BRANDEFENSE

RANSOMWARE TRENDS REPORT

Q3-Q4 | 2022

Methodology

Brandefense analysts identified a staggering 903 ransomware incidents in Q3-Q4/2022 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 of which is compiled into this comprehensive retrospective report on cybercrime activity around the world.

Key Insights

Ransomware has been steadily on the rise for the last quarter

The fourth quarter of 2022 saw a 33% increase in ransomware attacks compared to Q3, with the total number of attacks more than double that from Q3.

Costly damages in millions and reputation at risk

Financial losses exceeded 482 million dollars. Moral damage included slowed business development processes, unusable information if a company did not pay a ransom and tarnished reputation due to publicly published sensitive customer information.

Manufacturing: 151% spike in cyberattacks

The manufacturing sector has seen an astronomical increase of 151% in the last quarter compared with other industries making it now the most attacked industry.

Lockbit vs ~~CONTI~~: New King RISING !

Lockbit, a ransomware group, launched a bug bounty program in June 2022, where they awarded those who found vulnerabilities in their encryption software. Interestingly, the first recipient was an insider from a cybersecurity company, highlighting that threats can come from unexpected places.

903 Companies

All Around The World

12 Sector

Was Targeted By Ransomware Actors

93 Countries

Affected By Cyber Attacks

230.151 Thousand Gigabytes

Data Was Stolen

Table of Content

Statistics on Ransomware Attacks
p. 1-9

Ransomware Tactics
p. 10-14

Ransomware Overview
p. 15-18

About Brandefence
p. 19-21

Statistics on Ransomware Attacks

A Visual Breakdown of Top Targeted Countries and Sectors

01

Ransomware Attack Victims by Country: Q4 / 2022

The United States was the most targeted country in last quarter of 2022 (Q4), accounting for 40.84% of all victims. Followed by Germany with (5.08%), United Kingdom (4.40%), Canada (4.23%), Brazil (3.89%) and Australia (2.88%). Western countries are often the most targeted by ransomware attacks due to the perception that entities from such countries can afford a ransom.

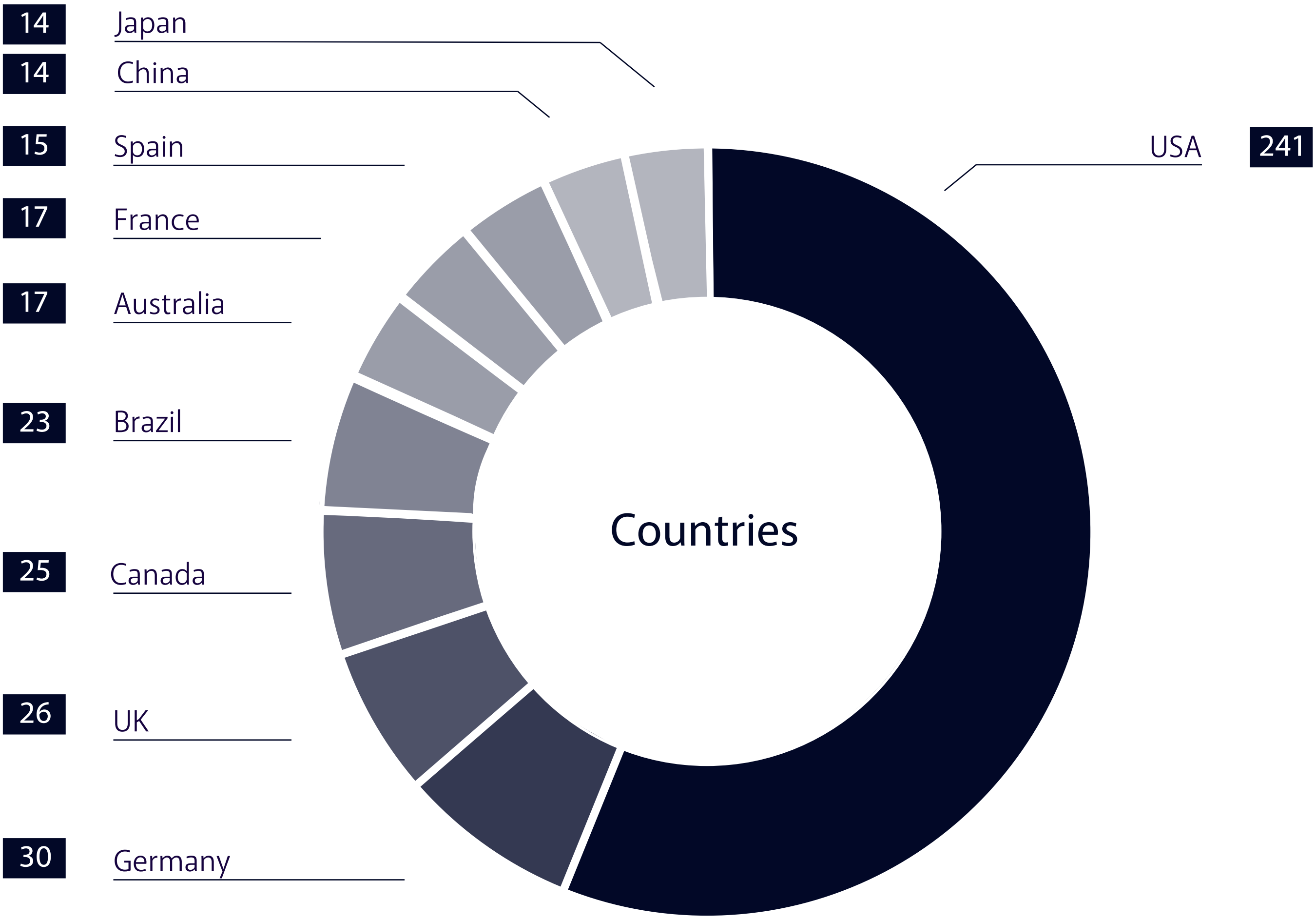


Figure 1: Attack numbers of the top 10 sectors compared to the last quarter (Q4) and previous quarter (Q3) of 2022

The United States	Germany	United Kingdom
40.84%	**5.08%**	**4.40%**

02

Ransomware Attack Percentage Increase by Country: Q3 vs Q4 / 2022

When the chart below is examined, the United States continues to maintain the leadership in Q3 and Q4. Compared to the previous quarter (Q3), the number of attacks on the United States increased by 82.57% in the last quarter. Followed by an increase of 87.5% in Germany, 70% in Australia, 30.76 in France and 23.80% in United Kingdom.

