BRANDEFENSE

# RANSOMWARE TRENDS REPORT Q2 | 2023

with comparison Q1 | 2023

# Executive Summary

*Dear Reader,*

Our Ransomware Trends Report is a comprehensive retrospective report on cybercrime activity worldwide. The report includes various sections with statistics on the size of the ransomware attack by industries, countries, ransomware groups, and company sizes. We aim to help security leaders infer the size trends of companies targeted in the ransomware sector and understand the scale of data for which threat actors have planned their attacks based on over 1383 studied incidents.

The report covers a six-month period from Q1/2023 to Q2/2023, encompassing recorded attacks of the 41 most active groups in Q2 alone. Alongside current statistics, significant news stories about ransomware attacks in the past three months have been compiled and included in the report to refresh the reader's memory.

Our analysts have identified staggering ransomware incidents across **27 industry sub-sectors** with devastating consequences. The statistical distribution of these events shows that **19.6%** of them were related to business, professional, and legal services, while **18.8%** of the events were in the manufacturing sector. Additionally, **8.7%** of the events were related to the Healthcare sector.

The report also provides insights into various ransomware groups' tactics and techniques during attacks regarding vulnerabilities.

Overall, our Ransomware Trends Report provides valuable information for security leaders to understand current trends in ransomware attacks and take proactive measures to protect their organizations from future threats.

*Sincerely,*
Brandefense CTI

# Methodology

Brandefense analysts identified staggering ransomware incidents in Q1/2023 - Q2/2023 across the deep and dark web. They collected valuable details such as targeted organizations, countries impacted, data stolen during attacks and demanded ransom payouts - all compiled into this comprehensive retrospective report on cybercrime activity worldwide.

In preparing this report, the focus has been on the attacks carried out by various groups closely monitored by our analysts between April and June. Within this scope, an attempt has been made to derive the 3-month trends of the attacking groups based on entities such as country, industry, amount of stolen data, ransom amount demanded, and annual revenue of the targeted companies. Additionally, statistics from the RTR 2022/Q4-Q3 report have been utilized to compare the trends in the second quarter of 2023.

Alongside the current statistics, significant news stories about ransomware attacks in the past three months have been compiled and included in the report to refresh the reader's memory. We have tried to gather the most interesting news in this section, hoping that it provides industry leaders with insightful and visionary perspectives.

**1383 Victims**

**83 Country**

**27 Industry**

**41 Ransomware Group**

# Key Insights

- The cybersecurity landscape is marked by a high prevalence of attacks across industries, with businesses, professionals, and legal services being the most targeted.
- Manufacturing consistently ranks as a top target, highlighting the sector's value to cybercriminals and the need for robust security measures.
- Lockbit emerges as the most prolific attack group, possibly due to more sophisticated tactics and a broader range of targeted industries.
- Industry-specific attacks, like Royal Group's focus on Manufacturing and Karakurt Group's focus on Healthcare, suggest that some cybercriminals develop specialized techniques for exploiting vulnerabilities in certain sectors.
- Finance and Transportation sectors, while not as frequently targeted, still face significant cyber threats, necessitating ongoing monitoring and protection.
- There was a significant increase in the number of cases with the use of the MOVEit exploit by the Cl0p group. And these increases caused serious losses to big companies.
- The majority of the victims of the Cl0p group were enterprise companies and mostly targeted the IT and financial sectors.
- The highest increase was in April, with 544 attacks, the majority of which belonged to the LockBit and Malas groups.

# Table of Content

# Statistics on Ransomware Attacks

A Visual Breakdown of Top Targeted Countries and Sectors

# 01

# Ransomware Attack Victims by Country Q2 / 2023

According to the data collected by our team, the USA, UK, and Canada became the most targeted countries during Q2 / 2023 by ransomware attacks.

Comparing the number of ransomware attacks on countries in recent periods, there has been a significant increase in rates of attacks in several countries, such as Italy, Australia, and Germany. Italy ranks first with an increase of %260. Our analysts have examined the over 41 active groups in recent times, conducting in-depth assessments aimed at providing readers with valuable insights into these groups.

To offer insights into the vulnerabilities exploited in ransomware attacks, the CVEs *(Common Vulnerabilities and Exposures)* leveraged by malicious groups over the past three months have been compiled from open sources. Details regarding these CVEs, such as risk scores and impact areas, have been provided in detail in section 13.

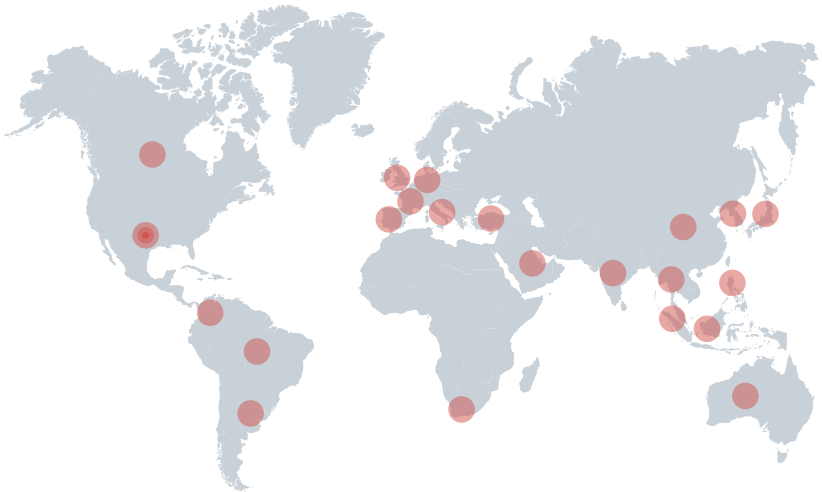


**Figure 1:** 2023 / Q2 - Heatmap of the attacked countries

- ▲ Italy **260 %**
- ▲ Australia **191 %**
- ▲ Canada **152 %**
- ▲ USA **132 %**
- ▲ Germany **130 %**
- ▲ France **117 %**
- ▲ Brazil **100 %**
- ▲ UK **51 %**

...there has been a significant increase in rates of attacks in several countries, such as Italy, Australia, and Germany

# 02

## Ransomware Attack Distributions by Country: Q2/ 2023

The graph below illustrates the total number of companies targeted for ransom demands by the monitored groups in each country during 2023.

- It was observed that the rise in ransomware attacks continued in the Q2/23 period, with the USA, UK, Canada, and Italy maintaining their places at the top of the list of the most targeted countries.
- It is also notable that ransomware attacks targeting the USA have more than doubled.
- Although Germany, France, and Spain saw a decrease in ransomware attacks compared to the previous quarter, they continued to be the target of attacks.

