ECHO

CYBER THREAT INTELLIGENCE

2023 ATTACK REPORT

Ransomware Attacks in 2023

Prepared by
EchoCTI Team

@echocti @echocti echocti.com

Contents

Executive Summary

Ransomware is a type of malicious software that infiltrates computer systems and encrypts files or blocks access. They usually demand a ransom to unlock files or systems.

They target individual users as well as corporate networks, government systems, healthcare and financial institutions. This malware usually infects systems using email attachments, malicious websites or security vulnerabilities over the Internet.

By encrypting files or blocking system access, ransomware can stop the normal functioning of organisations and cause serious financial damage. In addition, such attacks also damage the reputation of organisations.

This report can help organisations review their security policies and close security gaps by explaining to managers and relevant stakeholders the nature and impact of ransomware and the precautions that can be taken. At the same time, by highlighting the potential dangers of ransomware, this report aims to help organisations operate in a more secure environment.

Ransomwares in 2023

The rising impact of ransomware continued in 2023. This year, ransomware spread globally, causing serious impacts in various countries and sectors.

Targeted Countries

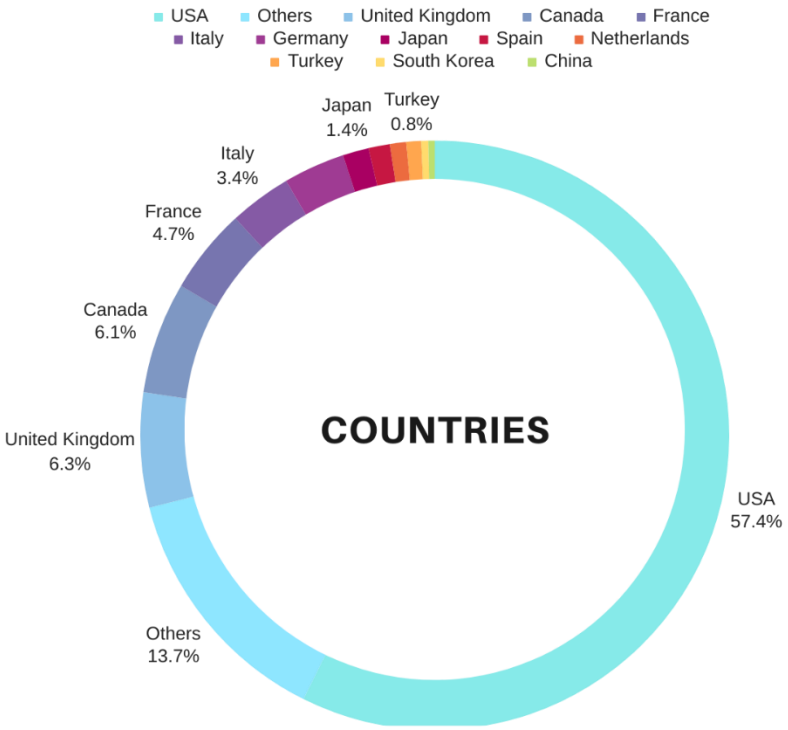

Figure 1 Targeted Country by Ransomwares

Ransomware had widespread effects around the world in 2023. Looking at the number of infected systems, the US is the most affected country with 1478 systems. The United Kingdom, Canada and Germany followed with 162, 158 and 87 infected systems, respectively.

On the other hand, China was affected at lower levels with 9, South Korea 10 and Turkey 21 infected systems. Italy 88, France 121, Spain 30, the Netherlands 23 and Japan 37 were among the other countries affected by ransomware.

This data shows that ransomware has geographically varying levels of impact and is particularly concentrated in certain countries.

