REGIONAL CYBER DEFENCE CENTRE

# CTAC 2023
# YEARLY REPORT





# CTAC 2023
# YEARLY REPORT

## NATIONAL CYBER SECURITY CENTRE

# Table of Contents

# List of Abbreviations

| Term/abbreviation | Meaning / explanation |
|---|---|
| AI | Artificial Intelligence |
| APT | Advanced Persistent Threat |
| ATT&CK | Adversarial Tactics, Techniques and Common Knowledge |
| CDN | Content Delivery Network |
| CERT | Computer Emergency Response Team |
| CISA | Cybersecurity & Infrastructure Agency |
| CTAC | Cyber Threat Analysis Cell |
| CVE | Common Vulnerabilities and Exposures |
| DDoS | Distributed Denial of Service |
| Disinformation | The term "disinformation" refers to false information that is intended to manipulate, cause damage, or guide people, organisations, and countries in the wrong direction. |
| ESG | Email Security Gateway |
| FBI | Federal Bureau of Investigation |
| FSB | Federal Security Service |
| FVEY | Five Eyes |
| GRU | The Main Directorate of the General Staff of the Armed Forces of the Russian Federation |
| ICS | Industrial Control System |
| IOC | Indicators Of Compromise |
| LOTL | Living Off the Land |
| Malinformation | The term "malinformation" refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm. |
| MFA | Multi-factor Authentication |
| Misinformation | The term "misinformation" refers to false information that is not intended to cause harm. |
| NCSC | National Cyber Security Centre of Lithuania |
| OT | Operational Technology |
| RCDC | Regional Cyber Defence Centre, part of NCSC |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information and Event Management |
| SSU | Security Service of Ukraine |
| SVR | The Foreign Intelligence Service of the Russian Federation |
| TTP | Tactics, Techniques and Procedures |

# CTAC year 2023 in review

- **Locked Shields 2023 and Amber Mist 2023** - two cyber security exercises where NATO members and their Allies play Red Team vs Blue Team scenarios to test their cybersecurity skills, learn and improve their knowledge. The Cyber Threat Analysis Team participated in both of those exercise as the Intel Team preparing daily cyber threat intelligence reports over the course of the exercise;
- **In 2023, during the NATO Summit in Lithuania**, CTAC started releasing daily reports over the course of the event. After the Summit, CTAC refined the process of daily reports and started releasing them regularly. By the end of 2023, CTAC managed to have released 45 daily reports;
- **CTAC also released 50 weekly reports** and, working side by side with NCSC colleagues, refined the process of information sharing and started sharing indicator data and information, like ransomware against the Lithuanian infrastructure, regarding key events.
- **Cyber-lessons learned during the war in Ukraine** - while the cruel war in Ukraine is still ongoing, last year, with major help from the rotating personnel from partner nations, especially Ukraine, CTAC managed to develop a comprehensive study about the cyber activity in Ukraine during the war, covering various sectors, from public, private to military and critical infrastructure. Information provided by first responders was analysed, pointing out what was successful, what mistakes were made, and how NATO and their partners can learn from it. One of the most extensive CTAC projects to date yielded dividends with many positive feedback and appreciation. The study was published on July 26, 2023, the very same day it was presented at the Cyber Summit 2023 in Wiesbaden, Germany.
- In 2022, CTAC engaged in the **Counter Ransomware Initiative** and was tasked to create an information sharing hub. After successfully deploying MISP with the help from NCSC colleagues, CTAC maintained it throughout 2023 and is still supporting the platform and goal of information sharing across a variety of countries worldwide;
- Continuing its support to Ukraine, CTAC provided a total of 12 Ukraine military cadets with a month-long **internship** at the RCDC. Future cyber security officers of the Armed Forces of Ukraine had the opportunity to learn from NCSC specialists and further deepen their cyber security skills.

# 01/ Summary

Over the year 2023, Ukraine remained as a focal point of cyber threats, with a particular proliferation of attacks aimed at its critical infrastructure. Malicious actors carried out a range of different attacks, frequently causing disruptions in vital services. The most common strategies included DDoS attacks and defacement of websites.

There has also been a worrying trend in Lithuania and in RCDC partner countries with increase of ransomware attacks which were widely affecting targets across different industries. This indicates a growing threat to cybersecurity and data integrity.

In 2023, Artificial Intelligence (AI) saw significant growth and adoption across industries, promising enhanced productivity and innovation. However, alongside its transformative potential, concerns about ethical implications, algorithmic bias, and job displacement highlighted the importance of establishing robust governance and ethical frameworks to guide AI development and deployment.

# 02/ Cyber threat landscape trends in 2023

Artificial Intelligence (AI) continued to develop and proliferate in 2023. The widespread application of AI in various industries signalled an enormous change in innovation and opening amazing possibilities for productivity, efficiency, and problem-solving. AI demonstrated its extraordinary ability to completely transform a range of industries, from healthcare diagnostics and personalised medicine to financial prediction analytics and the revolutionary potential of autonomous vehicles. Nevertheless, despite the excitement, worries about the ethical application and responsible advancement of AI have been growing. Global discussions have been triggered by concerns about algorithmic bias, data privacy, and the possibility of job displacement. To navigate the risks of unchecked AI advancement, the year underlined the urgency of developing strong frameworks for AI governance, regulation, and ethical guidelines. It also emphasised the need for cooperative efforts to harness AI's benefits while mitigating risks.