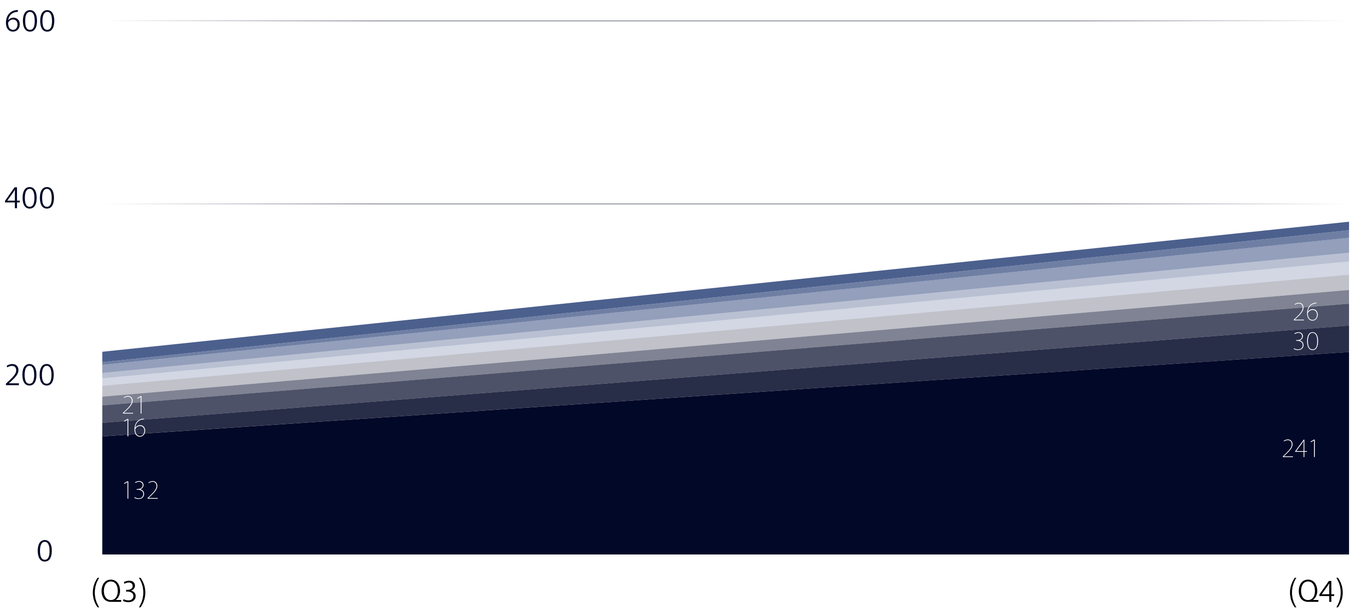


Figure 2: Attack numbers of the top 10 countries compared to the last quarter (Q4) and previous quarter (Q3) of 2022

■ United States ■ Germany ■ United Kingdom ■ Australia

■ France ■ Spain ■ China ■ Italy

■ Japan ■ Netharlands

The United States	Germany	Australia
82.57%	**87.5%**	**70%**

03

Ransomware Attack Victims by Sector: Q4 / 2022

In the last quarter of 2022 (Q4), the Manufacturing sector was the most targeted by a wide margin—accounting for 28.62% of victims—followed by the Business, professional and legal services (19.59%), Information Technology (10.56%), Education, Research and Innovation (8.51%) and Healthcare & Public Health Sector (6.81%) sectors. Like the previous quarter, industries that provide critical services were most often targeted, possibly because critical industries are considered more likely to pay a ransom to avoid costly downtime.

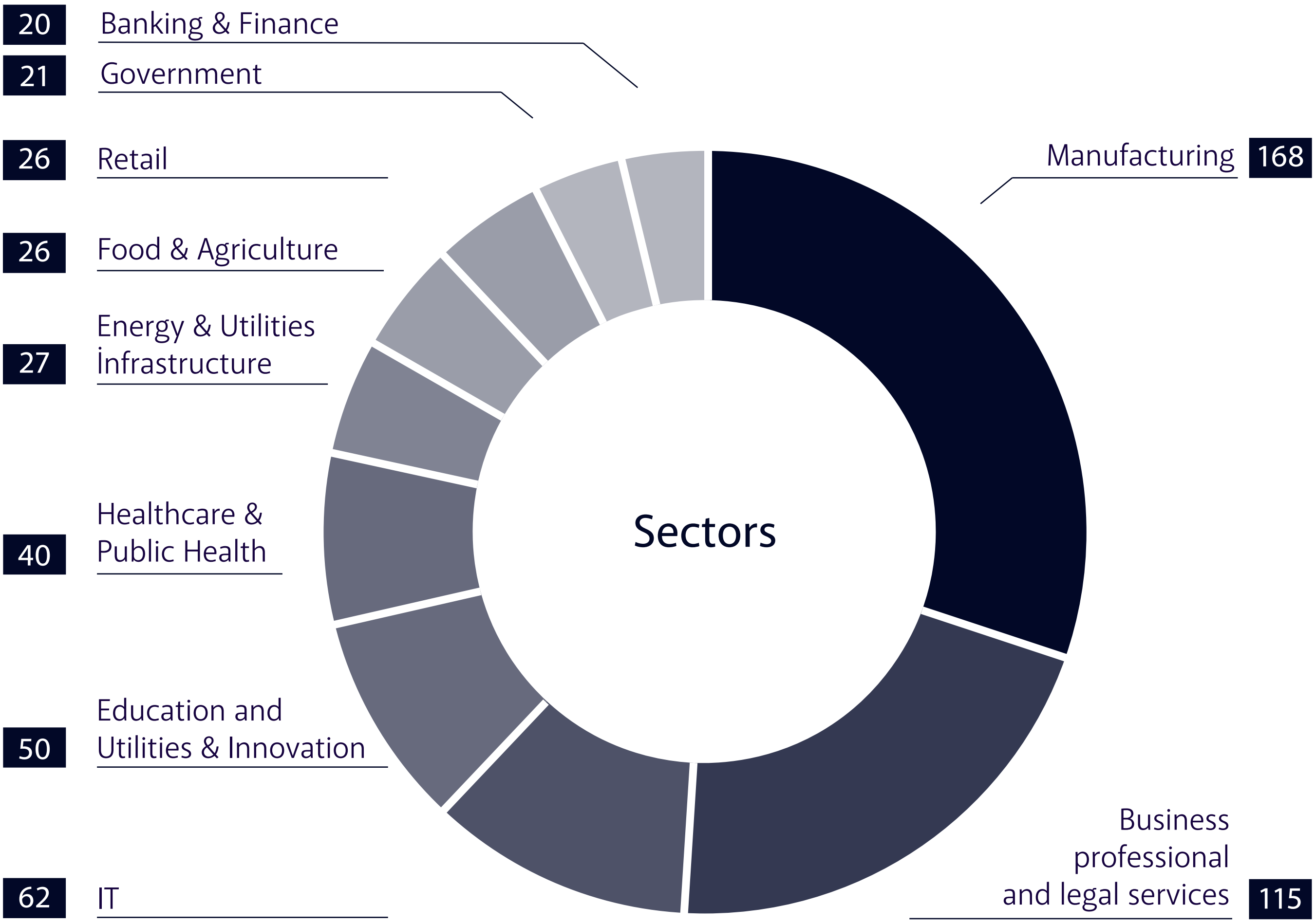


Figure 3: Number of targeted sectors by top 10 ransomware groups in the last quarter of 2022

Manufacturing	Business, Professional and Legal Services	Information Technology
26.82%	**19.59%**	**10.56%**

04

Ransomware Attack Percentage Increase by Sector: Q3 vs Q4 / 2022

When the chart below is examined, it is seen that there is an increase in all sectors. The highest increase is the Manufacturing sector with 151%. Following this, an increase is seen in the Information Technology sector with 20%, and the Education Research and Innovation sector with 106%. These increases are not surprising these days when ransomware attacks are on the rise.

