ECHO

CYBER THREAT INTELLIGENCE

CYBER THREAT REPORT

2024 Mid-Year

@echocti @echocti echocti.com

Contents

Executive Summary

In the first half of 2024, significant changes and challenges have emerged in the global cyber security environment. During this period, the rise and diversification of cyber threats raised critical security risks for organisations and individuals. Key issues such as ransomware attacks, data leaks and critical vulnerabilities have comprehensively shaped the current threat landscape.

The significant increase in ransomware attacks has been a serious concern in the field of cyber security. Compared to the same period in 2023, there was a 48% increase in such attacks, with LockBit, ransomhub and Play ransomware among the most common ransomware families. Changes in the number of attacks on a monthly basis show that ransomware threats are becoming increasingly complex and targets are expanding.

In terms of data leaks, the amount of leaked records in the first half of 2024 was 35,927,479,085. This situation reveals that the risks to the protection of personal and corporate data are increasing and data protection strategies need to be reviewed.

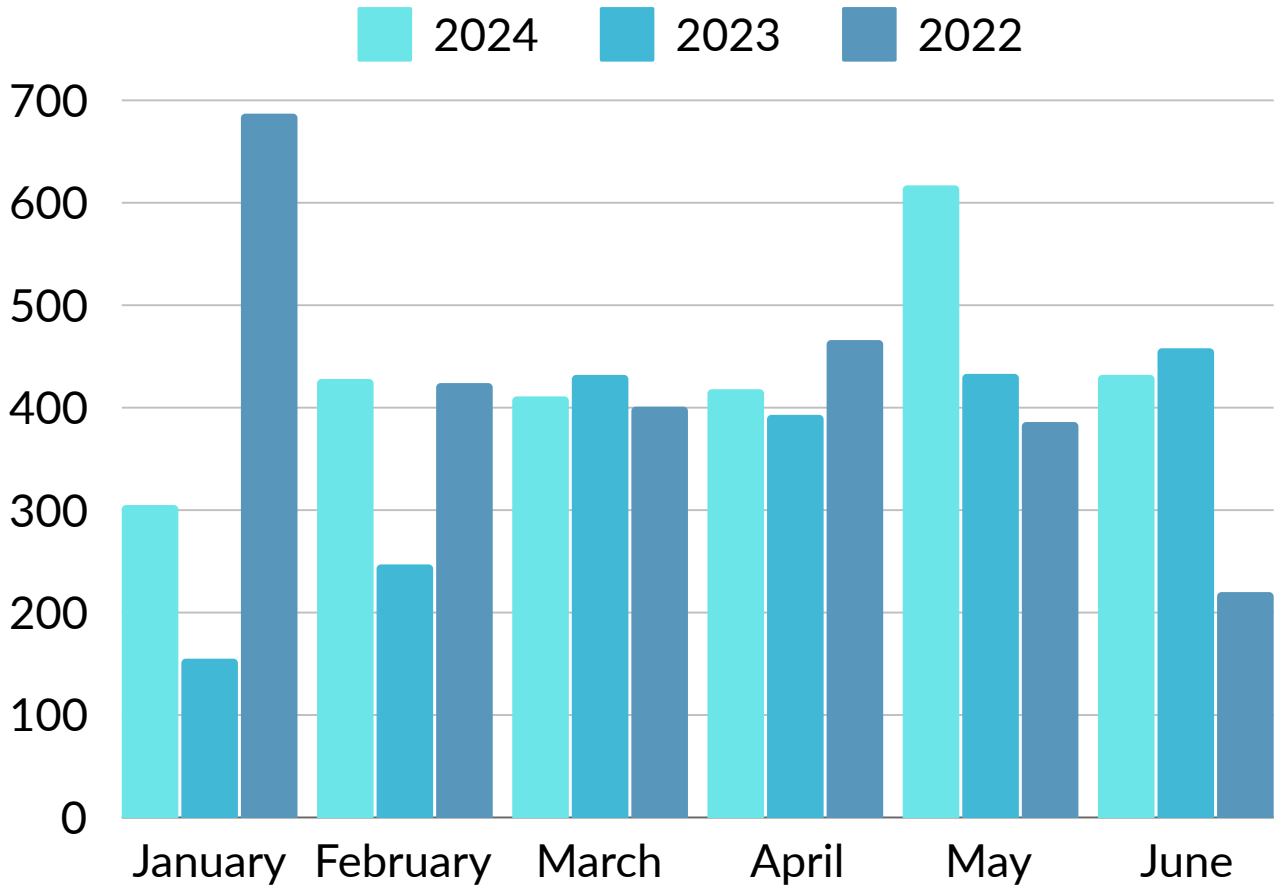
Critical vulnerabilities have increased the complexity of cyber threats and vulnerabilities. Important vulnerabilities such as CVE-2024-1709 and CVE-2024-23917 emphasise the need to strengthen security strategies and take effective measures against current threats.