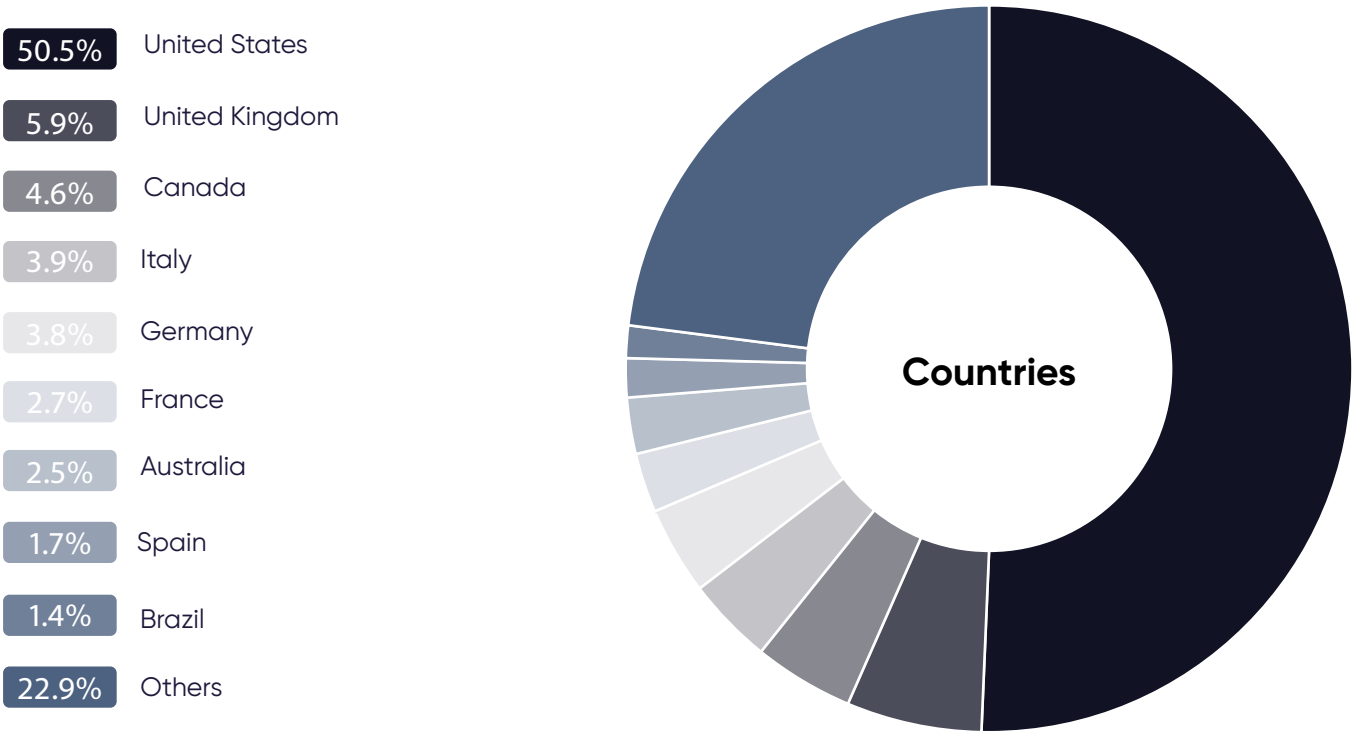



**Figure 2:** Distribution of ransomware attacks by country by 2023 / Q2

top of the list

**USA, UK, Canada**

# Ransomware Attack Changes by Countries from Q1/2023 to Q2/2023

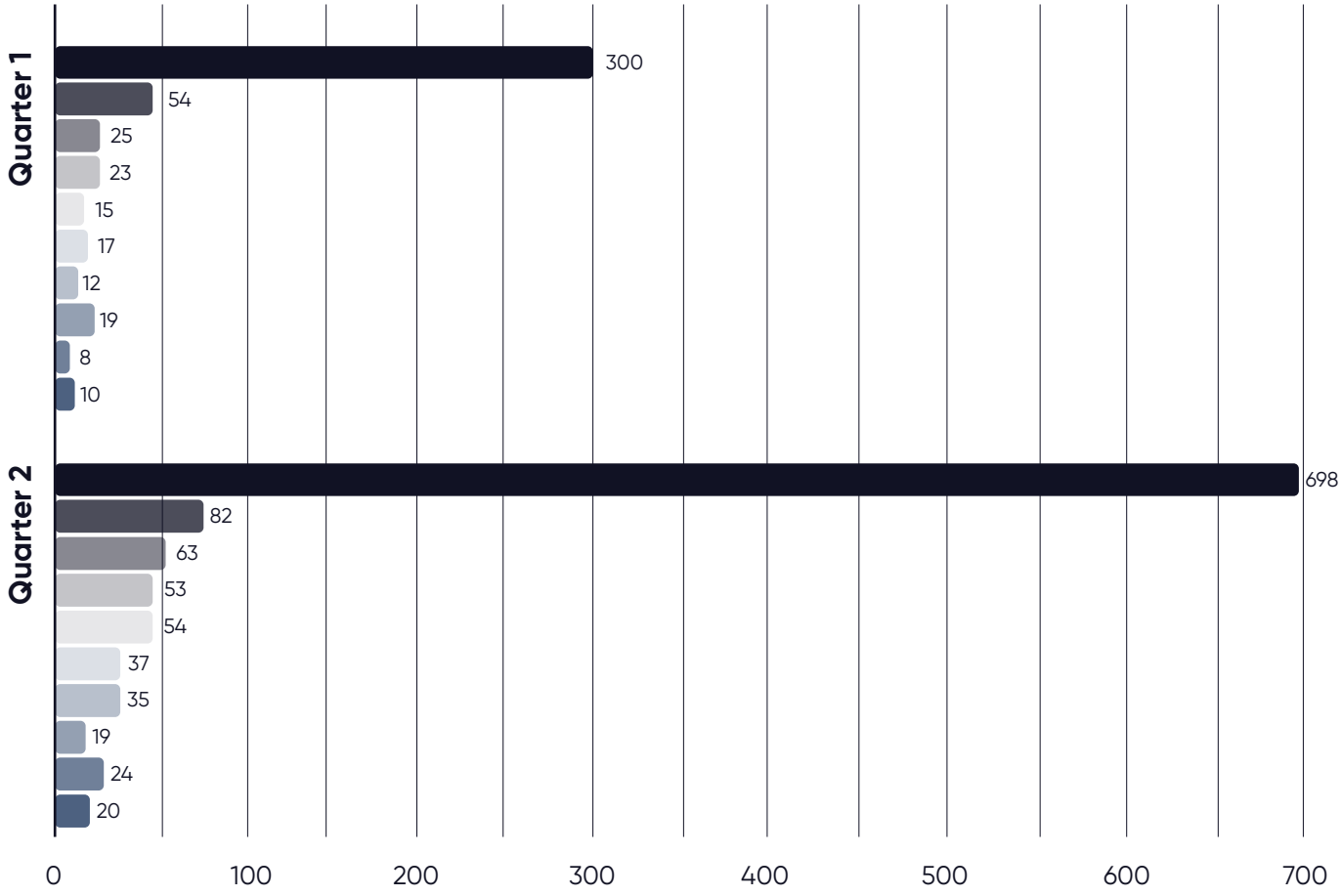



**Figure 3:** Comparison of ransomware attack numbers in countries compared to the last two quarters - TOP 10

Over the past three months, there have been over 1383 events where cybercriminals have targeted organizations across 83 different countries, with devastating consequences. The statistical distribution of these events shows that 50,5% of them were related to the United States of America, while 5.9% of the events were in the United Kingdom. Additionally, 4.6% of the events were related to Canada.

# 03

# Distribution of Ransomware Attacks by Quarters Over 12 Months

Over the past 12 months, ransomware attacks have witnessed a significant surge across various sectors, with the Healthcare & Public Health sector experiencing an alarming 188.09% increase, followed closely by Manufacturing at 182.60%, and Business, Professional, and Legal Services at 120.32%. This sharp rise underscores the growing importance of addressing cyber threats and implementing robust cybersecurity measures to safeguard sensitive data and critical infrastructure from malicious actors.

**Between Q3/2022 and Q2/2023**

**188.09%**
Healthcare & Public Health Sector

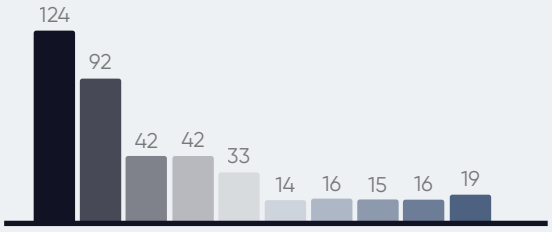
**182.60%**
Manufacturing

**120.32%**
Business, Professional and Legal Services

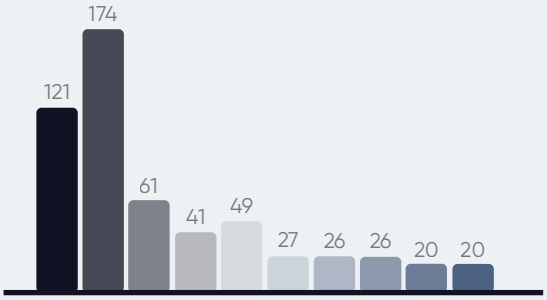
**116.07%**
IT

**71.42%**
Energy and Utilities Infrastructure

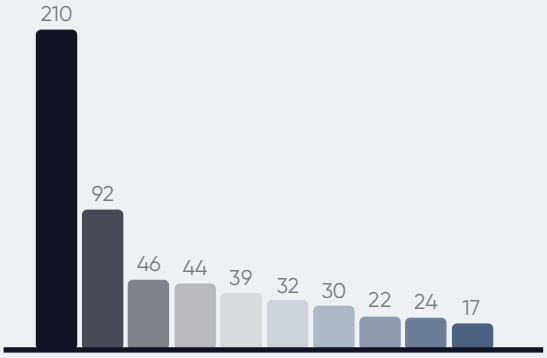
- Business, Professional and Legal Services
- Manufacturing
- IT
- Healthcare & Public Health Sector
- Education, Research & Innovation
- Energy and Utilities Infrastructure
- Food & Agriculture
- Retail
- Banking & Finance
- Transportation
- Construction



