and, if possible, only permit the execution of signed scripts. 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. The use of weaponized script files is used heavily by initial access malware.
- **Ensure comprehensive coverage**: Ensure coverage is enabled for Anti-Virus/Endpoint Detection and Response tools within your environment to provide as much visibility as possible into exploit or threat activity. Valuable detection use-cases require endpoint logging or visibility.
- **Use automatic updates:** Use the software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.

Account Recommendations

- **Inventory accounts:** Service and other privileged accounts in the environment should be accounted for. Ensure that they follow the principle of least privilege and are configured with long, complex passwords. Service accounts are highly targeted in ransomware intrusions given that they are often configured improperly with domain admin rights.
- **Use standard user accounts:** Internal systems should only use standard user accounts instead of administrative accounts, which allow for overarching administrative system privileges and do not ensure least privilege

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 ReliaQuest's Threat Research Team's intelligence requirements and thresholds and additional open-source reporting; there may have been exposures and events falling outside these parameters that are not included.

Our sources were:

- ReliaQuest's primary-source intelligence
- hxxps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-075a
- hxxps://www.cisa[.]gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf
- hxxps://www.sentinelone[.]com/wp-content/uploads/pdf-gen/1675698546/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available.pdf