3rd QUARTER REPORT 2023





3rd QUARTER REPORT 2023

1 July - 30 September

Table of Contents

01/Executive Summary

1.1/ What Happened?

The 3rd quarter of 2023 was an eventful time for Lithuania and its partners. The most notable event was the NATO Summit in Vilnius on 11-12 July 2023. Although the cyberattacks during the Summit were numerous, most of them were DDoS and caused no more than inconvenience and disruption to public service websites. Unfortunately, Lithuania also suffered a data breach resulting in NATO Summit-related information leak. It occurred on the last day of the Summit. In general, the period before and during the Summit witnessed a heightened cyber activity in the region.

1.2/ Why Is It So Important?

It is important to note that the majority of cyber activity was DDoS attacks against various targets of opportunity. These were conducted by the same pro-Russian hacktivist group as had been active since the beginning of the Russo-Ukrainian war. Namely, KillNet, NoName057(16). We did notice, however, a new hacktivist group called CyberTriadHT that had newly emerged and started its activity in the region.

1.3/ CTAC Assessment

The cyber threat landscape is dynamic and complex, with an increasing number of cyber threats targeting governments, industries, and individuals. The region faces a diverse range of challenges, including advanced persistent threats (APTs), ransomware attacks, phishing, social engineering, and vulnerabilities in critical infrastructure and IoT devices. State-sponsored cyber-espionage campaigns, particularly attributed to actors like APT28 and APT29, pose significant risks to national security and sensitive information.

The adoption of Internet of Things (IoT) devices and digital transformation initiatives has exposed new attack surfaces, making critical infrastructure, smart cities, and industrial control systems vulnerable to cyber-attacks. Additionally, supply chain attacks and data breaches have become prevalent, emphasising the importance of robust data protection and compliance with regulations, like the General Data Protection Regulation (GDPR).

02/Regional Cyber Threat Landscape

2.1/ The Dynamic and Complex Cyber Threat Landscape of the 3rd Quarter of 2023 with significant implications for various nations.

Key highlights include:

- Cyberattacks during the NATO Summit: several cyberattacks, mostly DDoS, caused interruptions during the NATO Summit in Vilnius. A data breach exposed sensitive information thus underlining the significance of cybersecurity in global events.
- Hacktivist Groups: Pro-Russian hacktivist organisations, including such threat actors as KillNet and NoName057(16), carried out DDoS attacks on a number of targets as a show tenacity.
- An Emerging Threat: CyberTriadHT, a new hacktivist organisation, has complicated the local cyber threat scene.
- Advanced Persistent Threats (APTs): Russian military entities are believed to be behind APT28 and APT29 which posed serious threats to regional national security and sensitive data.
- IoT Vulnerabilities: Increasing adoption of Internet of Things (IoT) devices exposed new attack surfaces, making critical infrastructure and industrial control systems vulnerable to cyberattacks.
- Supply Chain Attacks: Data breaches and supply chain attacks have become more frequent, highlighting the significance of data security and GDPR compliance.
- Region-wide Occurrences: Several nations in the area, including Lithuania, Ukraine, the United States, and Poland, have experienced such cyber threats as spear phishing campaigns, espionage, malware assaults, and ransomware occurrences.
- Tactics Evolution: Threat actors kept improving their strategies, including the use of social engineering through Microsoft Teams, vulnerabilities, and multi-stage attacks to elude detection. Worldwide Attribution: frequent attribution to nation-state actors, like Russia, highlighted the geopolitical aspect of cyberattacks.

Overall, the 3rd Quarter pointed out a need for more stringent cybersecurity measures, global cooperation, and constant watchfulness to combat the changing character of cyber threats and safeguard sensitive data, key infrastructure, and national security.

2.2/ PentestGPT: A New Tool for Automated Penetration Testing.

A tool called PentestGPT utilizes artificial intelligence and natural language processing to automate penetration testing operations. It can generate malicious payloads, craft convincing phishing emails, find vulnerabilities, and carry out post-exploitation actions. PentestGPT is intended to reduce the time and effort penetration testers must expend when doing security assessments, while also enhancing the caliber and precision of their conclusions. For various attacks, such as SQL injection, cross-site scripting, command injection, and others, PentestGPT may create unique payloads. If you provide PentestGPT with some basic details about the target system and the type of attack you want to conduct, it will create a suitable payload for you. Nmap, Metasploit, and Burp Suite are just a few of the pentesting tools that PentestGPT can provide commands and scripts for. Pentest GPT will generate a command or script for you if you just provide the tool to be used and the parameters that need to be given.

