REGIONAL CYBER DEFENCE CENTRE

3rd QUARTER REPORT, 2022




3rd QUARTER REPORT, 2022

1 July–30 September

Table of Contents

Executive Summary

More than half a year has passed since Russia invaded sovereign Ukraine. The democratic world supports the people of Ukraine in a wide variety of ways. The cyber domain is no exception, as Russia strikes not only physically, but virtually as well. Organizations focusing on the situation in Ukraine not only assist Ukraine, but study ongoing patterns and defend Ukraine's and Western infrastructure. Over 60% of intelligence gathered by the CTAC team this quarter was connected to the Ukraine-Russian war in one way or another, which shows the current trend in cybersecurity incidents.

01/Q3 Highlights

Regarding Q3 2022, unfortunately, the dominant trending topic remains the war between Ukraine and Russia. Ukraine showed its strong disposition and will by defending itself, doing very well on the kinetic battlefield as well as on the cyber battlefield. Because of the politics involved in supporting the military of Ukraine, more nations are now being attacked by Russian APT groups, such as KillNet, APT28, APT29, and Venomous Bear. It seems that Ukraine's IT specialists have made a huge improvement compared to the first two quarters of 2022, defending against DDoS attacks very efficiently and without major costs. Aside from DDoS, various malware distribution attempts using phishing and defacement were noticeable.

The most notable highlights during this period include:

Ransomware attacks on retail increased and the average payment grew to more than USD 200,000.

Studies have shown that mid-sized organizations in the retail sector are experiencing increased ransomware attacks.

The US National Security Council's Counter-Ransomware Initiative picks up pace.

The International Counter-Ransomware Initiative starts hands-on work as the Regional Cyber Defence Centre assumes its role as the information hub for ransomware intelligence.

Unprecedented DDoS attacks.

One of the largest DDoS attacks in the history of both Latvian government websites and the state-controlled energy holding company "Ignitis" was launched. The head of the "Ignitis" business resilience group, cyber security expert Edvinas Kerza, said, "It was a significant experience that I wish everyone could go through, to understand your infrastructure, to understand and use the best practice, because you can't have trained under conditions like that."

Cyber security exercise "Amber Mist 2022" took place.

The Lithuanian Armed Forces Defence Staff hosted the annual cyber security exercise "Amber Mist 2022". Multiple teams from Lithuania, the United States Army's Pennsylvania National Guard, the multinational PESCO CRRT, and Georgia participated in various roles, thereby developing their cybersecurity skills.

Figure 1. / AmberMist 2022 Exercise Opening Ceremony

02/Regional Cyber Threat Landscape

After the "Killnet" group declared cyberwar against most European countries in Q2 and conducted one of the biggest DDoS attacks against a large number of entities, the latest trends indicate that as Russian troops are struggling on the battlefield, Killnet hacktivists are also losing motivation. After an active summer in which the group launched numerous campaigns against organizations in many different countries, Killnet slowed its attacks in the autumn and moved to spreading disinformation about war. Killnet has also declared cyberwar against Japan and has targeted the Japanese government's online resources, the Tokyo and Osaka metro systems, the port of Nagoya, the social media platform mixi and the tax payment system eLTAX. At the end of July, the creator of Killnet, Killmilk, announced that he will part ways with the group and will conduct attacks by himself. That said, after some time it has been observed that Killmilk continues to work closely with Killnet, and the whole split-up has been an attempt to distance Killmilk from international attention. Killnet has announced that its new leader will be BlackSide. According to Killnet, BlackSide is the administrator of an unnamed cybercriminal special-access forum, which is allegedly hosted on the Tor network. Killnet has also announced that BlackSide is skilled in ransomware, phishing, and theft from European cryptocurrency exchanges.

03/Categories of Attacks Against RCDC Partners

Lithuanian state institutions and companies have been experiencing increased cyberattacks. The first half of July was intense because of the tension caused by the EU shutting down Russia-Kalin-

ingrad railway transit. This sanction made Lithuania a target for Russian APT groups. The National Cyber Security Centre and the Regional Cyber Defence Centre reported an increase in DDoS attacks. The majority of the assaults targeted government organizations and the communications and banking industries, temporarily disrupting certain services.

