ECHO

CYBER THREAT INTELLIGENCE

END OF YEAR REPORT

2023

@echocti

@echocti

echocti.com

Contents

Executive Summary

This report summarises the key developments in cyber security observed during 2023. The events reported under the relevant headings provide an analysis of specific cyber threats and key trends in the industry.

Phishing, malware attacks and ransomware attacks were among the prominent cyber threats during this period. Malicious actors increased phishing attacks to manipulate users and access sensitive information. Similarly, malware and ransomware attacks posed serious risks by negatively affecting the activities of organisations.

In 2023, the activities of certain cyber threat actors were observed. These actors distinguished themselves by using complex and variable attack techniques. At the same time, certain countries and sectors were more exposed to attacks. This situation emphasises that cyber security strategies need to be handled more carefully, especially on a sectoral and geographical basis.

Significant data breaches have compromised organisations' sensitive information and demonstrated once again that vulnerabilities are critical. These breaches highlighted the need to strengthen and improve cyber defence strategies.

Finally, the significant vulnerabilities discovered clearly demonstrated the vulnerabilities in our systems. It has become a critical priority to identify and fix these vulnerabilities and to create a stronger defence mechanism against future attacks.

Cyber security threats are constantly evolving, and as an organisation, we focus on updating and improving our security strategies. This report summarises the key cybersecurity trends in 2023 and will provide guidance to build a more robust security infrastructure for the coming year.

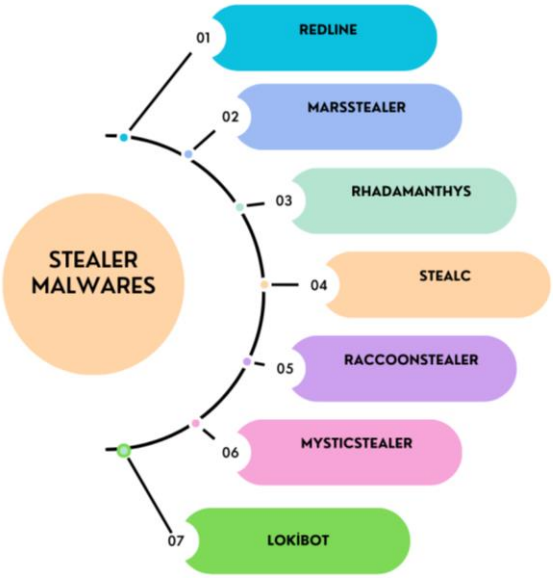
Malware Attacks

Malware attacks continued to pose a significant threat in the field of cyber security, and the development in this area was remarkable in 2023. Malware has evolved and become more sophisticated, posing a serious risk to organisations and individuals. This year, three types of malware attacks were particularly prevalent: Information Stealers (Stealer) and Remote Access Trojans (RAT).

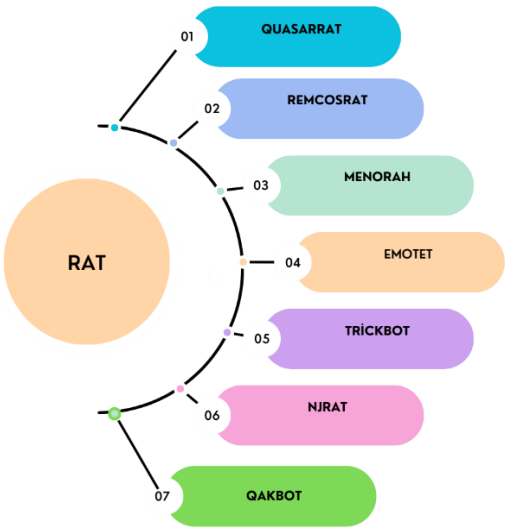
Stealer is a type of malware that aims to steal users' browser data, passwords, logins and other sensitive information. This year, keyloggers, cookie stealers, and other stealer software have become common tools used by attackers.

RAT (Remote Access Trojan) is malware that aims to remotely control the victim's computer by providing remote access to attackers. RATs allow attackers to hijack a computer, download files, and engage in other malicious activities. This year, several RAT attacks have had a serious impact on organisations and the use of such software has increased.

In 2023, the most affected Stealer Malware families are



RAT Malware families with the most impact in 2023



Measures that can be taken for protection include regularly updating security software, adopting strong password policies and implementing security measures such as multi-factor authentication. It is also important to provide regular security training to employees and raise awareness about not opening files and links from unknown sources.

