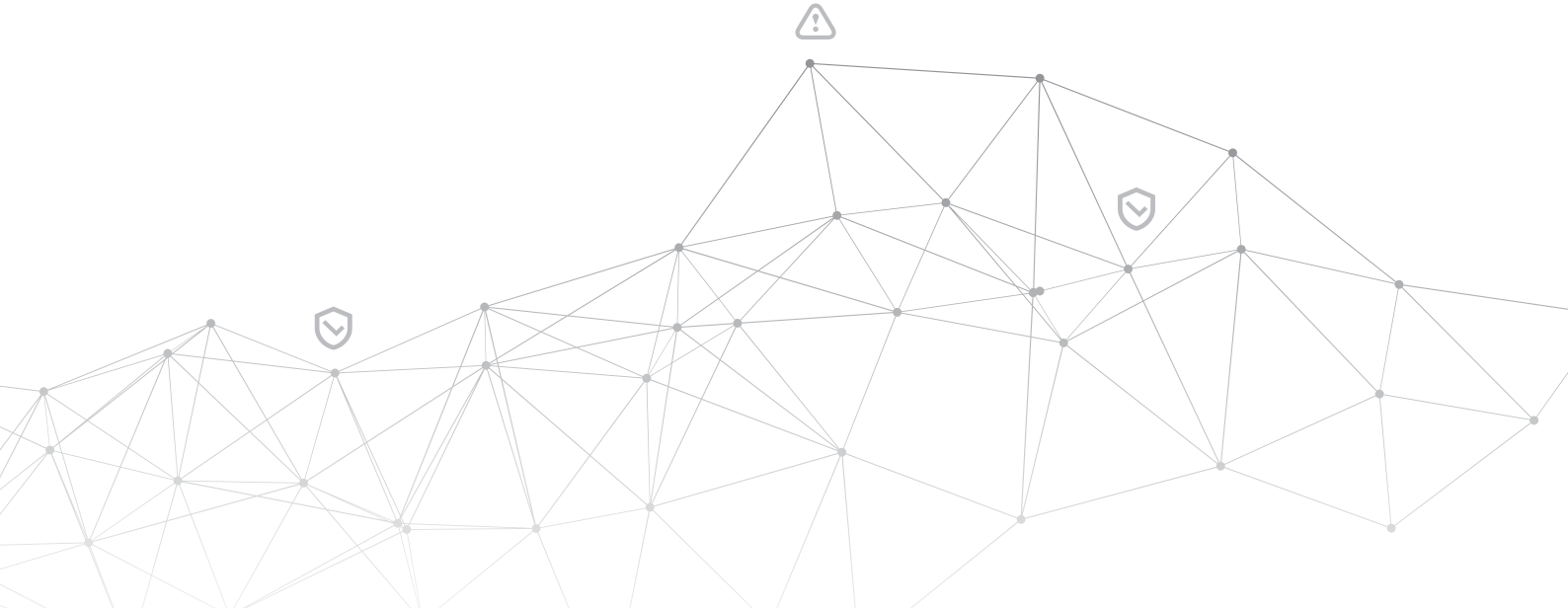
CTAC 2022
Yearly Report




CTAC 2022
YEARLY REPORT



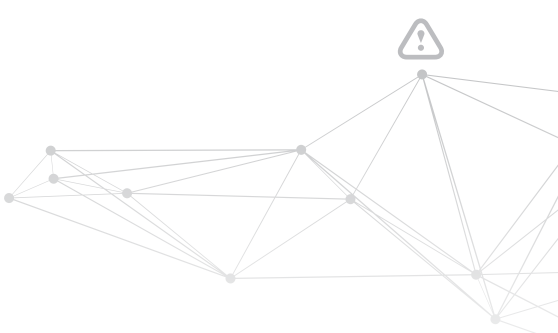
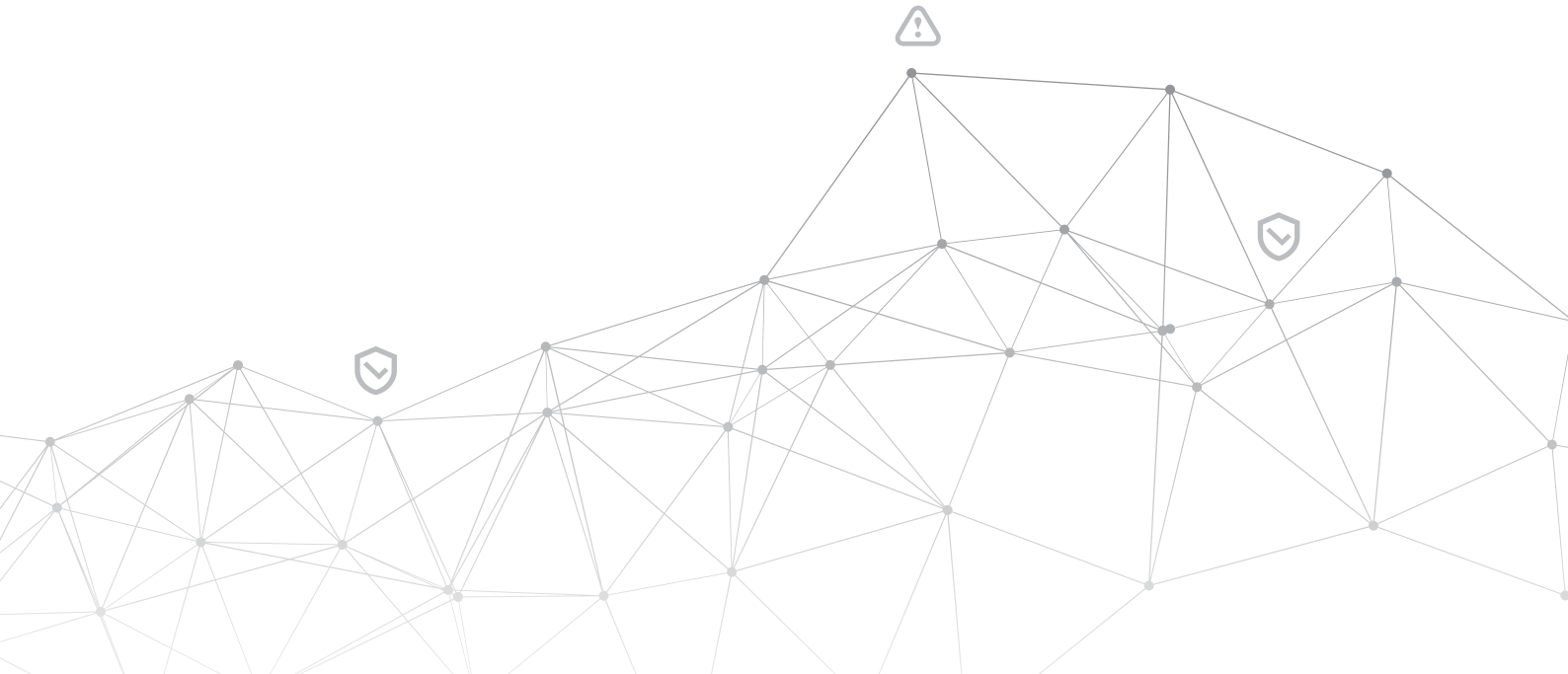


Table of Contents



Director's Foreword

Col. Romualdas Petkevičius,
Director of RCDC at CEE Digital Summit 2022 in Warsaw

In 2022, the cyber security landscape has evolved significantly as organizations and individuals strive to keep their data safe. Cybercriminals have become more sophisticated and risks associated with data security have become more complex. Cybersecurity professionals are in high demand as organizations look to protect their data and ensure their networks remain secure. New technologies such as AI and machine learning are used to detect and prevent cyber-attacks, while cloud computing provides a platform for data storage and transmission.

Companies are investing heavily in cyber security training and developing robust policies to protect their data. As the cyber security landscape continues to evolve, organizations must stay ahead of the curve to stay safe. I am glad that the Regional Cyber Defence Centre (RCDC), the Cyber Threat Analysis Cell (CTAC) in particular, marked its first fully operational year and delivered quite some products. Unfortunately, the war has shifted our international expert's rotations. Nevertheless, we came out strong and proved that international collaborations are powerful tools for fighting cybercrime.

List of Abbreviations

Term/abbreviation	Meaning/explanation
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CTAC	Cyber Threat Analysis Cell
DDoS	Distributed Denial of Service
Disinformation	Disinformation refers to false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction.
FSB	Federal Security Service
GRU	The Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ICS	Industrial Control System
IOC	Indicators Of Compromise
Malinformation	Malinformation refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.
Misinformation	Misinformation refers to false information that is not intended to cause harm.
NCSC	National Cyber Security Centre
OT	Operational Technology
RCDC	Regional Cyber Defence Centre
SCADA	Supervisory control and data acquisition
SIEM	Security Information and Event Management
SSU	Ukrainian Security Service
SVR	The Foreign Intelligence Service of the Russian Federation
TTP	Tactics, Techniques and Procedures

01/Summary

2022 was a very exciting and important year for the Regional Cyber Defence Centre. It has also been a rough and tumble year across the world when it comes to cybersecurity. Cyber warfare frequently kicks off contemporary conflicts by a variety of means, such as information manipulation, attacks on infrastructure, interference in elections, and reconnaissance. The physical conflict in Ukraine was sparked by years of cyber-attacks by the Russian adversary and dissemination of false information online. Following the rapid escalation of these information strikes into damaging cyber-attacks against vital service targets, forces descended on the ground for a military invasion. The stakes have never been so high ever before as the cybercrime epidemic drives the risk of even undermining public confidence in such treasured concepts as democracy, capitalism, and individual privacy. The RCDC's 2022 yearly report closely examines what happened this past year in a detailed analysis.

02/What CTAC Did in 2022

The RCDC started the year with a cooperative mission with the NCSC to Ukraine to help evaluate cyber security needs in the case of an aggressor attack. The mission took place between February 14 – 16 2022. RCDC representatives met with personnel of the Ukrainian Ministry of Energy and discussed possible cooperation between Lithuania and Ukraine on critical infrastructure cyber defense. In the discussion, there was a mutual understanding regarding the need to efficiently exchange cyber security information (TTP's, IOC's, etc.) through the MISP platform. The invasion of Ukraine by the Russian Federation paused these plans temporarily.

