REGIONAL CYBER DEFENCE CENTRE

1st QUARTER REPORT, 2023

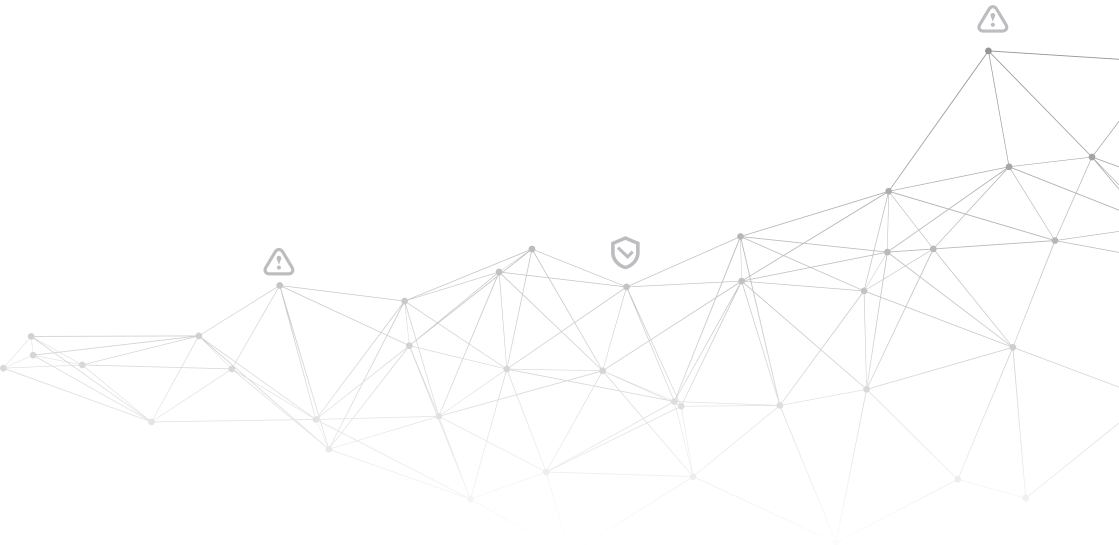




1st QUARTER REPORT 2023

1 January - 31 March

Table of Contents



Executive Summary

The 1st quarter of 2023 was anticipated to be very eventful not only in cyberspace but in the real world too. The Russo-Ukrainian war has reached its 1-year mark. It was predicted that a large invasion force from Russia would attempt another major offensive in February 2023 not only by means of kinetic warfare but in cyber as well. In reality, that did not happen. The Russian military forces and Wagner mercenaries got stranded near the city of Bakhmut, Ukraine. In cyberspace, there were several attempts to disrupt Western world networks by DDoS, data wipers, and ransomware. But that did not see any significant success either. It seemed that in Q12023 the Russian cyber forces ran out of resources and capacity to pose a significant threat to the allied world. But as the saying goes, the sea is the calmest just before the storm. Eternal vigilance is the price of freedom, and of security in cyberspace as well. Some notable cyber incidents and events are worth noting and discussing. What lessons can be learned and what mitigation techniques can be implemented to strengthen the defense of RCDC partners and the entire cyber community? The Q1 of 2023 was also eventful in a positive way for the RCDC: new partnerships and collaborations with NATO members and partners in various projects and events. The Q1 2023 Report provides an overview of it.

01/Q1 Highlights

2023 started well for the Cyber Threat Analysis Cell. CTAC had a pilot rotation from a newly added member Poland which we used to refine the information-sharing processes and engage in talks about further cooperation on the defence of our cyberspaces. The following rotation came from our partners of the U.S. Pennsylvania National Guard. It was a very fruitful opportunity, as we worked on completing CTACs first operational yearly report which can be found here: https://www.nksc.lt/rkgc/en_reports.html.