Ukraine has seen an increase in phishing campaigns related to topics about the war. Several Facebook pages linking to a malicious website entitled "Unified Compensation Centre for the Refund of Unpaid Funds" were detected. Upon entering card details, the victim's bank details were compromised. CERT-UA discovered a mass distribution of phishing emails entitled "Information bulletin" and "Combat order", allegedly sent by the National Academy of the Security Service of Ukraine. The emails were sent to private email addresses. If the user opens the malicious attachments, they will be infected with the "GammaLoad.PS1_v2" malware. A more notable attack was conducted by the XakNet Team which breached one of Ukraine's largest metal manufacturers, AV metal group, leaking over 2GB of data, including invoices and personal information, transactions, credit and debit card information as well as sensitive bank information from the 2016–2022 period. As for the 3rd quarter of the year, Georgia MOD has experienced persistent campaigns. As for the malware delivery mechanism for these campaigns email phishing was chosen, several users were prompted to download and open up an invoice or some sort of document, which was ultimately extracting "NanoCore RAT" and installing it on the victim system. Malware obfuscation levels varied depending on the success rate (increasing after failed attempts to infect the system), such as storing final actual payload in an encrypted form in the resources section of a file delivered to a victim, which was then loaded into memory directly and some other advanced techniques were used. Another worthy to note campaign was and is still present a "bumblebee campaign", which is also intended to be delivered via email phishing, regarding to this malware after several analysis sessions assumptions were made that this type of malwares delivers bumblebee packed payload (payloads are cobaltstrike payloads for c2 functionality basically). Relative modifications were made to email security system and endpoint security systems to decrease the risk of being infected with bumblebee packed malwares in general.

Both campaigns shared one common characteristic, phishing emails were sent from spoofed private company emails or from actual ones, which were compromised, Georgian CERT team has communicated with all those victims to avoid further infection too.

04/ Ukraine Dismantles Sophisticated Bot Farms and Cyber-Criminal Groups

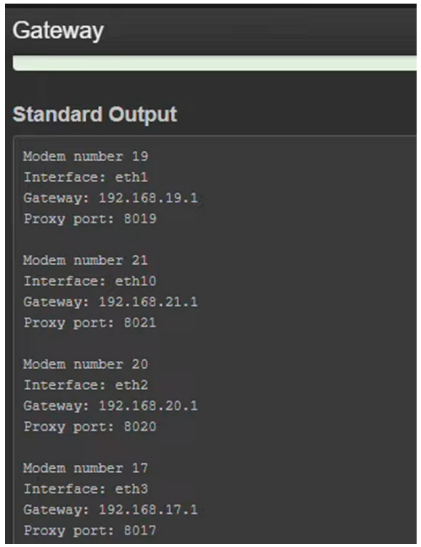

Figure 2. / The Proxy Gateway for 3G/4G Modem Farm

The Cyber Department of the Ukrainian Security Service (SSU) dismantled a number of bot farms that spread Russian disinformation on social networks and messaging platforms via thousands of fake accounts. These groups had sophisticated hardware and were utilizing large numbers of disposable SIM cards and 3g/4g USB modems connected to a centralized management server. In one instance, the SSU managed to confiscate 4 servers, more than 250 USB modems, and mobile phones with evidence of unlawful activity, bank cards, and over 400 SIM cards of mobile operators. It is possible to speculate on the operating methods of such farms. The main goals of such a farm are to create a large number of fake accounts on various social networks, to spread disinformation and to have a large pool of dynamic IP addresses that allow various attacks to be conducted without being easily blacklisted. Instructions on how to centrally manage a large number of 3g/4g modems are available on YouTube. One example: https://www.youtube.com/watch?v=jXdH1AGHT_Q. The main method is to connect all the modems to a powered USB hub and to connect them to the server. The server runs a proxy service and connects all modems via separated TCP port addresses. This allows the convenience of utilizing rotating IP addresses and different ISPs for each new account creation or even attack vector. Source: https://ssu.gov.ua/en/novyny/sbu-zablokuvala-shche-dvi-botofermy-yaki-rozghanialy-destruktyvnyi-kontent-v-ukraini

Another aspect of these bot farms is that they spread misinformation via more conventional means like SMS (Short Message Service). During the initial stages of the Russian war in Ukraine, it was observed that modern cell phones with Android or IOS operating systems and built-in GPS services are quite dangerous if compromised. These compromised phones can leak geo-location information. A lot of Ukrainians have opted to use less sophisticated phones for general communication and SMS exchange. The botnet operators have adapted to this and acquired GSM gateways to send SMS messages in bulk, spreading disinformation. We can see these gateways, combined with disposable sim cards, in operation. These GSM gateways can be cheaply purchased

from Chinese vendors like AliExpress. They have centralized management software and allow easy operation.