Sophisticated attack vectors have become more prevalent recently, moving beyond straightforward vulnerabilities and to complex schemes that combine sophisticated technological and social engineering techniques. This growing complexity is reflected in endpoint attacks, ransomware's expanding targets, which now include cloud servers and Linux systems, identity-based threats that take advantage of digital identities, and sophisticated supply chain attacks, like the 3CX event. As evidenced by the Cl0p ransomware and programs like AlienFox and Legion, cybercriminals are now focusing their inventive tactics on cloud services, indicating a shift toward taking advantage of cloud vulnerabilities and credential harvesting in a quickly changing threat landscape.

As the number of IoT devices increases, a greater emphasis is placed on security protocols. This includes the adoption of strong authentication, sophisticated encryption, strict access controls, and regular software updates. Establishing uniform security frameworks for a range of IoT applications is the goal of industry collaboration, guaranteeing data privacy within a network of networked devices. Furthermore, edge computing integration improves security by reducing the amount of sensitive data that is transmitted and implementing security-by-design principles from the beginning, thereby reducing vulnerabilities from the start of the device.

# 03/ Regional Threat Analysis

The cybersecurity landscapes of the United States, Poland, Lithuania, Sakartvelo, and Ukraine in 2023 demonstrated both shared challenges and distinct threats, underscoring the necessity of specialized defence tactics and the worldwide scope of cyberwarfare.

## 3.1/ Common cyber threats

State-sponsored cyberespionage, ransomware incidents, phishing campaigns, and distributed denial-of-service (DDoS) attacks were among the common cyberthreats observed in these countries. These threats are intended to cause havoc, steal confidential information, or disrupt critical infrastructure, government buildings, educational institutions, and private companies. The employment of complex strategies like malware distribution, social engineering, and software vulnerability exploitation highlighted the adversaries' growing technological prowess and the dynamic character of cyberwarfare.

3.1.1 **Distributed Denial-of-Service Attacks:** These attacks were frequently detected as a threat in the US, Poland, Lithuania, Sakartvelo, and Ukraine. Botnets and compromised devices were used by adversaries to overload servers, networks, and target websites with traffic, making them unavailable to authorized users. These attacks caused financial losses and reputational harm by interfering with essential services, such as financial institutions, government websites, and educational platforms.

3.1.2 **Phishing Campaigns:** phishing and spear-phishing attacks have been directed towards individuals and organizations among RCDC partner nations. Cybercriminals trick people into disclosing sensitive information, like login credentials, bank account information, or personal information, by using false emails, messages, or websites. These attacks, which frequently pretended to be trustworthy sources or urgent communications, took advantage of people's weaknesses and trust relationships to gain unauthorized access to accounts or install malware.

3.1.3 **Ransomware attacks:** ransomware has become a major cyberthreat, impacting organizations in Poland, Lithuania, Ukraine, and the US. Ransomware was used by adversaries to encrypt important information or systems, then demand payment for the decryption keys. These attacks put victims through monetary strain, interrupted operations, and resulted in data loss. The indiscriminate nature of ransomware was brought to light by high-profile incidents that targeted critical infrastructure, governmental entities, healthcare organizations, and educational institutions.

3.1.4 **State-Sponsored Cyber Espionage:** In countries like Poland, Sakartvelo, and Ukraine where cyber conflicts were fuelled by geopolitical tensions, state-sponsored cyber espionage operations were a common concern. Hacker groups with ties to Russia, including APT28, Sandworm, and Turla, carried out espionage operations aimed at critical infrastructure, government institutions, and military facilities. These adversaries aimed to undermine national security and worsen regional instability by stealing confidential data, obtaining intelligence, or interfering with operations to achieve their strategic goals.

3.1.5 **Hacktivist activities:** As a form of political protest or activism, hacktivist groups target financial institutions, media outlets, and websites run by the government with DDoS attacks. Coordinated attacks were carried out by organizations such as Anonymous Russia, NoName057(16), and KillNet to express grievances, advance political agendas, or seek vengeance for perceived injustices. These attacks demonstrated the link between cybersecurity and socio-political dynamics by interfering with online services, obstructing communication, and escalating social tensions.

3.1.6 **Exploitation of Software Vulnerabilities:** Software Vulnerability Exploitation: Cyber adversaries from all over the world continue to use software and network infrastructure vulnerabilities as a common tactic. Threat actors used misconfigurations, zero-day exploits, and known vulnerabilities to obtain unauthorized access, increase privileges, or run malicious code. Organizations were exposed to serious risks by vulnerabilities in web servers, industrial control systems, and widely used software applications. This underscores the significance of prompt patch management and vulnerability remediation efforts.

## 3.2/ Distinct Cyber Threats by Country

**Lithuania:** As a result of the NATO Summit in Vilnius, cybercriminals had Lithuania as a top target. DDoS attacks were carried out by pro-Russian hacker groups against summit-related websites, hackers disclosed private information about summit preparations. Ransomware attacks later in the year posed serious threats to data security and operational continuity, specifically targeting government agencies and education institutions.

**Ukraine:** Amidst its ongoing conflict with Russia, Ukraine has been subjected to constant cyber threats. Russian state sponsored hacker groups, like Turla (FSB) and Sandworm (GRU), targeted Ukrainian institutions and critical infrastructure as part of their cyberespionage operations. DDoS attacks were carried out by pro-Russian hacktivist groups, intensifying the online turmoil. Hacktivist groups such as KillNet and Sandworm were using shared infrastructure, which suggested that their efforts to disrupt Ukrainian cyberspace were coordinated.

**Sakartvelo:** Phishing, spear-phishing, and malicious software emerged as common attack vectors in the considerable number of cyber incidents reported to the Computer Incident Response Division in Sakartvelo. The division used the Traffic Light Protocol (TLP) to categorize incidents and emphasized the value of information sharing and incident response. Sakartvelo's emphasis on incident handling and classification demonstrated its proactive approach to cybersecurity, even in the face of threats comparable to those faced by other countries.