Figure 1. The Lithuanian Delegation (on the left) meeting with Ukrainian Minister of Energy

NCSC and RCDC personnel also met with representatives of the Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty (MITIT). A fruitful discussion with MITIT leaders has resulted not only in a partnership and exchange of useful information but also in an internship program for MITIT final-year cadets in the RCDC CTAC. For the pilot stage, the MITIT sent two of their most skilled students to evaluate the training program prepared by the RCDC. They provided plenty of positive feedback and pointed out what needed improvement.

The RCDC team had worked to include the latest know-how in the fields of the most relevance for the MITIT Cyber Defense cadets. The RCDC acquired a Cyber Range platform and a malware analysis laboratory to improve training quality. It was agreed to accept MITIT officers and cadets studying for bachelor's and master's degrees via the internship program regularly.

Figure 2. CTAC personnel with MITIT cadets

In 2022, CTAC also started a process of identifying and refining their daily tasks and routines.

- Starting in March, weekly reports on the regional cyber threat landscape were issued, making over 40 of these during 2022;
- At least 4 reports on specific cyber events with numerous updates were released;
- 2 recommendations on DDoS and Ransomware detailing cyber attacks and mitigation measures;
- 4 quarterly reports;
- 1 yearly report.

Our colleagues from Georgia and Ukraine were working in the Centre alongside the Lithuanian staff. A total of 84 days were filled in by CSB personnel, while due to war, Ukrainians only managed to work for October-December 2022. However, this input led CTAC to start working on an ambitious project that will be announced in 2023.

Besides the daily routine of generating intelligence reports, CTAC contributed to the:

- Counter-ransomware initiative - the United States initiative, the main idea is to bring together different countries to fight against the rising ransomware attack numbers. The CTAC input is semi-annual ransomware intelligence reports, as well as facilitation of a dedicated MISP platform for ransomware information exchange.
- Amber Mist 2022 - the Lithuanian Armed Forces Defence Headquarters hosted an annual cybersecurity exercise. CTAC provided daily intelligence briefings for Blue Teams in its part as Intel Fusion Element.
- On January 13th, 2023, documents were signed making Poland officially a new member of the RCDC family.

03/What CTAC Saw in 2022

A month before Russia launched a full-scale invasion of Ukraine we were witnessing a rise of data-wiper malware. In attacks on Ukraine's critical infrastructure facilities and information resources the Russian hacking groups used such malware as WhisperGate/WhisperKill, HermeticWiper (FoxBlade), IssacWiper (Lasainraw), CaddyWiper, AcidRain (SKYFALL), AwfulShred, SoloShred, SonicVote (HermeticRansom), Industroyer2, DoubleZero (FiberLake). At the same time, FoxBlade, CaddyWiper, Industroyer ICS, and Prestige are associated with the activities of the Sandworm hacker group, WhisperGate – with DEV-0586, AcidRain (SKYFALL) – with APT28, Cuba Ransomware – with UNC2596. Most of the list is quite new malware and before the beginning of the Russian invasion of Ukraine there were no recorded facts of its use which may indicate its intended purpose and use during the preparation and conduct of the so-called "special military operation".

DDoS was one of the most if not the most popular type of attack in 2022. Many fell victim to DDoS attacks but Ukraine, its supporters, and Russia were subjected to the biggest one. Scores of newly found hacktivist groups from Russia and Ukraine started sending numerous requests to the opposing side in hopes of crippling their infrastructure. The biggest attacks came when the hacktivists started using JavaScript DDoS which only requires people who are not even skillful in IT to could go to specific websites and forged requests start being sent to a target machine. Later in the year, as people grew tired of the war and hacktivists shifted to information campaigns, we saw the number of DDoS attacks decrease, but every once in a while the pro-Russian hacktivist group Killnet and its associated groups conducted DDoS attacks as geopolitical trends required.

As 2022 was passing by, we watched an increase in disinformation campaigns. Most of the campaigns were in one way or another related to Russia's war in Ukraine. Even though Russia has a long history of disseminating disinformation, Ukraine withheld and repelled its attempts and conducted very successful campaigns of its own. As well, IoT devices are gaining more and more appeal, and thus bring cybersecurity issues. Despite extensive explanation, warnings, and IoT security flaw fixes, basic safeguards, like requiring strong passwords and forbidding default logins and user accounts are still disregarded. IoT devices are hacked and turned into botnets which generate a huge source of DDoS traffic. Botnets are not going anywhere. Botnet attacks have become a commonplace due to the exponential rise in the number of vulnerable computers and poorly secured IoT devices that can be recruited into IoT botnets. Botnet and DDoS attacks used in cyberwarfare have been seen on both sides of the Russian war against Ukraine.

04/Regional Threat Analysis

The landscape of cyber threats has been significantly impacted by Russia's invasion of Ukraine. Russian-based phishing assaults against the email addresses of companies with headquarters in Europe and the US have skyrocketed since the start of the conflict. Without a clearly defined or tested plan, the IT Army of Ukraine was formed on the spot. The IT Army was created out of necessity, but over time, it transformed into a hybrid organization that is neither civilian nor military, public nor private. Taken approach is more like strategic move for Ukraine's defense and intelligence services to back off and allow the IT Army to operate freely and independently, especially during the time of war. At first, there were many questions whether the new organization could handle the pressure of the Russian-based DDoS attacks across Ukraine's cyberspace. The results showed a different outcome shortly, the IT Army managed to defend Ukraine's infrastructure quite well and even changed their game plan from defense to offense afterwards.

4.1. Cyber Activity in Lithuania

Lithuania was a target of numerous cyber-attacks in 2022. Most of them were noticeable during the early stages of the Ukrainian war with the Russian Federation. The figure below shows a sharp spike in cyber activity right after the start of the war in February, and then a large spike between June and July. This correlates with various pro-Russian and anti-Russian hacktivist group activities.

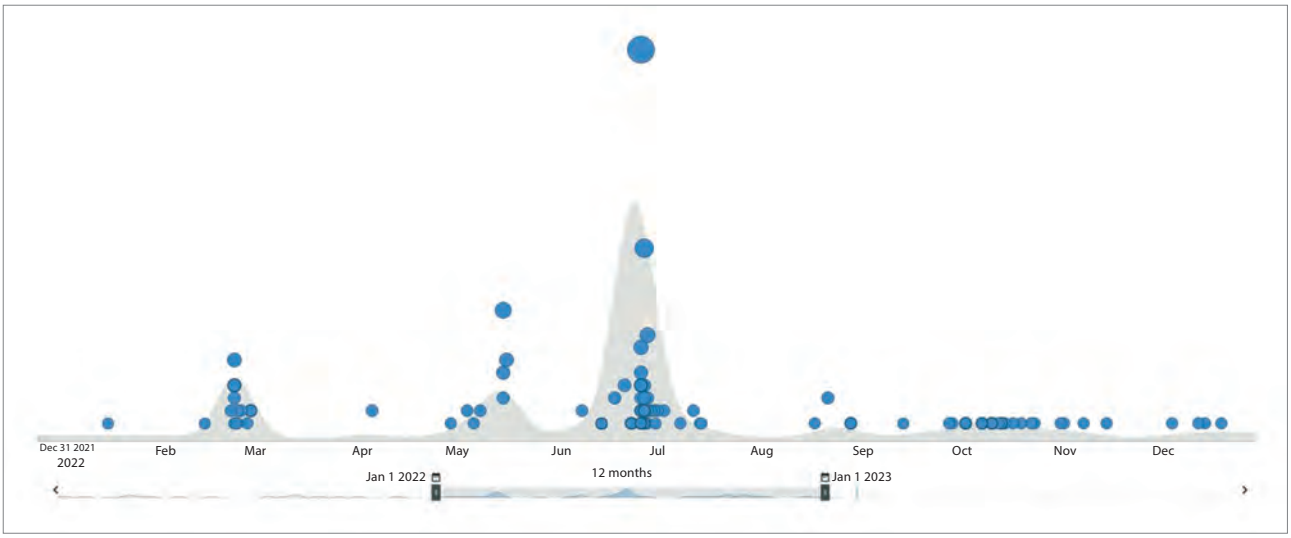


Figure 3. Graph of cyber incidents in Lithuania throughout 2022

The most notable of the attacks was the DDoS campaign against the Lithuanian governmental sector. Although numerous organizations were targeted, the attacks exposed a weakness in network infrastructure of the State Tax Inspectorate of the Republic Of Lithuania (VMI). The disruption in the electronic tax declaration system (EDS) was felt for over a week.

All the other governmental sectors recovered from attacks within the range of 1 to 24 hours by utilizing geolocation blocking or content delivery services (CDN).

There were a few instances of data breaches in the private and financial sectors with the Russian hacktivist group Killnet as the main suspect.