There are techniques and procedures on how to locate and combat this type of bot farm, but such efforts require the deep involvement of GSM operators and ISPs. They have the ability to track and correlate network or 2g/3g/4g traffic within their infrastructure. Simple logic applies here. If a single address from a specific triangulated location makes several hundred GSM/GPRS/EDGE/4G connections, it is a possible indicator of a bot farm, since it is unlikely that a single house or an apartment would have several hundred mobile phones or several hundred 3g/4g modems. With cooperation from CERT and Ukrainian law enforcement, it is possible to recon and raid such establishments, confiscating the hardware and arresting the perpetrators. Although we can see that different GSM providers are used to hide the perpetrators' tracks, cooperation among GSM operators and ISPs, coordinated by law enforcement or CERT, can easily detect such hot spots and find a well-funded bot farm. The hardware for such operations is quite expensive, so it is believed that these bot farms are funded by the Russian Federation.

Figure 3. /3G/4G Bot Farm Confiscated by Ukrainian Law Enforcement

Figure 4. /SMS/GSM gateway and SIM Card Batches Confiscated by Ukrainian Law Enforcement

05/The Decline of Malware Spreading via Vbs Macros

Hackers have opted for new attack methods after Microsoft blocked macros by default.

With Microsoft taking steps to block Excel 4.0 (XLM or XL4) and Visual Basic for Applications (VBA) macros by default across Office apps, malicious actors are responding by refining their tactics, techniques, and procedures (TTPs). "The use of VBA and XL4 Macros decreased approximately 66% from October 2021 through June 2022," Proofpoint said, describing this as one of the largest email threat landscape shifts in recent history. In its place, adversaries are increasingly pivoting away from macro-enabled documents to other alternatives, including container files such as ISO and RAR as well as Windows Shortcut (LNK) files in campaigns to distribute malware.

VBA macros embedded in Office documents sent via phishing emails have proven to be an effective technique, allowing threat actors to automatically run malicious content after tricking a recipient into enabling macros via social engineering tactics.

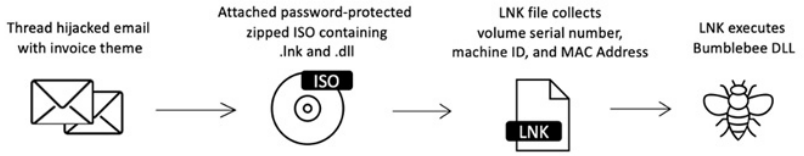

Figure 5. / Malware payload delivery via ISO and LNK files

However, Microsoft's plans to block macros in files downloaded from the internet have led to email-based malware campaigns experimenting with other ways to bypass Mark of the Web (MOTW) protections and to infect victims. This involves the use of ISO, RAR, and LNK file attachments, which have surged nearly 175% during the same period. At least 10 threat actors are said to have begun using LNK files since February 2022. "The number of campaigns containing LNK files increased 1.675% since October 2021," the enterprise security company noted, adding the number of attacks using HTML attachments more than doubled from October 2021 to June 2022.

Mark of the Web (MOTW) is a security feature originally introduced by Internet Explorer to force saved webpages to run in the security zone of the location the page was saved from. Back in the day, this was achieved by adding an HTML comment in the form of <!--saved from url=> at the beginning of a saved web page. This mechanism was later extended to file types other than

HTML. This was achieved by creating an alternate data stream (ADS) for downloaded files. ADS is an NTFS file system feature that was added as early as Windows 3.1. This feature allows for more than one data stream to be associated with a filename, using the format "filename:streamname". When downloading a file, Internet Explorer creates an ADS named Zone.Identifier and adds a ZoneId to this stream in order to indicate from which zone the file originates. Although it is not an official name, many people still refer to this functionality as Mark of the Web.