In conclusion, the increase in ransomware attacks, data leaks and critical vulnerabilities encountered in the first half of 2024 shows that cyber security threats and risks continue. To effectively deal with these threats, organisations need to strengthen their security measures, update their data protection strategies and continuously monitor critical vulnerabilities. Being prepared for these threats in the future will play a key role in reducing security risks.

Ransomware Attacks

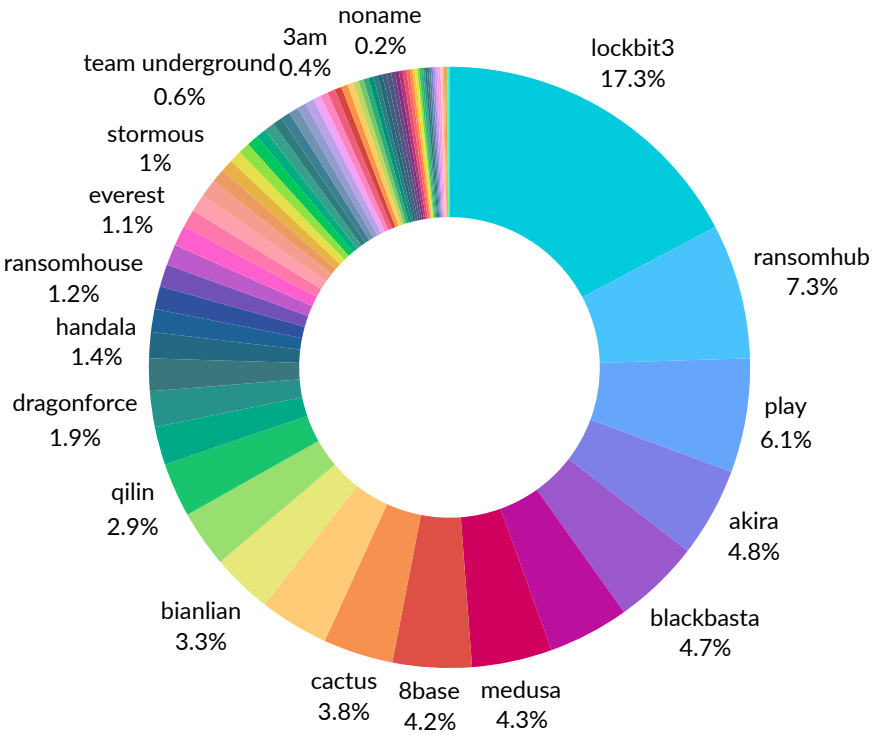
Ransomware Cases in the First Six Months of the Last Three Years

When analysed comparatively with 2023, it is seen that ransomware cases generally increased in the first half of 2024. The number of ransomware attacks, which was 158 cases in January, increased to 308 in 2024, representing an increase of 95%. The number of attacks increased from 253 in February to 441 in 2024, representing an increase of 74%. In March, the number of incidents increased from 434 in 2023 to 418 in 2024. However, this increase continued in April, May and June, and the number of cases, which were 395, 438 and 465 in 2024, respectively, shows a significant upward trend in 2024. These increases show that ransomware threats have become more widespread and sophisticated, and organisations need to be more careful and prepared for such attacks. The sharp increase, especially in May, indicates that attack activities that intensify in certain periods are critical to strengthen cyber security strategies.