PentestGPT has a lot of benefits for penetration testers and security enthusiasts, including:

- Simplified and automated penetration testing process.
- Increased performance in comparison to other language models and superior thinking.
- Use the interactive mode to get feedback right away and to enter commands.
- Ability to defeat easy to medium HackTheBox computers and CTF challenges.
- To maintain context and accuracy throughout the testing process, the concept of "test status awareness" was applied in the design.

03/ Categories of Attacks against RCDC Partners

3.1/ Georgia

Since lately, Georgian Ministry of Defence users have been experiencing a new targeted spear phishing campaign. They have been receiving emails containing an image and a link leading to the Discord channel, ultimately downloading a malicious file stored there onto the victim's machine and infecting it.

```
We kindly request you to review Telex-release BL of invoice SK20220305,

Your prompt attention to this matter is greatly appreciated.

Kind regards,
Laila Diaz | Vice-president International Sales
Lasante Vital SA

[REDACTED-URL]
```

Figure 1. Phishing message

Variants of the malware are spread via Discord, a very popular communication platform that has been utilized for storing and spreading malware. The URL pattern sent to users contain 3 parameters: serverID, channelID, and the malicious file itself, and several discord channels have been used as malware hubs. The first stage of the malicious file is an obfuscated Javascript file, a Trojan, which downloads another stage and then ultimately fetches the REMCOS variant, which is a really popular legitimate remote administration and surveillance tool, lately very actively used for malicious intents.

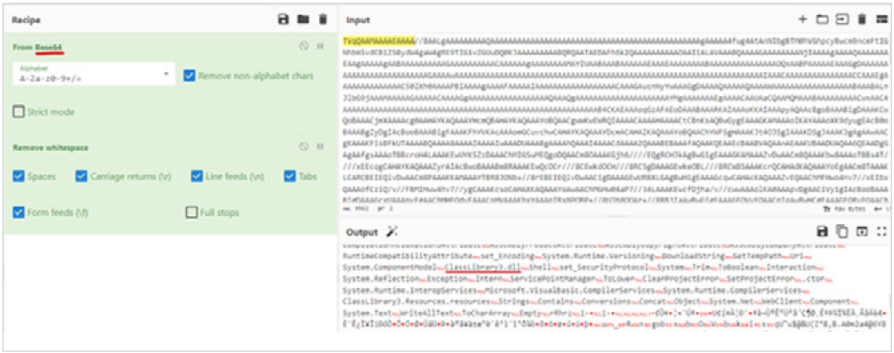

Figure 2. Deobfuscated code

The delivered malware samples are always multi-staged, avoiding detection mostly and degrading the ease of analysis. The campaign has been attributed to APT-C-36, BlindEagle.

Figure 3. Blindeagle logo

There are also several other ongoing campaigns against MOD users: camouflaged LNK files are sent via email, initializes obfuscated script upon activation, subsequently inquires to the C2 website and generates an additional malevolent file to infect systems with RAT. The CERT team has been able to eliminate all those kind of infection vectors.

Another campaign that also cannot be attributed at the moment is a Facebook advertisement video infection vector campaign, downloading the video infects victim computers; also several evasion techniques are used, such as sending a malicious file via email attachments in a nested

compression form (using layered compressed files; also using older compression algorithms which are not checked by many security solutions or cannot be checked automatically/statically). Other than that, the MOD has suffered a phishing campaign of sending emails with no attachment but rather a merchandise link ultimately leading to a phishing website for credential harvesting.

3.2/ Ukraine

Cyber espionage and cyberattacks against critical infrastructure remain the principal types of operations carried out against Ukraine. Most of them continue to be executed by means of spear phishing emails delivering malicious attachments or malicious links (TTPs: T1566.001 and T1566.002). Such emails often attempt to mimic email addresses of legitimate organisations and use different social engineering techniques to increase the count of infected machines. The malicious attachments often contain infected Microsoft Office documents which start a multistage infection chain to take control of the victim's machine for further operations. The most productive hacker groups are APT28, APT29, and Turla, all of which are tied to Russian military organisations. The Government and military sectors remain the main targets of cyberattacks against Ukraine.