4.2. Cyber Activity in Ukraine

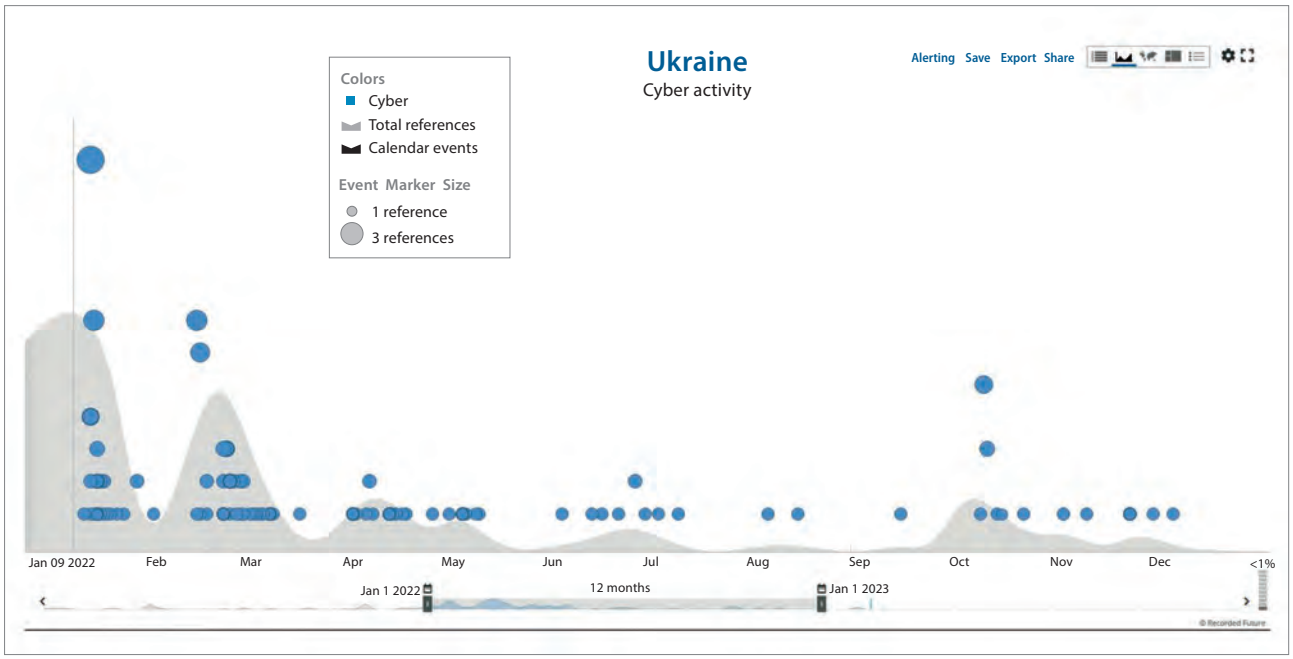


Figure 4. Graph of cyber incidents in Ukraine throughout 2022

The cyber war in Ukraine (mostly activities of Russian, but also Chinese, Iranian, Belarusian, and various other criminal groups) has been going on for many years, however, it has acquired an unprecedented size since December 2021, when the pro-Russian groups launched a full-scale open cyberwar against Ukraine. Various APT groups, affiliated with Russian military structures are suspected to have conducted a series of attacks on different sectors according to analytics available to the Ministry of Defense of Ukraine, virtually the entire information infrastructure of Ukraine and most of the critical and military infrastructure facilities were exposed to the cyber-attacks by the aggressor state:

- 20+ thousand complex targeted cyber operations.
- 200+ cyber-attacks per day on average.
- Energy sector: 600+ cyber-attacks.
- Other critical infrastructure: 400+ cyber-attacks.
- 3+ billion signals of primary abnormal cyber events.

The main purpose of the attacks was to access critical data and shut down or subvert Ukraine's critical infrastructure.

Ukraine had to establish a coherent cyber defense system to strengthen its cyber security extremely fast, including extension of the Cyber Teams capacity, adoption of new laws, regulations, incident handling instructions, etc., in accordance with the new challenges, especially in military and critical infrastructure sectors. To that end, Ukraine's cyber security forces:

- Established a Cyber Security Operations Centre under the Ministry of Defense to protect military-affiliated assets, provide threat analysis, and supervise the formation and operation of the Cyber Defense and IT Divisions at MoD, Armed Forces, and critical infrastructure cyber divisions.
- Equipped the Armed Forces of Ukraine with new cyber weapons and trained personnel assigned to perform tasks for the Armed Forces.
- Developed and strengthened strong communication channels (expertise sharing, data sharing platforms, linked incident response protocols, etc.) with cyber security centers inside the country.

- Expanded cooperation with foreign partners: training, expertise sharing, expert exchange, etc.
- The Government revisited laws and regulation instructions (especially for cloud technologies) to simplify usage of modern cyber defense tools in public and military sectors.
- A unified security information and event management system (SIEM) has been implemented, its functioning is based on the SCZK DKIB SBU and allows monitoring of events in real-time and analyzing the state of information security. The Cyber Attack Investigation Unit of the SBU DKIB switched to using telemetry analysis-based tools such as Endpoint Detection and Response.
- As part of countering propaganda of the Russian Federation, monitoring has intensified, as well as further blocking of individual information exchange platforms and mass media (Telegram, YouTube, Facebook, and other) that are used to spread false information.
- National cyber security entities of Ukraine pursue an intense information campaign to increase the level of cyber protection, and computer literacy of the population and business.

Although the main events are taking place on the battlefield, the cyber war continues with new challenges, new cyber weapons, and new levels of threats - adversaries are making huge efforts to destroy infrastructure, including digital resources, and also constantly try to steal important data and assets that can have an impact on the battlefield. This leads to constant pressure on all cyber forces of Ukraine in coordination and support of foreign partners; Ukraine became an important member of the entire European cyber security forces.