Most Popular Ransomware Families

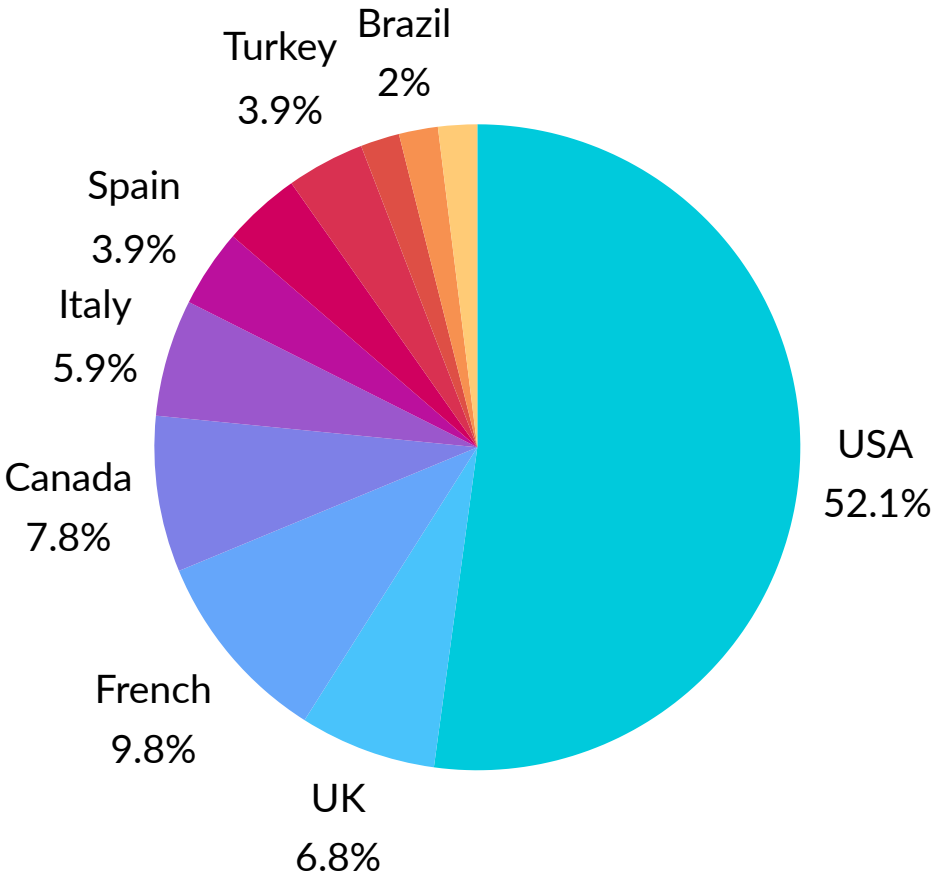
When analysed comparatively with 2023, it is seen that ransomware cases generally increased in the first half of 2024.The number of ransomware attacks, which was 158 cases in January, increased to 308 in 2024, representing an increase of 95%. The number of attacks increased from 253 in February to 441 in 2024, representing an increase of 74%. In March, the number of incidents increased from 434 in 2023 to 418 in 2024. However, this increase continued in April, May and June, and the number of cases, which were 395, 438 and 465 in 2024, respectively, shows a significant upward trend in 2024.



These ransomware families have carried out attacks with different methods and targets and occupy an important place in the overall threat landscape. In particular, LockBit 3 stands out as the most common threat with 504 victims.Other important threats include families such as RansomHub, Play, Akira, and BlackBasta.