Some of the notable malware families distributed through these new methods consist of Emotet, IcedID, Qakbot, and Bumblebee.

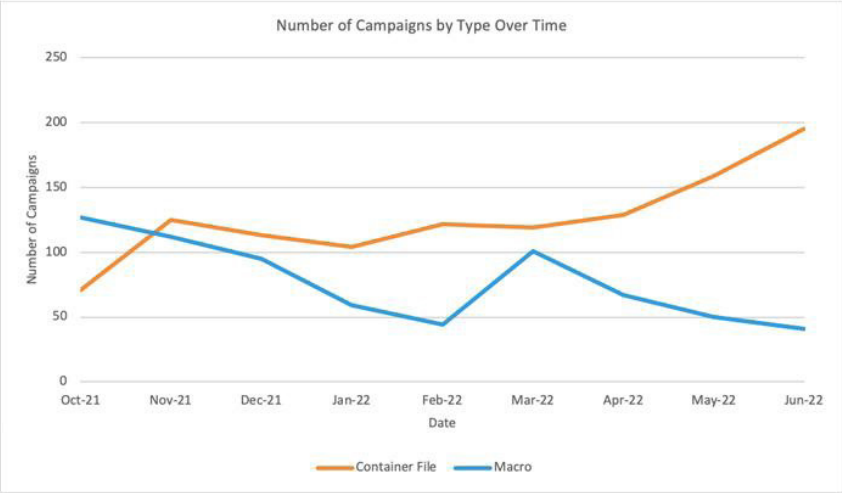

Figure 6. / Drop in MS Office MACRO virus usage and rise in Container usage

Generally speaking, these other file types are directly attached to an email in the same way we would previously observe a macro-laden document. There are also cases where the attack chains are more convoluted, for example, with some recent Qbot campaigns where a .ZIP containing an ISO is embedded within an HTML file directly attached to a message.

As for getting intended victims to open and click, the methods are the same: a wide array of social engineering tactics to get people to open and click. The preventive measures we use to avoid phishing still apply here.

https://thehackernews.com/2022/07/microsoft-resumes-blocking-office-vba.html

06/ Cyber activity In The Region: Chronological Order

2022

1. **July 1, Russian hackers allegedly target Ukraine's biggest private energy company**

   Russian hackers launched a cyberattack on the largest private energy company in Ukraine in retribution for the owner's resistance to Russia's attack on Ukraine. The hack was intended to "destabilize the technological processes" of DTEK Group's distribution and general businesses, spread misinformation about the company's operations, and "leave Ukrainian consumers without electricity" according to the company, which owns coal and thermal power plants in various regions of Ukraine.

2. **July 4, Hackers revealed the data of about fifty thousand customers of "Švaros broliai"**

   Hackers released data taken from "Švaros broliai", a major car wash company in Lithuania, including names, surnames, vehicle license plates, emails, and phone numbers. Bank account and credit card information, as well as other sensitive information such as home addresses and national identity numbers (personal codes), were not part of the compromised database.

3. **July 4, Lithuanian website was defaced**

   One of the hacktivist groups associated with "Killnet", "NoName057(16)", posted on their Telegram channel about the defacement of the Lithuanian logistics company "ExpressTrip". On the defaced web page, there were claims about the "correct" attitude to the ban on the transit of Russian cargo to the Kaliningrad region. In addition, the defaced web page supported the Russian war against Ukraine and called it "the special operation of the RF armed forces".

4. **July 9, "Ignitis" was hit by the most significant DDoS attack in a decade**

   In the early hours on Saturday, the Russian hacking group "Killnet" announced on its Telegram channel that it had attacked ESO (Energy Distribution Operator). "Killnet" announced that the ESO page was 100% blocked. As of Saturday morning, neither the ESO website nor the Ignitis Group website were available. An ESO public relations representative stated that Ignitis Group was facing the biggest cyberattack in a decade. Since Saturday night, they had been experiencing strong DDoS attacks, which disrupted the Group's websites and the availability of electronic services.

5. **July 9, Pro-Kremlin hackers Killnet hit Latvia with the biggest cyberattack in its history**

   According to a senior NATO officer, Latvia witnessed the most severe wave of cyberattacks in its history, including a 12-hour assault on its public broadcasting centre. Due to several forceful actions taken by Latvia, including bringing back conscription and compiling a list

of Soviet monuments to be demolished, it appears that the nation has become a target for pro-Kremlin hackers. Killnet, a group of cyber activists who have sided with Russia and declared "war" on 10 Western nations that support Ukraine, including the USA and Great Britain, has coordinated the digital onslaught.