Target Sectors

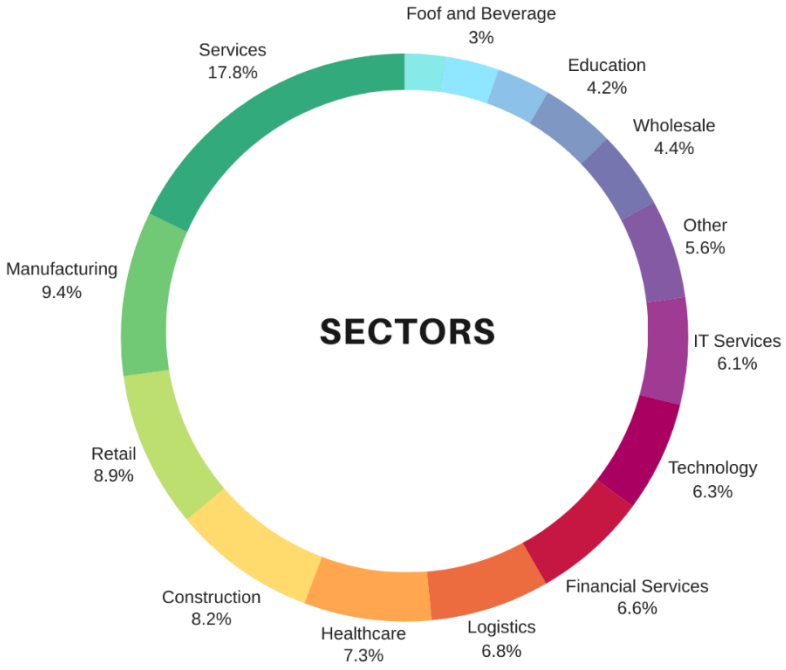

Figure 2 Target Sectors

This data shows that ransomware poses a threat to a wide range of industries. Different sectors are affected at different levels in terms of the number of attacks and these attacks pose a serious threat in various industries.

The Most Effective Ransomware Families

Ransomware has become one of the most serious threats of the digital world in 2023. The sophisticated and complex nature of this software can target organisations and individuals, causing data loss and financial damage. In particular, certain ransomware families are known for targeted and systematic attacks. Ransomware families such as LockBit, BlackCat and Clop often demand large ransoms by managing to overcome the defence mechanisms of organisations. These attacks usually consist of manually managed and targeted actions, causing financial losses and reputational damage to organisations.