RCDC assisted the C-IED COE with an ADOMEX Pilot

In January the RCDC was contacted by the Counter Improvised Explosive Devices Centre of Excellence (C-IED COE) and offered an opportunity to participate in the C-IED COE-organized Document and Media Exploitation Advanced Pilot Experiment (ADOMEX) from 23 to 27 January 2023 in Madrid, Spain. The RCDC contributed its engineers with expertise in digital forensics and information extraction from various IT and IOT devices. The ADOMEX pilot is an attempt to improve the C-IED COE-organized DOMEX courses for various military and law enforcement personnel. DOMEX's goal is to provide Level 1 Exploitation Enablers the initial capability to collect hard copy documents and electronic media while using elementary tools and software to extract information at the tactical level and to transfer to and integrate it in the upper level in the exploitation system (Level 2). The goal of ADOMEX is to provide training on more in-depth and advanced methods of evidence extraction from various sources like hard drives, RAM dumps, and hardware devices (routers/IP cameras/smartphones). It also includes an introduction to passport and ID card counterfeiting detection and exploitation. Additionally, there is a section on UAV (unmanned aerial vehicle) exploitation, evidence/log collection, scenario development, and flight path analysis. The training went very well: the contribution was top-rated and highly appreciated by other attendees. The RDCD will continue to cooperate with the C-IED COE in the future endeavors.

Figure 1. C-IED COE-organized Document and Media Exploitation Advanced Pilot Experiment (ADOMEX)

The second rotation of Ukrainian MITIT cadet internship

The second rotation of cadets of the Ukrainian Military Institute of Telecommunications and Information Technologies named after the Heroes of Kruty (MITIT) completed their one-month internship at the RCDC Cyber Threat Analysis Cell. During the month, CTAC personnel trained them in various cyber defense and offense topics, ranging from IT infrastructure hardening and defence to Red Team operations, cyber threat intelligence, and digital forensics. The internship program is designed to operate not only in a simulated environment but also to incorporate real-life scenarios and real-life data. RCDC personnel are highly motivated to share their knowledge and experience and to contribute to the future cybersecurity of Ukraine.

Figure 2. Patch of cadets

Figure 3. CTAC team with cadets after completion of internship

Cooperation with Japanese representatives on the project "How to recognize cyber threats originating from China"

During the year 2022 and the start of 2023, the entire world focused on the Russo-Ukrainian war. Unfortunately, the war serves as a perfect distraction for advanced persistent threat (APT) offensive cyber operations, both, independently and on state sponsoring. One specific region, the Asia-Pacific, and to be more precise – China, is currently on the rise with regard to this specific malicious cyber activity. Due to its size, China is home to numerous independent and government-sponsored APT groups. Their activity has been constantly on the rise and poses a significant threat to the Western-aligned world. To mitigate it, it is necessary to raise awareness and develop expertise in detection and identification of this threat. For this reason, the RCDC CTAC team with support from the Japanese Toyo University and Capy Corp Japan has started an initiative for developing a guidebook on "How to recognize cyber threats originating from China". The purpose of this initiative is to create a guidebook that is readily available for everyone and includes basic guidelines for identification of tactics, techniques and procedures most commonly used by the largest China's APT's. The guidebook will present a summary mitigation and defensive techniques to protect critical assets and information from cyber threats.

Figure 4. Meeting with the Japanese Ambassador and representatives

02/ Regional Cyber Threat Landscape

The most sophisticated AI (Artificial Intelligence) chatbot ever made available for public use, ChatGPT, which has human-like natural language abilities, startled the world in December 2022. When they observed the chatbot's capacity to write both, normal language and code, there were voices concerned about the technology's potential for being abused for bad reasons. In actuality, ChatGPT is not the only system that poses a risk of being utilized in a cyberattack. The AI of today is quite good at making malware and producing tailored phishing messages. To carry out widespread social engineering and phishing assaults or to check for vulnerabilities in targeted systems, several advanced persistent threats (APT) have been using AI-based technologies already.

2.1/ The Rise of ChatGPT-4

The official release of ChatGPT-4 confirms the long-running reports about its enhancements to OpenAI's ChatGPT's already astounding linguistic abilities. It is the company's "most sophisticated algorithm, providing safer and more helpful solutions," according to OpenAI. Here is all we

currently know about it. The ability to comprehend photographs the most recent version of the program has is one of the greatest differences between Chat GPT-4 and Chat GPT-3. This is due to Chat GPT-4's multimodality which allows it to comprehend a variety of informational formats, including both words and visuals. Conversely, Chat GPT-3's application cases were constrained by the fact that it only supported text-based inputs and answers. Here are a couple of examples how anyone can use this sophisticated tool:

- Language translation: GPT-4 may be helpful for machine translation applications due to its capacity to comprehend and produce natural language content. To increase its precision and fluidity, it might be trained on a sizable collection of translated texts.
- Text summarization: as the output text of this task must be easy to comprehend and read, GPT-4's capacity to produce text that resembles human speech may be helpful.
- Answering questions: GPT-4 can do so, which may be helpful in applications, like customer service or technical assistance.
- Picture and video creation: ehe Transformer design, which is the foundation of GPT-4, has been proven to be efficient for a range of machine learning applications, including computer vision. This indicates that GPT-4 may be employed for producing images and videos.
- Additional uses: GPT-4 is a potential tool for a variety of natural language processing jobs due to its flexibility and versatility. Chatbots, automated news writing, and even creative writing could benefit from its utilization.