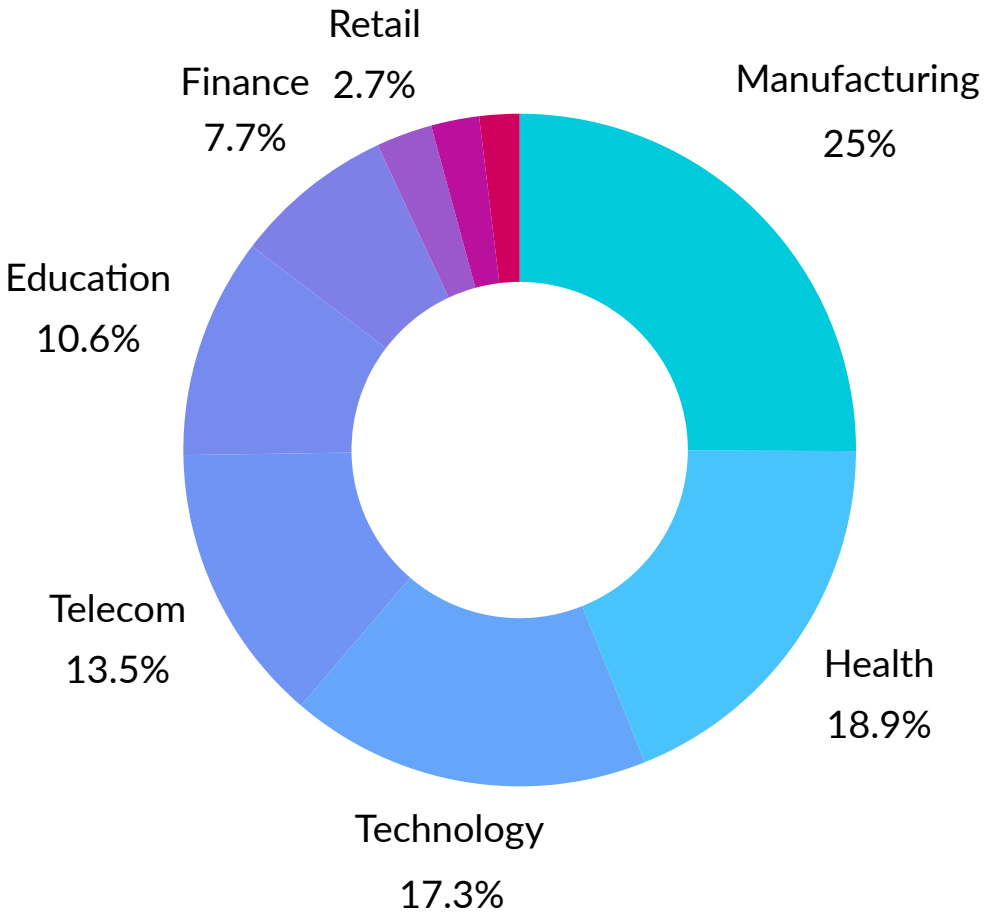
The fact that ransomware threats are so widespread and diverse shows that organisations need to be more prepared and resilient against such attacks. This necessitates continuous review and strengthening of security strategies. In addition, the development of customised defence mechanisms against specific ransomware families will play a critical role in reducing the impact of attacks.

Distribution of Ransomware Attacks by Country



This table shows the distribution of ransomware attacks on organisations in the top 10 countries. The United States leads the way significantly with 52.1 per cent of mentions, followed by the United Kingdom and France. This data reflects the geographic focus of ransomware threats and the countries where organisations are most frequently discussed in the context of these cyber risks.

Distribution of Ransomware Attacks by Sector

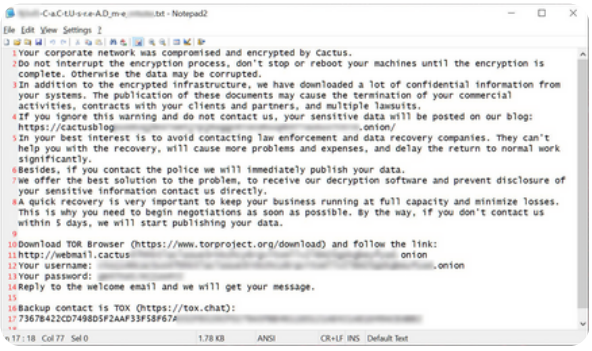


This chart shows the top 10 sectors targeted in ransomware attacks. Manufacturing tops the list, accounting for 25 per cent of positions, followed by sectors such as Healthcare, Technology and Telecommunications.