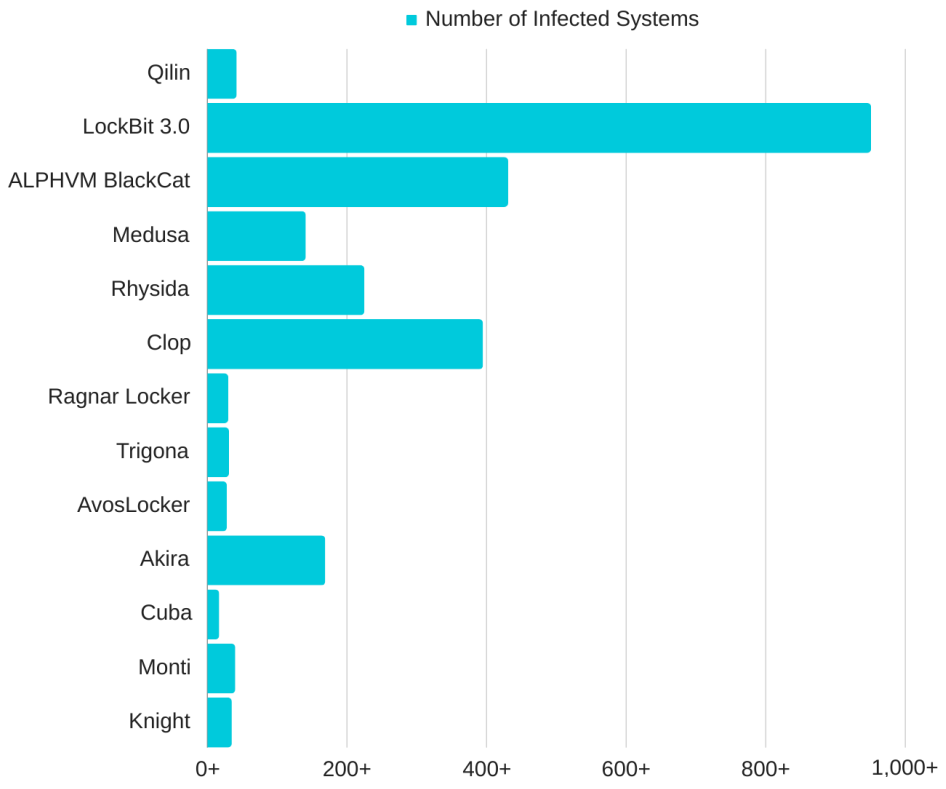

Figure 3 Number of Infected Systems

LockBit

LockBit 3.0 has been an extremely dangerous member among ransomware families since its first appearance in 2019. As such, it poses a serious cybersecurity threat to many organisations around the world. LockBit works by encrypting data on victim systems and then demands a ransom in exchange for the decryption of the data. However, LockBit 3.0 not only encrypts data, but also coerces victims with the threat of publishing this data online, which damages the reputation and credibility of organisations. LockBit 3.0 uses highly sophisticated encryption algorithms when deployed on victim's systems. This makes data extremely difficult to decrypt and forces victims to pay a ransom. The ransom is usually paid in cryptocurrencies, so it can be impossible to trace the ransom paid. For more information about the LockBit Ransomware Family, see also.

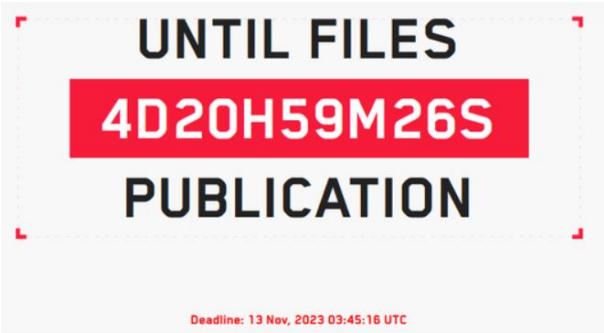

Figure 4 Stopwatch of LockBit 3.0

BlackCat

ALPHV, also known as BlackCat or Noberus, is a family of ransomware distributed as part of Ransomware as a Service (RaaS) operations. ALPHV is written in the Rust programming language and supports running on Windows, Linux-based operating systems (Debian, Ubuntu, ReadyNAS, Synology) and VMWare ESXi. ALPHV is marketed as ALPHV in cybercrime forums, but is often referred to as BlackCat by security researchers due to a black cat icon appearing on the leak site. ALPHV has been observed to be used in ransomware attacks since 18 November 2021.

CLOP

Clop is a ransomware that uses the ".clop" extension after encrypting the victim's files. Another unique feature of Clop is the string: "Dont Worry C|0P" is included in the ransom notes. It is a variant of CryptoMix ransomware, but attempts to disable Windows Defender and remove Microsoft Security Essentials to avoid user-space detection.