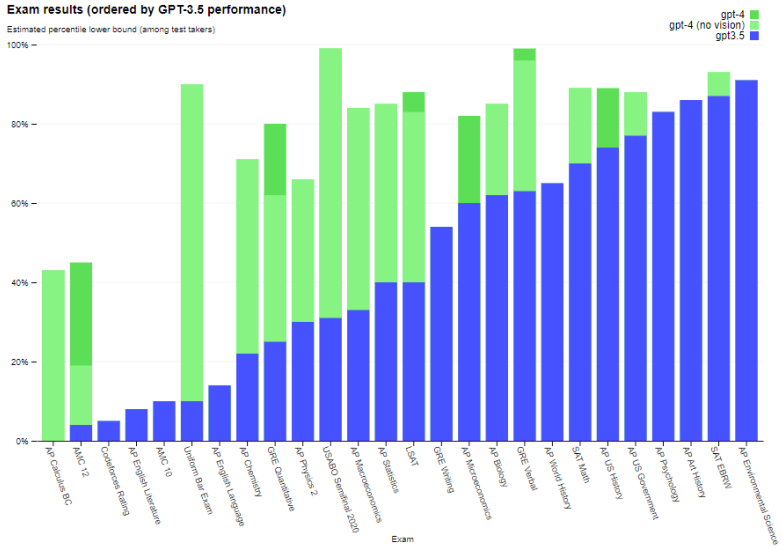


Figure 5. Difference between the older version of ChatGP and the newer.

The world is anticipated to be significantly changed by OpenAI's GPT-4, opening the door for a variety of interesting inventions and discoveries.

2.2/ Microsoft Outlook Elevation of Privilege Vulnerability (CVE-2023-23397)

In mid-March of 2023 a new critical privilege elevation/authentication bypass vulnerability was discovered in Outlook. The vulnerability (CVE-2023-23397), which affects all versions of Windows Outlook, has a CVSS rating of 9.8, and it is one of two zero-day exploits that surfaced on March 14. It is a zero-touch exploit, which means that little user interaction is needed to take advantage of the security hole.

Attackers can take advantage of CVE-2023-23397 by sending the victim a message with an extended Message Application Program Interface (MAPI) property and a Universal Naming Convention (UNC) path to a server message block that is under the attacker's remote control. (SMB, via TCP 445). Whether or not the recipient has seen the message, the vulnerability is taken advantage of because it is shared-hosted on a server under the attacker's control. Using PidLidReminderFileParameter, the attacker remotely sends a malicious calendar invitation that is represented by the.msg message format which Outlook uses to support reminders to activate the vulnerable API (Application programming interface) endpoint PlayReminderSound. (the custom alert sound option for reminders). The attacker can utilize the user's New Technology LAN Manager (NTLM) negotiation message which is automatically sent to authenticate against other systems that support NTLM authentication when the victim connects to the attacker's SMB server. The most recent authentication protocol used by Windows is called NTLMv2 hashes. It is used for a variety of services and each response includes a hashed version of the user's data, such as username and password. Threat actors can thus attempt an NTLM relay attack to access other services, or, if the compromised users are admins, a full domain compromise. The Microsoft 365 Windows Outlook app is still vulnerable to this attack even though online services like Microsoft 365 are not as they do not support NTLM authentication. It does not require high privileges or user interaction to be activated. A zero-touch vulnerability known as CVE-2023-23397 is activated when the victim client is prompted and informed (e.g. when an appointment or task prompts five minutes before the designated time). For remote users, it is challenging to block outbound SMB traffic. The same credentials could be used by the attacker to access other resources.