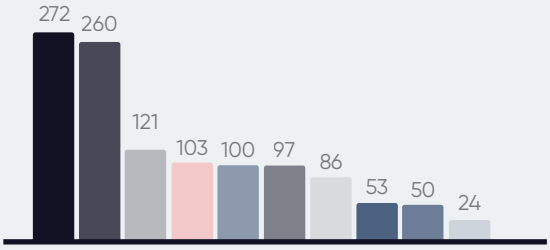
Quarter 3, 2022



Quarter 4, 2022



Quarter 1, 2023



Quarter 2, 2023

**Figure 4:** Attack numbers of the top 10 sectors that received the most attacks, broken down by quarters.

04

# Ransomware Attack Victims by Sector Over Q2/2023

Brandefense has been closely monitoring ransomware groups for almost a year, analyzing the attack patterns of more than 41 ransomware groups. In light of this extensive research, we have drawn the following conclusions regarding the evolving cybercriminal landscape.

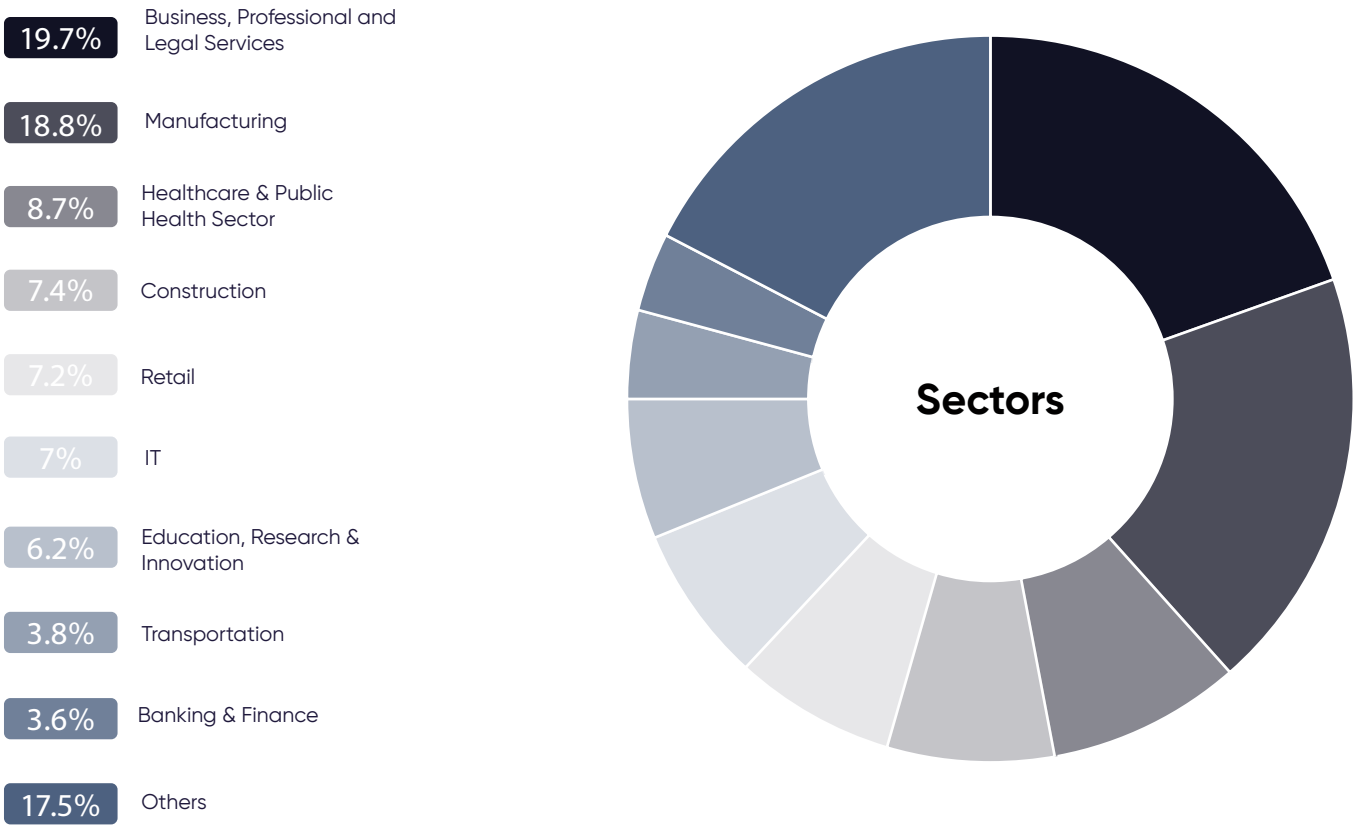



**Figure 5:** Distribution of ransomware attacks by sectors by 2023 / Q2

Business, Professional, Legal Services
**19.7%**

Manufacturing
**18.8%**

Healthcare & Public Health Sector
**8.7%**

05

# Ransomware Groups Attack Distribution Across Sectors: Q2/2023 Analysis

The data reveals an alarming prevalence of cyber-attacks across various industries, totalling 1383 attacks in the second quarter, with five primary attack groups—Lockbit, Clop, Malas, ALPHV/Blackcat, and Bianlian—driving these incidents. Business, professionals, and legal services stand out as the most targeted industry, with 271 ransomware incidents, indicating that these organizations may possess valuable and sensitive data attractive to cybercriminals.

The data also suggests that these organizations may have weaker cybersecurity measures or be more susceptible to social engineering tactics. Meanwhile, the manufacturing sector emerges as another popular target, with its reliance on intellectual property and sensitive information about supply chains and production processes potentially making it an appealing target for cybercriminals.

Analysis of attack patterns reveals Lockbit to be the most active group with 227 incidents in Q2 / 2023, suggesting that they may have developed more sophisticated or effective tactics or targeted a wider range of industries.

Moreover, some attack groups display preferences for specific industries, such as the Royal group's focus on Manufacturing and the Karakurt group's focus on Healthcare, indicating that these groups may have devised specialized techniques to exploit vulnerabilities in these sectors or perceive them as having higher payoffs. Although the Transportation and Government sectors experience fewer attacks, they should not be overlooked, as they store sensitive information and provide crucial services to society. Continued monitoring and vigilance in these sectors are essential for safeguarding valuable data and resources.