**Poland:** A rise in cybercrime attacks, especially phishing and financial fraud, presented a challenge for Polish cyber defenders. Additionally, they had to deal with cyber espionage threats from organizations connected to Belarusian and Russian special services, such as UNC1151 and Winter Vivern. Ransomware attacks on critical systems and the exploitation of vulnerabilities in software like JetBrains TeamCity were among the major incidents.

**United States:** The country faced a variety of cyberthreats, which were made worse by the extensive use of AI platforms. The attack on a small-town water authority by an Iranian-backed group was one example of the difficulties caused by a lack of qualified cybersecurity specialists. Significant data breaches, such as the 23andMe hack, the Cl0p MOVEIT breach, and the use of Barracuda ESG vulnerabilities, have highlighted the necessity of strong cybersecurity protocols and fast incident response times. Furthermore, Volt Typhoon, a Chinese cyber-espionage group, threatened the US energy industry, raising concerns about the security of critical infrastructure and its potential for disruption during geopolitical tensions. Because of its sophisticated technological environment and vast digital infrastructure, the US has become a top target for cyber adversaries looking to compromise systems and cause disruptions.

## 3.3/ Conclusion

Even though these nations were subject to common cyberthreats like ransomware, phishing, and DDoS attacks, the type and intensity of cyber incidents varied depending on their distinct geopolitical settings and cybersecurity capacities. In an increasingly digitally reliant and interconnected world, cooperative efforts, information sharing mechanisms, and customized defence strategies are necessary to effectively mitigate cyber risks and protect critical assets.

# 04/ Threat Actors and Cyber Threats

## 4.1/ Most Exploited Vulnerabilities in 2023

Microsoft was still at the top of the CISA Known Exploited Vulnerability (KEV) catalogue in 2023, with a significant presence on threat actors' radars, as well as in terms of exploited vulnerabilities. Microsoft reported a significant 27.4% share among other vendors in 2022, but in 2023 that percentage dropped to 15.5%. With a 10.9% share, Apple is the second most frequently targeted vendor, closely followed by the networking industry leader Cisco and tech giant Samsung. The top 10 vendors whose products had security flaws which put them on CISA's list of known exploited vulnerabilities 2023 are broken down below.

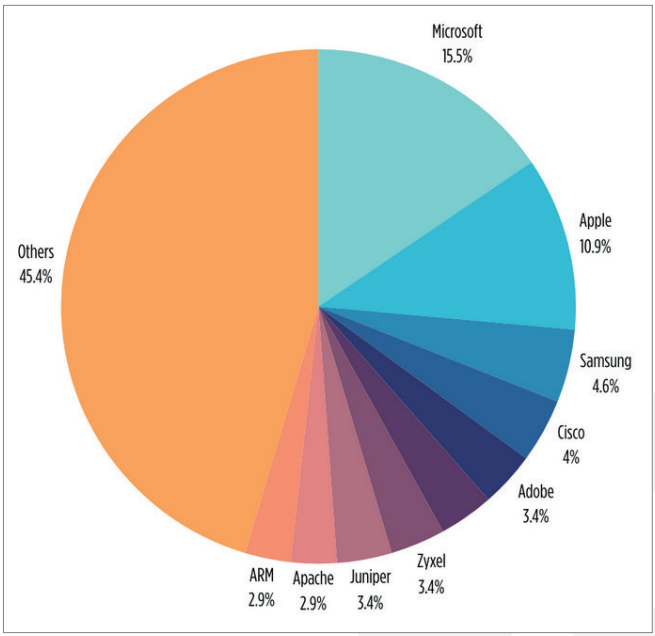


**Figure 1.** Top vendors with exploited vulnerabilities in CISA KEV 2023 (SOCRadar)

There is a notable change in trends of exploitation and threat actor behaviour in 2023. In CISA KEV 2023, privilege escalation vulnerabilities top the list with 12.1%.

Privilege escalation is the most common vulnerability in the current landscape of 2023 after Remote Code Execution (RCE) vulnerabilities dominated the CISA KEV list in 2022. RCE comes second, closely followed by Command Injection vulnerabilities. The dynamic shift in vulnerability types highlights the need for adaptive defence strategies and the ever-changing nature of cybersecurity challenges.

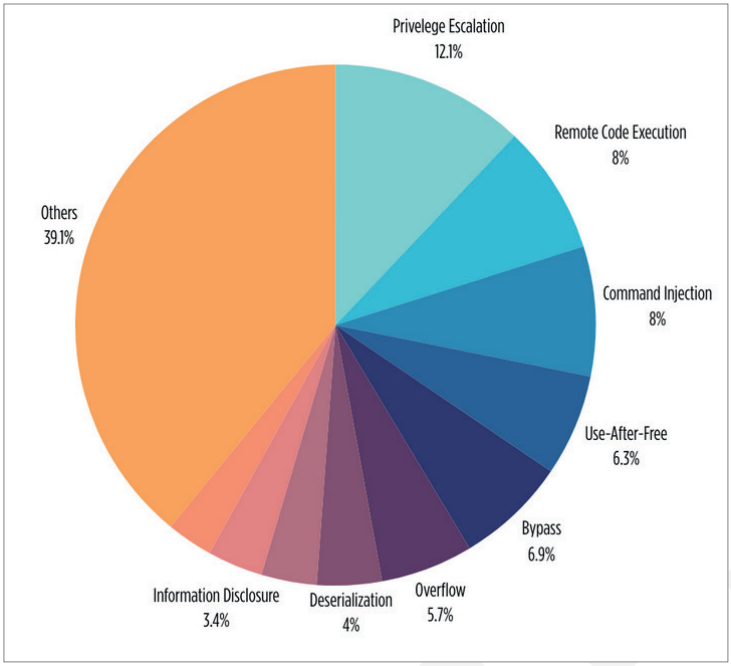


**Figure 2.** Top vulnerabilities in CISA KEV 2023(SOCRadar)

## Top 5 vulnerabilities of 2023

### 1. CVE-2021-41617 (OpenSSH 6.2 through 8.7)

CVE-2021-41617 was found in OpenSSH, a popular networking software suite that uses the SSH protocol. Through the vulnerability, an authenticated user can circumvent the source-address-dependent restrictions specified in the sshd_config file. It might make access to systems or sensitive data possible for unauthorised users too.