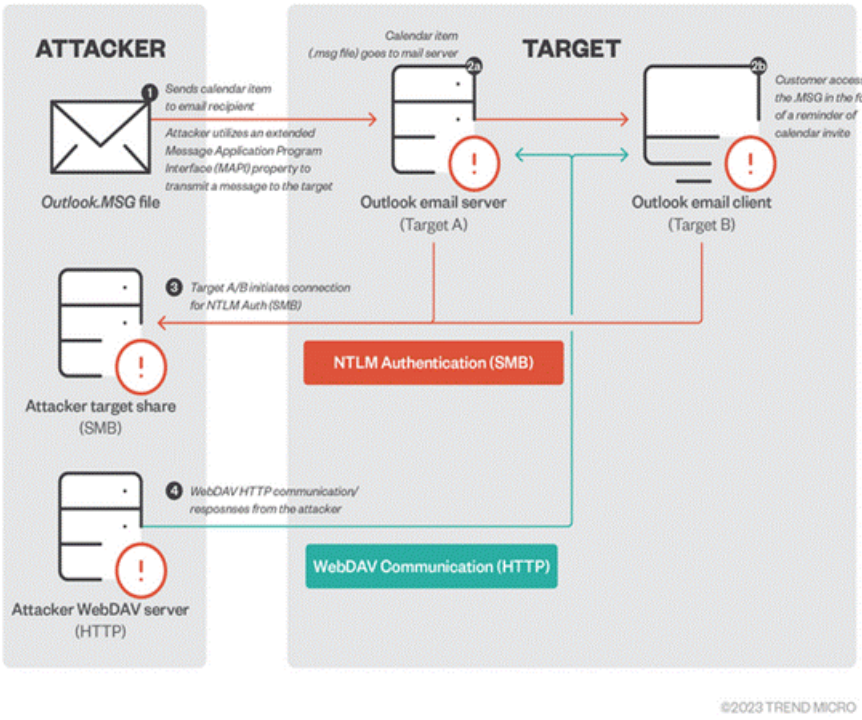


Figure 6. General exploitation routine of CVE-2023-23397 Trend Micro

03/ Categories of Attacks Against RCDC Partners

In Lithuania, the year 2023 started slowly. Looking back a year, when cyberattacks against various infrastructure objects in Lithuania were happening as a commonplace, we anticipated that attacks coming from hostile actors would not stop and perhaps pick up speed – and become even more common as a result. In Q1 of 2023, there were a few instances reported of Ukrainian refugees in Lithuania targeted by phishing attacks in an attempt to collect their data. Luckily, apart from the phishing campaigns and a couple of DDoS episodes, Lithuania did not suffer any significant cyberattacks. That said, we have to stay sharp, knowing that Lithuania is an advocate for Ukraine and Taiwan, threat actors from Russia and China could strike any moment and it is crucial to be prepared for any attack.

In Ukraine, CERT-UA handled over 300 cyber incidents and cyberattacks from January to February 2023. Civil infrastructure remains a major target for Russian hackers, first of all, the national government. Meanwhile, CERT-UA specialists are also recording a significant number of attacks against local authorities starting this year. In addition, CERT-UA notes that an increasing count of attacks target at espionage, focusing on maintaining an open access to target organizations this year. The malware spread by Russian hackers is dominated by applications for data collection and remote access to user devices.

In Poland, the ICT (information and communications technology) systems of the Polish administration and subsidiary organizations have become the primary target of hostile cyber activities carried out on Polish territory. In the first quarter of this year, national cyber security institutions found an increase in activities carried out by actors linked to the state administration of the Russian Federation (RF):

- 27.02.2023, a distributed denial of service (DDoS) attack was carried out by the hacktivist group NoName057(16) linked to the Russian governmental threat actors. The attack targeted tax website Podatki.gov.pl. The said web portal is run by the Polish Ministry of Finance. No data was detected to be leaked in the incident.
- An increased disinformation campaign on Polish-language social media (Twitter) has been identified. The campaign targeted the Polish involvement in military operations in Ukraine. A significant amount of tweets have been noticed spreading disinformation about the creation of military units of the Polish Armed Forces (PAF) in Ukraine and formation of the Polish Volunteer Units. The mentioned entities were to be supplemented with professional soldiers of the PAF. The above campaign is thematically related to the news about the Polish Government's transfer of modern weapons systems to Ukraine, including Leopard 2A4 tanks.
- Actors associated with security institutions of the Russian Federation (RF) distribute disinformation on the Polish-language Internet about the mandatory military mobilization of the Ukrainian population residing on the Polish territory. In addition, a poster concerning a compulsory military mobilization of Ukrainians was found on the streets of several Polish provincial cities. The above campaign invokes Polish state entities (Office for Refugees) to collect information about the Ukrainian population through QR codes on the posters.