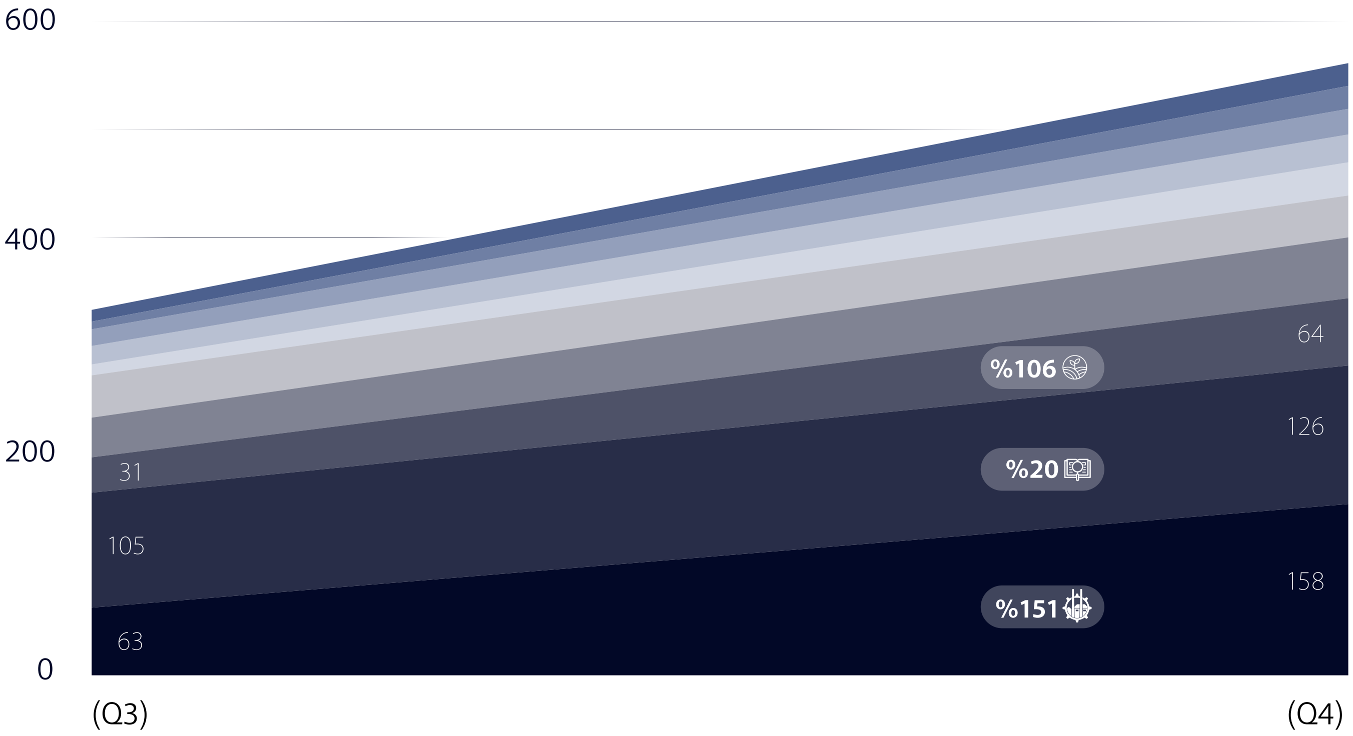


Figure 4: Comparison with Q3 & Q4 by industries

- ■ Manufacturing
- ■ Business Professionals & Legal Services
- ■ Information Technology
- ■ Education Research & Innovation
- ■ Healthcare & Public Health
- ■ Energy and Utilities Infrastructure
- ■ Food & Agriculture
- ■ Retail
- ■ Goverment
- ■ Banking & Finance

Manufacturing	Information Technology	Education Research and Innovation
151%	**20%**	**106%**

The graphic below shows the attacks received by the sectors in the last 6 months of 2022. Especially Manufacturing and Business, Professionals & Legal (such as law office, hotels, insurance companies) sectors take the biggest share of the pie. Moreover, the education, health and information technologies sectors are among the sectors most preferred by threat actors.

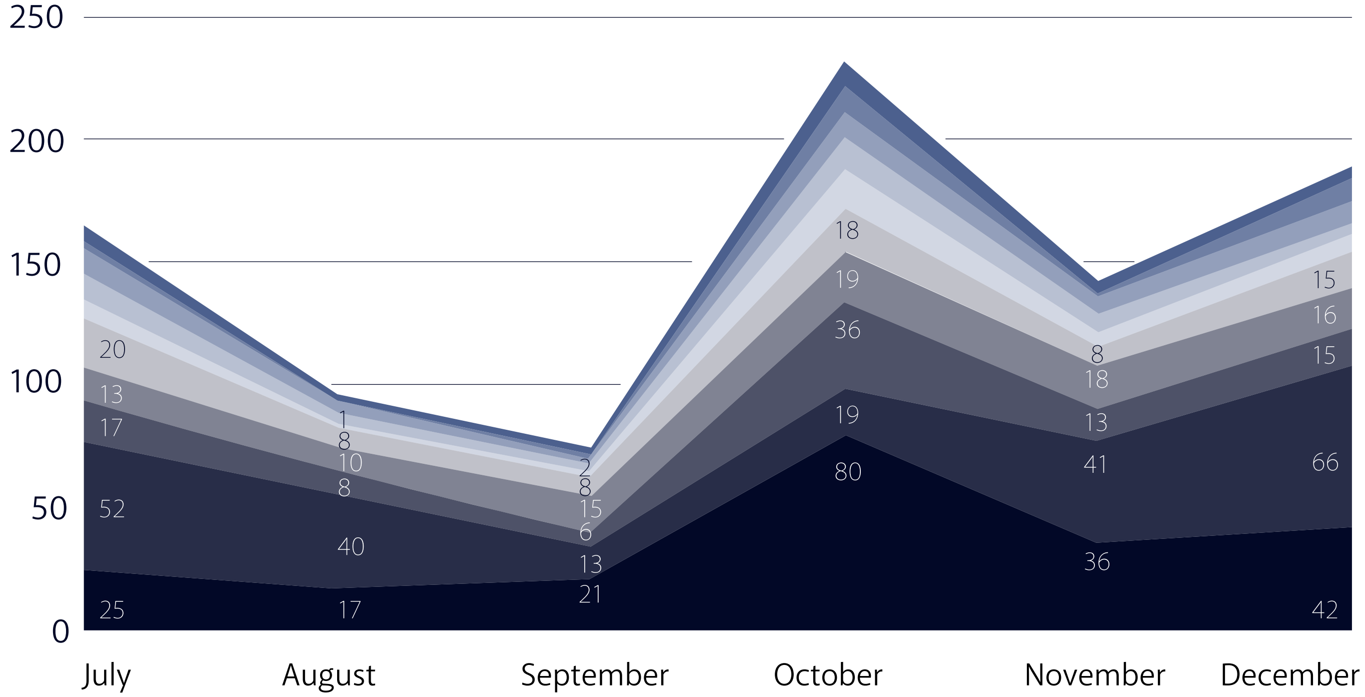


Figure 5: A comparison of the proportion of attacks by sector over a 6-month period.