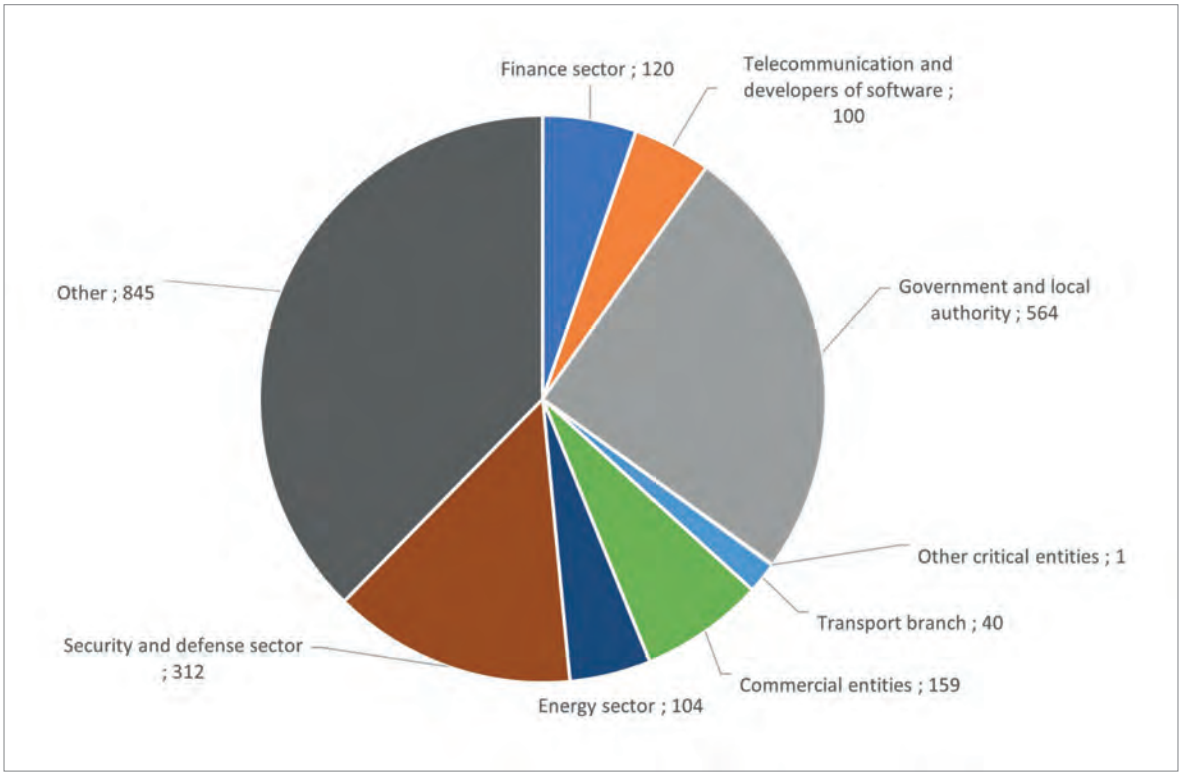


Figure 5. Quantity of cyber incidents in each sector in 2022

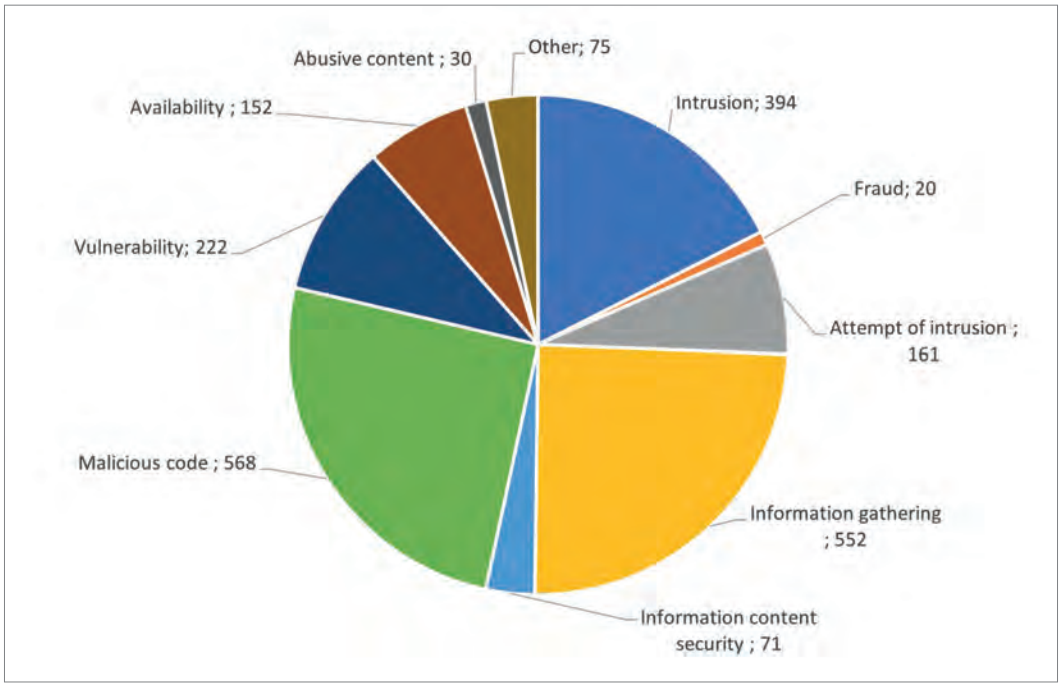


Figure 6. Types of cyber incidents in 2022

4.3. Cyber Activity in Georgia

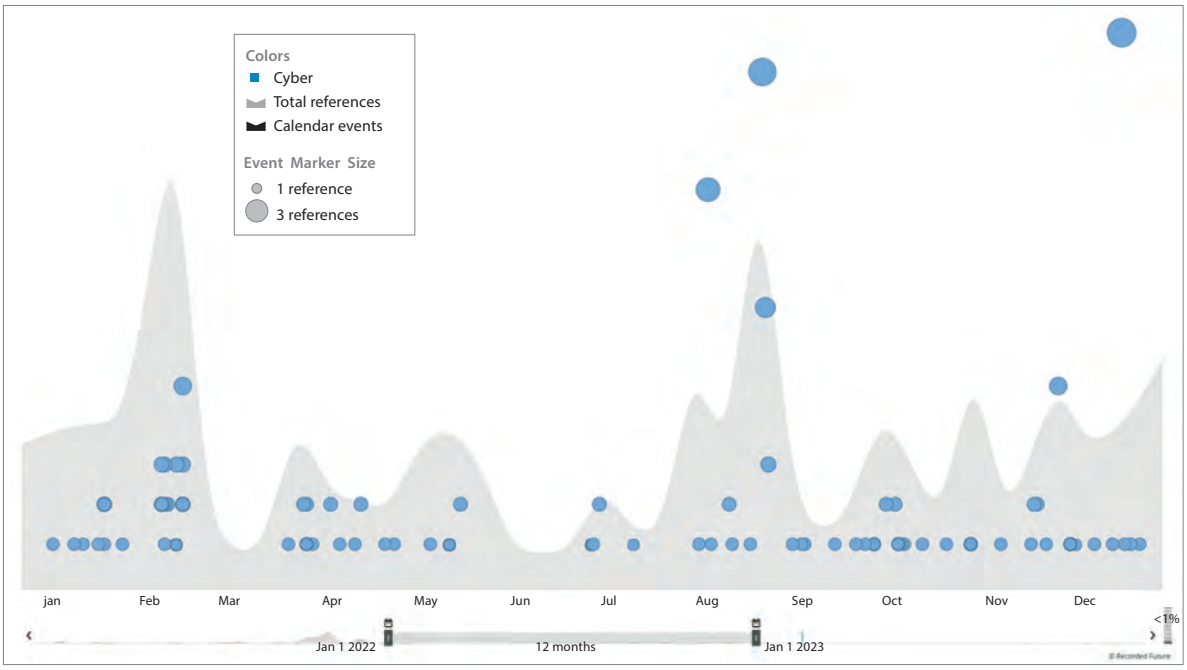


Figure 7. Graph of cyber incidents in Sakartvelo throughout 2022

The relationship between the Russian Federation and the Republic of Georgia remains tense after the 2008 Russo-Georgian War that lasted for 5 days. In 2022, the cyber activity of Georgia remained quite calm due as the main focus was captured by the Russo-Ukrainian war. The majority of Russian-sponsored cyber threat actors have their attacks on Ukraine and Allied countries, like the United States of America or members of the European Union. A review of the Georgian incident statistics reveals a trend and concern of malware and computer virus incidents. Although Georgia has suffered its fair share of DDoS attacks, those were small in scale due to attackers' resources being spread thin.

Some risks might emerge in 2023 due to the political situation in Georgia. A large number of Russian citizens are fleeing mobilization and relocating to Georgia since Russians have an option of staying in the country for 12 months without requiring a visa. This could cause problems in 2023 similar to the problems seen in Ukraine where Russian nationals, with support from their Government, established cyber bot farms, ran misinformation campaigns, and conducted offensive cyber operations against Ukraine and its partners. The RCDC will continue to monitor the situation in Georgia and will continue to work with the Georgian Cyber Security Bureau to mitigate the related threats as much as possible.

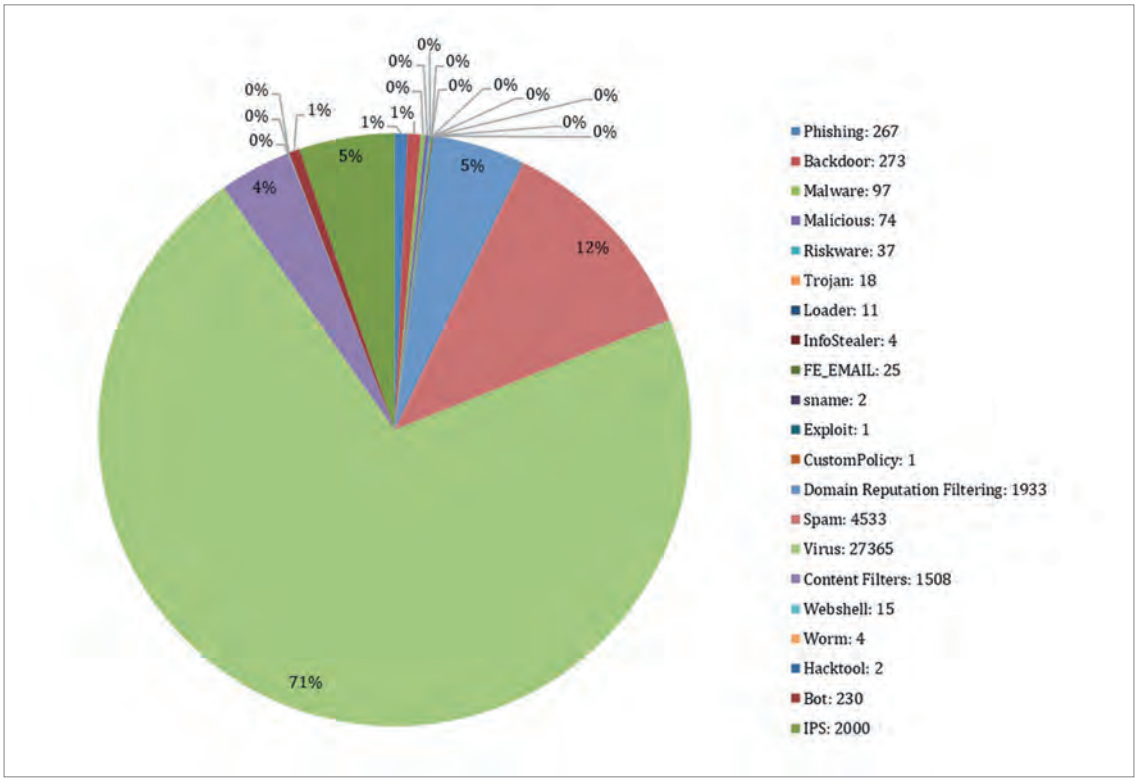


Figure 8. Types of cyber incidents in 2022 in Sakartvelo

4.4. Cyber Activity in the United States

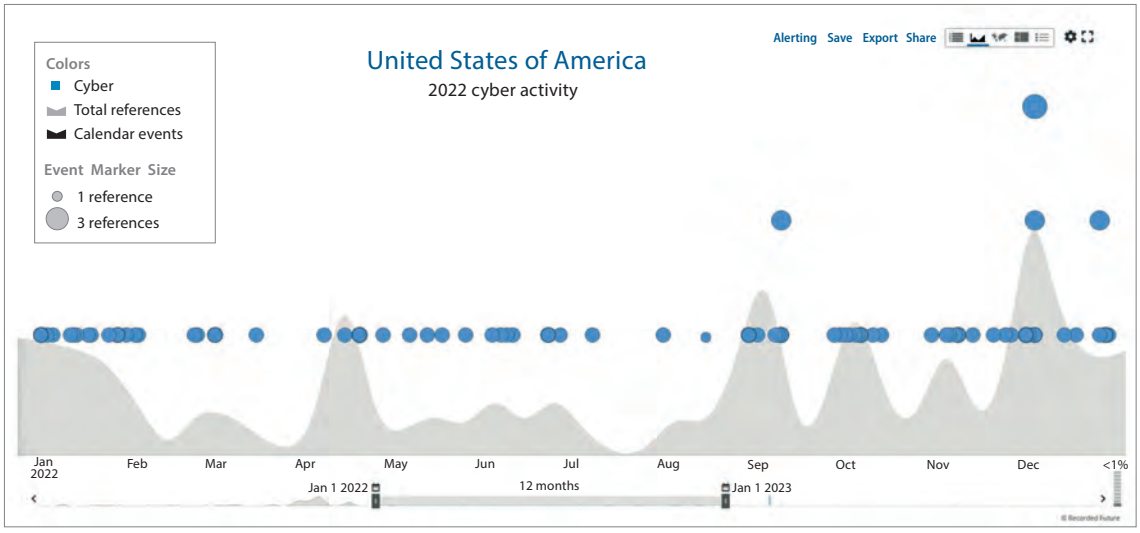


Figure 9. Graph of cyber incidents in the United States throughout 2022

The United States, due to the size of the population (approximately 333 million) and role in the world as a superpower, is a constant target for malicious cyber activity. The graph above shows a steady stream of cyber incidents during 2022. It is worth noting that threat actors attempt to use holidays and specific financial dates to conduct their attacks. That is usually particularly noticeable during April when US citizens have to submit their tax information. Additionally, there is a noticeable spike in activity at the end of the year, during Black Friday, Cyber Monday, and in general, during national holidays such as the Christmas season.

4.5. US Threat Landscape: 2022 Year in Review

The United States continues to view state-sponsored cyber activities as some of the most robust and progressive threats to the US governmental and civilian networks. For example, the state-sponsored PRC (People's Republic of China) cyber actors have readily exploited vulnerabilities to compromise unpatched network devices. Network devices, such as Small Office/Home Office (SOHO) routers and Network Attached Storage (NAS) devices, served as additional access points to route command and control (C2) traffic and acted as midpoints to conduct network intrusions on other entities. PRC state-sponsored cyber actors regularly used open-source tools, such as RouterSploit and RouterScan, for surveillance and vulnerability scanning.

According to the assessment of CISA, the FBI, and the Department of Energy (DOE), state-sponsored Russian cyber operations continue to pose a threat to the US critical infrastructure organizations, including those in the Defense Industrial Base (DIB), Healthcare, and Energy Sector networks. Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics–including spear phishing, brute force, and exploiting known vulnerabilities to gain initial access to target networks. Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware.