In the USA, Ransomware Attacks in the US Education sector have been on the rise so far. In the recent months, ransomware attacks have increasingly targeted schools and universities across the United States: hackers demanding payment in exchange for returning the control of computer systems and data have disrupted teaching and learning in numerous institutions. The rise in ransomware attacks in the education sector is attributable to a combination of factors, including the increasing reliance on technology and the growing sophistication of hackers. Schools and universities need to take steps to protect themselves, such as backing up their data regularly and ensuring that their systems are up to date with the latest security patches.

In Georgia, in the latest quarter, the CSB (Cyber Security Bureau) experienced several targeted

attacks utilizing email phishing campaigns against the PR (Public Relations), procurement, and several other departments, sending them fake Microsoft Teams links and fake invoices. Such attempted attacks lead to credential theft or persistent data exfiltration which was luckily prevented because the attacks were detected in the early stage (mostly in the phishing stage/email). Other than that, the CSB has experienced several cryptocurrency-oriented attacks, such as crypto stealers, and crypto miners. The total number of incidents varies between 70-80 incidents based on the threshold of detection.

The CSB has also been subjected to targeted network scanning and web application scanning run by automated solutions and proactive measures. There were also several attempts to seliver web-based exploits via Email attachments that were also unsuccessful.

04/ Cyber Activity in the Region: Chronological Order

2023

1. **January 8, Russian Turlahackers take advantage of decade-old malware infrastructure to install new backdoors.**
The Russian cyberespionage group Turla was seen using an outdated malware attack infrastructure as a springboard to deliver its surveillance and backdoor tools to Ukrainian targets. The servers taken over correspond to a variant of a common malware called ANDROMEDA (also known as Gamarue), according to Google-owned Mandiant, which monitors the operation under the uncategorized cluster identifier UNC4210. UNC4210 re-registered at least three expired ANDROMEDA command-and-control (C2) domains, and in September 2022, it started victim profiling to deploy KOPILUWAK and QUIETCANARY only to particular targets.

2. **January 11, Lithuanian Ministry of Defence and Government websites were targeted by a DDoS attack.**
At around 17:43 to 17:49 local time, websites of the Lithuanian Ministry of Defence and Government suffered a DDoS attack. The attack was an HTTP (Hypertext Transfer Protocol) flood and took place in layer 7 (application) of the OSI model sending 627.99k forged requests in the 6-minute attack duration. The DDoS attack was successfully thwarted due to the CloudFlare protection in place.

3. **January 13, pro-Russian Group DDoS-ing Governments, Critical Infrastructure in Ukraine, NATO Countries.**
NoName057(16), a pro-Russian cyberterrorist organization, actively launched distributed denial-of-service (DDoS) attacks against organizations in NATO and Ukraine. SentinelOne, a cybersecurity company, claims that the group initially targeted Ukrainian news websites but eventually shifted attention to NATO-affiliated targets. NoName057(16) uses a Telegram channel "NoName057(16)" to make threats, defend its behavior, take credit for disruptions, and ridicule its targets.

4 **January 17, a cyber-attack against the Ukrinform information and communication system.**

At around 12:39, information about a disruption in the normal operation of several components of the information and communication system (ICS) of the Ukrinform Ukrainian National Information Agency was announced in the Telegram channel "Cyber Army of Russia Reborn." The Government Computer Emergency Response Team of Ukraine (CERT-UA) took to action to look into a cyberattack on January 17, 2023, at the request of the Agency. The preliminary data indicates that a malicious CaddyWiper program was launched centrally to compromise availability and integrity of information using Group Policy (GPO).

5 **January 20, Gamaredon group launched cyberattacks against Ukraine via Telegram.**

Gamaredon, a state-sponsored cyber espionage organization operating out of Russia, continued its digital assault on Ukraine targeting the latest operations against the nation's military and law enforcement. The BlackBerry Research and Intelligence Team stated in a report on The Hacker News that: "The Gamaredon group's network infrastructure relies on multi-stage Telegram accounts for victim profiling and confirmation of geographic location, and then leads the victim to the next stage server for the final payload."

6 **January 24, a new phishing campaign in Poland.**

A disinformation campaign took place in Poland, it was followed by CERT-PL. This time, the threat actor sent an email from e-mail address sekretariat.dsmim@mswia-gov.pw with an image with a fake announcement. The cyber threat actor impersonated the Polish Ministry of the Interior and Administration again to claim that all Ukrainian refugees are required to be registered. On this occasion it was sent to local authorities and the announcement instructed them to organize an information campaign about the refugee registration in the local media.