Important Ransomware Cases

Schneider Electric Hit by Cactus Ransomware Attack

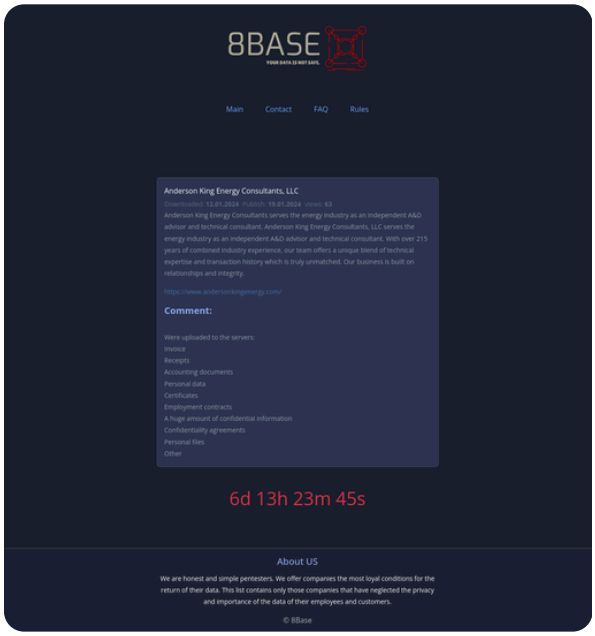
Schneider Electric, an energy management and automation company, was hit by the Cactus ransomware attack. The attack targeted Schneider Electric's Sustainability Business division and disrupted the company's cloud platform.



The ransomware gang stole terabytes of corporate data during the attack and threatened to leak it unless a ransom was paid to the company. The Sustainability Business division affected by the attack provides consulting services to corporate organisations and advises on renewable energy solutions. The stolen data may contain sensitive information about power usage, industrial control systems and energy regulations.

Schneider Electric announced that the attack only affected the Sustainability Business division. Schneider Electric has been previously targeted by the Clop ransomware group and is similar to these new attacks.

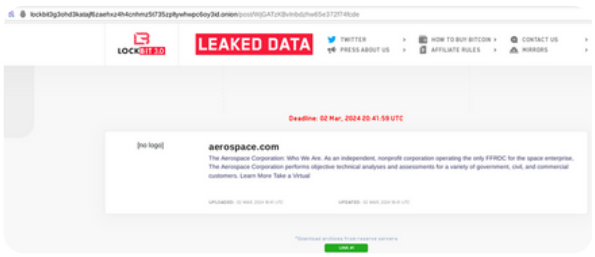
Anderson King Energy Consultants Hit by 8Base Ransomware Attack



Anderson King Energy Consultants, which provides A&D consultancy and technical consultancy services, was attacked by 8Base ransomware.

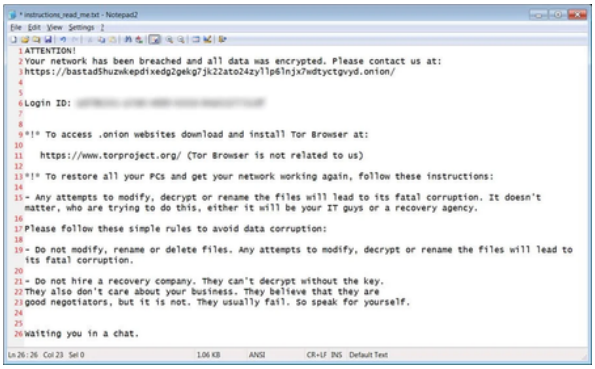
Aerospace Hit by LockBit Ransomware Attack

India's Aerospace Laboratories (NAL), a major aerospace research company, was attacked by the notorious ransomware group LockBit. LockBit added NAL to its dark web leak site, threatening to publish the organisation's data. According to the leaked information, LockBit published eight allegedly stolen documents, including confidential letters and an employee's passport.



As NAL's website is down, neither the company nor the Indian cyber agency CERT-In has yet to make an official statement on the matter. Last month, LockBit targeted the US branch of the Industrial and Commercial Bank of China (ICBC), disrupting transactions in the US Treasury market, and the bank reportedly paid a ransom. LockBit's business model is known as "ransomware-as-a-service", selling its malware to other hackers.