**1383**
attacks.

Business, professionals, and legal services stand out as the most targeted industry

**LockBit**
most active group with

**227**
incidents

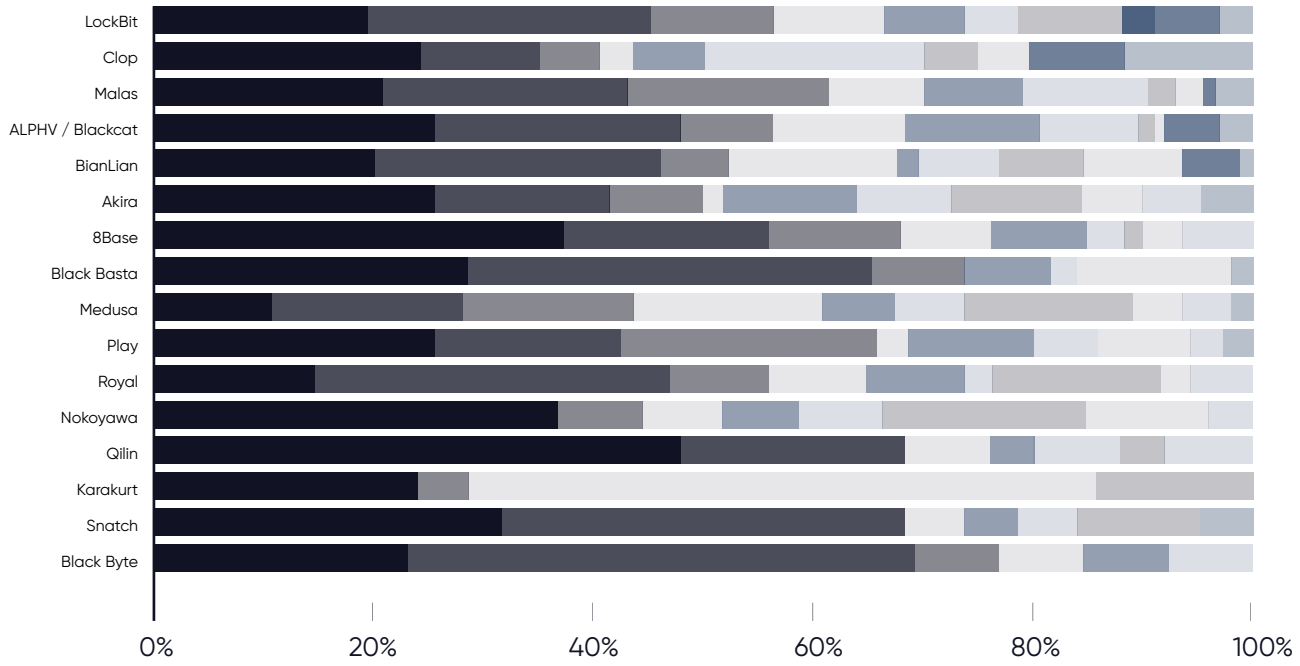



**Figure 10:** Proportion of Ransomware groups attacks across sector Q2/2023

Business, Professional and Legal Services
Manufacturing
Construction
Education, Research & Innovation
Information Technology
Healthcare & Public Health Sector
Finance
Retail
Banking & Finance
Transportation

## Impact of Active Groups: Victims Overview

| | |
|---|---|
| LockBit | 227 |
| Clop | 146 |
| Malas | 129 |
| ALPHV/ Blackcat | 118 |
| BianLian | 74 |

## Most Targeted Sector

271 attacks

Business, Professionals, and Legal Services with 271 attacks.

Transportation and Government sectors experienced comparatively fewer attacks but still warrant attention and ongoing monitoring.

06

# Financial Impacts of Ransomware Attacks in 3 to 6 Months

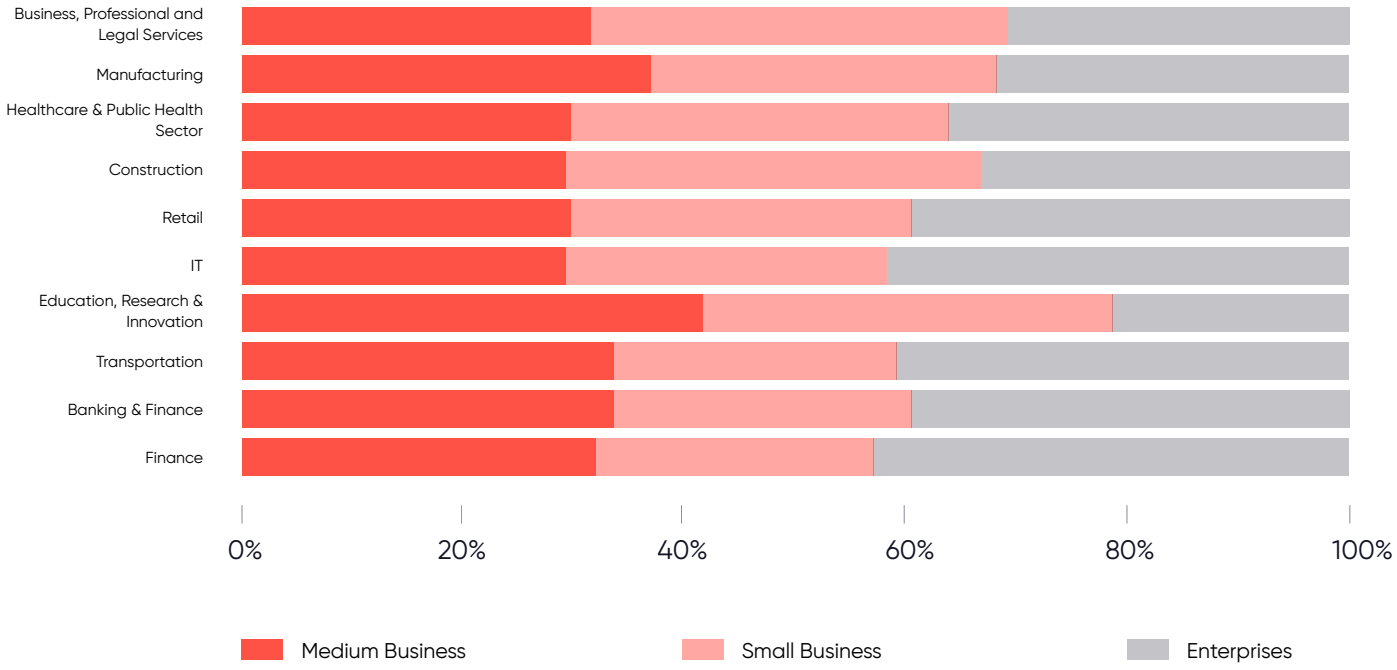
Brandefense analysts covered 1383 cyber-attacks across 83 countries, revealing that the U.S., the UK, and Canada are top targets due to their high revenue-generating victims.

Small businesses, often seen as easy prey, are attacked the most, while large enterprises suffer greater financial losses.

Cybercriminal groups like Lockbit, Cl0p, and Medusa adapt their tactics to exploit diverse industries. This highlights the need for robust security measures and continuous vigilance in today's ever-evolving cybersecurity landscape.

The LockBit, Cl0p, and Malas attacker groups are the most active across different countries and organization sizes. These groups target a wide range of industries, showing their adaptability and diverse tactics in selecting victims.

## Q2/2023 Company Size Distribition by Industry: A Visiual Overview




Across

**83 Countries**

Top Targets

**USA, UK, Canada**

# Most Active Ransomware Groups: Q2/2023 Analysis

- Lockbit emerges as the most prolific attack group, possibly due to more sophisticated tactics and a broader range of targeted industries.

- Industry-specific attacks, like Royal Group's focus on Manufacturing and Karakurt Group's focus on Healthcare, suggest that some cybercriminals develop specialized techniques for exploiting vulnerabilities in certain sectors.

- The financial and transportation sectors, although not frequently targeted, are still valuable targets for dangerous groups such as Cl0p and Malas, which have recently increased the number of attacks, and require constant monitoring and protection.

