cyberthint

RANSOMWARE REPORT

JANUARY

2024 JANUARY

PREPARED BY CYBERTHINT THREAT HUNTERS

CYBERTHINT.IO

Table of Contents

Introduction

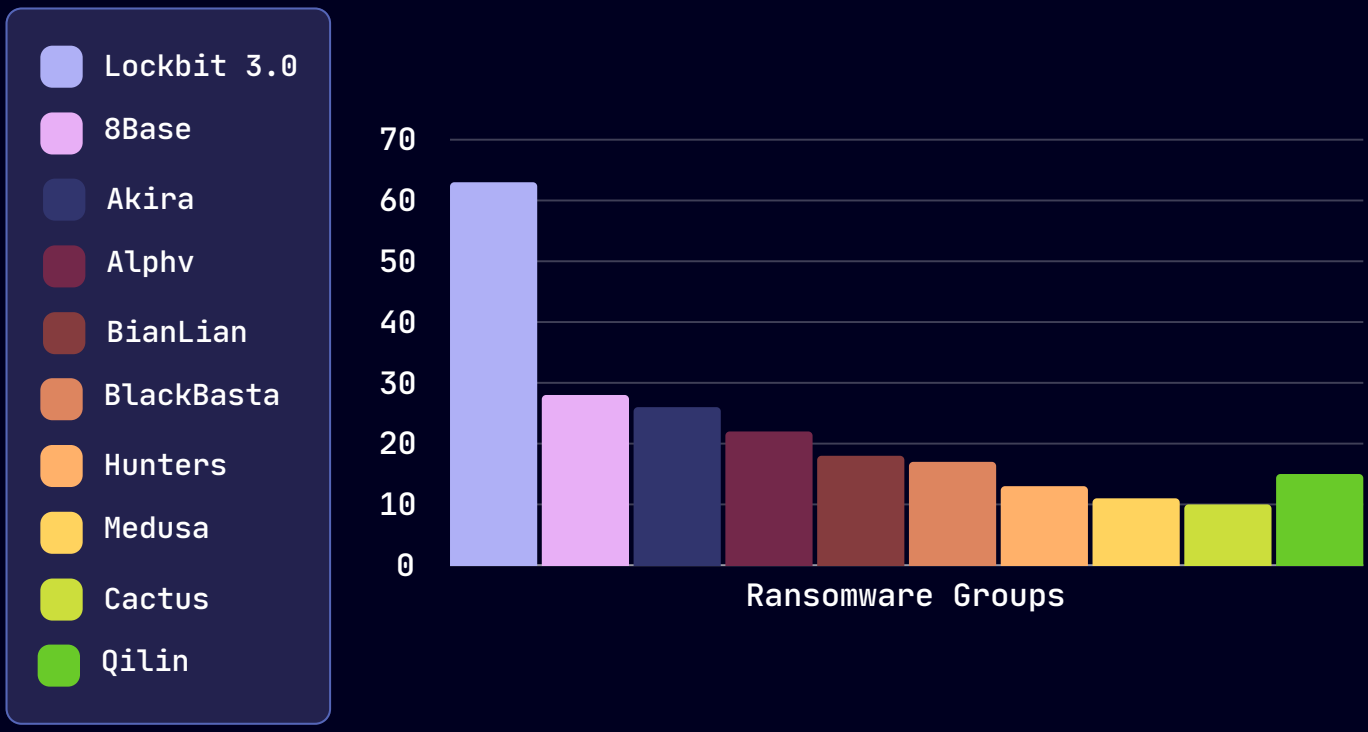
Welcome to Cyberthint's monthly Ransomware Tracking report, a compilation of statistical data gathered as Cyberthint threat hunters closely monitor the activity and behavior of ransomware groups.

Cyberthint threat hunters use the following six-point methodology when tracking ransomware groups on the Darkweb.

#	Ransomware Tracking Methodology
1.	**Collecting Data Sources:** We collect all data from sources related to ransomware groups operating on the Darkweb.
2.	**Data Analysis and Classification:** We analyze the data collected from the related sources and classify them according to ransomware groups.
3.	**Examination of Distribution Methods:** We analyze the distribution methods and strategies of ransomware groups using the available data that we have.
4.	**Monitoring Ransomware Campaigns:** By tracking large-scale ransomware campaigns, we observe changes in strategies adopted by ransomware groups.
5.	**Monitoring Ransom Payments:** We track crypto wallets that we have identified as belonging to ransomware groups and in this way, we can predict the sectors and countries they may target in the future.
6.	**Protection and Recommendations:** Based on the data and statistics collected and analyzed during Ransomware Tracking, we identify measures to safeguard against these attacks.