7 **January 28, Ukraine hit with new Golang-based 'SwiftSlicer' Wiper Malware in latest cyber attack.**

Russia launched a new cyber offensive against Ukraine using the previously undocumented Golang-based data wiper, SwiftSlicer. ESET attributed the attack to Sandworm, a nation-state organization connected to Military Unit 74455 of the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

8 **January 30, servers of the Lithuanian National Art Museum hacked.**

Arūnas Gelūnas, DIrector of the Lithuanian National Art Museum (LNDM), announced that the LNDM's operations would probably not run smoothly for the foreseeable future due to the server hack on the previous weekend. The LNDM Director assured that everything was being done to eliminate the problems as soon as possible. "Servers have been hacked, and data ransom is demanded as a traditional pirate method to paralyze activities, but we are promptly solving this issue. We will inform both, the Ministry and the Cyber Security Center," A. Gelūnas informed us about the planned next steps.

9 **February 2, group UAC-0114 (Winter Vivern) took actions against the state agencies of Ukraine and Poland.**

The Ukrainian Government's CERT-UA computer emergency response team discovered a website posing as the Ministry of Foreign Affairs of Ukraine and inviting to download software for "detection of infected computers". Clicking on the provided link tarts the BAT file "Protector.bat" download, when opened, it causes the computer to download and run PowerShell scripts, one of which performs a recursive search for files with the following extensions: .edb, .ems, .eme, .emz, .key, .pem, .ovpn, .bat, .cer, .p12, in desktop directories. It allows for creation of scheduled tasks that are intended to guarantee persistence.

10 **February 6, Cyber-attack UAC-0050 against the state bodies of Ukraine using Remcos program for remote control and surveillance.**

Ukraine's governmental computer emergency response team CERT-UA detected a widespread distribution of emails purportedly sent by Ukrtelecom JSC. Their subject line read "Court claim against your personal account # 7192206443063763 dated: 06.02.2023" , the e-mail included a RAR archive attachment named "court letter, information on debt.rar." The archive included a text file called "Your personal access code-254507.txt" and another password-protected RAR archive called "court letter, information on debt. pdf.rar". The second archive contained an executable file "court letter, information on debt.pdf.exe," more than 600 MB in size. Running the EXE file installed on the target computer the Remcos remote monitoring and surveillance program created by BreakingSecurity company.

11 **February 8, new information-stealing malware named Graphiron used against a wide range of targets in Ukraine by UAC-0056 espionage group.**

Espionage group UAC-0056 (Saint Bear, Bleeding Bear, EmberBear, UNC2589, TA471, Nodaria) was found using a novel version of information-stealing malware against targets in Ukraine. The malware (Infostealer, Graphiron) is written in Go and designed to harvest a wide range of information from the infected computer, including system information, credentials, screenshots, and files.

12 **February 8, suspected Russian threat actors hacked into UK politicians' emails.**

A British MP admitted that his personal email account was compromised by alleged Russian threat actors. In a tweet sent on February 8, Stewart McDonald of the Scottish National Party (SNP) emphasized the spear phishing event. The message said: "Over the past couple of weeks I have been dealing with a sophisticated and targeted spear phishing hack of my personal email account, and the personal email account belonging to one of my staff."

13 **February 13, cyberattack employing Remote Utilities software targets Ukrainian institutions and organizations.**

The governmental Computer Emergency Response Team of Ukraine (CERT-UA) recorded a mass distribution of emails allegedly sent on behalf of the National Security and Defense Council of Ukraine with a subject saying "RE: Critical security update" and an attachment in "the form of a RAR archive named "KB5017371 security system update.rar". The mentioned file contains a decoy image called "Instructions important to read.jpg" and a split archive containing an executable file "KB5017371.exe". Running the latter will install Remote Utilities on the target computer. The detected activity is tracked by UAC-0096.

14 **February 13, Killnet pro-Russian hacktivists targeted NATO servers with DDoS attacks.**

Several distributed denial-of-service (DDoS) attacks against servers of the North Atlantic Treaty Organization (NATO), the Special Operations Headquarters (NSHQ) relief operations website, and the Strategic Airlift Capability were taken responsibility for by the pro-Russian hacktivist group Killnet. The attack was designed to impede relief efforts in support of earthquake victims in Türkiye and Syria. The reports of cyberattacks were confirmed on the official NATO website. NATO determined no classified information theft had taken place.