# 07

# LockBit 3.0

***Who is LockBit?***

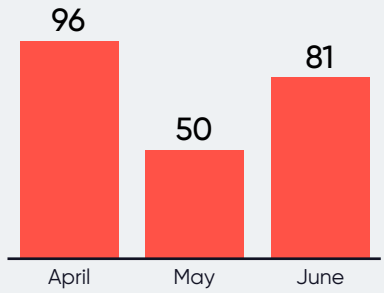
*The group has been active since 2019 and is responsible for numerous high-profile attacks, causing significant financial losses and business disruption. LockBit 3.0 is the latest version of the LockBit ransomware, known for its advanced tactics and ability to cause significant damage to organisations and businesses.*

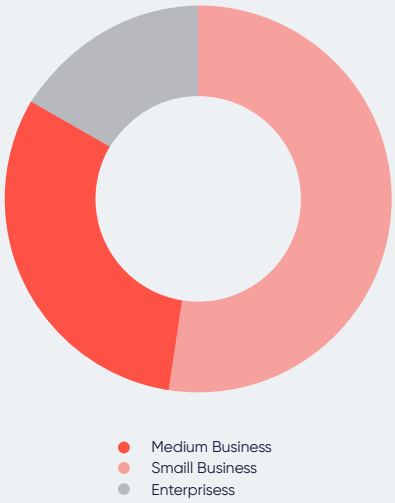
LockBit, one of the most notorious cybercrime organizations, emerged around mid-2019, primarily targeting enterprises and government bodies over individuals. They initiated their attacks in September 2019 with the ".abcd virus" signature. By March 2022, LockBit released its 3.0 version, and by April 2023, they expanded their targets to include macOS operating systems.

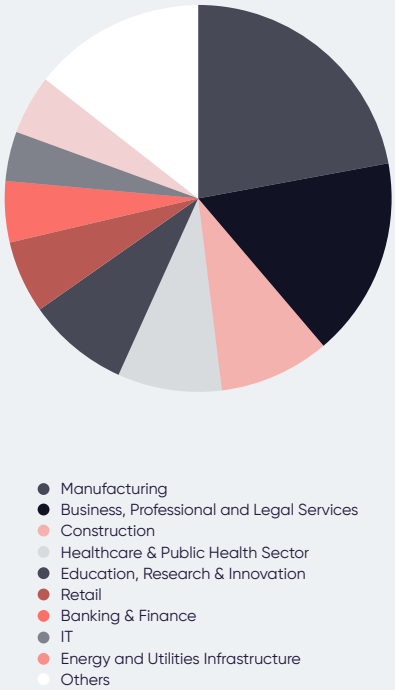
In 2022, LockBit adopted the triple-extortion method, comprising encryption, data leaks, and DDoS attacks. To enhance their dominance, they recruited individuals proficient in DDoS attacks, ensuring institutions that previously ignored their threats would take them seriously. Originating from Russian-language cybercrime forums in January 2020, the group has released several versions, with LockBit 3.0 or LockBit BLACK in March 2022 repurposing the source code from the BlackMatter ransomware. January 2023 saw the introduction of LockBit GREEN, a variant of LockBit 3.0.

LockBit 3.0 employs a myriad of techniques to breach networks, including brute-forcing credentials for RDP and VPN portals, using credentials from initial access brokers, phishing campaigns, and exploiting known software vulnerabilities. By the second quarter of 2023, LockBit became the most active cybercrime group, responsible for 227 incidents, indicating their evolving and effective tactics and a broader target range.

**Attack Trends of the Lockbit Group**



# 08

# ALPHV/BlackCat

***Who is ALPHV/Blackcat?***

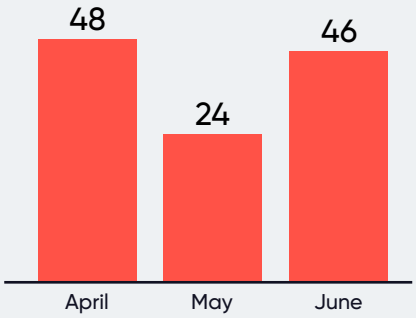
*The group is considered highly dangerous due to its advanced tactics and ability to cause significant financial losses and disruption to organisations. BlackCat is a relatively new player in the world of ransomware, but it has already established itself as a significant threat to businesses and organisations of all sizes.*

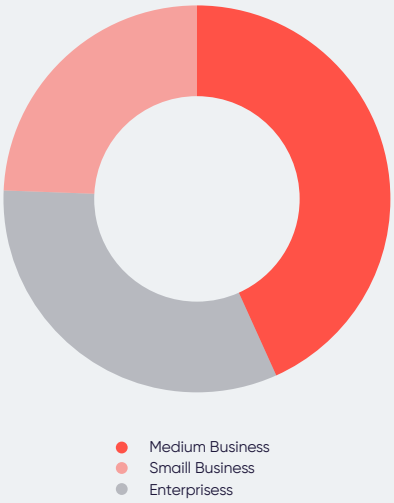
ALPHV, or "BlackCat," utilizes a Ransomware-as-a-Service (RaaS) model, where affiliates share some of their ransom profits with ALPHV operators in exchange for access to the ransomware and related services. Once distributed, ALPHV encrypts corporate assets, rendering them inaccessible, and subsequently provides victims with communication instructions for post-encryption negotiations.

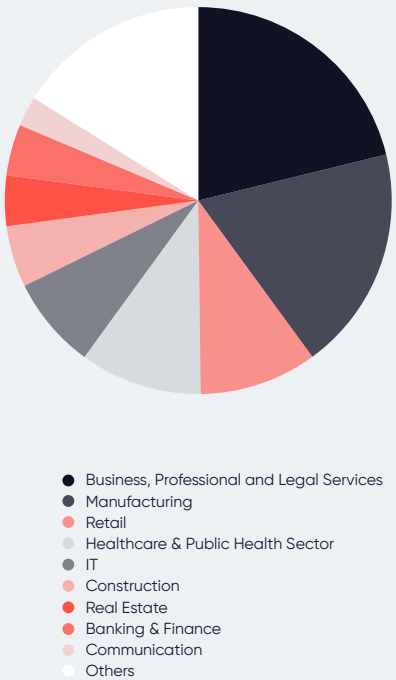
The reach of ALPHV spans multiple countries and industries, with its affiliates targeting diverse corporate infrastructures. Beyond simple encryption, these affiliates employ various extortion methods. Notably, they might upload compromised data to a designated leak site (DLS) or threaten victims with Distributed Denial of Service (DDoS) attacks, escalating the urgency to fulfill ransom demands.

To penetrate target systems, ALPHV threat actors exploit vulnerabilities and leverage real credentials, often obtained from phishing schemes or related to RDP and VPN interfaces. In July 2023, ALPHV introduced a data leak API, complemented by a Python-based scanner, to amplify attack visibility and pressure on its victims.

**Attack Trends of the ALPHV/BlackCat Group**



# 09

# Cl0p

***Who is Cl0p?***

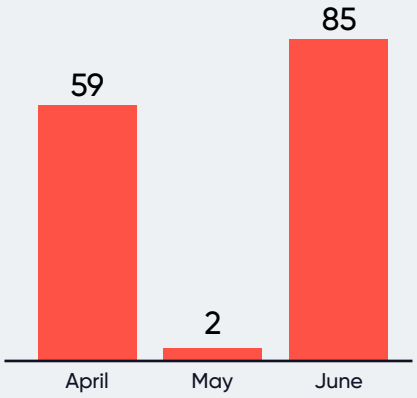
*Cl0p ransomware, run by a criminal group, targets various sectors, encrypting victims' files and demanding ransoms. Delivered via phishing emails, Cl0p emerged in 2019 and is likely operated from Russia, with potential government ties.*

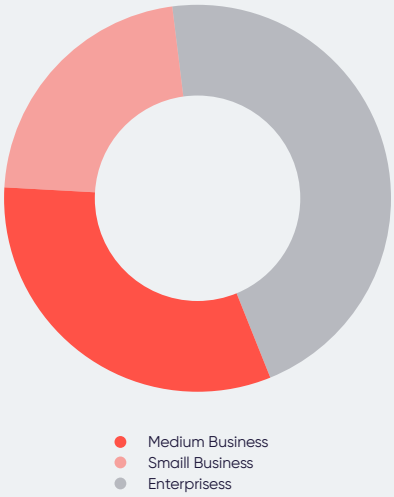
In February 2019, CL0P operated as a Ransomware-as-a-Service (RaaS) using digitally signed binary files for spear-phishing campaigns, which enabled it to bypass security measures. The ransomware gained notoriety for its "double extortion" method, which involved encrypting and stealing data and then threatening to release it on the CL0P^_-LEAKS Tor site. However, by 2021, CL0P shifted its focus from encrypting to purely stealing data.