Ransomware attacks increased substantially in 2022 across multiple sectors, with the manufacturing sector experiencing the highest increase at 151%. Other sectors, such as energy and utilities, manufacturing, banking and finance, and IT, also saw notable increases. But not every sector has had large attack numbers. Some sectors were less affected. Examples of these are Retail, Government, Food & Agriculture, Banking & Finance. It should not be forgotten that there is always a risk of cyber attack.

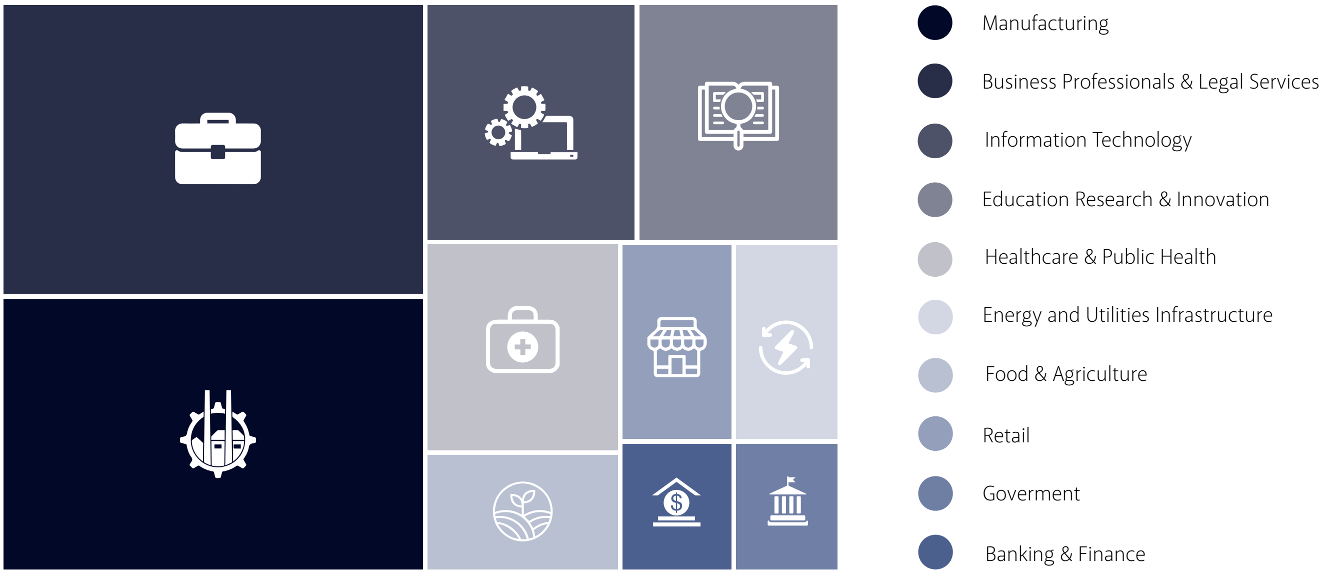


Figure 6: Proportional Overview of Ransomware Attacks by Different Industries in (Q3-Q4)

05

Number of Ransomware Attacks by Groups

When the chart below is examined, LockBit continued to maintain its lead in last quarter. According to the collected information, 160 out of 590 attacks in Q4 (October-November-December) 2022 belonged to the LockBit group, which accounted for 27.11% of all ransomware attacks. In second place were ALPHV/Blackcat with 10.58%, followed by Black Basta with 7.62%, Royal with 7.45%, Karakurt with 6.94%, and Vice Society with 5.08%.

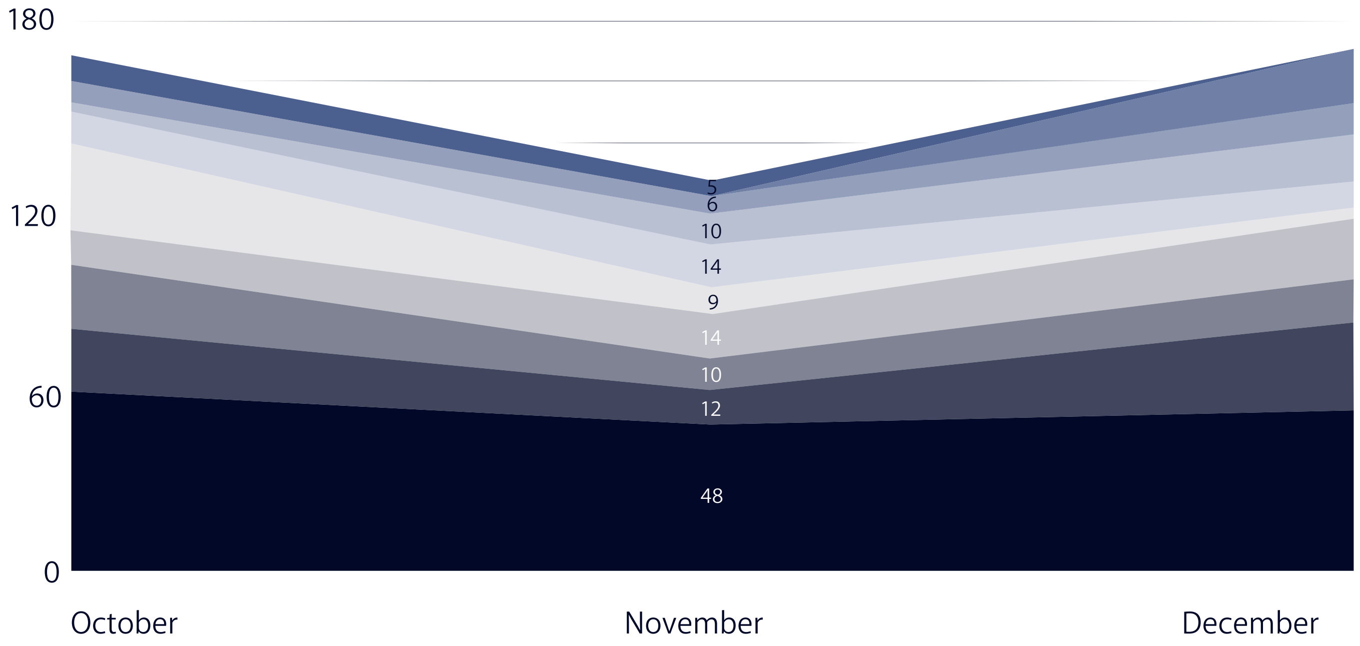


Figure 7: Number of attacks by top 10 ransomware groups in the last quarter of 2022

■ Lockbit ■ ALPHV/Blackcat ■ Black Basta ■ Royal ■ Karakurt

■ Vice Society ■ Hive ■ Snatch ■ Play ■ Black Byte

LockBit	ALPHV/Blackcat	Black Basta
27.11%	**10.58%**	**7.62%**

06

The most active Ransomware Groups

In this section, we will introduce the three most active ransomware groups in the last quarter. Our groups will be LockBit, ALPHV/Blackcat and Black Basta. We'll take a look at the past and current status of these groups. We'll examine at the sectors they attack the most and their number of attacks over time.