The Iranian government-sponsored APT actors were observed exploiting known Fortinet and Microsoft Exchange vulnerabilities to gain initial access to multiple U.S. critical infrastructure sectors in furtherance of malicious activities, including ransom operations. These actors have been observed using the following tools:

- Fast Reverse Proxy (FRP) for command and control (C2).
- Plink for C2.
- Remote Desktop Protocol (RDP) for lateral movement.
- BitLocker for data encryption.
- SoftPerfect Network Scanner for system network configuration discovery.

Since May 2021, the FBI has observed and responded to multiple Maui ransomware incidents at Healthcare and Public Health Sector organizations. North Korean state-sponsored cyber actors used Maui ransomware to encrypt servers responsible for healthcare services. Despite these state-sponsored attacks throughout 2022, the United States has seen a slight decrease in publicly-reported ransomware attacks. As reported by Comparitech researchers, 2022 saw half the amount of attacks (from 676 in 2021 to 335 in 2022). That same trend follows the demand for payment, and records/data impacted by these attacks.

Depicted below is the ransomware heatmap for the year 2022. This displays the location of ransomware attacks, all associated ransomware strains, and ransom statistics.

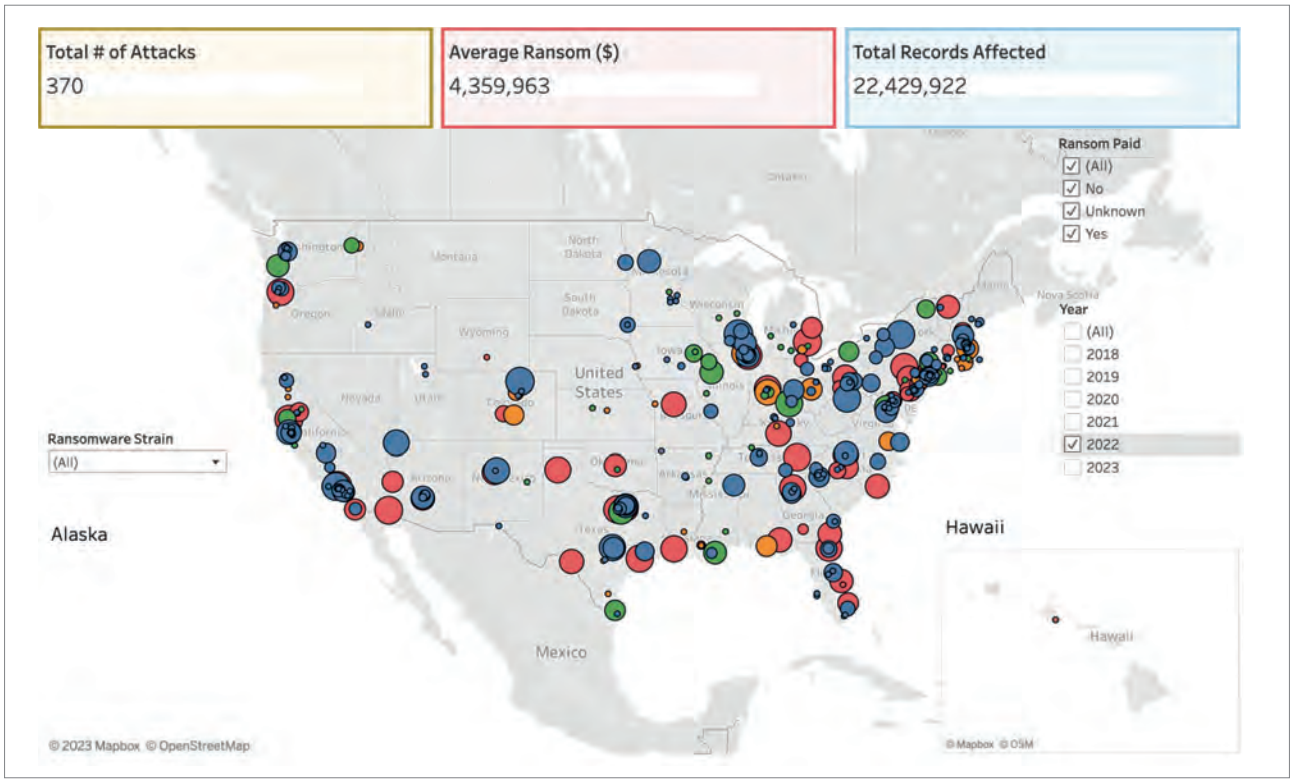


Figure 10. Map of US ransomware attacks from 2018 to present

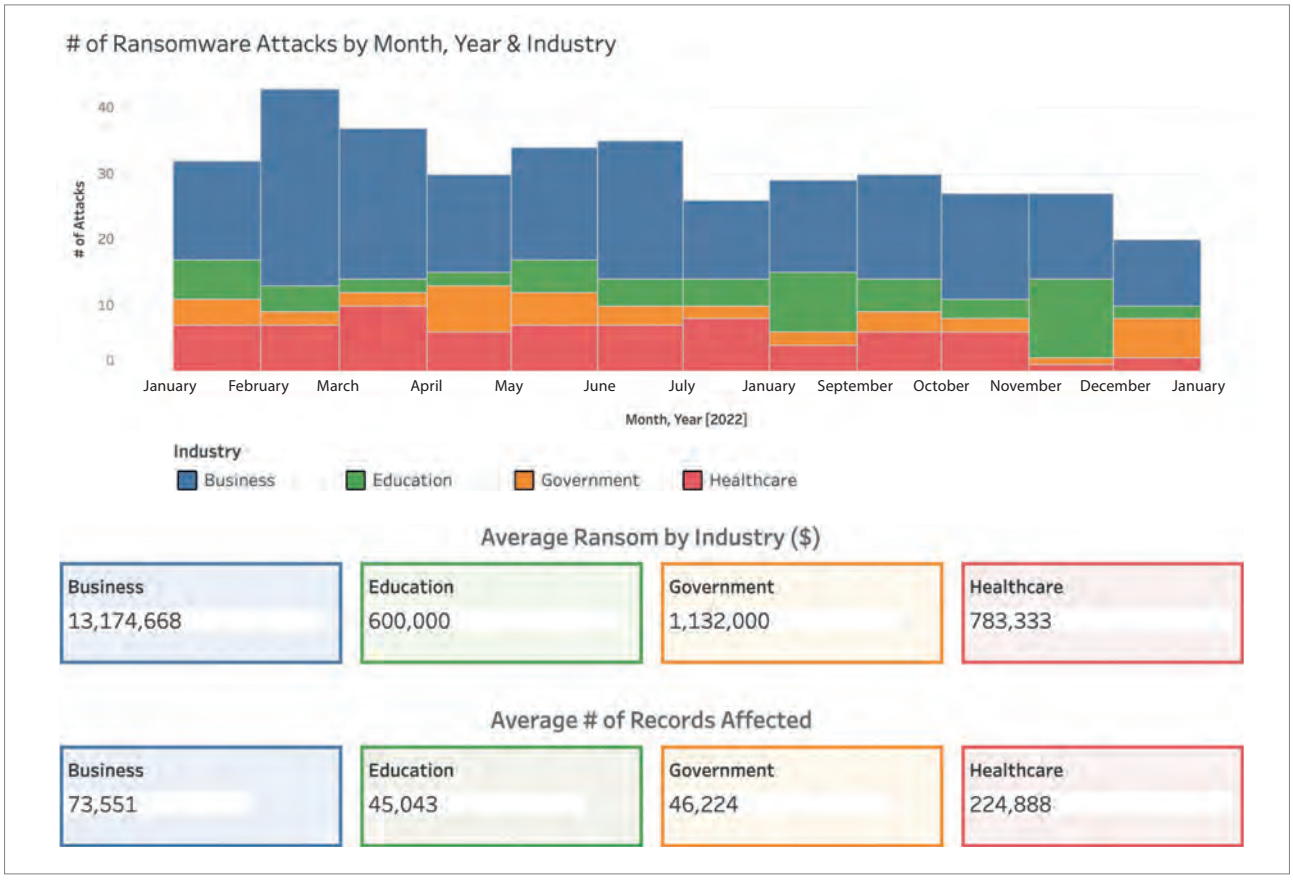


Figure 11. The monthly and cumulative breakdown of attacks in 2022 per industry sector

The next chart displays the monthly and cumulative breakdown of attacks in 2022 per industry sector.

However, the US saw an increase in other forms of cyber attacks and cybercrime. Healthcare facilities in the US alone saw an average of 1,410 weekly cyberattacks per organization in 2022, an 86% increase compared to the previous year. The FBI and the NSA have been actively working to thwart cyber attacks and cybercrime. Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in demanded ransom.

Additionally, through operational collaboration with Defense Industrial Base (DIB) companies and their service providers, the National Security Agency's Cybersecurity Collaboration Center (CCC) has also played a leading role in protecting key critical infrastructure sectors. In 2022, the CCC nearly tripled its partnerships, growing from 110 partners to more than 300 collaborative relationships. The CCC also doubled its analytical exchanges with these partners. Thanks to more than 10,000 bidirectional collaborations – primarily focused on Russian and PRC cyber threats and responding to world events – billions of endpoints have been hardened against nation-state threats.

While the CCC's primary goal is to defend the DIB, its efforts address protection across all 16 US critical infrastructure sectors, reach businesses and consumers, and even protect US allies.

4.6. Threats to the US Energy Sector in 2022

Besides the increase in cyber-attacks, the year 2022 saw the addition of two new threat actors, CHERNOVITE and BENTONITE, which target industrial control systems (ICS) and operational technology (OT). In 2022 alone, a total of 39 separate threat actors have made it their objective to target ICS and OT assets in the United States (US). Due to the importance of maintaining high availability, ICS/OT systems are often targeted by ransomware attacks where governments and industries alike are forced to pay ransom to keep power or other critical infrastructure available. North America has been the primary target of global ransomware attacks on industrial infrastructure. This constituted 40%, or 247 incidents, of the 605 total ICS/OT-related ransomware attacks seen worldwide in 2022.