Most Active Ransomware Groups

Cyberthint threat hunters have identified the top 10 ransomware groups that made the most attacks in December as a result of the data they collected. This data is sourced from victim announcements shared on the groups' Darkweb websites, and attacks not announced on these sites are not included in this analysis.



Ransomware Attacks Decreased in December

Ransomware attacks decreased by 13% compared to December. A total of 315 ransomware attacks were recorded in January.

Lockbit Decreased the Number of Victims

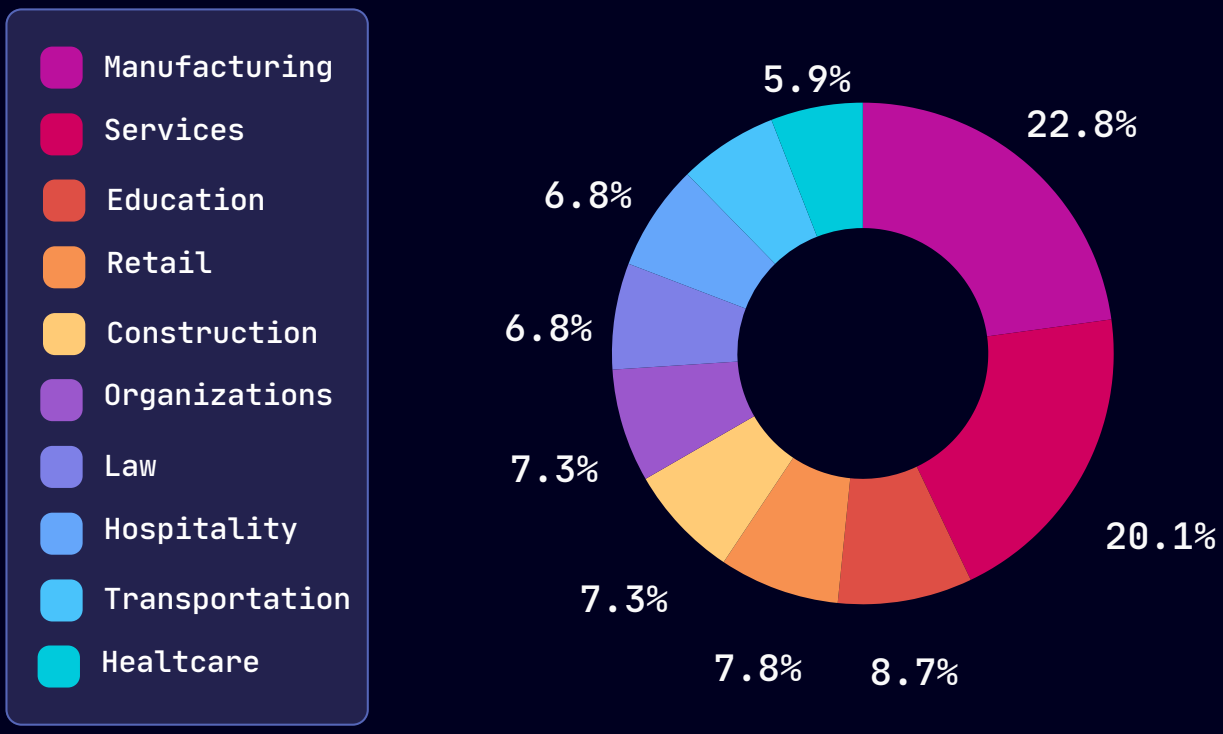
The number of victims of the Lockbit ransomware group decreased by 24% compared to December.

Alphv Decreased the Number of Victims

The number of victims of the Alphv ransomware group decreased by 40% compared to December.