3.3/ United States of America

In the past quarter, the U.S. infrastructure witnessed a return of the Racoon Stealer malware after a six-month hiatus. The malware developers have taken to hacker forums to promote a new 2.3.0 version of the malware for cyber criminals. In addition to the data stealing capabilities previously deployed by the malware, its new features include an advanced admin panel that allows threat actors to easily retrieve stolen data, a new Log Stats panel that provides an overview of their operations, a new system to detect unusual activity patterns, and a reporting system that detects and blocks IP addresses used by crawlers and bots, both which aid in evading detection.

Another noteworthy cyber occurrence was a phishing attempt that mostly targeted a well-known energy corporation in the U.S. The phishing emails were sent as counterfeit Microsoft security notices and asked recipients to scan QR codes to access PNG or PDF documents. Researchers point out that this approach offers a number of benefits over a phishing link that is directly included in an email. Given that the phishing link is concealed inside a QR image, as opposed to the QR image being embedded inside a PNG image or PDF attachment, QR code distribution methods have a significantly better probability of reaching an inbox.

Additionally, it was discovered that the Clop ransomware gang had changed its extortion tactics. The renowned gang has recently started using torrent sites to effortlessly release stolen data.

Law enforcement has relatively limited opportunity to intercept data from torrent sites. In order to leak the stolen data, the group also constructed clearweb pages for each victim. The transmission speeds are faster with torrents than with regular Tor data leak sites since they use peer-to-peer transfer between multiple users.

3.4/ Poland

The UNC1151/Ghostwriter group has been attacking mailboxes of Polish citizens for more than a year. Mandiant and Google have stated in their publications that this group is most likely linked to the Belarusian Government. According to our observations, the activity of this group has not decreased over time and the techniques they use are constantly changing. The main targets of attacks continue to be people who hold government positions, members of the boards of directors of state-owned companies, or representatives of local authorities.

One of the most common attack methods used by the UNC1151 group is sending phishing emails designed to trick people into logging into their mailboxes. The compromised mailboxes are then searched for sensitive documents and used to take over associated social media accounts and spread disinformation. Recently, however, in addition to standard phishing attacks, the UNC1151 group has also been carrying out attacks designed to infect victim computers with malware. The group is aware of the general elections taking place in Poland this autumn and the leitmotif of the messages is the ongoing election campaign. UNC1151 carried out attacks on all political parties, both the largest and the lesser known. However, it seems that each wave of attacks targets representatives of a single political party at a time.

Malicious messages are sent from free accounts set up with Polish webmail providers to the victims' personal email accounts. Email content is not personalised to a specific recipient but sometimes they are sent from an email address impersonating a person known to the recipient. The emails are set in the context of the ongoing election campaign, mimicking an invitation to a specific event and stating that details are in the attachment. The attachment is an unencrypted archive in RAR format, titled similarly to the message and containing a single CHM (Microsoft Compiled HTML Help format) file with the same name. When opened, it presents to the user a webpage with an image that actually contains information about the upcoming event. The website is built dynamically, its entire source code is a heavily obfuscated JavaScript. In the background, it initiates execution of a PowerShell code that downloads and executes the Cobalt Strike beacon and additional tool written in Golang. From this moment, attackers have unlimited access to the victim's machine and can steal saved passwords, session cookies or sensitive documents from disk.

04/ Cyber Activity in the Region: Chronological Order

2023 Q3

1. **July 3. Hackers target European government entities with a SmugX campaign.**
Security researchers have identified a phishing effort called SmugX that targets foreign affairs ministries and embassies in the UK, France, Sweden, Ukraine, Czech Republic, Hungary, and Slovakia. SmugX is believed to be the work of a Chinese threat actor. When examining the assaults, Check Point researchers found similarities to activities previously linked to Advanced Persistent Threat (APT) organisations, such as Mustang Panda and RedDelta. The researchers observed that the themes in the luring documents were frequently related to European domestic and international politics.

2. **July 8. The APT28 group (UAC-0028) used phishing attacks to obtain authentication data for public mail services.**
The UKR.NET and Yahoo.com web interfaces were imitated by HTML files that implement the technical ability to leak authentication data submitted by the victim via HTTP POST requests, according to the government computer emergency response team of Ukraine, CERT-UA. At the same time, previously hacked Ubiquiti devices (EdgeOS) were used to transport stolen data.

3. **July 10. Two cyberattacks took place in Lithuania changing broadcast content.**
The National Cyber Security Center (NCSC) identified two cyber incidents related to music broadcasts, the Ministry of National Defense (MoND) reported. In both incidents, a third-party online music streaming service was allegedly disrupted the original playlist being replaced with recorded disinformation.