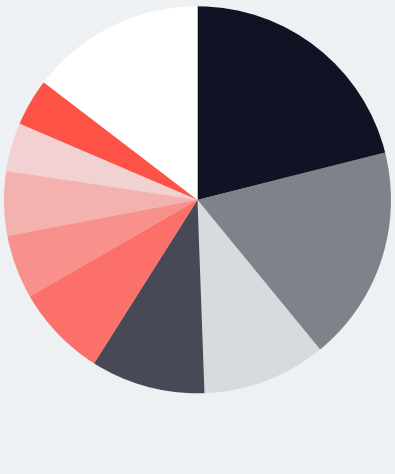
In 2019, TA505 threat actors took advantage of CL0P in a phishing scheme, using a malicious document to deliver Get2 malware that led to the download of SDBot and FlawedGrace. Fast forward to January 2023, the group targeted the GoAnywhere MFT platform and leveraged the CVE-2023-0669 vulnerability, affecting nearly 130 organizations within ten days.

Cl0p has become a major global threat, exploiting vulnerabilities across various sectors, from education to aviation. In a unique approach, Cl0p directly contacts victims' associates, warning of data exposure on the dark web, thereby escalating the severity of their attacks and prompting more victims to meet their ransom demands.

**Attack Trends of the Cl0P Group**



# 10

# MalasLocker

***Who is MalasLocker ?***

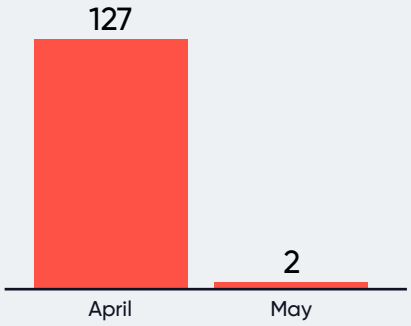
*BleepingComputer has identified a new ransomware operation known as MalasLocker that has infiltrated Zimbra servers to encrypt files and steal emails. This group is characterized by an unusual approach to ransom demands: instead of paying a typical ransom, they ask affected parties to contribute to a charity of their choice. MalasLocker, which began its operations in late March 2023, mainly targets small and medium-sized businesses  in the first quarter of their operations, they expanded their victims to include entesprises and medium-sized businesses in the second quarter. However, the worrying factor is the type of data they have leaked, including unencrypted passwords from Zimbra and LDAP systems, further indicating that their motives could be more sophisticated than just charitable donations.*

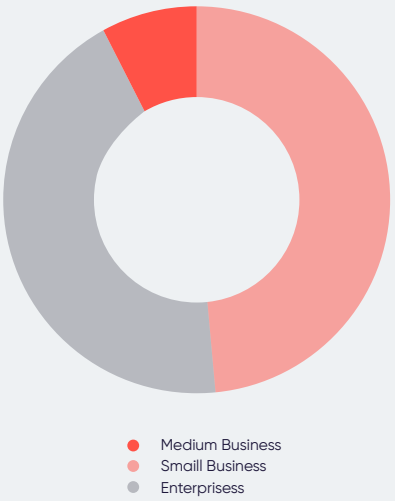
MalasLocker is a ransomware that specifically targets Zimbra servers. This campaign takes a unique approach by encouraging victims to donate for decryption instead of demanding a ransom. Researchers discovered MalasLocker in March 2023, and it operates by encrypting server data and hijacking emails. Victims are then prompted to make charity donations, which they believe will help them recover their files.

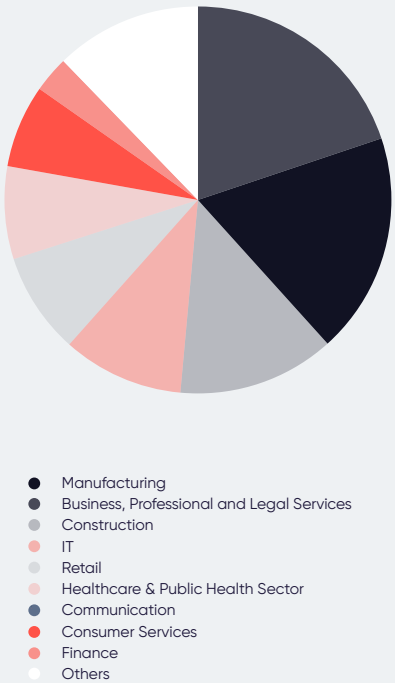
MalasLocker markets itself as a "Robin Hood" of the cyber world, opposing large corporations and financial disparities. However, there is skepticism surrounding their intentions and whether they genuinely decrypt data after receiving charity donations.

Cybercrime groups like Cl0p and MalasLocker are adapting their tactics as the ransomware landscape evolves. They are leveraging known vulnerabilities and automating their attacks to increase their reach and impact. This trend highlights the concerning sophistication of cybercrime.

**Attack Trends of the Malas Group**



# 11

# BianLian

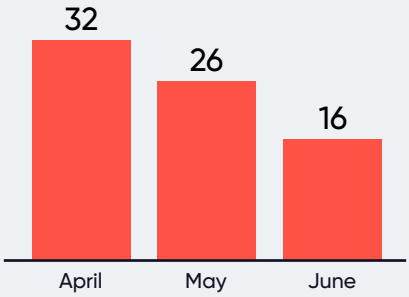
***Who is BianLian?***

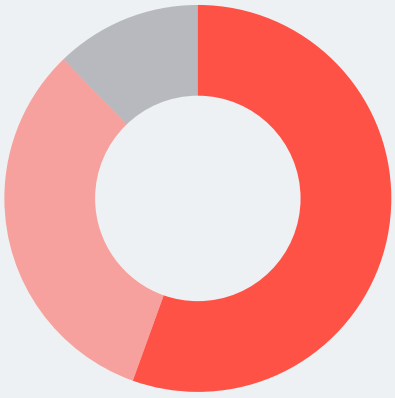
*Bianlian emerged in June 2022. It typically targets various sectors such as financial institutions, healthcare, manufacturing, education, entertainment and energy in numerous countries around the world. This cybercrime group, motivated by financial gain, first infiltrates organizations using legitimate Remote Desktop Protocol (RDP) credentials. Once access is gained, they use open-source tools and command-line scripts to transfer victims' data via FTP, Rclone or Mega. However, their strategy changed in January 2023 after security researchers released a free BianLian ransomware decryptor. Instead of encrypting victims' files, the group started focusing on data exfiltration attacks.*

Since June 2022, BianLian has expanded its data extortion activities globally, focusing on corporate networks in various countries. This ransomware group demonstrates exceptional sophistication, presenting significant threats to USA IT networks.

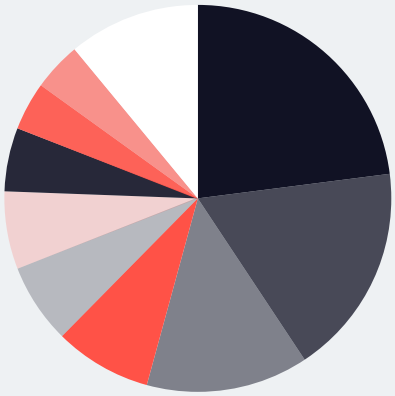
In January 2023, BianLian changed its approach to emphasize the extortion of infiltrative data. Utilizing advanced techniques, they identify IT system vulnerabilities, focusing on weak spots exposed by remote management and shadow IT access. Their strategy has moved from straightforward ransom demands following encryption to primarily threatening the release of stolen data. BianLian utilizes a custom backdoor developed using Go to conduct its operations. They also employ accessible remote access tools and command scripts for network exploration. The stolen data is transferred through FTP, Rclone, or the Mega cloud service. An advisory highlights their use of tools like PsExec and RDP, navigating networks with genuine credentials and manipulating user account access to their advantage.