Malware attacks remain important as a constantly evolving threat that targets weaknesses in cyber security strategies. Therefore, it is critical to ensure an effective defence against malware by adopting an up-to-date and comprehensive security policy.

Ransomware Attacks

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. For more detailed information, you can review our 2023 Ransomware Attack Report.

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.

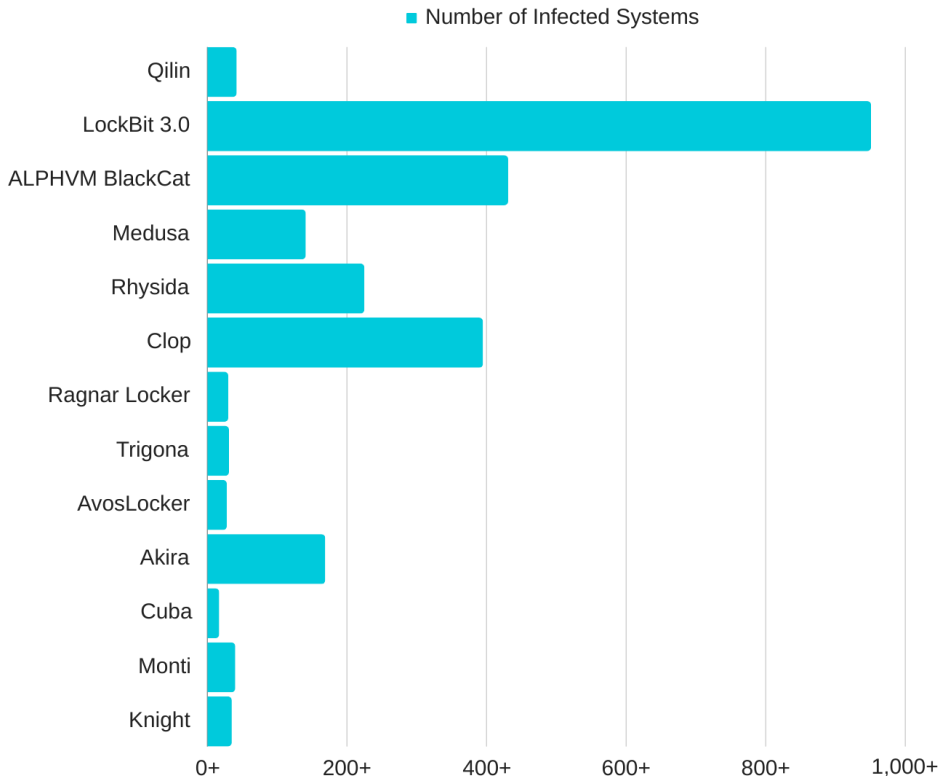


Figure 1 Number of Infected Systems

Most Active Threat Actors

In the field of cybersecurity, certain groups and actors are shaping the cyber threat landscape by standing out with their complex and effective attacks. In 2023, certain groups attracted attention by carrying out high-profile cyber attacks.

North Korea-based **Lazarus Group**

The Lazarus Group is known as a group associated with North Korea that has carried out sophisticated attacks involving financial theft as well as espionage activities. This group is known for attacks on banking institutions and cryptocurrency exchanges.

The Lazarus APT group stole over $240 million in crypto assets in 2023. In the last year alone, the Lazarus APT group has stolen over $100 million in crypto assets from various businesses, including Atomic Wallet ($37.3 million), CoinsPaid ($37.3 million), Alphapo ($60 million), and Stake.com ($41 million). The group is also under suspicion of recently stealing $31 million from CoinEx, a professional global cryptocurrency exchange.

Russia-based **Fancy Bear (APT28) and Cozy Bear (APT29)**

Fancy Bear and Cozy Bear are APT (Advanced Persistent Threat) groups often associated with Russian intelligence. While Fancy Bear carries out espionage and information theft operations by targeting various institutions such as government institutions, media and energy sectors of target countries, Cozy Bear focuses on technology companies and defence sector.

China Based **APT40 and APT41**

China-based APT40 and APT41 are groups associated with the Chinese state and have carried out wide-ranging attacks against various sectors. APT40 focuses on the maritime industry and government institutions, while APT41 targets a wider range of areas such as telecommunications, the gaming industry and the healthcare sector.