6 **July 14, Lithuanian advertising website hit by cyberattack, warns of a possible customer data leak**

Following a cyber-assault against the Lithuanian advertising website alio.lt, the data of thousands of clients may have been compromised. According to a press release from Kristijonas Šiaulys, head of IT at alio.lt, "It looks like it could have been yet another Russian attack against Lithuania's online space, the kind of attack which most corporate entities are unable to resist."

7 **July 16, Cyberattacks using the Emotet malware are on the rise in Taiwan**

Taiwan News published information that Taiwan government departments were the target of a sharp rise in Emotet malware attacks in June. In total, investigators discovered 72,185 suspicious incidents that posed a danger to government email accounts and websites. Overall results showed that 48% of the incidents were of a malicious nature.

8 **July 19, Russian hackers tricked Ukrainians with fake "DoS Android Apps to Target Russia"**

Russian threat actors used the current crisis in Ukraine to disseminate Android malware disguised as an app for pro-Ukrainian hacktivists. The virus was traced to Turla, an advanced persistent threat also known as Krypton, Venomous Bear, Waterbug, and Uroburos, which are connected to Russia's Federal Security Service (FSB), the Google Threat Analysis Group (TAG) stated.

9 **July 22, Ukrainian radio stations hacked to broadcast fake news about Zelenskyy's health**

The Ukrainian radio station TAVR Media became the latest target of a hack, which led to the transmission of a hoax message about President Volodymyr Zelenskyy.

10 **July 26, Cyber attacks of the UAC-0010 group (Armageddon) using the malicious program GammaLoad.PS1_v2**

The government computer emergency response team of Ukraine CERT-UA discovered the fact of mass distribution of emails with the subjects "Information bulletin" and "Combat order", ostensibly from the National Academy of the Security Service of Ukraine. At the same time, emails were sent to the private email addresses of the targets of the attack.

11 **July 26, Internet disruptions hit Kherson as Ukrainian forces advance**

The Ukrainian city of Kherson went offline for several hours on Tuesday, according to observers of network operations, continuing a trend of connection problems that have afflicted Ukraine as it struggles to resist Russia's invasion. Falling in March, Kherson became the first significant Ukrainian city to be taken by Russian forces during the invasion this year. The Ukrainian authorities are now counterattacking to retake the city and the surrounding southern region.

12 **August 2, Taiwanese government sites were disrupted by hackers**

Several websites run by the government of Taiwan were disrupted by distributed denial-of-service (DDoS) attacks hours before U.S. House Speaker Nancy Pelosi became the first high-ranking U.S. official in 25 years to visit the country.

13 **August 2, Ukrainian intelligence services disrupted domestic social media bot farm intended to destabilize domestic political and military affairs**

The Security Service of Ukraine (in Ukrainian, SBU) declared it had dismantled a social media bot farm that attempted to destabilize Ukrainian society and the political landscape by spreading false material to undermine the Ukrainian political and military leadership. The network, which had over a million accounts, was active in Kyiv, Kharkiv, and Vinnytsia. It registered social media accounts using 5,000 SIM cards and used 200 proxy servers to hide its location and to avoid discovery.

14 **August 9, China-linked group TA428 used PortDoor malware to target defence and public institutions in Eastern Europe**

Kaspersky published a report regarding a TA428 cyberespionage campaign that targets defence and public institutions in Eastern Europe. The TA428 attack chain starts through phishing emails containing weaponized Microsoft Office documents that exploit CVE-2017-11882, a remote code execution (RCE) vulnerability that could allow attackers to run arbitrary code, namely, the PortDoor malware payload, in the context of the current user. The emails are well-crafted, using specific details on the organization's operation, suggesting that TA428 stole the document before sending it to the target organization.

15 **August 15, Microsoft disrupted a Russia-linked hacking group targeting defence and intelligence organizations**

Microsoft published new details about a suspected Russian hacking group that has carried out cyberespionage attacks against government organizations, think tanks, and defence contractors in NATO countries since at least 2017. Microsoft's Threat Intelligence Centre (MSTIC) also said it has "taken actions to disrupt campaigns" launched by the group, which they call SEABORGIUM, but is also referred to as Callisto, COLDRIVER, and TA446 by other security researchers.