Mitigation: To guard against this exploit, users are advised to update to the most recent version of OpenSSH software already patched by the OpenSSH team.

### 2. CVE-2020-14145 (OpenSSH 5.7 through 8.4)

CVE-2020-14145 was also found in OpenSSH, impacting versions 5.7 through 8.4. The vulnerability is defined as an observable discrepancy that results in information leak in the algorithm negotiation process. A man-in-the-middle attacker may exploit this vulnerability to focus on first-time connection attempts which would allow to ascertain whether a client is already aware of the fingerprint of the remote host.

Mitigation: The OpenSSH team does not currently have any plans to modify OpenSSH behaviour triggering this vulnerability. Nonetheless, there has been mitigation options offered. Users are advised to connect to SSH servers only using verified host keys to prevent the chance of a man-in-the-middle attack.

### 3. CVE-2022-22719 (Apache HTTP Server 2.4.48 and earlier)

Apache, the most popular web server software in the world, has been a frequent target to well-known vulnerabilities. First discovered in 2022, CVE-2022-22719 is a high-severity vulnerability linked to the Apache HTTP Server. The Apache HTTP Server Project states that an attacker may be able to create a Denial of Service (DoS) condition through exploitation of the vulnerability. The problem stems from an error in the way the server processes particular requests, which may cause excessive CPU use.

Mitigation: 2.4.48 and earlier versions of Apache HTTP Server are vulnerable. Version 2.4.49 of the Apache Software Foundation contains a fix. It is highly recommended that users update to the most recent version to address this vulnerability.

### 4. CVE-2022-22721 (Apache HTTP Server 2.4.52 and earlier)

The Apache HTTP Server 2.4 versions prior to 2.4.52 has a flaw that allows for the handling of specific requests (CVE-2022-22721). This vulnerability might allow an attacker to run arbitrary code or produce a denial of service.

Mitigation: Affected organisations must establish a value for the LimitXMLRequestBody option that is less than 350MB, but not zero. A system-wide out-of-memory condition would result from using a hard limit.

### 5. CVE-2022-22720 (Apache HTTP Server 2.4.52 and earlier)

There is a vulnerability in the Apache HTTP Server known as CVE-2022-22720. The server is vulnerable to a Denial of Service (DoS) attack that affects versions 2.4.0 through 2.4.51. The cause of the vulnerability is an error in the Apache HTTP Server's mod_proxy module. When the server handles a specially constructed request to a proxied host, the vulnerability is activated. This results in an infinite loop on the server and using up all CPU resources, resulting in a denial of service.

Mitigation: The Apache Software Foundation has patched version 2.4.52 of the Apache HTTP Server to address this vulnerability. To reduce the risk associated with this vulnerability, it is advised that all users of affected versions upgrade to this version or apply the patch.

## 4.2/ Most Active Threat Actors


**KillNet** - a pro-Kremlin hacker group known for targeting European governments and infrastructure via disinformation campaigns.
**Origin:** Russia.
**Target countries:** USA, Lithuania, Ukraine, Latvia, Norway, Japan, Czech Republic, etc.
**Target sectors:** Government, Healthcare, Energy, Transportation, Military, Private.
**Tactics & Techniques:** Distributed Denial of Service (DDoS), Brute-force dictionary attacks, disinformation.

---


**NoName057(16)** – a pro-Russian hacker group well-known for its cyberattacks against US, EU, and the Ukrainian Government, media, and private company websites. It is thought of as a loosely affiliated, unrestrained pro-Russian activist group trying to gain notoriety in the West.
**Origin:** Russia.
**Target countries:** USA, Ukraine, and the European Union.
**Target sectors:** Government, Media, Finance, Telecommunications, Transport.
**Tactics & Techniques:** Distributed Denial of Service (DDoS)

---


**Rhysida** - is a new ransomware group that operates on a Ransomware-as-a-Service (RaaS) model, with developers creating and distributing ransomware, infrastructure to support it and affiliates carrying out the attacks. In May 2023, it sent its first ransomware sample to a public file scanning service.
**Origin:** unknown.
**Target countries:** USA, European countries.
**Target sectors:** Government, Healthcare, Energy, Transportation, Education,
**Tactics & Techniques:** phishing, spear-phishing, data breach, ransomware, file encryption.

**Inc. Ransom** - is a ransomware extortion operation that emerged in July of 2023. Operators of Inc. Ransomware position themselves as a service to their victims. Victims can then pay the ransom to 'save their reputation' though the threat actors indicate their intention to reveal their methods, making the victim's environment 'more secure' as a result. Inc. ransomware is a multi-extortion operation, stealing victim data and threatening to leak said data online should the victim fail to comply with their demands.
**Origin:**
**Target countries:** USA, European countries
**Target sectors:** Healthcare, Education, Government, Technology,
**Tactics & Techniques:** data breach, ransomware, file encryption.