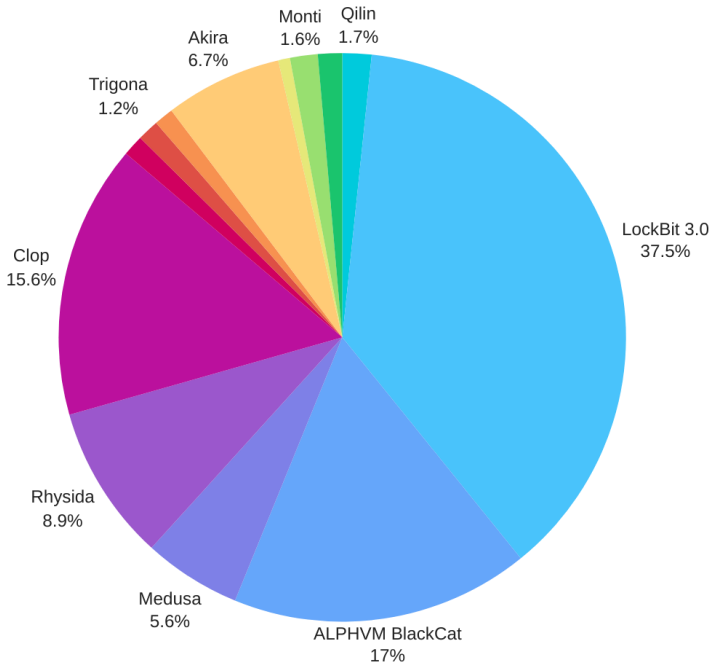

Figure 5 Rate of effects of Ransomware Families

Most Used Infiltration Techniques (Initial Access)

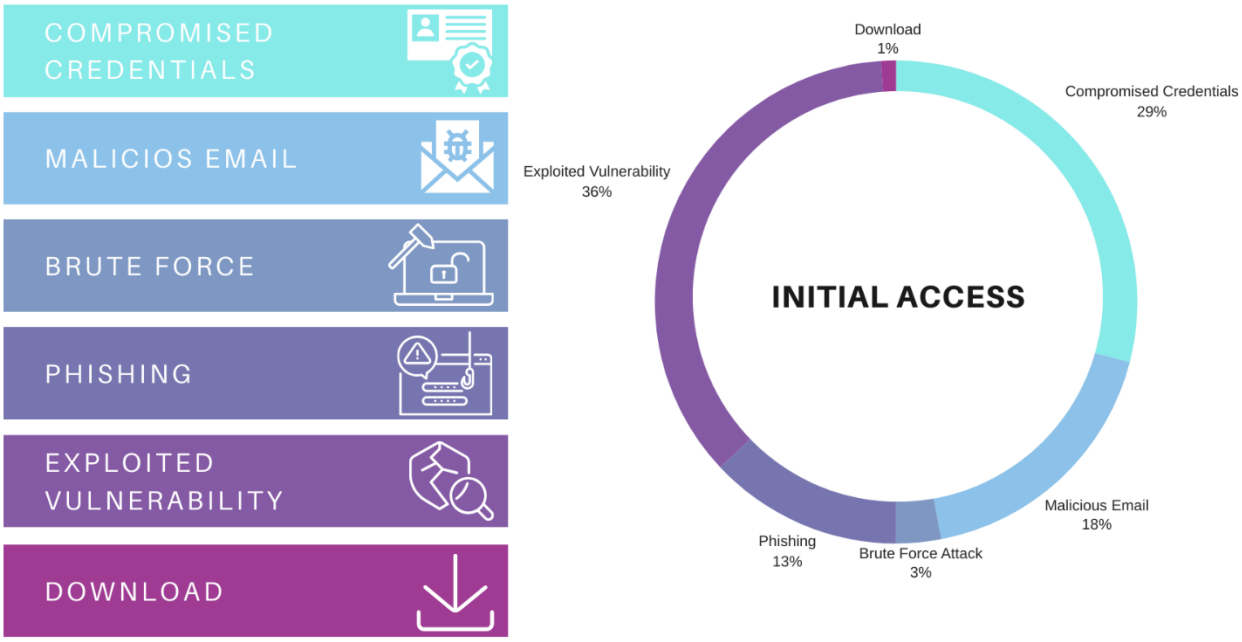

Figure 6 Most Initial Access Methods

Various infiltration techniques used in ransomware infections showed different levels of impact in 2023. Among the most preferred techniques, "Exploited Vulnerability" (36 attacks) stood out as a common method to infiltrate the system by targeting and exploiting vulnerabilities in systems infected by ransomware. With this technique, attackers usually try to spread ransomware by exploiting software or application vulnerabilities.