**Attack Trends of the BianLian Group**



- Medium Size Organizations
- Smaill Business
- Enterprisess



- Manufacturing
- Business, Professional and Legal Services
- Healthcare & Public Health Sector
- Transportation
- IT
- Education, Research & Innovation
- Construction
- Banking & Finance
- Real Estate
- Others

# 2023/Q2 Spotlight: Ransomware's Most Active Groups

Uncovering the Significant News Surrounding the Quarter's Top Threats

# 12

# 2023/Q2 Important Ransomware News

**In Q2 / 2023, especially in April,**

It was observed that ransomware attacks increased "as new groups joined the game".

## BianLian


**Figure 6:** CISA has published a advisory for BianLian *(https://thecyberwire.com/podcasts/cisa-cybersecurity-alerts/49/notes)*

**CISA Advisory: BianLian Ransomware Group Shifts Towards Extortion Model**

The BianLian ransomware group has recently undergone a shift in its modus operandi, moving away from traditional ransom payments and focusing on data theft and extortion tactics.

To infiltrate targeted organizations, the group leverages stolen Remote Desktop Protocol (RDP) credentials. Subsequently, they maneuver within the network using PowerShell scripts to identify valuable data, including financial, customer, business, technical, and personal files. The attackers then exfiltrate this sensitive information and demand ransom from the victims.

Notably, BianLian has adopted a distinctive approach. Rather than solely encrypting the data, they now threaten to publicly expose the stolen data if the ransom is not paid.

This strategy aims to exert pressure on victim organizations and increase the likelihood of receiving payment. This data theft and extortion model has gained popularity among ransomware groups in recent times.

Additionally, the BianLian group employs additional pressure tactics against victims. For instance, they send ransom notes to printers on the compromised network, further intimidating the targets. Some victims have also reported receiving threatening phone calls from individuals associated with the group.

To better protect against ransomware attacks, security organizations recommend implementing robust cybersecurity measures and data protection strategies. Restricting the use of RDP and other remote desktop services can provide additional defense against such attacks.

## MalasLocker

**An Unconventional Ransomware Operation Demands Charity Donations Instead of Ransom**

The recent ransomware operation named "MalasLocker" is targeting Zimbra servers to encrypt emails and seize files. However, this attack follows an unusual approach compared to other ransomware. Instead of demanding a ransom, the attackers request victims to make a donation to a charity organization in exchange for providing a decryptor and preventing the leakage of stolen data.

The MalasLocker operation deviates from the traditional tactics of ransomware attacks and exhibits a form of hacktivism. The encrypted files contain a message at the end stating, "This file is encrypted, look for README.txt for decryption instructions."

The operation employs a different method for decryption called "Age encryption." This encryption technique was developed by Filippo Valsorda, a cryptographer and Go security lead at Google, and includes X25519 (ECDH curve), ChaChar20-Poly1305, and HMAC-SHA256 algorithms.

Age encryption is not commonly used in ransomware attacks, and it does not target Windows devices. MalasLocker operation shares similarities with a previous ransomware operation called AgeLocker, which also targeted QNAP devices.

The nature of the ransom demand creates uncertainty about whether the attackers keep their promise when victims make donations to charities for a decryptor. Consequently, this raises significant concerns regarding the true intentions of the operation and the security of the victims. The claims and demands of the attackers highlight the need for careful consideration in dealing with ransomware threats, as cyber attackers continue to evolve their tactics and adopt new and unpredictable approaches in the cybersecurity landscape.


**Figure 7:** Malaslocker Targeting Zimbra mail servers (https://www.bleepingcomputer.com/news/security/malaslocker-ransomware-targets-zimbra-servers-demands-charity-donation/)

## LockBit

**US Organizations Paid $91 Million to LockBit Ransomware Gang**

LockBit ransomware, a Ransomware as-a-Service (RaaS) operation, has reportedly extorted approximately $91 million following around 1,700 attacks on U.S. organizations since 2020, according to a joint advisory by the U.S. and international cybersecurity authorities, including partners from Australia, Canada, UK, Germany, France, and New Zealand.

Identified as the top global ransomware threat in 2022, LockBit targeted a range of critical infrastructure sectors and claimed the most victims on their data leak site. The joint advisory details over 40 tactics used by LockBit affiliates and provides mitigation measures to help organizations defend against such attacks.

LockBit first emerged in 2019, resurfaced as LockBit 2.0 in 2021 following a ban on ransomware groups on cybercrime forums, and has since upgraded to LockBit 3.0 with advanced extortion methods, a bug bounty program, and new payment options.

## Cl0p

**CISA and FBI Offer $10 Million for Information about Cl0p Ransomware Gang**

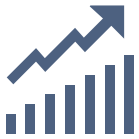
The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI are offering a $10 million reward for information about the Cl0p ransomware gang, a Russian group that threatens to publish private data of its victims. The ransomware group has targeted hundreds of victims, including U.S. government agencies, exploiting various MOVEit vulnerabilities. The reward, announced by the U.S. Department of State's "Rewards for Justice" program, seeks information linking Cl0p or other malicious cyber actors to a foreign government, especially those targeting the U.S. critical infrastructure. In light of possible retaliation risks, the Department recommends using encrypted messaging systems for tip submissions.

## BlackCat

**BlackCat Ransomware Pushing Cobalt Strike Through WinSCP Search Ads**

The BlackCat ransomware group, also known as ALPHV, has been discovered running malvertising campaigns that entice users to fake pages imitating the official website of WinSCP, a popular file-transfer application for Windows. The fake pages offer malware-laden installers instead of legitimate software. The scheme, which primarily targets system administrators, web admins, and IT professionals, was identified by security analysts who noticed ads promoting the malicious pages on Google and Bing search results.

The cyberattack process begins with victims seeking "WinSCP Download" and clicking on the malicious results that rank above the safe WinSCP download sites. The victims are then redirected to fraudulent sites mirroring the official WinSCP site, where they download an ISO file with malware-ridden components. The malware subsequently installs a trojanized python310.dll, establishes a persistence mechanism, and connects to a command-and-control server via a Cobalt Strike beacon.



The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI are offering a **$10M** reward...

++

# BONUS
# News from Brandefense



This chapter presents the intelligence gathered by Brandefense analysts and the information gathered through the analysis of the findings detected by Brandefense sensors.

As part of intelligence efforts conducted by Brandefense analysts, an announcement of the NoEscape raaS service was detected on an underground forum. Based on this detection, Brandefense's resources revealed that the threat actor was looking for penetration testers to target organizations before making the announcement.

## Born and Rise of NoEscape Ransomware

Noescape Ransomware Service was first released as a RaaS by its developer on May 22, 2023. The threat actor stated that the ransomware malware was written from scratch with C++ coding language and did not originate from a different ransomware. Announced the features of the ransomware and the control panel and stated that registration for the affiliate program has started.

According to the threat actor, there is a DDoS / Call / Spam menu on the panel while listing the features of the control panel. It is possible to both perform a DDoS attack on the targeted company through the panel and to abuse it by calling. He stated that this feature can only be used for ransoms over 500,000 dollars.

According to the developer, a feature was added to the dashboard to put pressure on companies to pay the ransom. This tactic, known as "triple extortion", has become more common since last year.

The fact that this can now be done through the dashboard shows that ransomware attacks are increasingly easily combining various types of threats.

The NoEscape developer was also observed looking for vulnerability researchers and penetration testers on different underground platforms. It was even found that he started looking for these people before announcing NoEscape. It was thought that the threat actor wanted to collaborate with these people and probably planned to infiltrate company networks and distribute the ransomware.

The operation affected 4 companies in the second quarter of the year. It is thought that the attacks conducted by Noescape ransomware will continue to increase in the 3rd quarter.

# Most Used CVEs by Ransomware Groups 2023/Q2 Analysis

A Study of Prevalent CVE Vulnerabilities

# 13

# Critical Vulnerabilities Analysis Over 2023/Q2

The exploitation by the Clop hacker group (aka CLOP, CL0p) leading to a series of data breaches and ransomware attacks on various organizations, including banks, federal agencies, and corporate entities, has become one of the most significant events in the cybersecurity world. These attacks were carried out by exploiting a security vulnerability in the MOVEit software.