---


**Народная CyberАрмия** - The group is associated with a pro-Russian hacking group that emerged in 2022, following the start of the war in Ukraine. They claim responsibility for carrying out distributed denial-of-service (DDoS) attacks and website defacements against various targets, primarily in countries seen as supporting Ukraine. These targets have included government websites, critical infrastructure, and private companies.
**Origin:** Russia.
**Target countries:** Ukraine, USA, Lithuania, Latvia, Gibraltar, Turkey, Macedonia, Poland
**Target sectors:** Government, Media, Finance, Telecommunications.
**Tactics & Techniques:** Distributed Denial of Service (DDoS), website defacement, data breach.

---


**Lazarus group** - North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. The group has been active since at least 2009.
**Origin:** North Korea
**Target countries:** South Korea, the United States, Japan, and other countries in the Asia-Pacific region.
**Target sectors:** Financial institutions, critical Infrastructure, government organizations, technology and defence companies, media and entertainment, healthcare.
**Tactics & Techniques:** Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. Zero-days, spearphishing, malware, disinformation, backdoors, droppers.

## 4.3/ Different Types of Attacks

Just like in the year 2022, DDoS was the most exploited attack vector in 2023. The only difference here is the count. There was a huge increase in DDoS attacks seen in 2023 and the factor of it might be that these types of attacks do not require sophisticated knowledge and skills to conduct them. Pro-Russian hacktivists prefer this type of attack because it is easy to execute and they can boast in their disinformation campaign about taking down major government entities or other companies. DDoS attacks have no long-term impact and, as mentioned previously, are used to show-off. Overall, the count of attacks in the year 2023 has increased significantly. This trend might point to an increasing pattern of less sophisticated and opportunistic attacks throughout the digital space. Below you can find a graph with statistics of the diverse types of attacks worldwide throughout the 2023.

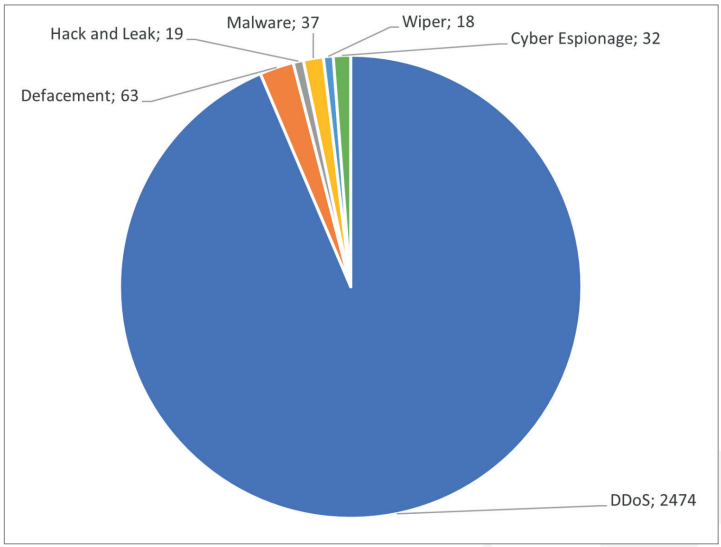


**Figure 3.** Types of cyber-attacks worldwide throughout 2023 (CyberPeace Institute)

## 4.4/ Targets of Cyber Attacks

Just like in the year 2022, transport and public administration sectors were the most attractive to adversaries. Public administration was the most attacked sector in 2023 and the transport sector came second, in reverse to 2022. Public administration and transportation sector targeting points to an intended focus on critical infrastructure that could have a broad impact as the sectors are essential to the operation of society and their compromise could have a significant impact on the governance, services, and public safety. Hackers' focus on this area suggests an increased risk to government operations and essential services and a need to deploy strong cybersecurity defence and strategic measures to prevent potential attacks potentially designed to take advantage of weaknesses and disrupt the system.

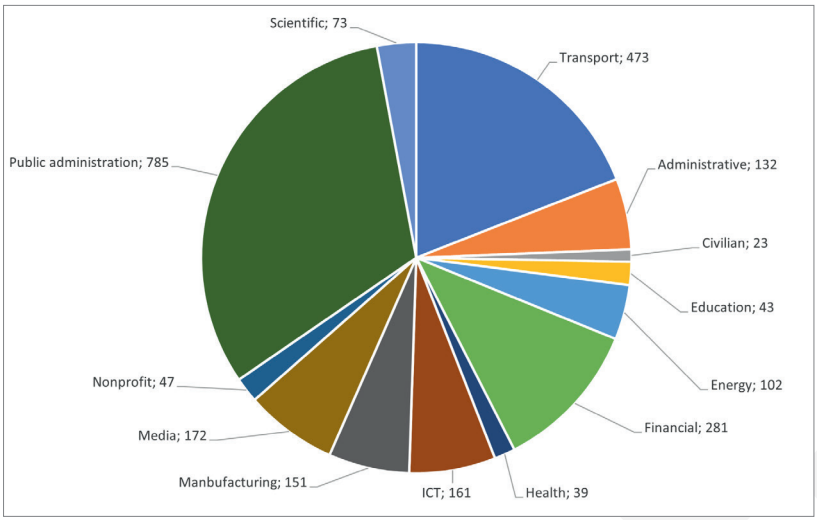


**Figure 4.** Most attacked sectors in 2023

# 05/ The Most Notorious Events of 2023

## ESXi Ransomware Attacks

Early in February 2023, there were reports of a widespread ransomware campaign targeting VMware ESXi servers that led to a noteworthy cyber event. Threat actors exploited a known vulnerability, CVE-2021-21974, to carry out a heap overflow in the OpenSLP service, which allowed them to remotely execute code on the impacted servers. Threat actors have been able to use this vulnerability to spread ransomware for the last two years, even though there is a patch available for it. The campaign, marked by ransom pages accessible via the Internet, however, made unprecedented insight into malware infections possible. The presence of Bitcoin addresses on ransom pages, a feature exclusive to this ransomware, made it easier to track transactions and unearthed about $88,000 USD in funds received since early February. Interestingly, most of the compromised servers were found in France, which had an especially negative effect on the cloud hosting company OVH.