Organized entities have been appearing over the past several years with objectives geared specifically toward targeting ICS/OT organizations. KOSTOVITE, for example, is a threat group that sought to compromise a US-based energy company that services North America and Australia, and their capabilities include the use of zero-day exploits and internet remote access device compromise. Likewise, KAMACITE is a threat group whose victims include industrial infrastructure in European countries, notably Ukraine, as well as the US. Similar to the alleged Russian threat group Sandworm, KAMACITE employs phishing and credential replay tactics in addition to building custom malware used to compromise critical infrastructure.

While there were no observed ICS Cyber Kill Chain Stage 2 attacks (Develop, Test, Deliver, Install/Modify, Execute ICS Attack) against US energy entities in 2022, the growing number of threat actors targeting ICS and OT resources has triggered legislation seeking to better protect critical infrastructure in the US. For instance, in 2022 the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was signed into law mandating that CISA implement defined reporting instructions. These new reporting instructions require certain asset owners to report incidents within 72 hours of occurrence. CIRCIA aims to shorten response time and coordination, as well as provide advanced warning to other organizations in the energy sector that could also fall victim to the same attack.

05/Threat Actors and Cyber Threats

5.1. Most Exploited Vulnerabilities in 2022

1. Log4Shell/Log4j (CVE-2021-44228)

The Apache Tomcat server software's logging module has a bug called Log4Shell. It was found in 2021 and gave hackers access to the server to run any arbitrary code by sending a specially crafted request. The flaw was fixed in a later version of Tomcat but many systems were left vulnerable and unpatched.

2. Follina (CVE-2022-30190)

Ruby on Rails, a popular web framework, has a flaw called Follina. It was found in 2022 and gave attackers the ability to send a malicious request to the server and have any arbitrary code run on it. The flaw was fixed in a later version of Ruby on Rails but numerous systems were left vulnerable and unpatched.

3. Spring4Shell (CVE-2022-22965)

Applications using the data-finding feature in the spring framework that are running JDK 9+ versions are affected by spring4shell, which enables unauthenticated remote code execution (RCE). This problem has been exploited in the wild and still is being exploited against unpatched systems.

4. F5 BIG-IP (CVE-2022-1388)

The CVE-2022-1388 flaw allowed for remote code executions on systems running iControl REST API and affected versions of F5 BIG-IP, giving the attacker complete control over these servers.

5. ProxyNotShell (CVE-2022-41040 and CVE-2022-41082)

An SSRF (Server-side request forgery) vulnerability exists in the first of the two bugs, CVE-2022-41040. When exploited, it enables a remote trigger of CVE-2022-41082 which permits remote code execution (RCE) when PowerShell is accessible to a threat actor. Both flaws are a part of the attack process and need an authenticated session to be exploited.

6. Zimbra RCE (CVE-2022-27925 and CVE-2022-41352)

The Zimbra Collaboration Suite, a well-known platform for email, calendaring, and other collaboration services, was found to contain these vulnerabilities. By sending a malicious request, they allowed attackers to run any arbitrary code on the server.

7. Atlassian Confluence Vulnerability (CVE-2022-26134)

This vulnerability was used in the wild to support crypto-mining and other malware because it affected all supported versions of the Confluence server. This critical unauthenticated OGNL injection Remote Code Execution vulnerability that impacted the Confluence server and data center was made public on GitHub and had numerous proof of concepts available to exploit it.

8. ZyXEL Vulnerability (CVE-2022-30525)

Rapid7 discovered an unauthorized remote command injection affecting Zyxel firewalls supporting ZTP (ATP, VPN, USG flex series). An unauthenticated, remote attacker could take advantage of this flaw to execute arbitrary code on the vulnerable device as the nobody user.

9. Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882)

When Microsoft Office software does not handle memory objects correctly, a remote code execution vulnerability appears. In the context of the current user, arbitrary code could be run by an attacker who succeeded in exploiting the vulnerability. The attacker could take over the affected system if the user logged on at that moment had administrative user rights. This would allow the attacker to install software, view, edit, or delete data, as well as create new accounts with full user rights. Users who use the system with administrative user rights may be more negatively affected than users whose accounts are set up with restricted user rights.

5.2. 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.

Aliases: Legion, RAYD, Kajluk, Jacky, Impulse, Sakurajima, Mirai.

APT28 (FancyBear) - a Russian-based threat actor whose attacks have ranged far beyond the United States and Western Europe.

Origin: Russia.

Target countries: Ukraine, USA, Lithuania, Georgia, Poland, South Africa, Lebanon, China, etc.

Target sectors: Government, Defense, Military, Transportation, Telecommunications, Healthcare, Financial, Chemical, Law Enforcement, Construction, Industrial Energy, Aviation, Engineering, Embassies, Oil and Gas, IT, Education, Media, Pharmaceutical, Think Tanks, Automotive, NGOs.

Tactics & Techniques: Spear-Phishing, Mimikatz, Coreshell.

Aliases: Yttrium, SIG40, TsarTeam, ATK 5, The Dukes, Swallowtail, ATK 7, STRONTIUM.

APT29 (CozyBear) - threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).

Origin: Russia.

Target countries: Belgium, China, India, Japan, Kazakhstan, New Zealand, South Korea, Turkey, Ukraine, USA.

Target sectors: Government, and Private.

Tactics & Techniques: HAMMERTOSS, TDISCOVER, UPLOADER.

Aliases: Dukes, Group 100, Cozy Duke, EuroAPT, OfficeMonkeys.

APT1 (PLA Unit 61398) - a China-based cyber-espionage group.

Origin: China.

Target countries: Singapore, Canada, South Africa, USA, Switzerland, Norway, Taiwan, Israel, Luxembourg, UAE, UK, Belgium, France, India, and Japan.

Target sectors: Construction, Energy, Engineering, food and agriculture, research, mining, IT, education, media, high-tech, nonprofits, manufacturing, government, satellites, entertainment, transportation, telecommunications, healthcare, private, financial, and chemical.

Tactics & Techniques: Spear-Phishing, Remote access Trojan, Poison Ivy, Mimikatz, SeaSalt.

Aliases: Group 3, Shanghai Group, BrownFox, Comment Panda, Comment Group.

Mustang Panda (RedDelta) - a China-based cyber espionage threat actor that was first observed in 2017 but may have been conducting operations since at least 2014.

Origin: China.

Target countries: U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam.

Target sectors: government entities, nonprofits, religious, and other non-governmental institutions.

Tactics & Techniques: Phishing, CobaltStrike, Command, and Scripting Interpreter: Windows Command Shell, Visual Basic.

Aliases: TA416, RedDelta, BRONZE PRESIDENT.

Sandworm (Voodoo bear) - a Russian cyber-military unit of the GRU, the organization in charge of Russian military intelligence.

Origin: Russia.

Target countries: Ukraine, France, Georgia.

Target sectors: Government, Energy.

Tactics & Techniques: Zero-day exploiting, Cyberespionage.

Aliases: ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear.

5.3. Different Types of Attacks

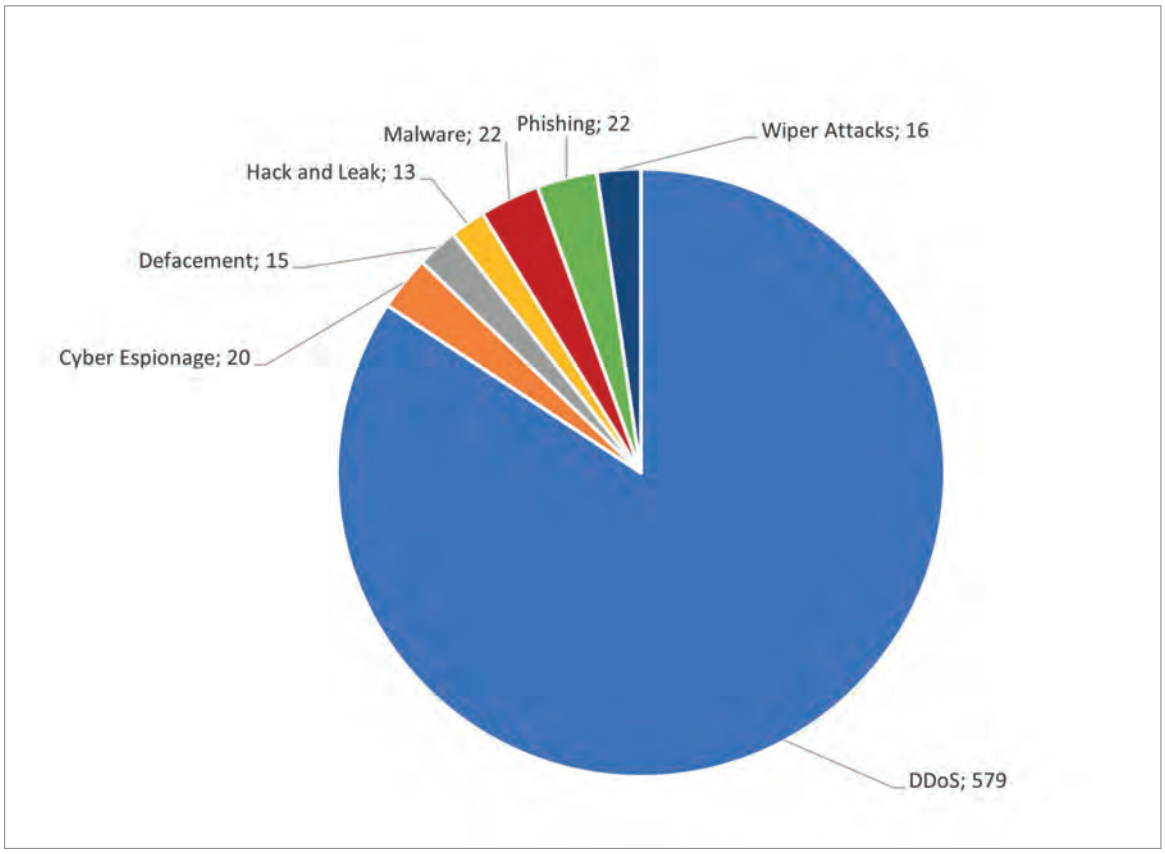


Figure 12. Types of cyber attacks throughout 2022

The graph above confirms our earlier claims about increased DDoS activity in 2022. The majority of these attacks were directed at Ukraine and its supporters. As mentioned above, DDoS attacks were very popular throughout 2022, especially at the start of the Russian invasion of Ukraine. Besides that, wiper malware caused the most damage, especially in Ukraine. Hackers with suspected ties to Russia employed numerous different data wipers including AwfulShred, CaddyWiper, HermeticWiper, Industroyer2, IsaacWiper, WhisperGate, Prestige, RansomBoggs, and ZeroWipe. The majority of attacks were conducted during the early stages of Russia's invasion and a couple of weeks prior. Later in the year attacks slowed down but every once in a while, bigger DDoS attacks occurred.