15 **February 14, Cloudflare says it stopped the largest DDoS attack on record.**

The greatest distributed denial-of-service (DDoS) attack ever recorded was detected and handled over the second weekend of February 2023, according to Internet infrastructure company Cloudflare. The DDoS attack generated 71 million requests per second (RPS), or 35% more than the 46 million rps record previously set in June 2022. Unidentified attackers targeted a well-known game provider, bitcoin businesses, hosting corporations, and cloud computing platforms. Cloudflare collaborated with the numerous cloud providers used as the DDoS source to take down the botnet responsible for the attack.

16 **February 21, Gamaredon deployed Hoaxshell in the latest campaign against Ukrainian organizations.**

Reports were published about a newly discovered and at that time still ongoing campaign by the Gamaredon APT. The campaign involved delivery and deployment of malware to Ukrainian target computers and heavy use of obfuscated PowerShell and VBScript (VBS) scripts in the infection chain. The used WebShell malware executes remote commands from the attacker and deploys binary and script-based payloads on the infected machine.

17 **February 21, UAC-0050 used Remcos remote administration tool in an attack against Ukraine using.**

CERT-UA detected a mass distribution of e-mails allegedly on behalf of the Pechersk District Court of Kyiv City of with "Pechersk district court of the city of Kyiv" in the subject line and a RAR-archive named "Electronic court request no. 7836071. rar"' attached. Opening of the embedded archive and launching the EXE file leads to Remcos remote control and monitoring program installation on the victim's computer.

18 **February 23, cyber-attack aims to violate the integrity and availability of state information resources**

The Computer Emergency Response Team of Ukraine found that a web shell was used on one of the websites leading to modifications of the main page content. Web shell was injected into devices of the victim organizations. Also, SSH-backdoor, HoaxPen and HoaxAge backdoors were found on the webserver after the attack. In the first step, the attacker used GOST (Go Simple Tunnel) and Ngrok program. Based on the set of signs, it was concluded that the infection and work disruption of web resources was carried out by the UAC-0056 group.

19 **March 7, Russia-aligned TA499 (also known as Vovan and Lexus) phishing campaign report.**

New information emerged regarding a phishing campaign by the Russia-aligned TA499 (also known as Vovan and Lexus) whose malicious email campaigns have been tracked by Proofpoint researchers since early 2021. TA499's campaigns began to ramp up in late January 2022, culminating in increasingly aggressive attempts in the wake of Russia's invasion of Ukraine in late February 2022. Since that time, the threat actor has engaged in a steady activity and expanded its targeting to include prominent businesspeople and high-profile individuals that have either made large donations to the Ukrainian humanitarian efforts or public statements about the Russian disinformation and propaganda.

20 **March 13, STALKER 2 game developer lost data to Russian hacktivists.**

GSC Game World announced that their systems had been compromised, allowing threat actors to steal game assets during the attack. The publisher of Stalker 2, which is planned to be published later this year, claims that a "community from a Russian social network" was behind the hack and is extorting money from the business.

21 **March 14, New APT29 phishing campaign against European institutions.**

The BlackBerry Research & Intelligence Team reported about the new APT29 campaign. BlackBerry researchers claim that it is creating decoy files on the topic of a recent visit by representatives of the Polish Foreign Ministry to the US, and is abusing LegisWrite, a legal electronic official EU document exchange system. It partially coincides with a previous campaign discovered by researchers in October 2022. APT29 used targeted phishing emails containing a malicious document with a link to download a HTML (HyperText Markup Language) file.

22 **March 21, Unknown actors deploy malware to steal data in occupied regions of Ukraine.**

Government, agricultural, and transportation institutions in the cities of Donetsk, Lugansk, and Crimea have been reported to be attacked as part of an ongoing campaign using a modular framework known as CommonMagic. Details of the subsequent stage indicate the use of spear phishing or other similar techniques, even though the initial vector of compromise is unclear. The use of booby-trapped URLS leading to a ZIP archive housed on a malicious web server is one of the components of the attack chains. When the file is opened, it contains a fake document and a malicious LNK file, which leads to install the PowerMagic backdoor.