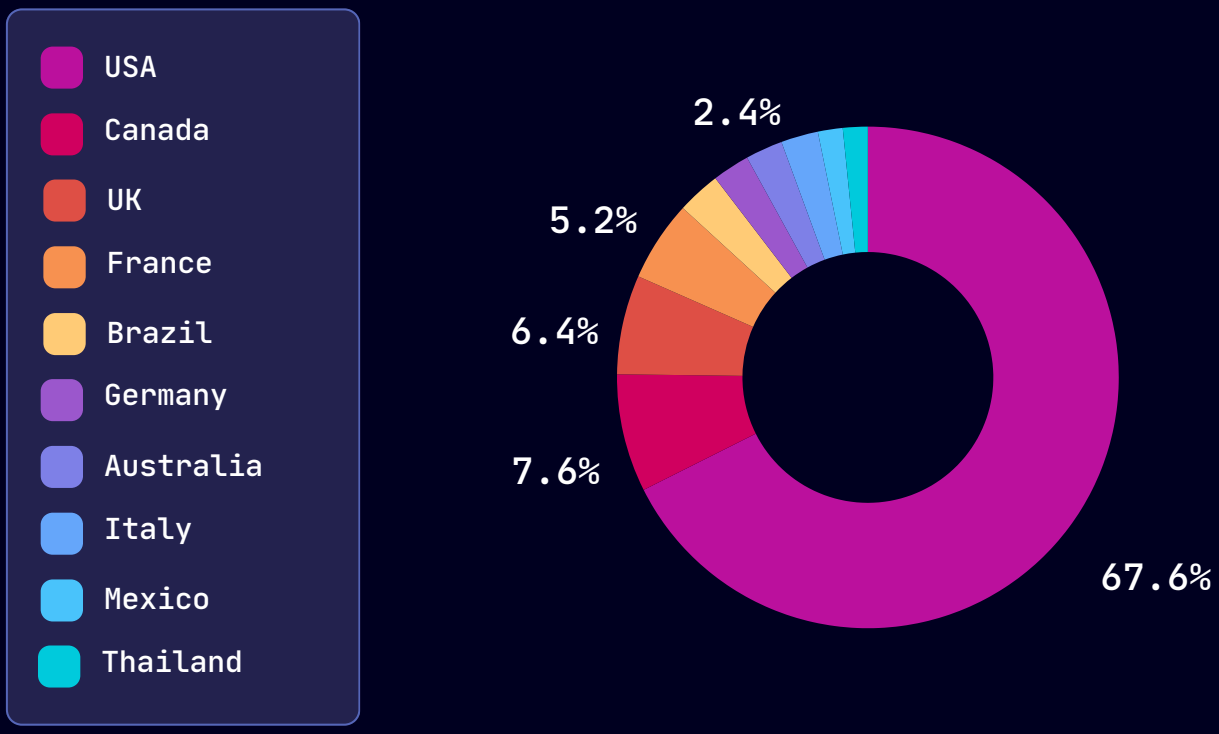
Sectors Most Affected by Ransomware Attacks

Cyberthint threat hunters have identified based on the collected data the sectors most targeted by ransomware attacks in December. This data is derived from victim announcements posted by ransomware groups on their own websites on the darkweb, and does not include attacks that they did not announce on their websites.



Countries Most Affected by Ransomware Attacks

Cyberthint threat hunters collected data to identify the countries that suffered the most ransomware attacks in December. This data is derived from victim announcements posted by ransomware groups on their own websites on the darkweb, and does not include attacks they did not announce on their websites.



Ransomware Operators Exploit TeamViewer

Ransomware operators continue to use TeamViewer to gain first access to their victims' devices. Security experts have found that TeamViewer, the popular remote access tool, is still being used by actors carrying out ransomware attacks to intrude into organizations' endpoints. A similar incident had happened in 2016. It was revealed after victims reported on various forums that their devices had been breached using TeamViewer and files had been encrypted with Surprise ransomware. At the time, TeamViewer's statement about the unauthorized access was that the attack was carried out using leaked credentials of users. In other words, the attackers had not exploited a zero-day in the software.

In a statement shared with BleepingComputer about the incident, TeamViewer said: "Our analysis shows that most instances of unauthorized access involve a weakening of TeamViewer's default security settings. This often includes the use of easily guessable passwords which is only possible by using an outdated version of our product. We constantly emphasize the importance of maintaining strong security practices, such as using complex passwords, two-factor-authentication, allow-lists, and regular updates to the latest software versions. These steps are critical in safeguarding against unauthorized access."

KCATA Hit by Ransomware Attack

The Kansas City Area Transportation Authority (KCATA) was hit by a ransomware attack by the Medusa ransomware group on Tuesday, January 23. A day after the attack, the company announced that it had suffered a ransomware attack that affected all of its communications systems. "A ransom cyber-attack hit the KCATA early Tuesday, January 23. We have contacted all appropriate authorities, including the FBI," the company said, without disclosing information about the ransomware family that compromised its systems or whether there was a data breach.

The Medusa ransomware group claimed responsibility for the attack on KCATA on January 26 and posted data samples allegedly belonging to the company on the dark web leak site. The ransomware group threatens to release all stolen data if the company does not pay the $2 million ransom.

loanDepot Hit by Ransomware Attack

loanDepot, a major US mortgage lender, was hit by a ransomware attack in early January. The company had to shut down some IT systems to contain the breach. The company said in a statement that they were victims of a ransomware attack and that threat actors were able to successfully encrypt files on the compromised systems. The company did not directly comment on the details of the compromised data, but said, "Although its investigation is ongoing, the Company has determined that an unauthorized third party gained access to sensitive personal information of approximately 16.6 million individuals in its systems."