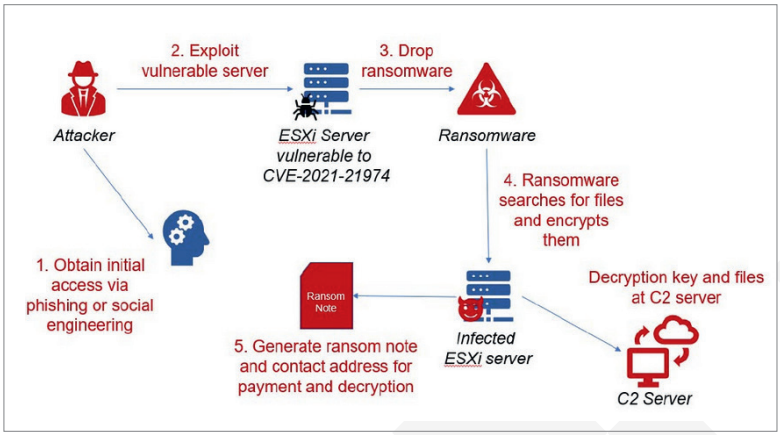


**Figure 5.** Example of ESXi ransomware attack chain (Forescout)

In the overall, ransomware has been a hot topic throughout 2023 with diverse groups utilizing increasingly more sophisticated tactics and damaging more organizations. The comparison by quarter shows a significant increase in incidents, with the second and third quarters of 2023 showing a clear peak. The comparatively lower recorded numbers in 2022 indicate a rapid evolution in the strategies and tactics used by cybercriminals in 2023. Several factors, such as the growing use of double-extortion tactics, improvements in malware delivery systems, and an increased emphasis on targeting critical infrastructure, may be responsible for the spike in attacks in 2023.

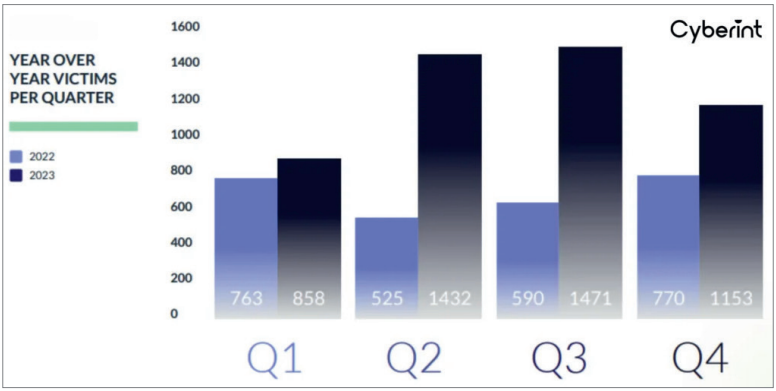


**Figure 6.** Ransomware attacks comparison by quarters (CyberInt)

In 2023, Lockbit 3.0 stands out as the most active ransomware gang. LockBit 3.0 is a prominent ransomware family that has been active since 2019 and continues to be active in 2023.It is known for its high-impact activities and various organizations targeted worldwide. The LockBit Gang, the group behind the malware, exploit vulnerabilities in software, such as Citrix's software, commonly referred to as "Citrix Bleed," to gain the initial access to systems. Once inside a network, LockBit 3.0 encrypts data and makes ransom demands to release it. The group has also adopted a double-extortion technique which includes also threatening to leak the stolen data if the ransom is not paid.

ALPHV, also referred to as BlackCat Ransomware, comes second as the most active ransomware group of 2023. It is a highly active ransomware group that has been operating since at least November 2021. ALPHV is known for its innovative use of the Rust programming language and has been involved in various high-profile attacks targeting organizations worldwide. The group utilizes

a double-extortion technique encrypting victim's data and threatening to leak it if the ransom is not paid. They have been observed using malicious infrastructures hosted on onion domains. ALPHV has claimed responsibility for compromising numerous organizations, including law firms, construction companies, chemical manufacturers, and IT service providers. They have targeted victims in different countries such as Canada, the United States, France, Saudi Arabia, and Nigeria.

Finally, in the third place in 2023 is the CL0P ransomware gang. It is a financially motivated cybercrime group that has been active since early 2019. The group targets organizations in a range of sectors, such as manufacturing, retail, and healthcare. The gang is well-known for both its aggressive negotiation strategies and its use of zero-day exploits to obtain early access to victim networks. The group installs their ransomware payload which encrypts all files on the hacked systems as soon as they get access to the victim network. The attackers then send the victim a ransom note demanding for cryptocurrency payments in exchange for decryption key. Law enforcement agencies from all around the world have been attempting to locate and dismantle the CL0P ransomware gang, however, the CL0P ransomware group is still active and continues to attack companies worldwide despite the best prevention efforts.