16 **August 17, Ukraine's state-owned nuclear power operator said Russian hackers attacked its website**

Ukraine's state nuclear power company Energoatom said that Russian hackers had launched an "unprecedented" cyberattack on the company's official website. The Russian hacktivist group People's Cyber Army, which claims to include more than 8,200 volunteer members, used 7.25 million bot accounts to flood Energoatom's website with junk traffic, making it unreachable. The attack lasted three hours but had no larger impact on the company's operations. Energoatom said in a statement that it managed to quickly regain control of the website and limit the attack.

17 **August 23, Ukraine and Poland agreed to jointly counter Russian cyberattacks**

Ukraine and Poland signed an agreement to strengthen cybersecurity collaboration as offi-

cials warn of potential cyberattacks from Kremlin-linked hackers. The countries decided to jointly fight cybercrime and share their experience in combating cyber threats, including those from Russia, according to the Ukrainian Ministry of Digital Transformation.

18 **August 30 and 31, Mass distribution of the AgentTesla malware to Ukrainian, Austrian and German organizations**

The government computer emergency response team of Ukraine CERT-UA recorded mass mailings of emails with the topic "Technisches Zeichnen" among Ukrainian, Austrian and German organizations. The email contains an IMG file that when opened will run JavaScript code, ensuring that the node.txt file is downloaded and run using PowerShell. The IMG file also contains a CHM file with the same name that will execute the same code when opened. PowerShell code that will decode, decompress (Gzip), and execute DLL and EXE files is contained in the mentioned file. AgentTesla malware is contained in the EXE file.

19 **August 30, Facebook phishing campaign targeting Ukrainian citizens**

The government computer emergency response team of Ukraine CERT-UA revealed an increase in the number of fraudulent pages on the Facebook social network. The content of announcements on such pages usually refers to the topic of monetary compensation, the eHelp platform, and financial assistance from various organizations. In the ads, it is suggested to click on a link leading to the phishing page of the so-called "Unified Compensation Centre for the Return of Unpaid Funds". There, it is offered to receive a payment, for which it is necessary to provide personal information and to make an additional payment. As a result, payment card data will be compromised.

20 **September 7, Ukraine dismantled more bot farms spreading Russian disinformation**

Two more bot farms that used hundreds of fake accounts to promote Russian misinformation on social media and messaging services were taken down by the Cyber Department of the Ukrainian Security Service (in Ukrainian, SBU). The SBU found that this "army of over 7,000 accounts" of bots was employed to undermine the Ukrainian Defence Forces, defend Russia's military actions, and polarize social and political life in Ukraine. The SBU seized hundreds of mobile SIM cards and USB modems during searches at the suspects' homes, working with the National Police, the Odesa and Kyiv Regional Prosecutor"s Offices, and other law enforcement agencies.

21 **September 13, Pro-Ukraine hackers claim an attack on Russian TV broadcasts**

Pro-Ukrainian hackers took credit for breaching Russian TV channels and broadcasting anti-war messages comparing Russia's attack on Ukraine to the September 11 terrorist attacks in New York. Members of a pro-Ukrainian hacktivist group called "hdr0" said on Telegram that several Russian channels, including Channel One Russia, Russia-24, and Russia-1 were affected by the hack. The group did not provide details about how they carried out the attack or how many people saw the message. The hacked broadcast over the weekend showed footage of Russian attacks on Ukrainian cities and excerpts from interviews with Ukrainian President Volodymyr Zelenskyy and other world leaders condemning Russia for the violence in Ukraine.

22 **September 15, Gamaredon APT targets Ukrainian government agencies in a new campaign**

Cisco Talos discovered Gamaredon APT activity targeting users in Ukraine with malicious LNK files distributed in RAR archives. The campaign, which is a component of an ongoing espionage operation that was detected in August 2022, uses a number of modular PowerShell and VBScript (VBS) scripts to infect Ukrainian victim machines with information-stealing malware. A malware program known as an info-stealer serves two purposes: it can exfiltrate particular file types and send additional binary and script-based payloads to an infected endpoint.