4. **July 13. Malicious campaigns targeted Ukraine and Poland's government, military, and civilian entities.**
Cisco Talos has discovered a threat actor conducting several campaigns against government entities, military organisations, and civilian users in Ukraine and Poland. The fact that the behavior was encountered both in April 2022 and earlier this month demonstrates the persistency of the threat actor. Ukraine's Computer Emergency Response Team (CERT-UA) attributed the July campaign to the threat actor organization UNC1151, as a component of the GhostWriter operational actions purportedly tied to the Belarusian Government. The assaults employed a multistage infection chain started by malicious Microsoft Office documents—most frequently in the Excel and PowerPoint file formats. An executable downloader and payload that was cloaked in an image file to avoid detection was then included.

5 **July 16. Russian hacking group Armageddon increasingly targeted Ukrainian state services.**

During Ukraine's conflict with Russia, the Moscow-affiliated hacker organization Armageddon remains one of the most active and dangerous threat actors. According to the Ukrainian Computer Emergency Response Team (CERT-UA), the group, also known as Gamaredon, primarily conducts cyberespionage operations against Ukrainian security and defence services, but it has also been connected to at least one destructive cyberattack against an publicly unidentified information infrastructure facility.

6 **July 19. Russia's Turla hackers targeted Ukraine's defence with spyware.**

According to recent findings from the nation's Computer Emergency Response Team (CERT-UA), the Russian hacker outfit Turla targets Ukrainian military personnel with surveillance software. Turla, a cyberespionage organization known as Waterbug and Venomous Bear, has strong ties to the FSB, the Russian intelligence service. CERT-UA said that the gang used Capibar and Kazuar malware to attack Ukrainian defence troops.

7 **July 24. The UAC-0006 group carried out the third cyberattack in 10 days.**

The UAC-0006 group has been employing the SmokeLoader malware to conduct frequent assaults, according to the Government Computer Emergency Response Team of Ukraine (CERT-UA). At the same time, attackers use ZIP-polyglot, the contents of which are available to the user depending on the archiver program with which this archive is opened.

8 **July 28. BlueBravo deployed GraphicalProton backdoor against European diplomatic entities.**

To deploy a new backdoor named GraphicalProton, the Russian nation-state actor known as BlueBravo has been seen targeting diplomatic institutions around Eastern Europe, this illustrates the threat's ongoing development. The phishing campaign's use of lawful internet services (LIS) for command-and-control (C2) obfuscation is its defining characteristic.

9 **August 4. MerlinAgent: a new open-source tool for conducting cyberattacks against state organisations of Ukraine.**

The Government Computer Emergency Response Team of Ukraine CERT-UA received information on distribution of letters with the topic "CERT-UA recommendations on MS Office program settings." and an attachment in the form of the file "INTERNAL CYBER THREAT.chm", allegedly on behalf of "CERT-UA" using email address cert-ua@ukr.net.

10 **August 15. PDF lures containng a Russian clue aimed at NATO countries.**

According to new research, the most recent attempts by hackers to spy on government organisations in NATO nations contain a variation of malware called Duke which has ties to Russia. Two malicious PDF files were recently distributed in a campaign that targeted the foreign ministries of NATO-aligned nations. One of the PDFs contained a Duke malware variant that has been connected to APT29, also known as Nobelium, Cozy Bear, and The Dukes, a group of Russian state-sponsored cyber spies.

11 **August 17. Cuba Ransomware Group exploited CVE-2023-27532 in targeting of U.S. critical infrastructure organizations.**

The Cuba Ransomware Gang has been seen targeting important infrastructure companies in the U.S. and IT companies in Latin America. CVE-2023-27532, a vulnerability affecting Veeam products, has recently been used by Cuba Ransomware to steal passwords from configuration files. Attackers may be able to access the backup infrastructure hosts thanks to CVE-2023-27532 which "allows an unauthenticated user operating within the backup infrastructure network perimeter to obtain encrypted credentials stored in the configuration database."

August 31. Cyberattack hit one of Ukraine's state institutions.

12 The Sandworm group carried out a cyberattack against information resources of one of the state institutions of Ukraine. As a result of using the SDelete tool, functioning of the information and communication systems of the institution was disrupted. As in the group's previous attacks, the group of Russian hacktivists "Солнцепек" took responsibility for its activity.