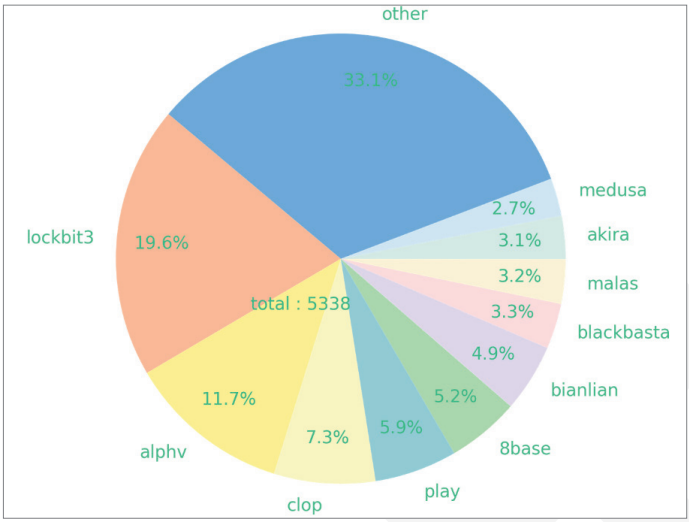


**Figure 7.** Victims by group in 2023 (Ransomware.live)

## Cisco IOS-XE ZeroDay

Another incident that caught everyone off guard involves a zero-day privilege escalation vulnerability (CVE-2023-20198) that affects Cisco devices running the web administration interface and IOS XE software. With a Cisco severity rating of 10 out of 10, this vulnerability enables remote exploitation without authentication, giving attackers total administrative control over devices that have been compromised. Skilled attackers have used this vulnerability to gain access to tens of thousands of devices worldwide and install backdoors for a persistent access. The exploitation activity was made possible by an existing rule for CVE-2021-1435 that suggests a multiple attack strategy. Over several days, the situation escalated to a significant number of compromised hosts. Geographically, the infection spread throughout the world, primarily affecting the US, the Philippines, and Mexico. The main targets were telecommunications companies represented by autonomous systems, like UNINET and GLOBE-TELECOM-AS. Such companies are vulnerable to cyberattacks because they usually offer internet services to both homes and businesses. The effect is not limited to big businesses, highlighting the importance of vulnerability to less sizeable organizations and people.

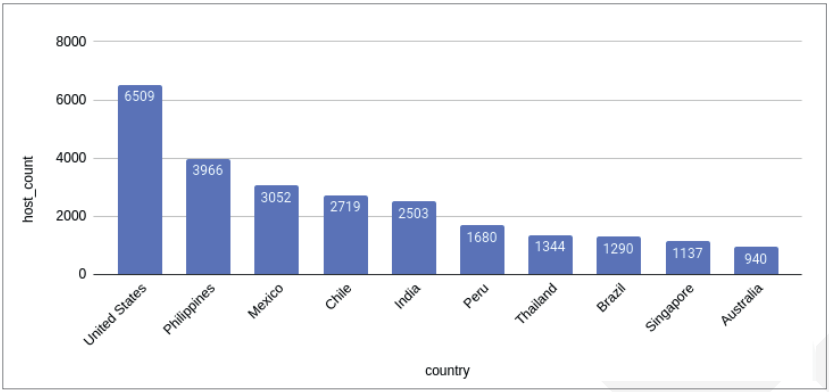


**Figure 8.** Compromised host per countries (Censys)

# 06/ 2023 Trends & 2024 Predictions

With the rise of double extortion techniques, the ransomware evolution has taken a disturbing turn. A new dimension has been added to the toolkit of threat actors who were previously restricted to exfiltrating and encrypting sensitive data. Aside from locking the data, the double threat aims to leak or auction it if ransom is not paid. This development highlights the meaningful change in ransomware tactics presenting enormous challenges to conventional backup and recovery procedures – and demonstrating the evolution of ransomware groups into essential actors in the larger cybercrime ecosystem.

The exponential growth in remote work has led to an increase in cyber threats that target vulnerabilities through collaboration and remote access technologies. The growing trend highlights the importance of strengthened security protocols in remote work setups. There are serious risks for businesses using remote or hybrid work environments if vulnerabilities in commonly used tools, like Atlassian Confluence and Citrix's NetScaler ADC, are exploited. Notably, threat actors have taken advantage of vulnerabilities in Citrix products, such as CVE-2023-3519 and CVE-2023-4966, which permit remote code execution and bypassing authentication, respectively. The sophistication of cyber threats reflected in these breaches is concerning: the adversaries are able to implant web-shells, hijack legitimate user sessions, and circumvent multi-factor authentication. This indicates that the attackers have a thorough understanding of and the ability to exploit vulnerabilities within remote work infrastructure. In addition, the ease of exploitation and the widespread use of remote collaboration tools, such as Atlassian Confluence, highlight the increased vulnerability of these environments to cyberattacks. Furthermore, people are still a major cybersecurity risk because they are frequently seen as the weakest link in the system and are easily tricked by social engineering techniques, like phishing, which can compromise otherwise well-defended systems. Robust cybersecurity measures, thorough employee training, and ongoing vigilance are required in this complex landscape to mitigate the ever-evolving threats against remote work infrastructure. In addition, the ease of exploitation and the widespread use of remote collaboration tools, such as Atlassian Confluence, highlight the increased vulnerability of these environments to cyberattacks.

Malicious actors are using AI and machine learning to increase the sophistication and effectiveness of their attacks, therefore AI-driven cyber risks are becoming a greater concern. These threats are more challenging to identify since they automate and optimise different cyberattack stages using sophisticated algorithms. Malware with AI capabilities may change and adapt in real time which allows it to get around conventional protection measures. Threat actors can use AI for social engineering, phishing attempts, and even creating ransomware that is specific to a certain situation and context. Furthermore, data manipulation, creation of lifelike deep fake content, and exploitation of flaws in newly developed technologies, like Internet of Things devices, are all instances of how AI is used in cyber threats. As businesses depend increasingly on artificial intelligence for operations, cybersecurity professionals face enormous obstacles in creating adaptable defences against these sophisticated and ever-evolving attacks due to the possibility of AI-driven cyber threats.