LockBit

The LockBit gang, previously known as ABCD, is the operator of the ransomware LockBit, LockBit 2.0, and LockBit 3.0, which was released in June 2022 as part of the group's new campaign. Their ransomware operation, first launched in 2019, has grown to be one of the most active and impactful operations. LockBit, which works as a Ransomware-as-a-Service (RaaS) model, recruits affiliates in underground forums in order to launch prolific attacks. It appears that the group only accepts to work with experienced and technically proficient affiliates.

LockBit is a financially motivated actor, and it has launched attacks on victims across different sectors, including professional services, construction, retail, manufacturing, and the public sector. While the cybercrime group is responsible for attacks around the world, the majority of its victims are located in the US, Italy and Germany. Similarly, to other ransomware groups, it appears that the LockBit ransomwares avoid targeting systems that are set in Eastern European languages.

When the attack numbers graph is examined from the graphs on the right, it is seen that the LockBit group stably keeps the attack numbers at high amounts. The most important reason for this is that it adopts the RaaS model and has about 100 employees, as they stated in an interview. Another graphic is that they mostly target the manufacturing sector. The reason for this is thought to be reaching high profit rates.

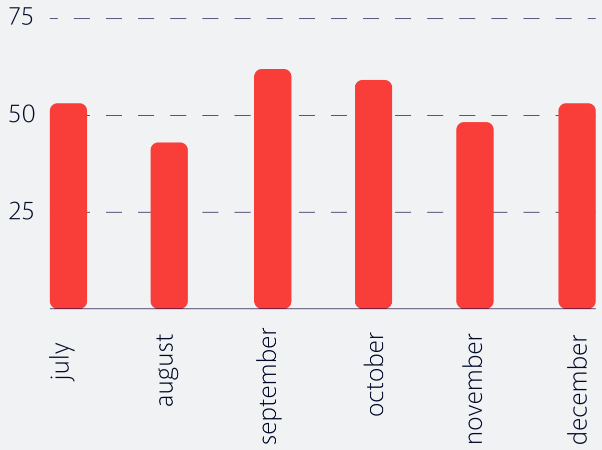


Figure 8: Monthly attack numbers for the last two quarters

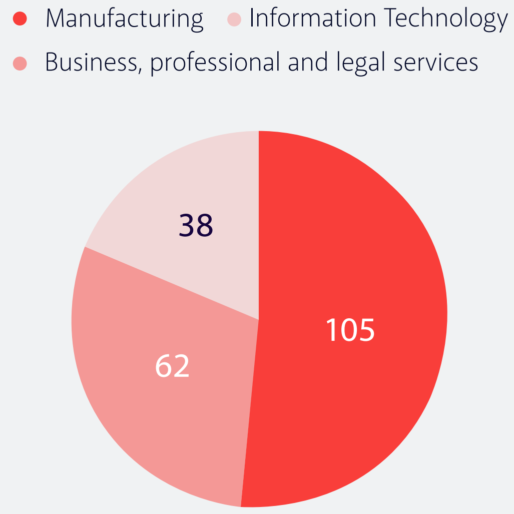


Figure 9: Attack numbers of the most attacked

ALPHV/Blackcat

ALPHV is a ransomware variant that encrypts data on infected systems and threatens to leak stolen data if the ransom payment is not made. It is highly customizable, which enables threat actors to easily tailor an attack to the target environment. ALPHV was first observed in November 2020 and is believed to be the first active ransomware coded in the Rust programming language. ALPHV is a strain of ransomware that encrypts files using AES encryption (although the process can be overridden to use ChaCha20) and demands a large ransom for their decryption. ALPHV has used Rust's cross-platform capabilities to develop both Linux and Windows variants of the ransomware. You can see that they are a dangerous group by examining the graphs below.

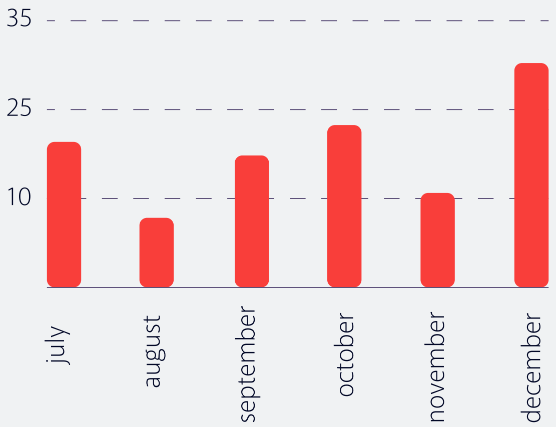


Figure 10: Monthly attack numbers for the last two quarters

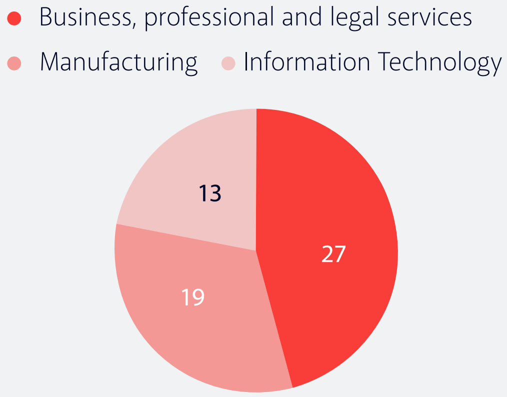


Figure 11: Attack numbers of the most attacked

Black Basta

Black Basta is a ransomware group operating as ransomware-as-a-service (RaaS) that was initially spotted in April 2022. However, evidence suggests that it has been in development since February. The Black Basta operator(s) use the double extortion technique, they also maintain a dark web leak site where they threaten to post sensitive information if an organization chooses not to pay ransom. You can see that they are a dangerous group by examining the graphs below.

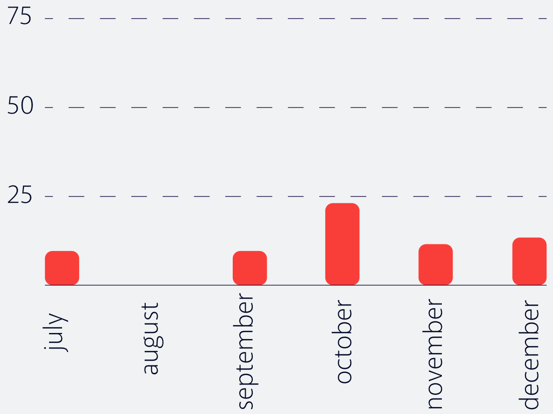


Figure 12: Monthly attack numbers for the last two quarters

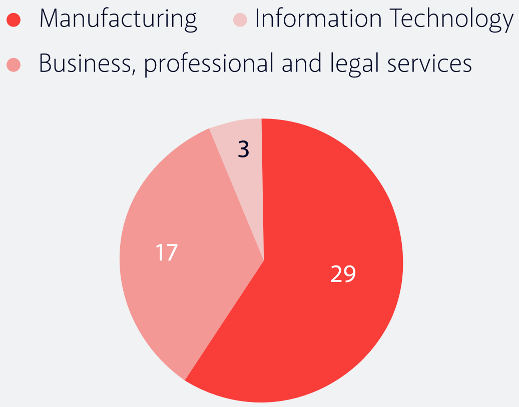


Figure 13: Attack numbers of the most attacked

Understanding Ransomware Tactics

A Study of Prevalent CVE Vulnerabilities

07

Top Critical Vulnerabilities Used by Ransomware Groups

Ransomware continues to be a significant threat to businesses and individuals worldwide, with attacks causing billions of dollars in damages every year. One of the ways that ransomware groups can infect systems is by exploiting vulnerabilities in software and systems. These vulnerabilities are often tracked and cataloged by the Common Vulnerabilities and Exposures (CVE) system, which the MITRE Corporation maintains. We will examine some of the most common CVE vulnerabilities ransomware groups use to infect systems and hold data, hostage. In addition, we will explore some of the most commonly exploited vulnerabilities and technologies and provide recommendations for protecting against ransomware attacks.