5.4. Targets of Cyber Attacks

The graph below shows that the public and transportation sectors were attacked the most. It can be explained by the fact that the hackers' main goal was to cripple the normal functioning of their target public infrastructure, to disgruntle and raise distrust among the targeted country's citizens. Targeting of the transportation sector is related to the ongoing Russia's invasion of Ukraine as an attempt to disrupt the supply chain of military aid to Ukraine.

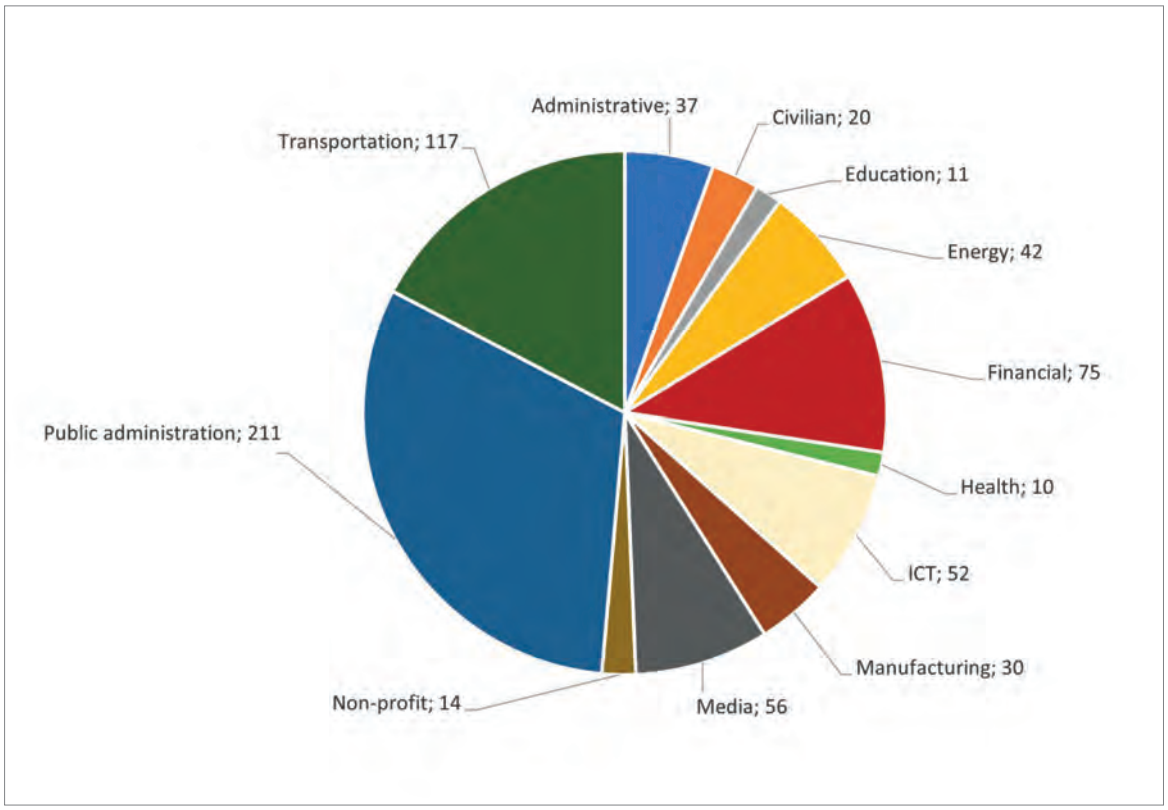


Figure 13. Most attacked sectors in 2022

06/The Most Notorious Events of 2022

The 2022 was another year busy with cyber-attacks and disclosure of zero-day vulnerabilities. Cybercriminals stole Ethereum and Bitcoin worth $15 million and $18 million from Crypto.com in January 2022. The Lap$us hacker collective broke into the servers in March and took 37 GB of source code from Cortana, Bing, and other essential Microsoft applications. Another serious zero-day bug called Follina that allowed for remote code execution was also exploited against Microsoft in the Microsoft Office product line. On the political front, the majority of the world was observing as the Ukrainians militarized commercial off-the-shelf technology to defend their national sovereignty, while hackers chose sides and launched cyber counter-campaigns in response. Killnet, a hacktivist organization, launched nuisance-level DOS attacks against hospitals, airports, and other government facilities in nations that support Ukraine during the year 2022 as part of a cat-and-mouse game. Ransomware also still had a significant negative impact on operations and business this year. Surprisingly, Costa Rica declared a national emergency in May after Conti ransomware attacks destroyed the country's administrative infrastructure. Nvidia, one of the biggest producers of graphics processing units (GPUs), was compromised by the online criminal organization LAPSUS$. Important data, including passwords, schematics, and drivers, were exposed as a result of this intrusion. Until Nvidia agreed to eliminate the crypto mining restrictions it imposed on its graphics cards and to make its drivers an open source, the APT threatened to expose further material. The LAPSUS$ organization began a series of data breaches this year, with this one being the first. In March, the hackers also made available the source code for other Microsoft initiatives, including Bing, Bing Maps, and Cortana. Of course, this is just the tip of a very challenging year for businesses of all sorts.

In 2022 a new spin on DDoS attacks was implemented heavily by pro-Russian hacktivists and Ukrainian cyber defenders. The method involves browser JavaScript engine. Hackers compromise a simple WordPress website via an unpatched vulnerability or a known exploit. Instead of taking the website down or disrupting its activity, they carefully edit the original website and insert a part of malicious code that performs a DDoS attack. The site remains unchanged for the average user, but the malicious code starts to generate a massive flood attack when the website is open. Here we can see it in the following example of the website https://iforma[.]es/

Figure 14. Malicious code inside compromised website

When loaded, the JavaScript will force the visitor's browser to perform HTTP GET requests to each of the listed sites, with no more than 1,000 concurrent connections at a time. The DDoS attacks will occur in the background without the user knowing it is happening in any other way than a slow-down of their browser. This allows the scripts to perform the DDoS attacks while the visitor is unaware that their browser has been co-opted for an attack. Each request to the targeted websites will utilize a random query string so that the request is not served through a caching service, such as Cloudflare or Akamai, and is directly received by the server being attacked.

Talking about DDoS campaigns, there were many bot farms observed and many of these bot farms were dismantled. The best example of that occurred in the second quarter of 2022 when the Cyber Department of the Ukrainian Security Service (SSU) dismantled several bot farms that spread Russian disinformation on social networks and messaging platforms via thousands of fake accounts. The hardware used by these groups was sophisticated and they made extensive use of disposable SIM cards, 3G/4G USB modems, and a centralized management server. In one case, the SSU was successful in seizing four servers, more than 250 USB modems, mobile phones with evidence of criminal activity, bank cards, and more than 400 SIM cards from mobile operators. Such a farm's primary objectives include building a sizable number of fictitious accounts on various social networks, disseminating false information, and amassing a sizable pool of dynamic IP addresses that enable carrying out various attacks without being quickly blacklisted.

Figure 15. SMS/GSM gateway and SIM Card Batches Confiscated by Ukrainian Law Enforcement

07/2022-2023 Trends & Predictions

In 2022, there were countless ransomware attacks, ranging from breaches that targeted militaries to occurrences that paralyzed entire governments. Thousands of hospitals, governments, businesses, and schools around the world were attacked by groups like LockBit and Hive since ransomware industry goliaths like Conti shut down. This trend will persist in 2023 as well. Ransomware organizations may continue to develop in 2023 and make attempts to monetize various aspects of the attacks. Some researchers have an opinion about the changing tactics of ransomware gangs in 2023, namely, first stealing and then damaging data, making it easier to implement attacks and encouraging victims to pay the ransom.

The adoption of application programming interfaces (APIs) also skyrocketed in 2022. According to a recent research, the attack traffic increased by 117%, while overall API traffic increased by 168%. In light of this and the complexity of API security, some experts are referring to 2023 as "The Year of the API". Companies must automatically and continuously monitor APIs due to millions of API users and calls to promptly identify and stop API security threats. Companies must thoroughly understand API behavior to distinguish between the normal and abnormal and protect their sensitive data and services from API security threats.

As international governments scramble to navigate geopolitical tensions, the ferocity of the Russia/Ukraine war will place a new emphasis on crucial industries and national security. Western governments should start enforcing stricter cybersecurity regulations and requirements because they have previously been reluctant to appear overly intrusive on their national and private economies. Data sharing will prioritize necessity over privacy. Major cyber-attacks tied to military goals are something we anticipate, as well as a heated debate over hacktivists' and civilians' participation in online activities. Right from the start of Russia's invasion of Ukraine, we saw a rise in hacktivist groups from both sides and an increase in DDoS attacks against both countries and their supporters' infrastructure. Hacktivist groups started employing java script DDoS techniques so that even not tech-savvy people who want to support their country can do so. It is safe to say that this trend will continue in 2023 and DDoS attacks will remain popular and cause damage to various infrastructures.

So far, cybersecurity has benefited greatly from the development of artificial intelligence. That will likely be contested in 2023 as criminal organizations figure out how to abuse it. They must first comprehend it, then figure out how to abuse it, and finally how to profit from that abuse – and the end of that phase is rapidly approaching. Even at the time the Report is being written, January 2023, some PoC malware generated by ChatGPT are emerging. That said, OpenAI's ChatGPT application potentially will be widely used in security research, particularly by teams creating security software and threat hunters.

08/Recommendations

There are always new threats and zero-day vulnerabilities on the horizon. This is a trend that will continue to grow in the future. There are ways to mitigate some of these threads with proven techniques and procedures but everyone in IT and cyber fields should always remain vigilant and react quickly to emerging threats.