Iran-based **APT33 and APT34**

APT33 and APT34 are cyber espionage groups originating from Iran and focused on sectors such as energy, aviation and finance. APT33 was particularly active in the energy sector, while APT34 focused on technology and financial institutions.

Most Targeted Countries and Sectors

2023 was more risky for certain countries and sectors in terms of cyber attacks. Three countries and three sectors attracted attention as the areas where cyber attacks were the most intense.

Most Targeted Countries

1st United States of America (USA)

The USA is one of the countries most targeted by cyber attacks. In particular, government agencies, technology companies and the financial sector have faced continuous and complex attacks. Cyber espionage and ransomware attacks are among the sectors where the US is sensitive in terms of cyber security.

2nd United Kingdom

The United Kingdom is another country targeted by cyber attacks. In particular, the energy, health and education sectors have become the target of intense and targeted attacks. Different groups and actors have created serious risks by targeting infrastructures in various industries of the country.

3rd Germany

Germany is also one of the countries affected by cyber attacks. In particular, the manufacturing industry, technology companies and the healthcare sector are among the sectors that are constantly targeted. Data breaches and ransomware attacks pose a significant threat to the country's cyber security.

Most Targeted Sectors

Finance Sector: The financial sector is one of the most targeted sectors by cybercriminals. Banks, financial institutions and cryptocurrency exchanges are constantly exposed to ransomware attacks and data breaches.

Health Sector: The healthcare sector has been a targeted sector, especially during the pandemic period. Hospitals, healthcare organisations and medical research units have been subject to attacks by cybercriminals trying to access sensitive health data.

Education Sector: Educational institutions have been the target of cyber-attacks due to the weak points of distance education systems as well as student information and academic data. Especially the vulnerabilities in online education processes have attracted the attention of cyber criminals.

Most Targeted Sector in Turkey: In Turkey, the financial sector has been the most targeted by cyber-attacks. Banks, financial institutions and payment systems have become the target of attacks by ransomware and other malware.

Significant Data Breaches

Yakult Australia faces 95 GB data breach

Yakult Australia has confirmed that it has experienced a "cyber incident" and announced that it was affected as a result of an attack carried out by a cybercriminal group called DragonForce. While the company stated that its IT systems in Australia and New Zealand were damaged, the DragonForce group allegedly leaked 95 GB of data. The leaked data includes sensitive information such as company documents, employee records and identity documents. DragonForce follows the tactic of leaking such data publicly if companies do not pay.

Canadian government discloses data breach

In Canada, it was announced that two subcontractors, Brookfield Global Relocation Services (BGRS) and SIRVA Worldwide Relocation & Moving Services, were attacked by hackers and sensitive information was leaked. These attacks led to the theft of data from the systems of subcontractors serving Canadian government employees. The LockBit ransomware gang claimed to have infiltrated SIRVA's systems and disclosed 1.5TB of documents.

McLaren Health Care says data breach affected 2.2 million people

McLaren Health Care announced that a data breach in late July and August compromised the sensitive personal information of 2.2 million people. The leak included social security numbers, health insurance information, medical records and more.

Seiko says ransomware attack exposed sensitive customer data

Seiko has confirmed that a Black Cat ransomware attack earlier this year exposed customer, partner and staff information. A total of 60,000 'personal data' held by Seiko's 'Group', 'Monitoring' and 'Instruments' departments were damaged as a result of the attack. The ransomware group claimed to have stolen information including production plans, employee passport scans, new model release plans, specialised laboratory test results and confidential technical schematics of current and future Seiko watches.

BHI Energy announces 690 GB data breach

BHI Energy shared in detail how Akira ransomware hacked their network. Akira logged into the BHI network with VPN credentials in May 2023 and stole 767,000 files, including 690 GB of data. The company immediately notified the authorities and worked with external experts to recover the systems affected by the attack. The company was able to restore data and restore its systems without paying a ransom. Employees' personal information was stolen as a result of the attack; victims were instructed to sign up for a two-year identity theft protection service through Experian.

Casio discloses data breach affecting customers in 149 countries

The data breach by an attacker who infiltrated the servers of Casio Company's ClassPad education platform revealed that it affected customers from 149 countries. As a result of the attack, it was determined that information such as personal information, payment methods, licence codes and order details were leaked. The company stated that the attack occurred due to misconfiguration of network security settings in the development environment and inadequate operational management.

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.

CYBER THREAT INTELLIGENCE