# 07/ Recommendations

2023 showed that ransomware attacks are here to stay and not only that but also constantly evolving, and hackers are getting increasingly creative. Tactics like double extortion are getting increasingly common. Ransomware attacks have historically focused on encrypting company data and demanding for ransom to unlock it. Now threat actors go one step further with double extortion: extracting confidential information, encrypting it, then the victim is then subjected to increased pressure and blackmail using the stolen data as leverage. If the ransom is not paid in a timely manner, threat actors threaten to publish or auction the stolen data on the dark web or other platforms. This tactic not only puts the victim at greater financial risk due to the possibility of data exposure and the ensuing fallout, but it also makes the response procedure more difficult. Now victims not only have to focus on restoring and accessing encrypted data, but also must make sure that exfiltrated data does not get leaked and end up in the hands of adversaries ready to use it in further attacks. Using zero-trust or least-privileged access policy is a vital line of defence against cybercriminals, especially considering the growing reliance on cloud processing. This method enforces the idea of inherent trust and considers everything to be potentially hostile unless verified and given permission. The key principles of a zero-trust architecture for ransomware defence are limiting the attack surface by hiding users and apps from the internet, limiting lateral movement by limiting data exposure through micro segmentation, and putting in place comprehensive inspection for efficient threat and data loss prevention. Organisations can be made even more resilient against ransomware attacks by utilising deception technologies and a proxy-based brokered exchange, which secure access, reduce potential damage, and thoroughly inspect all traffic. As always, having backup and recovery procedures is crucial in defending against ransomware attacks. Not only that, but periodically testing and running backups and procedures is as important as having them in the first place.

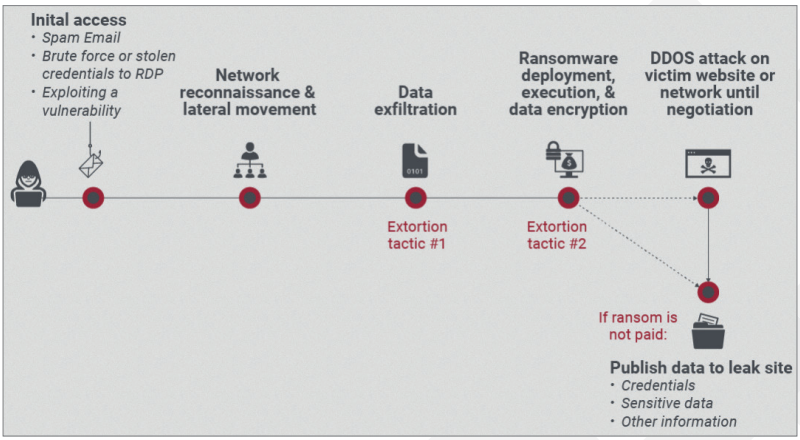


**Figure 9.** Attack chain of double extortion ransomware (Zscaler)

Employee training is another crucial step to keeping an organisation safe against emerging cyber threats. Ransomware gangs frequently use strategies like phishing and social engineering to take advantage of people's weaknesses. Proper training aims to reduce these risks by raising staff members' awareness. It includes training to identify phishing emails, confirming legitimacy of the sender, and refraining from actions that might compromise security. Employees receive safe internet practices training, such as following links, downloading files, and interacting with unidentified sources with caution. To improve the overall security hygiene, strong password policies, frequent software updates, and significance of multi-factor authentication are emphasised. These at first sight easy and simple precautions can highly improve an organisation's security posture when facing potential cyber threats.

Organisations need to implement a thorough and flexible defence strategy to effectively combat the increasing number of AI-driven cyberattacks that target business operations: starting with putting in place sophisticated AI-based threat detection tools that can identify patterns and anomalies that point to attacks driven by AI. Use AI algorithms alongside behavioural analytics to track and examine user behaviour, establish baselines and identify any deviations that might indicate a security breach. Implement AI-driven endpoint security solutions to instantly identify and stop malware. When implementing AI technologies, make sure to follow secure development practices, ensure regular software updates, and patch software. To stay up to date on the newest AI-driven threat vectors, participate in cooperative threat intelligence sharing and adopt a zero-trust architecture with strict access controls and ongoing monitoring.

# 08/ Endnote

Our current view of cyber-threat landscape today shows that the dynamic and ever-evolving nature of cyber threats demands constant vigilance and adaptation. In the upcoming year, several trends could affect the cybersecurity scene. Organisations must strengthen their cyber defences considering the increasing frequency of sophisticated ransomware attacks, emergence of state-sponsored threat actors, and the growing targeting of critical infrastructure. It may become more complicated to integrate machine learning and artificial intelligence into offensive and defensive cyber operations. Furthermore, the emergence of IoT and 5G technologies present previously unheard-of difficulties as a result of increased attack surface. To mitigate emerging cyber risks, cooperation, sharing of threat intelligence, and proactive defence strategies will be essential as we navigate this terrain. Staying one step ahead of tomorrow's cyber adversaries will require a commitment to innovation and resilience, even though the specifics are still unknown.


ISSUED BY THE REGIONAL CYBER DEFENCE CENTRE,
PART OF NATIONAL CYBER SECURITY CENTRE OF LITHUANIA

Layout by the Visual Information Division
of the General Affairs Department of the Ministry of National Defence,
Totorių g. 25, LT-01121 Vilnius


REGIONAL CYBER DEFENCE CENTRE

# CTAC 2023 Yearly Report