The software has reported three critical security vulnerabilities (CVE-2023-34362, CVE-2023-35036, and CVE-2023-35708). However, the group only leveraged CVE-2023-34362 to gain unauthorized access to sensitive data. Considering the risks posed by ransomware groups exploiting security vulnerabilities like CVE-2023-34362, it is crucial to stay informed about the latest security vulnerabilities and adopt a robust cybersecurity strategy.

Brandefense Vulnerability Intelligence Service can help you stay proactive by providing immediate alerts on new exploits and community intelligence on popular CVEs and related GitHub repositories. By utilizing resources like Brandefense and implementing security best practices, you can significantly reduce the risk of falling victim to ransomware attacks and ensure the safety of your data and systems.

| 9.8 - Critical | 9.8 - Critical | 9.8 - Critical |
|---|---|---|
| MOVEIT<br>CVE-2023-34362<br>**Group** Cl0p | GoAnywhere MFT<br>CVE-2023-0669<br>**Group** Cl0p | Microsoft Exchange Servers<br>CVE-2021-26855<br>**Group** BlackCat |
| **9.8 - Critical** | **7.8 - High** | **7.8 - High** |
| PaperCut<br>CVE-2023-27350<br>**Group** Cl0p | Microsoft Exchange Servers<br>CVE-2021-26857<br>**Group** BlackCat | Micrisoft Windows Common Log File<br>CVE-2023-28252<br>**Group** Nokoyawa |
| **7.8 - High** | **5.4 - Medium** | **4.4 - Medium** |
| GoAnywhere MFT<br>CVE-2021-27065<br>**Group** BlackCat | Microsoft Windows Smart Screen<br>CVE-2022-44698<br>**Group** Magniber | Microsoft Windows Smart Screen<br>CVE-2023-24880<br>**Group** Magniber |

14

# Dipe Dive in Tactics, Techniques and Procedures

In this section, various tactics, techniques, and procedures (TTPs) used by threat actors to exploit system vulnerabilities for conducting ransomware attacks are explained. These attackers target predetermined security flaws and attempt to gain access to the system through malicious software. By leveraging remote code execution methods, they gain unauthorized access to the target system and take control of it.

Moreover, they bypass authentication mechanisms and exploit privilege escalation vulnerabilities to bypass authorization and obtain broader access rights within the system. The attackers activate the ransomware by restricting access to the data and encrypting it, then proceed to demand a ransom from the victims in exchange for recovering the data.

Ransomware attacks are becoming increasingly sophisticated, with attackers developing new methods every day. Therefore, it is essential for security experts to constantly monitor current threats and take preventive measures to patch security vulnerabilities.

## 1.TTP Bypassing Security Measures and Tampering with Security Mechanisms

**CVE-2021-27065:** Attackers can remotely access the targeted Exchange Server, execute desired code, and perform unauthorized operations on the system.

**CVE-2021-26857:** "ProxyLogon," also known as a critical security vulnerability in Microsoft Exchange Server, enables remote code execution (RCE) capability on the email server, allowing attackers to execute malicious code without authentication and take control of the server as they desire.

**CVE-2021-26855:** Attackers can infiltrate the email server in Microsoft Exchange Server's Proxy service without remote authentication and conduct phishing attacks on devices.

## 2.TTP Exploiting Vulnerabilities in Backup and Recovery Solutions

**CVE-2023-34362:** Attackers can gain access to the database through specially crafted SQL codes sent to the web application.

## 3.TTP Exploiting Remote Code Execution Vulnerabilities

**CVE-2023-28252:** It allows the attacker to gain elevated privileges that they wouldn't normally have on the device, thus bypassing the authorization that affects the system and granting them greater control and access.

## 4.TTP Bypassing Authentication and Exploiting Pre-Authentication Vulnerabilities

**CVE-2023-0669:** This vulnerability may allow an attacker to inject commands into the system without authentication. Such a vulnerability can lead to serious security risks, including unauthorized access, data theft, and even gaining full control over the system.

**CVE-2023-27350:** Attackers can bypass remote authentication and execute arbitrary code in the context of SYSTEM.

# Why digital risk protection is important?

*"Digital risk protection, attack surface management and threat intelligence are critical to organizations; because these three elements form the basis of cybersecurity defense."*

15

# Why Brandefense?

Cybercriminal organizations exploit your company's weaknesses to access sensitive information, organize phishing activities, and infiltrate your organization. With these actions, they aim to generate income or damage your reputation.

Brandefense module provides proactive protection against cyber threats by constantly monitoring potential risks to your brand, employees, executives, and customers.

- For over a decade, Brandefense has been at the forefront of the cybersecurity sector.
- We have been protecting over 600 brands since this time.
- Through our extensive experience in this field, we developed a deep understanding of cybersecurity concepts.

## How Does Brandefense Help You?

- Get continuous and real-time cyber intelligence from Dark web & Surface Web
- Minimize false-positive records by machine learning and analysts' knowledge
- Integrate your security devices like firewalls, SIEM, SOAR with incidents and intelligence indicators.

# Brandefense Solutions



### Brand and Reputation

- Data Breach Monitoring
- Malicious Domains Tracking
- Botnet Intelligence
- VIP Protection

### External Attack Surface

- Attack Surface Monitoring
- Vulnerability Intelligence
- Security Scan

### Cyber Threat Intelligence

- Dark Web Monitoring
- Recent TTP Insights
- Fraud Protection
- Strategic Intelligence

# What Brandefense Provides

**Risk-Free Exploration**
Safeguard your sensitive data and avert unauthorized access without venturing into the perilous dark web realm.

**Strategic Intelligence Power**
To avoid potential harm to your business, proactively guard against threat actors and attacks targeting your sector and region with foresight.

**Controlled Attack Surfaces**
Effortlessly assess the risks of potential attacks and new applications on our servers while keeping tabs on their ever-evolving, openly-accessible surfaces.

**Guard Against Fraud**
Detect stolen cards and alert your employees and customers to stolen information and thwart fraudulent actions carried out in your name online.

**Secure Critical Staff**
Monitor data breaches specific for who have access to important information, and protect your company's reputation by monitoring suspicious activity and fake accounts.

**Protection from CVEs**
To prevent the chain of attacks, prevent possible ransomware attacks with vulnerability intelligence that allows you to take timely action against vulnerabilities.

# Real Experiences Shared on Gartner Peer Insights »

Don't just rely on our claims; hear it straight from our satisfied customers. Delve into the authentic user reviews on Gartner Peer Insights, where our clients candidly share their experiences with our products and services. Discover how our solutions have made a real difference in their businesses, and learn why they trust and recommend us

**Very Good CTI And Brand Monitoring Source**
Brandefense acts as the backbone of our Cyber Threat Intelligence and brand monitoring activities.

*25.04.2023*

*IT Security and Risk Management*

**Very Good CTI And Brand Monitoring Source**
Brandefense acts as the backbone of our Cyber Threat Intelligence and brand monitoring activities.

*25.04.2023*

*IT Security and Risk Management*

**Intelligence Beyond The Borders**
The product helped us to mitigate our brand risk with giving us very valuable intelligence. The most I liked about Brandefense are user friendly interface, low false positive ratio, proactive use cases.

*05.04.2023*

*IT Security and Risk Management*

**User Friendly**
%90 of our users says Brandefense is very easy to use. With actionable tables and filtering you can easly track of incidents

**Budget Friendly**
Whether you have a small business or a large enterprise.
Brandefense adjusts to your budget and meets your demands.


**14-day Free Trial**
Experience Brandefense with a 14-day free trial. Try Brandefense platform with all Premium features and there are no users limit!

**24/7 Analysis Support**
Our dedicated team of Threat Intelligence Analysts are available to provide further details on incidents, analyze suspicious files, and offer additional assistance whenever needed.

See in Action :
**Request a Demo**


BRANDEFENSE

United States · 300 Delaware Ave. Ste 210 #328 Wilmington, DE 19801 / USA
Turkey · Üniversiteler Mh. 1605 Cd. Cyberpark Vakıf Binası No: B25 Çankaya/Ankara

brandefense.io · info@brandefense.io