The company has set up a website to inform its customers, partners and employees about the cyber incident, where it is sharing updates on developments related to the cyber incident.

Ways to Prevent Ransomware Attacks

1. **Use Strong Passwords:** Create complex, long and unique passwords for each account.
2. **Don't Ignore Software Updates:** Regularly update the operating system, applications, services and antivirus programs.
3. **Use Antivirus and Security Software:** Regularly scan your system for malware using reliable antivirus software.
4. **Beware of Emails:** Avoid clicking on suspicious email attachments or links.
5. **Secure File Sharing:** Share your files using trusted and secure sharing platforms.
6. **Backup Data:** Back up all your important data regularly. Also pay attention to the security of the backup.
7. **Training and Awareness:** Educate yourself and your employees about ransomware and cyber threats.
8. **Use Advanced Authentication:** Increase the protection level of your accounts by taking additional security measures such as two-factor authentication.
9. **Network Security:** Protect your network using firewalls, network monitoring and security solutions.
10. **Malware Protection:** Take effective measures to detect and block malware that may be come via email, web and other means.
11. **Application Permissions:** Do not give unnecessary permissions to applications and files. You can defend against attacks by restricting permissions you don't need.
12. **Download from Trusted Sources:** Download software and applications only from official and trusted sources. Stay away from pirated or suspicious sources.

Checklist During a Ransomware Attack

1. Isolate Infected Systems: Immediately isolate affected systems from the network to prevent the ransomware from spreading further.

2. Alert Management: Notify relevant stakeholders, including management, legal, and IT teams, about the attack.

3. Gather Information: Document all available information about the attack, including the ransom note, malware samples, and affected systems.

4. Engage Incident Response Team: If available, involve your incident response team to lead the investigation and recovery efforts.

5. Assessment: Determine the scope and impact of the attack on your systems and data.

6. Containment: Identify the ransomware variant and apply appropriate measures to contain the attack, such as disabling compromised accounts or network segments.

7. Data Backup Check: Verify the integrity of your data backups to ensure they are not compromised. Use clean backup data for recovery.

8. Communication Plan: Develop a communication plan for informing employees, customers, and partners about the situation, while adhering to legal and regulatory requirements.

9. Malware Analysis: Conduct analysis on the ransomware to understand its behavior, possible decryption methods, and potential vulnerabilities.

10. Engage Law Enforcement: If necessary, involve law enforcement agencies and share relevant information with them.

11. Recovery Strategy: Develop a recovery strategy based on the nature of the attack, whether it's possible to decrypt files, or if you need to rebuild systems from scratch.

12. Negotiation Consideration: Evaluate the risks and benefits of negotiating with the attackers for decryption keys. This is a complex decision with legal and ethical considerations.

13. User Education: Reinforce user education on cybersecurity practices to prevent future attacks.

14. Patch and Update: Identify and patch vulnerabilities that were exploited to deliver the ransomware.

15. Monitor and Analyze: Continuously monitor for signs of the ransomware reactivating or any new vulnerabilities being exploited.

16. Forensics: Conduct a thorough forensic analysis to understand how the attack occurred and whether any data was exfiltrated.

17. Post-Incident Review: After the attack is contained, conduct a review of the incident response process to identify areas for improvement.

18. Risk Mitigation: Implement security measures to prevent similar attacks in the future, such as endpoint detection and response (EDR) solutions, email filtering, and user training.

How Cyberthint Can Help You To Prevent Ransomware Attacks

Data Leakage Monitoring

It regularly inspects whether there is a data leak related to your organization. If it detects anything, it notifies you.

Attack Surface Detection

Every asset open to the internet is a potential attack point. Cyberthint detects them for you and notifies you of potential breach points.

Vulnerability Intelligence

It notifies you about the vulnerabilities detected by regular vulnerability scans with its solutions.

Brand Monitoring

It detects potential phishing attacks on you and your employees by impersonating your organization in advance and takedown the impersonated/fake; domain name/social media account before the attack can be made.

We know what information hackers have on you!

Cyberthint is an unified cyber threat intelligence platform that allows you to take precautions against cyber threats that may affect your company and employees in cyberspace.

Be aware of cyber threats targeting your organization in advance with Cyberthint's advanced cyber threat intelligence technology!

With Cyberthint, you can monitor and identify advanced threats and take early action.

Follow Us Cyberthint.io Cyberthint Cyberthint Cyberthint