Hospital Corporation of America (HCA) BlackBasta Attack



The major US hospital chain HCA was targeted by the BlackBasta ransomware group. This attack caused operational disruptions in many hospitals and resulted in the encryption of patient data. The company had a difficult time paying the ransom, but eventually managed to recover from the attack.

Data Leaks

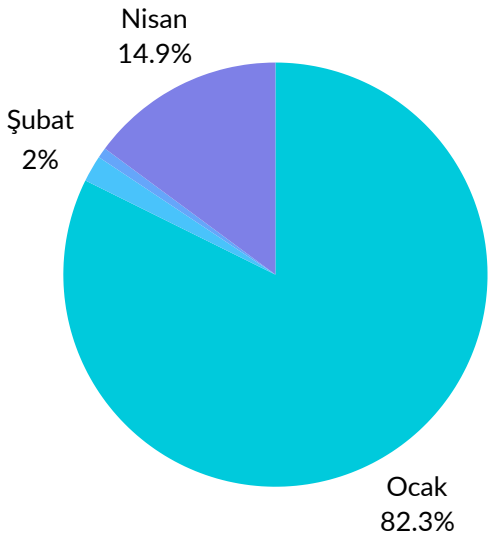
In the first half of 2024, data breaches have been a serious concern in the cyber security environment. During this period, millions of records were leaked as a result of various attacks, posing significant security risks for both individuals and organisations.

35,927,479,085
Leaked Records

Throughout 2024, the size of the total reported data breaches and the number of leaked records illustrate the magnitude of this threat. Data breaches in the first six months of 2024 reveal that a total of 35,927,479,085 records were leaked. These large-scale data breaches once again show how critical the security of personal and corporate data is. In addition to user information, financial data and other sensitive information have also been compromised in such breaches.

MOAB (Mother of All Breaches)

In the first half of 2024, one of the biggest data breaches was the so-called "Mother of All Breaches" (MOAB). In this data breach, the personal information of millions of users was compromised by cybercriminals. The MOAB breach is particularly notable for its wide scope and impact. The leaked data included names, e-mail addresses, telephone numbers and even financial information. This breach greatly increased the risk of users being exposed to identity theft and financial scams. In the wake of the incident, it has become imperative to take swift and effective measures to ensure that affected users can safeguard their personal information.



Discord Data Breach

The popular messaging and social media platform Discord suffered a massive data breach in 2024. This breach led to the leak of personal and account information of millions of users. Attackers gained access to Discord's databases, accessing sensitive information such as usernames, email addresses, passwords, and private messages. Following this breach, Discord reviewed its security protocols and warned its users to use strong passwords and take additional security measures such as two-factor authentication (2FA). Affected users have also been advised to be wary of potential identity theft and scams.

916 Google Firewall Data Breach

In the first half of 2024, Google Firewall, one of Google's popular security services, experienced a major data breach. In this incident, known as the "916 Google Firewall Breach", cybercriminals exploited a vulnerability in Google's security systems and gained access to the data of millions of users. The leaked data included usernames, IP addresses, browser histories and other sensitive information. This breach seriously compromised users' online privacy and security.

Following this incident, Google launched a comprehensive review to close security gaps and prevent similar breaches. Users were advised to change their passwords regularly and tighten their security settings to keep their accounts secure.

iSharingSoft Data Breach

iSharingSoft, which provides location sharing and tracking services, faced a major data breach in 2024. This breach resulted in the leak of location information, personal information and account data of millions of users. Cybercriminals infiltrated iSharingSoft's databases and obtained users' real-time location information and historical location data. This compromised users' physical security and violated their privacy. iSharingSoft notified its users and increased security measures following the breach. Users were advised to review their location sharing settings and only share location information with people they trust.