Some vulnerabilities were exploited by ransomware groups in 2022. Some of the most significant ones included:

1- Unpatched vulnerabilities in software and operating systems
Ransomware groups often target unpatched vulnerabilities, such as Windows and Linux, to gain access to the victim's systems.

2- Outdated software
Ransomware attacks often target systems running obsolete software that no longer receives security updates.

3- Weak and easily guessable passwords
Ransomware groups exploit weak or easily guessable passwords to access victims' systems.

4- Phishing attacks
Ransomware was often delivered via phishing attacks, in which victims were tricked into clicking on a link or opening an attachment that contained the ransomware.

5- Lack of backup
Many victims of ransomware attacks could not recover their files because they had not adequately backed up their data.

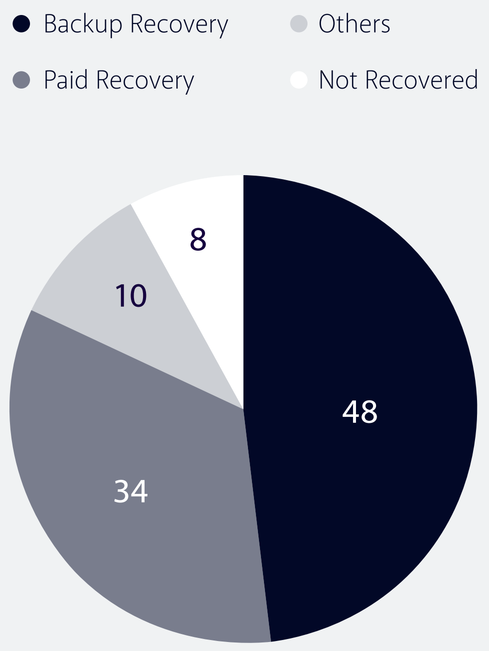


Figure 14: This chart represent ransomware recovery results according to open sources

Ransomware can infect any device, but some technologies are more commonly targeted than others. One of the most widely exploited technologies is the Windows operating system, targeted by high-profile ransomware attacks, including REvil and Conti. Other commonly used technologies include productivity software such as Microsoft Office Atlassian, virtualization software, servers, and cloud-based systems. Ransomware groups often target Remote Desktop Protocol (RDP). In a study, more than any other method, RDP vulnerabilities were exploited in nearly half of all ransomware attacks. VPNs encrypt internet traffic to protect users and can also be vulnerable to attack if they have unpatched vulnerabilities or are using outdated versions. If your business uses remote collaboration tools like RDP or VPNs, it may be at risk of cyber attacks. To protect against ransomware and other malware, it is essential to keep all of these technologies up to date with the latest patches and updates and to take additional security measures.

Pulse Secure VPN CVE-2021-22893 CVE-2020-8260 CVE-2020-8234 CVE-2019-11510 CVE-1019-11510	Citrix CVE-2020-8196 CVE-2020-8195 CVE-2019-11634 CVE-2021-22941	Microsoft Exchange CVE-2021-34523 CVE-2021-34473 CVE-2021-31207 CVE-2021-26855
Fortinet CVE-2020-12812 CVE-2019-5591 CVE-2018-13379	Sonicwall CVE-2021-20016 CVE-2020-5135 CVE-2019-7481	F5 CVE-2021-22986 CVE-2020-5902
QNAP CVE-2021-28799 CVE-2020-36198	Sophos CVE-2021-12271	Sharepoint CVE-2020-0604
Log4J CVE-2021-45046	Microsoft Windows CVE-2019-0708 CVE-2020-1472 CVE-2021-31166 CVE-2021-36942	Microsoft Office CVE-2017-0199 CVE-2017-11882 CVE-2021-40444
vCenter CVE-2021-2198	Accellion (mostly used by Cl0p) CVE-2021-2701 CVE-2021-27104 CVE-2021-27102 CVE-2021-27103	FileZen CVE-2021-20655
Atlassian CVE-2021-26084	Zoho Corp CVE-2021-40539	Microsoft Azure CVE-2021-38647

Security is an ever-burgeoning concern, and it's no surprise that the world of security vulnerabilities (CVEs) continues to grow. To provide insight into what lies ahead for cybersecurity professionals in 2022, we researched the Technology Alerts module and Tweet wall within our Brandefense Platform. It revealed Microsoft, Accelion, Citrix Pulse Secure VPN, Fortinet Sonicwall, Filezen, F5, and Log4j as some of the most sought-after CVE-related services or products this year. Though they don't make up a comprehensive collection by any means—there are plenty more options detailed in reference links via Cvss v3 score lists! —it gives everyone greater clarity over their choices when considering which route to take towards ensuring cyber safety moving forward into next year

» The most used CVEs' based on the Risk Scores

CVE-2018-13379 9.8
A path traversal vulnerability in FortiOS SSL VPN web portal allows unauthenticated attacker to download system files via specially crafted HTTP requests.

CVE-2019-0708 9.8
A remote code CVE, when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests.

CVE-2019-9510 7.8
An attacker could potentially bypass the lock screen and gain access to the session without proper authentication.

CVE-2020-0610 9.8
This CVE do not require any interaction from the user and only affects the UDP transport, which runs on UDP port 3391 by default.

CVE-2020-12812 9.8
FortiOS SSL VPN CVE. that allows a user to login without being prompted for a second factor of authentication (FortiToken).

CVE-2020-0609 9.8
This CVE do not require any interaction from the user and only affects the UDP transport, which runs on UDP port 3391 by default.

CVE-2021-21985 9.8
vCenter Server CVE. That allows a malicious actor with network access to port 443 to execute commands with unrestricted privileges.

CVE-2021-28310 7.8
Win32k Elevation of Privilege Vulnerability is a security flaw that allows an attacker to gain elevated privileges on a Windows operating system.

CVE-2021-26084 9.8
An OGNL injection vulnerability exists that allows an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance.

CVE-2021-38647 9.8
An attacker can execute operating system command as root user on OMI management endpoint by removing the authentication header, which was fixed in OMI 1.6.8-1

CVE-2021-26855 9.8
This Metasploit module allows attacker to bypass admin authentication on Microsoft Exchange Server, writing arbitrary files, and gaining Remote Code Execution (RCE)

CVE-2021-45046 9.0
Apache Log4j2's Thread Context Message and Context Lookup Patterns are vulnerable to a denial of service attack.