23 **March 27, Russian hackers strike the French National Assembly website.**

An online attack that was claimed by hackers with ties to Russia shut down the website of the National Assembly of France. "We decided to repeat our recent trip to France where protests against [French President Emmanuel] Macron, who decided not to give a damn about the French and continues to 'serve' Ukrainian neo-Nazis, still do not subside," NoName057(16) hacker group wrote on its Telegram channel. Officials from the National Assembly told Franceinfo that while they were working on "identifying," they couldn not yet establish that Russian hackers were behind the incident.

05/ Recommendations

Even though DDoS attacks do not have a long-term effect against the targeted infrastructure, they will still be a common attack since it is easy to utilize. CTAC has reported on DDoS attacks numerous times and the recommendations for defence remain the same:

- The most effective defense against DDoS attacks is a content delivery system (CDS). CDS uses of a reverse proxy and thus serves as a middleman between clients and servers, mirroring and caching websites. A CDS can assist in preventing a DDoS attack from reaching the origin server, which would cause the website to become fully unavailable. When a server receives more traffic than it can handle, the traffic is sent to other servers, usually the ones located in the same country as the initial addressee of the request was sent. Users will not experience any downtime on the hacked site, and there will not be any disruptions.
- A Denial of Service Response strategy should always be in place. It could take some time but the DDoS response plan needs to be the more detailed the more complicated the infrastructure is. A trained reaction team, a systems checklist, a list of internal and external contacts who need to be made aware of the incident, and a communication strategy for all other stakeholders and clients should all be included. Consider using various networks for your data centers, and make sure that not all organizations are in the same physical location. Keep an eye out for strange traffic on the network. Organizations can avoid DDoS attacks by making a few easy hardware configuration changes. Using a firewall or router, for instance, to prevent DNS (Domain Name System) replies from outside the network or to delete inbound ICMP (Internet Control Message Protocol) packets. This will help to protect against certain DNS and ping-based volumetric attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) has introduced a new service called pre-ransomware notifications to help organizations prevent these attacks from succeeding. This service provides organizations with information about potential ransomware attacks before they occur, giving them time to take steps to prevent the attack from succeeding. The pre-ransomware notifications are based on threat intelligence collected by CISA and its partners, including the FBI (Federal Bureau of Investigation) and the Department of Homeland Security. When CISA detects a potential ransomware attack, it will send an alert to the affected organization, providing details about the attack, including the type of ransomware used, the target systems, and the tactics employed by the attackers. Organizations receiving the alerts can use the information to take proactive measures to prevent the attack from succeeding. This might include patching vulnerable systems, updating anti-virus software, or implementing additional security measures to protect against the specific tactics the attackers are using. CISA's pre-ransomware notifications are one valuable tool that can help organizations stay ahead of this threat and prevent attacks before they occur. As the threat of ransomware attacks continues to grow, schools and universities need to take steps to protect themselves and their data.

With CISA's pre-ransomware notifications, educational institutions can proactively ensure their systems are safe from any potential attacks. By taking advantage of the service and implementing other cybersecurity measures, they can continue providing uninterrupted education to their students and avoid paying hefty sums to cyber criminals.

06/ Endnote

Understanding the benefits and dangers that come with new technology is one approach to staying on top of the changing threat landscape. Nobody wants to play catch-up with rapidly changing technological trends. The need for ability to manage cyber risk will suffer more for those unwilling to adapt to technological changes. One example is the growing significance of 5G, which can enable new use cases like telemedicine, asset monitoring in manufacturing, and augmented reality for advanced training. Adopting 5G will require designing and integrating security measures from the beginning, but doing so would be extremely hard. Nevertheless, Cyber AI may be a force multiplier as firms battle with security breaches, enabling security teams to not only respond quicker than cyber attackers can move but also to predict these moves and act in advance. Organizations may use AI and automation to eliminate some analysts' monotonous tasks and then educate those analysts for more strategic jobs that could be hard to fill.

Fast cloud migration left little time for cybersecurity to catch up. The cloud security market is growing quickly due to various cloud vulnerabilities as well as poorly protected remote work environments, which are frequently used to access cloud services. The scalability of virtual private networks may offer problems. In contemporary hybrid contexts, VPN technology may be vulnerable to cyberattacks and vulnerabilities. The zero trust strategy, in comparison, is safe and scalable. Cybersecurity experts are expected to expand current techniques for managing supply chain risk in addition to pursuing novel approaches to supply chain security. The majority of these examples of espionage, state-sponsored cyberattacks, and geopolitical unrest that have an impact on the global supply chain are exactly the reason for it.

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