13 **September 5. Ukraine said an energy facility was disrupted at a Fancy Bear intrusion.**

Ukraine's Computer Emergency Response Team (CERT-UA) has reported that the Russian cyberespionage group Fancy Bear attempted to breach a critical energy facility in Ukraine. The attack, attributed to Kremlin-controlled hackers, used a phishing email with an unusual approach, featuring images and a deceptive message about girls on a website. This marked a departure from Fancy Bear's previous tactics of faking government documents or distributing bogus software updates.

14 **July 28. BlueBravo deployed GraphicalProton backdoor against European diplomatic entities.**

To deploy a new backdoor named GraphicalProton, the Russian nation-state actor known as BlueBravo has been seen targeting diplomatic institutions around Eastern Europe, this illustrates the threat's ongoing development. The phishing campaign's use of lawful internet services (LIS) for command-and-control (C2) obfuscation is its defining characteristic.

15 **September 7. North Korean hackers targeted security researchers with new zero-day.**

North Korean hackers were targeting security specialists backed by the government and exploiting at least one zero-day flaw. Google issued early warning and contacted the affected vendor who is currently working to fix the issue, despite the attackers' study still being underway. Researchers have found that the North Korean hackers used social networking sites, like X (formerly Twitter) and Mastodon, to interact with their targets and security specialists who were looking for vulnerabilities.

16 **September 15. Peach Sandstorm password spray campaigns enabled intelligence collection at high-value targets.**

The Iranian nation-state threat group APT33 launched a global password spray campaign targeting thousands of organisations, with some successful breaches. Microsoft reported that this campaign, initiated in February, demonstrated more advanced tactics compared to previous APT33 attacks.

17 **September 18. Earth Lusca used Cobalt Strike for lateral movement and new Linux backdoor.**

A Linux-based virus that appears to have come from the open-source Windows backdoor Trochilus was found by Trend Micro while keeping track of Earth Lusca. The company gave it the nickname SprySOCKS because of its quick actions and SOCKS implementation.

18 **September 18. APT36 state hackers infected Android devices using YouTube app clones.**

At least three Android applications that resemble YouTube are used by the APT36 hacking gang, also known as Transparent Tribe, to infect devices with their infamous remote access Trojan (RAT), CapraRAT. Once the virus has been put on a victim's device, it may basically function as a spyware tool by collecting data, recording audio and video, or accessing sensitive communication data. The victims are probably persuaded to download and install the malicious APKs using social engineering as they are made available outside of Google Play, the official app store for Android.

19 **September 21. NoName057(16) launched Distributed Denial of Service Attacks targeting EU government and public transportation infrastructure.**

NoName057(16) launched Distributed Denial of Service attacks targeting the EU government and public transportation infrastructure. The group claims the wave of cyberattacks is in response to the support for Ukraine. The group's DDoS strategies are not brand-new. The group's infrastructure is notable for using an encrypted target list and an automated Telegram bot. Their software consists of GO scripts that implement an HTTP stressor.

20 **September 25. The Ukrainian military was targeted in a phishing campaign leveraging drone manuals.**

Ukrainian military entities were reportedly under a phishing attack that exploited their use of drones by using fake drone manuals to deliver a post-exploitation toolkit named Merlin, tracked under the name STARK#VORTEX.

2023 Q4

05/ Recommendations

Comprehensive cyber defence strategies are needed immediately to reduce the threat risk in the wake of the recent cyberattacks, like the ones conducted during the NATO Summit in Vilnius. The first and foremost priority is improving DDoS mitigation capabilities. Utilization of traffic filtering solutions and investments in strong network infrastructure can stop such disruptive attacks and protect global events from interruption. Strict access controls and encryption protocols must be implemented in order to prevent data breaches and sensitive information disclosure. Potential breaches can be quickly identified and dealt with by implementing advanced threat detection systems and continuously monitoring network activity. Additionally, to proactively find vulnerabilities, regular security audits and penetration testing should become a standard. International cooperation is crucial for combating persistent hacktivist organisations, like KillNet and NoName057(16). NATO members should work closely together to exchange threat intelligence and jointly thwart the threats. The emergence of CyberTriadHT serves as further evidence of the necessity of timely threat intelligence sharing to keep up with constantly changing threat actors. A multifaceted defence strategy is necessary to counter the threat posed by Russian military entities' Advanced Persistent Threats (APTs). To reduce potential harm, this entails bolstering network segmentation, improving endpoint security, and regularly practising incident response.

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

REGIONAL CYBER DEFENCE CENTRE

3rd QUARTER REPORT 2023