23 **September 20, Hacktivists Supporting Ukraine Make the claim to have breached the notorious Russian Mercenary Group**

The hacktivist organization known as the Ukraine IT Army released a screenshot of a website they claimed to have broken into, associated with the Wagner gang. "We have all the personal data of mercenaries! Every executioner, murderer, and rapist will be severely punished. Revenge is inevitable!"

24 **September 26, Hackers attacked the Lithuanian banking systems, which many companies use - it's possible that they intercepted the data of money transfers**

BankingLab, the developer of Lithuanian banking systems, suffered a cyber attack during which customer data and financial transactions could have been leaked. The data is shared publicly by malicious actors. "BankingLab" is a financial technology company that previously merged four Lithuanian fintech companies: "Baltic amber solutions", "GIRO sistema", "Mokėjimų vizija" and "AutoKYC". The main clients of BankingLab are Bankera, Vialet, Connect Pay, Simplex, PayRay bank, Perlas Finance, Mano Bankas, SH Financial, and others. At breached. to, there is a 3.4-gigabyte archive of Perlas Finance data which according to hackers contains flows of financial transactions and data of ordinary users.

07/ Recommendations

In the 3rd quarter, we have seen a wide variety of cyber attacks. But the main trends remain the same: DDoS, malware delivery, website defacement, and data stealing/leaking attacks. Some recommendations on how to defend against and mitigate these threats:

1. **DDoS:** In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. There are various methods to defend against this or to mitigate the impact, from proper gateway configuration to configuring javascript challenge or outsourcing protection to content delivery service providers (CDN) like Cloudflare or Akami. RCDC has created a brief recommendation document with a checklist for small to medium businesses and public sector organizations. It is available online here: https://www.nksc.lt/rkgc/en_reports.html
2. **Malware:** Threat actors have started to adopt new techniques to spread malware. In the past, VBscript and MS Office macros were the most often-used attack vectors, but recently new techniques using container files such as ISO and RAR as well as Windows Shortcut (LNK) files have surfaced. It is recommended to filter these files on email gateways and proxy servers to prevent execution and infiltration into end devices. New malware detection techniques that use sandboxing for analysis are successful in detecting this type of malware. It is recommended to use the most up-to-date antivirus and endpoint protection tools.
3. **Defacement:** Defacement usually follows after a website has been compromised and a malicious actor has managed to get administrative privileges on a content management system. To prevent this, it is recommended to keep your CMS system up to date. The most popular CMS is WordPress. Here are some common steps to harden its security:
    - Use a reverse proxy with a hardened configuration;
    - Disable PHP Execution in the "Uploads" folder;
    - Protect WordPress wp-config.php file;
    - Protect .htaccess from unauthorized access;
    - Disable directory browsing in WordPress;
    - Block cross-site scripting (XSS);
    - Restrict all access to WP-includes;
    - Restrict Direct Access to plugin & theme PHP files;
    - Access to wp-admin only by IP;
    - Secure important files;
    - Protect /wp-content/.

08/ Endnote

To sum up, CTAC states that cyber threats are growing rapidly due to current events and they affect us in various ways. As of now, the government and private sectors take more seriously the task of securing their infrastructure. Facts show that not everybody is safe from DDoS or phishing campaigns, and more attention to detail is necessary. However, security should be a concern for each employee in an organization, not only the IT professionals. Cybersecurity policies are important because cyberattacks and data breaches are potentially costly. At the same time, employees are often the weak links in an organization's security. Strengthening defences against a constantly changing threat will be easier with knowledge of new cybersecurity technology, methodologies, tactics, and organizational structures. Cybersecurity is a never-ending battle. There will not be a lasting, conclusive answer to the issue anytime in the foreseeable future. The complexity of information technology systems, the inherent nature of information technology (IT), and human fallibility in making judgments about what actions and information are safe or unsafe from a cybersecurity perspective - especially when such actions and information are highly complex - are the leading causes of cybersecurity problems. Threats to cybersecurity also change over time. Intruders adjust by creating new tools and tactics to undermine security when new protections are developed to counter more recent attacks. Therefore, improving a system's cybersecurity posture - and, by extension, the organization in which it is embedded - must be seen as a continuous process rather than something that can be completed once and then ignored.

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