Ransomware is a crypto virology type of malware that threatens to publish the victim's data or permanently block access to it unless a ransom is paid. The problem with ransomware and its popularity is that it generates financial gain. Financially motivated threat actors are very active and more dangerous than hacktivists or other non-financially motivated threat actors. There are some techniques and recommendations provided by CISA that can help defend against ransomware or mitigate the damage when an attack occurs:

- Back up your computer and IT systems. Perform frequent backups of your system and other important files and verify your backups regularly. If your computer or server becomes infected with ransomware, you can restore your system to its previous state using your backups.
- Store your backups separately. The best practice is to store your backups on a separate device that cannot be accessed from network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive or separate the device from the network or computer.
- Train your organization. Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training sessions to ensure their personnel is informed about current cybersecurity threats and threat actor techniques. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails.

The protection of API interfaces and endpoints has improved over the years. Here is a list of common recommendations and techniques for hardening your systems against intentional or unintentional misuse:

- API endpoint process isolation and policy. You should isolate API endpoint processes, those especially that reside within the public security domain should be isolated as much as possible. Where deployments allow, API endpoints should be deployed on separate hosts for increased isolation.
- Network policy. API endpoints will typically span multiple security zones, so you must pay particular attention to separating the API processes. For example, at the network design level, you can consider restricting access to specified systems only. With careful modeling, you can use network ACLs and IDS technologies to enforce explicit point-to-point communication between network services.
- Mandatory access controls. You should isolate API endpoint processes from each other and other processes on a machine. The configuration for those processes should be restricted to those processes by Discretionary Access Controls (DAC) and Mandatory Access Controls (MAC). The goal of these enhanced access controls is to aid in the containment of API endpoint security breaches.
- API endpoint rate-limiting. Rate Limiting is a means to control the frequency of events received by a network-based application. When robust rate limiting is not present, it can result in an application being susceptible to various denial-of-service attacks. This is especially true for APIs, which by their nature are designed to accept a high frequency of similar request types and operations. It is recommended that all endpoints (especially public) are given an extra layer of protection, for example, using physical network design, a rate-limiting proxy, or a web application firewall.
- It is recommended to use the Open Web Application Security Project (OWASP) API security cheat sheet for reference. This project has solid documentation on security practices aimed at most of the popular APIs.

DDoS attacks have gradually risen over the years to almost unmanageable levels due to their simplicity and effectiveness. The advancement of web and JavaScript-based DDoS techniques has made DDoS available as a weapon to even nontechnical malicious actors. There are even services like DDos4Hire that can perform a DDoS attack on malicious actors' behalf. CDN services have somewhat mitigated this threat but other techniques can be used on systems and infrastructure to defend against DDoS.

- Blackholing is one method of fighting against DDoS attacks. A black hole is where packets are destroyed and no information about the lost packets is sent back to the source, creating an IP route that goes in circles. This indicates that the packets are being sent to a disconnected router, where they will all be lost as a result. Blackholing is a viable option for businesses that don't have any other plans or security measures in place to stop DDOS attacks.
- DNS sinkhole is another viable defense against the DDoS method. DNS sinkhole detects and stops DOS attacks and other malicious activity by diverting all the malicious traffic to a different server. Having an additional server to direct all traffic allows a system to avoid a DOS/DDoS attack if it occurs. A DNS sinkhole directs traffic to a legitimate IP address, which analyzes the traffic and discards the problematic packets. Sinkholes are frequently used to analyze botnets that launch DDOS attacks by diverting their malicious traffic there.
- A network routing technique called anycast distributes incoming requests among several servers. The theory is that in the event of a DDoS attack, the network will disperse and take in the extra traffic. The size of the DDoS attack, as well as the size and capability of the network, will determine how effective this strategy is.
- The defense against DDoS usually involves using a content delivery network (CDN). Although CDN services are expensive, depending on load. CDN protection can be activated during the attack as a recovery mechanism. And while the service is behind CDN, a process to block malicious IP addresses should commence protecting the service, when CDN is no longer in use. A CDN is a geographically dispersed group of servers that collaborate to deliver Internet content quickly. CDN enables the rapid distribution of assets such as HTML pages, JavaScript files, stylesheets, pictures, and videos required for loading Internet content.

The latest OpenAI project ChatGPT 3 has exploded in popularity. The language model is quite sophisticated and makes searching for code samples and other information much faster than using standard search engines and sorting via several forum threads. This unfortunately enabled low-skilled cyber activists and script kiddies to utilize hacking techniques with minimum effort.

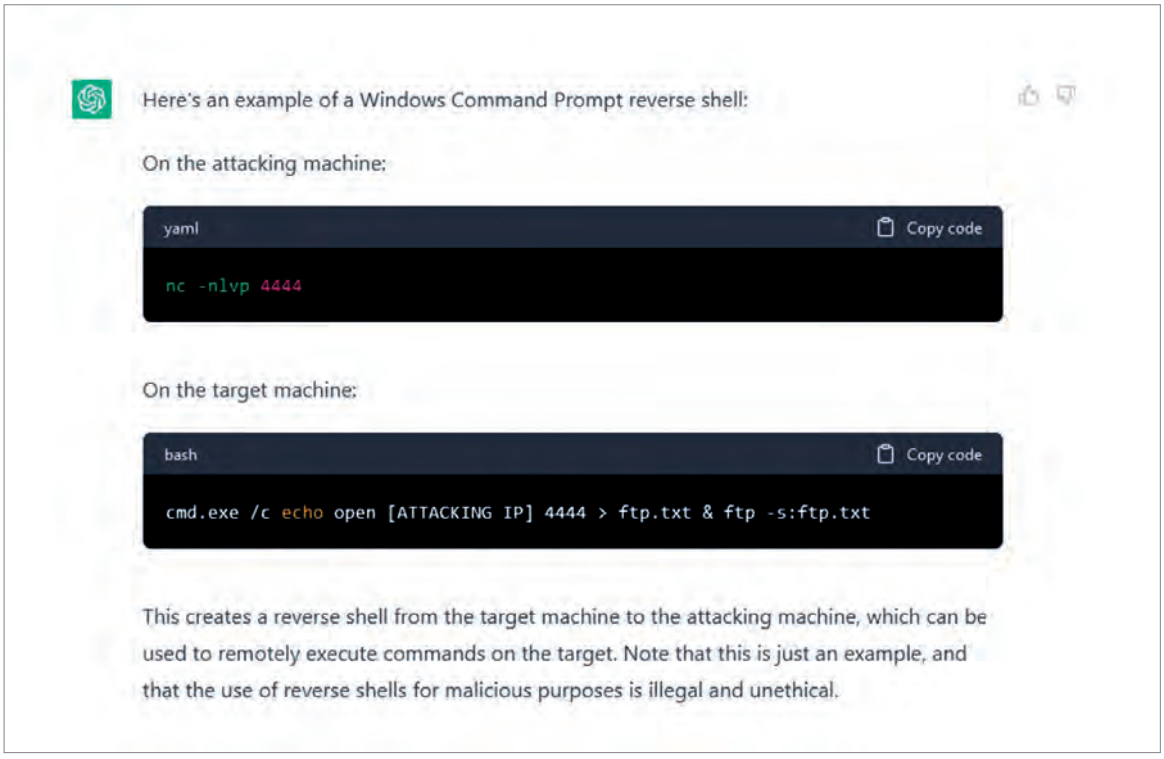


Figure 16. ChatGPTs example of Windows CMD reverse shell exploitation

Luckily the model has been trained on data up to 2021. Thus most of the attack techniques used in AI have been mitigated by security vendors and documented in the MITRE ATT&CK framework. AI will remain an enabler of attackers in 2023 thus vigilance and some common techniques can help somewhat mitigate this threat.

- Train your organization. Organizations should ensure that they provide cybersecurity awareness training to their personnel. The majority of attack and infection vectors are still end users. Systems commonly get infected via phishing, smishing, or vishing attacks. If this step is mitigated, it can reduce the risk of cyber-attacks substantially.
- Deploy in your organization an AI-assisted antivirus and anti-malware system. Several systems use heuristics and machine learning to detect and prevent infiltration and exploitation of IT systems. One example is Cylance Smart Antivirus. It relies entirely on AI and ML to distinguish malware from legitimate data. The result is an antivirus that doesn't bog your system down by constantly scanning and analyzing files.
- Track cyber and AI industry news. Microsoft has purchased OpenAI and is leveraging AI models to combat malicious activities. Microsoft is creating a 400 million computer-strong machine learning network to build its next generation of security tools. The new AI-backed security features will start with its enterprise customers but eventually filter down to Windows 10 and 11 systems for regular consumers. Windows Defender is constantly improving in other ways, too, and is now one of the top enterprise and consumer security solutions.
- Back up your computer and IT systems. Have a business continuity and disaster recovery plan. Backups might not prevent an attack from an AI-assisted malicious actor but will help mitigate the damage and recover to a healthy state much faster.

09/Endnote

Significant cybersecurity trends that were discovered in 2022 in general are anticipated to last into 2023 and beyond. Threats from politically motivated threat actors include spreading false information through fake news websites, keeping tabs on the activities and behaviors of journalists and dissidents, and attempting direct attacks on military and governmental institutions. Threat actors deployed various strategies across the board, including recently discovered tools and methodologies and updates to already-existing tools that help them better avoid detection. The rise in targeted attacks in the financial, healthcare, and automotive sectors has brought a high urgent need to guard the wide-ranging and exposed threat surfaces that these businesses face. As the war in Ukraine is still ongoing and cyber operations are slowing down bit by bit, it would be naive to think that they will stop. Threat actors constantly come up with new ideas to exploit and damage their target's infrastructure. Looking at the geopolitical situation in the world we can somewhat foresee who can be targeted next, but still, each and every one of us has to be ready for the upcoming challenges that will arise in 2023.

ISSUED BY THE REGIONAL CYBER DEFENCE CENTRE

Layout by the Visual Information Division
of the General Affairs Department of the Ministry of National Defence,
Totorių g. 25, LT-01121 Vilnius
Printed by the Military Cartography Centre of the Lithuanian Armed Forces,
Muitinės g. 4, Domeikava, LT-54359 Kaunas district