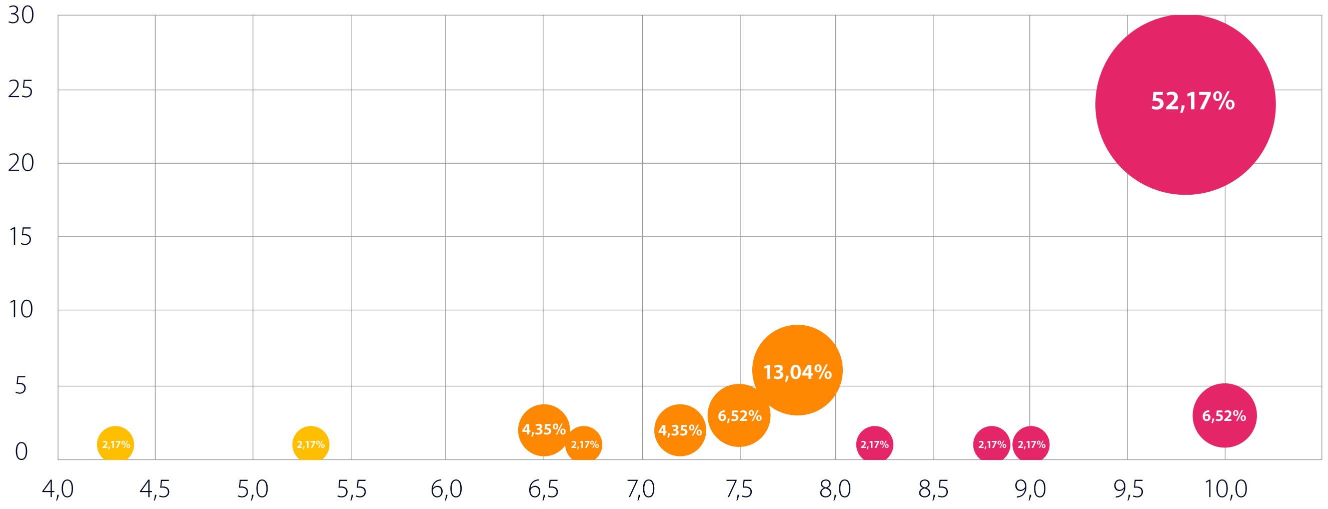


Figure 15: This chart shows risk scores by density in which the most used CVEs in 2022

You can see the CVEs grouped by risk scores below

4.3

CVE-2020-8196

5.3

CVE-2021-36942

6.5

CVE-2019-5591
CVE-2020-8195

6.7

CVE-2020-36198

7.2

CVE-2020-8260
CVE-2021-31207

7.5

CVE-2019-7481
CVE-2021-2701
CVE-2021-20655

7.8

CVE-2021-27102
CVE-2017-0199
CVE-2017-11882
CVE-2021-40444
CVE-2019-9510
CVE-2021-28310

8.2

CVE-2021-2198

8.8

CVE-2020-0604

9.0

CVE-2021-45046

10

CVE-2021-22893
CVE-2019-11510
CVE-2020-1472

9.8

CVE-2020-8234
CVE-2020-12812
CVE-2018-13379
CVE-2021-28799
CVE-2021-26084
CVE-2019-11634
CVE-2021-22941
CVE-2021-20016
CVE-2020-5135
CVE-2021-12271
CVE-2019-0708
CVE-2021-31166
CVE-2021-27104
CVE-2021-27103
CVE-2021-40539
CVE-2021-34523
CVE-2021-34473
CVE-2021-26855
CVE-2021-22986
CVE-2020-5902
CVE-2021-38647
CVE-2020-0610
CVE-2020-0609
CVE-2021-21985

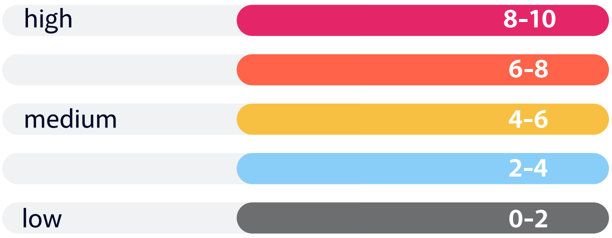


Figure 16: CVE Risk score legends by colors

» Our analysis reveals

the prevalence of high-risk CVEs in 3rd party technology usage. While malicious actors are likely to capitalize on this trend, it is interesting that medium-risk scores remain competitive when considered by density. It appears organizations need to take a holistic approach and consider more than just threat level for optimal defence strategies moving forward.

Ransomware Overview

Analysis of Impact and Important News within 6 months

08

A Summary:
The Financial Impact of Ransomware

1 Ransomware Threats: Increasing Sophistication and Intensity

Ransomware groups are a growing menace, advancing in sophistication and intensity with each passing day. Recently, they have started using ransomware to make money by working together to target people. They force these victims to pay a ransom or lose important information. Hospitals have become particularly vulnerable targets, culminating in one reported case of patient death due to an attack this past year alone. With such consequences at stake, security professionals remain vigilant against these cyber threats that threaten our safety on multiple fronts.

2 Ransomware Surge in 2022: Hospitals, Schools, Defence Industry Companies and Critical Infrastructure Facilities Under Attack

In the last six months of 2022, Brandefense identified a surge in attacks on hospitals, schools, defence industry companies and other critical infrastructure facilities. We have recorded 903 cases and detected over 30 ransomware groups, notably Conti, which caused significant damage to the sector until LockBit superseded it. Over 230 thousand Gigabytes of data were stolen during this period, consisting mainly of invaluable R&D documents and employee personal information demanding ransoms totalling 482 million dollars or more from some victims.

3 Ransomware Attacks on Western Countries Reaches 93 with Manufacturing Sector as Top Target

Our CTI analysts have identified 93 countries targeted by ransomware groups, primarily in the western world. According to our observations from the deep web and the dark web, the Manufacturing sector was hit hardest, with 221 malicious attacks resulting from these threats, representing a 24.61% share of all reported impacts over the last two quarters. Several other sectors also experienced damage - Business and Professional services (25.72%), Information Technology (10.57%), and Education & Research/Innovation & Healthcare/Public Health were not far behind with 10.13% and 8.5%, respectively; LockBit group attributed to most of those incidents followed closely by ALPHV / Blackcat, Royal, Black Basta Karakurt Vice Society Hive Group.

4 Consequences and Prevention

Companies faced extensive losses of not only financial but also moral destruction. Business operations nearly halted as their sensitive data was held hostage and published for the public, ultimately damaging their reputation. Tragically, ransomware attacks made history when one resulted in a fatality – emphasizing why organizations must heed warnings by implementing regular backups systems with proactive defence measures against these malicious actors who plague our digital world.