Critical Vulnerabilities

In 2024, many critical vulnerabilities were identified in the cybersecurity world and were actively exploited by attackers. These vulnerabilities seriously threatened the security of software and systems and caused large-scale security breaches. Some of the prominent critical security vulnerabilities and their effects are as follows:

- **CVE-2024-1709:** This vulnerability was identified in the Microsoft Windows operating system. It allows attackers to steal users' data or run malware on the system. This vulnerability is due to a bug in the operating system components and has been fixed by updating the systems.
- **CVE-2024-27322:** This vulnerability, identified in the Atlassian Confluence product, allows attackers to remotely execute code. Confluence users should close this vulnerability by updating their systems to the latest version.
- **CVE-2024-2389:** This vulnerability, identified in VMware vSphere Client, allows attackers to bypass authentication and gain administrative rights. This vulnerability could result in the theft of sensitive data or system takeover.
- **CVE-2024-20353:** A vulnerability identified in the Apache Log4j library allows attackers to remotely execute code and gain access to systems. Log4j users should use the current version of the library to close this critical vulnerability.
- **CVE-2024-20359:** A vulnerability in Adobe Acrobat Reader allows attackers to execute malicious code via PDF files. Users should install the latest version of the software to close this vulnerability.
- **CVE-2024-26234:** This vulnerability, identified in Cisco IOS and IOS XE software, could allow attackers to remotely execute code and take control of network devices. This vulnerability has been fixed with patches released by Cisco.
- **CVE-2024-29988:** A vulnerability identified in the Linux kernel allows attackers to perform local privilege escalation and gain root privilege on the system. This vulnerability was closed by updating the kernel.

- **CVE-2024-23917 (TeamCity):** This vulnerability was identified in TeamCity On-Premises versions. It allows an attacker with HTTP(S) access to gain administrative privileges by bypassing authentication checks. Affected versions include all versions 2017.1 through 2023.11.2. This vulnerability was fixed with version 2023.11.3.
- **CVE-2024-30051 (Windows DWM Core Library):** This local elevation of privilege vulnerability in Microsoft Windows DWM Core Library was assessed with a CVSSv3 score of 7.8. It allows an attacker to gain SYSTEM authorisation on the system. This vulnerability was discovered and actively exploited by Google Threat Analysis Group, Google Mandiant and Kaspersky researchers.
- **CVE-2024-30040 (Windows MSHTML):** This vulnerability was identified as a security feature bypass vulnerability in the Windows MSHTML (Trident) engine and has a CVSSv3 score of 8.8. Attackers can use social engineering methods to get the victim to open a specially crafted document and execute code on the target system after opening this document.
- **CVE-2024-3400:** A vulnerability identified in the Google Chrome browser allows attackers to steal users' data via malicious websites and execute code in the browser. Chrome users should close this vulnerability by updating their browser to the latest version.
- **CVE-2024-21678 (Atlassian Confluence):** A stored XSS vulnerability identified in Atlassian Confluence Data Centre and Server products allows attackers to inject malicious code. This vulnerability, along with several DoS vulnerabilities, has been assessed as high severity.

How Can You Be Protected From Cyber Attacks?

If you want to ensure the security of your organisation in cyber space, there are some precautions to be taken.

Are There Vulnerabilities in the Software We Use?

If the software described as vulnerable is also used in your organisation, this software should be updated. If the software you use does not provide update support for a long time, a competing product should be used. Otherwise, attackers can access the network within the institution by taking advantage of these software vulnerabilities and damage the system by performing harmful behaviours on endpoint devices.

Has Personal Information of Our Employees Been Leaked?

Especially corporate account information of corporate managers can be leaked due to third-party software. Phishing campaigns can be carried out using this leaked account information, or depending on the type and importance of the leaked account information, damage can be done to the organisation through the individual. In order to prevent these situations, personnel may be asked to change their corporate account passwords at certain periods.

Do Our Employees Have Sufficient Awareness on Cyber Security?

Perhaps the most important measure to be taken is human awareness. In particular, it is essential that employees who are relatively distant from the IT field but are in the same network receive cyber security awareness training. The defined employee profile is the first targets taken by cyber attackers. At this point, you can prevent this issue with awareness trainings.

To summarise,
Even in a situation where all precautions are taken, you may be cyber-attacked and damaged by this attack. The important thing is to minimise the potential damage.

CYBER THREAT INTELLIGENCE