In addition, "Compromised Credentials" (29 attacks), i.e. compromised credentials, was another common technique used by attackers to gain unauthorised access to target systems. Attacks via "Malicious Email" (18 attacks) included phishing attacks, which usually attempt to spread ransomware by misleading users or through malicious attachments. "Phishing" (13 attacks) and "Brute Force Attack" (3 attacks) were among the other common techniques used to infiltrate the system by taking advantage of users' carelessness or weak passwords. "Download" (1 attack) was a less common technique and was usually used to infect ransomware through insecure downloads.

This data shows that ransomware uses various techniques to infiltrate the system and the frequency of use of these techniques can vary. Therefore, taking preventive steps such as closing security gaps, educating users, and keeping security software up to date is an important factor in reducing the impact of ransomware.

Important Ransomware Attacks in 2023

Henry Schein and the BlackCat Attacks: Healthcare Giant Suffers Third Ransomware Attack

Henry Schein has been attacked twice in the last month by the BlackCat/ALPHV ransomware gang. The company reported that its applications and e-commerce platform were disabled, but continued to receive orders and ship to customers through alternative channels.

Toyota Financial Services Data Breach with Medusa Attack: $8 Million Claim

Toyota Financial Services (TFS) confirmed the Medusa ransomware attack on the company and announced that it detected unauthorised access. Unauthorised access was detected in some of the company's systems in Europe and Africa, which were under the threat of data leakage, and the ransomware demanded $ 8 million.

Boeing's Data Leaked with LockBit Ransomware: Gigabytes of Data at Risk

The LockBit ransomware gang leaked Boeing's data, releasing more than 43GB of data from one of the largest aerospace companies serving commercial aircraft and defence systems. Because Boeing refused to pay the ransom, the hacker group made the data publicly available. This data includes configuration backups for IT management software and records of monitoring audit tools.

SysAid Zero-Day Vulnerability Used in Clop Ransomware Attacks

The Microsoft Threat Intelligence team has discovered that a zero-day vulnerability in the service management software SysAid was used for Clop ransomware attacks. This vulnerability was exploited by malicious actors to gain access to corporate servers and distribute the Clop ransomware.

Data Breach of US Energy Company with Akira Ransomware: Comprehensive Attack Details Shared

BHI Energy has demonstrated a rare example of transparency by detailing how the Akira ransomware gang infiltrated its networks and stole data during the attack. The energy services firm revealed that the Akira ransomware group infiltrated its networks in May 2023, stealing a large amount of data and carrying out the ransomware attack.

ALPHV Ransomware Gang Attacks Florida Court Systems

The ALPHV (BlackCat) ransomware gang has claimed responsibility for an attack affecting the courts of the Northwest District of Florida (part of the First Judicial Circuit). The attackers claim to have compromised the Social Security numbers and resumes of employees, including judges.

BlackCat Ransomware Targets Azure Storage Services with Sphynx Encryptor

The BlackCat (ALPHV) ransomware gang began encrypting targets' Azure cloud storage by stealing Microsoft accounts and using the newly discovered Sphynx encryptor. A total of 39 Azure Storage accounts were encrypted in this attack.

Siemens Energy and Schneider Electric Suffered Data Leakage as a Result of Clop Ransomware Attack

SIEMENS energy

Siemens Energy confirmed that Clop ransomware attacks resulted in data leakage using a zero-day vulnerability in the MOVEit Transfer platform.

Clop Ransomware Attack: Ontario Agency Data Leak Affected 3.4 Million People

Better Outcomes Registry & Network (BORN), an Ontario government-funded health organisation, was one of the victims of the Clop ransomware MOVEit hack.

Lockbit 3.0 Ransomware Attack on Italian Cloud Service Provider: Negatively Impacted Public Services

The Lockbit 3.0 ransomware attack on Italy's Westpole cloud service provider led to the collapse of PA Digitale's services and affected more than 1300 public organisations. ACN is making efforts to recover the data of more than 1000 organisations affected by the attack. This attack is characterised as one of the most serious threats ever faced by the Italian public administration.

ECHO

CYBER THREAT INTELLIGENCE