09

Q3 and Q4 Important Ransomware News

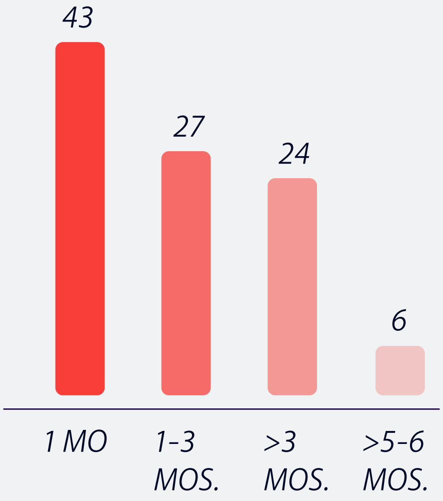
Over time, the number of ransomware groups increased, their attacks became more sophisticated and professional, and as a result, more destructive cyber attacks began to occur. And naturally, these events started to be reflected in the news headlines. And as Brandefense Analysts, we have selected the most important of these news headlines for you.

%62

Organization paid the ransom

%17

Organization paid more than once



01

LAPSUS$

LAPSUS$ exfiltrates confidential data from breached organizations and then threatens to leak or disclose data if the demanded ransom was not paid. The first target of LAPSUS$ was Nvidia. After that, they targeted big companies such as Microsoft, Octa, Samsung and leaked very critical information specific to companies.

02

LockBit does not target Russia and some nearby countries

When LockBit malware was examined, it was determined that it did not target countries such as Russia, Azerbaijan, Kazakhstan, Tajikistan, Uzbekistan and Kyrgyzstan. This information also supported that LockBit is a pro-Russian group.

03

LockBit vs Entrust

One day, LockBit announced on their homepage that they were targeting a firm called Entrust. Immediately after this incident, a DDos attack started on LockBit servers. In the message part of the attack, there was the phrase "DELETE_ENTRUSTCOM_MOTHER****ERS". It is not yet known whether this event was actually made by Entrust.

04

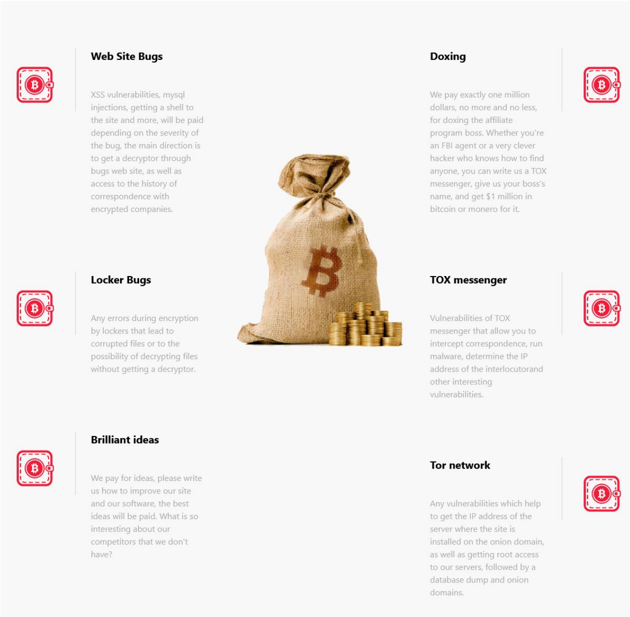
LockBit introduces the first ransomware bug bounty program

With the release of LockBit 3.0, the operation has introduced the first bug bounty program offered by a ransomware gang, asking security researches to submit bug reports in return for rewards ranging between $1000 and $1 million. Furthermore, LockBit is not only offering bounties for rewards on vulnerabilities but is also paying bounties for "brilliant ideas" on improving the ransomware operation and for doxing the affiliate program manager.

05

Attack on critical systems

On august 15, the Clop ransomware group announced on their leak website the breach of South Staffordshire Water, a privately owned UK water supply company. This news was of great value because threat actors claimed they could change the amounts of chemicals added to the water.



Web Site Bugs

XSS vulnerabilities, mysql injections, getting a shell to the site and more, will be paid depending on the severity of the bug, the main direction is to get a decryptor through bugs web site, as well as access to the history of correspondence with encrypted companies.

Locker Bugs

Any errors during encryption by lockers that lead to corrupted files or to the possibility of decrypting files without getting a decryptor.

Brilliant ideas

We pay for ideas, please write us how to improve our site and our software, the best ideas will be paid. What is so interesting about our competitors that we don't have?

Doxing

We pay exactly one million dollars, no more and no less, for doxing the affiliate program boss. Whether you're an FBI agent or a very clever hacker who knows how to find anyone, you can write us a TOX messenger, give us your boss's name, and get $1 million in bitcoin or monero for it.

TOX messenger

Vulnerabilities of TOX messenger that allow you to intercept correspondence, run malware, determine the IP address of the interlocutorand other interesting vulnerabilities.

Tor network

Any vulnerabilities which help to get the IP address of the server where the site is installed on the onion domain, as well as getting root access to our servers, followed by a database dump and onion domains.

06

Interview with LockBit ransomware gang

A person claiming to be the Lockbit founder answered some questions from the vx-underground team. In this interview, he explained that the LockBit manager has a total of 100 employees in the group, money laundering is not difficult at all, they do a lucrative business and he resides in Russia and has never been caught.

07

LockBit first bug bounty payment

We previously announced that the lockbit ransomware group has launched a bug bounty program. They announced that they paid their first prize of $50,000 as part of this program. They gave this award to anyone who found a vulnerability in their encryption program. The important thing here is that the person they gave the award was working for an anti-ransomware company.

About Brandefense

Brandefense is a cloud-based platform that protects businesses from digital risks by detecting vulnerabilities, staying updated on attack vectors, and preventing reputation damage by monitoring brand-related information.

It helps you maintain a comprehensive security strategy, minimising the risks of data loss or privacy breaches by performing regular attack surface exploration, delivering relevant IOCs to SIEM and SOAR systems, and following news related to user accounts and brand activity.

10

Why Brandefense?

- For over a decade, Brandefense has been at the forefront of the cybersecurity industry.
- We have been protecting over 300 brands and organizations since this time.
- To raise awareness about cyber security, We organize events such as Hacktrick and Hacknights every year.
- 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 Darkweb & Surface Web
- ✓ Minimize false-positive records by machine learning and analysts' power
- ✓ Integrate data to your SIEM with API or Stix/TAXII server

Learn more

www.brandefense.io

Follow us on

» Uncover the Benefits of Our Solution

› Don't let your attack surface grow out of control

Exposure

- Keep track of every IP address connected to you
- Ensure all ports are properly secured
- Monitor DNS activity & SSL certifications

Learn More

› Can't track underground communication? We can.

Brand & Reputation Protection

- Get alerted when sensitive data is shared among hackers.
- Prevent corporate data leaks before they happen.
- Keep your company's confidential information safe and secure.

Learn More

› Worried about the safety of your data?

Intelligence

- Get alerted to security incidents in your organization
- Stay informed of the latest vulnerabilities, exploits, and fraud methods
- Detect credit card fraud in near real-time.

Learn More

Don’t forget to share this report!

Start a free trial today

BRANDEFENSE

BRANDEFENSE

United States • 300 Delaware Ave. Ste 210 #328 Wilmington, DE 19801 / USA
Turkey • Üniversiteler Neighborhood, 1605.Road, Door No:3/1, Apartment No: 204,
Çankaya/Ankara - 06800

brandefense.io · sales@brandefense.io