REGIONAL CYBER DEFENCE CENTRE

4th QUARTER REPORT, 2022




4TH QUARTER REPORT
2022

1 October - 31 December

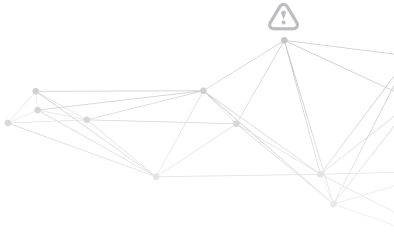
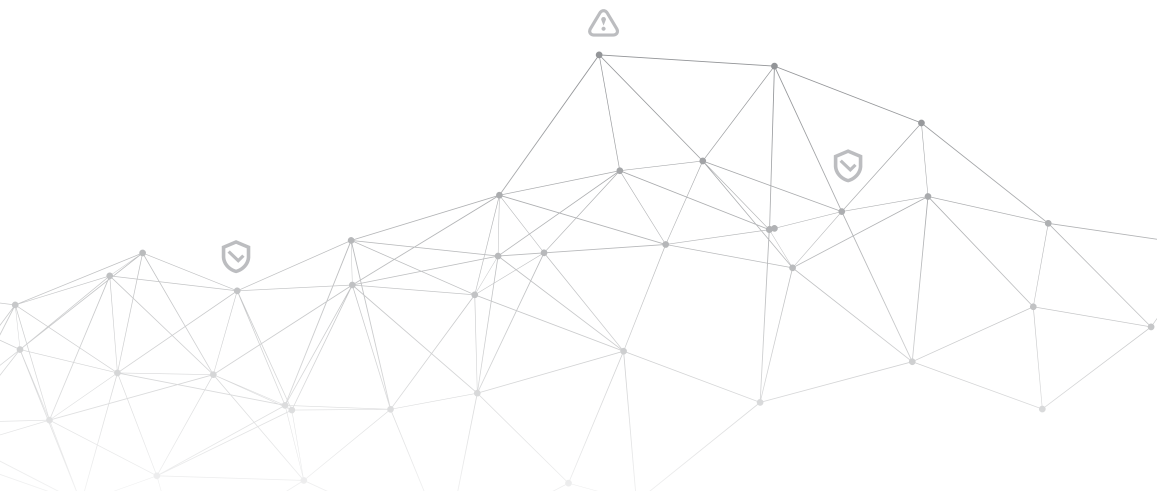


Table of Contents



Executive Summary

The fourth quarter of 2022 was the least eventful as compared with others. Seeing that it had used most of its offensive cyber capabilities at the start of the war, Russia slowed down and focused on spreading disinformation about the unprovoked war that they had begun. One of their focuses is targeting Ukraine's energy infrastructure in order to disrupt power supply around cities. Ukraine, on the other hand, is conducting more offensive cyber operations which seem to be very effective and have an impact on Russia's cyber domain. Independent hackers from all over the world conducted counter-cyberattacks, stole and revealed Russian government and financial data, including emails, details of banking operations, energy production, and propaganda efforts, as well as identities of soldiers and FSB agents. The private information is then given to international activists in retaliation for Russia's actions in Ukraine. Hackers' success in creating mayhem in the Russian cyber systems and dispelling the myth of the unbreakable Russia's cyber defense is another result of their recent activity. Other than that, RCDC partner nations did not see extraordinary amounts or types of attacks against their infrastructure.

01/Q4 Highlights

Although it seems that we have witnessed a decrease in cyber operations this quarter, not much has changed in reality. As cyber-attacks take place every day, the CTAC team offers several highlights that actually show successful efforts of managing and mitigating the daily attacks and ensuring that the possible damage is reduced as much as possible. On a positive note, we can see more and more public and private sector organizations are becoming aware of the cyber threats that surfaced during the last year. We can see an increase in investment in cyber defence. Modern technologies and services like UTM and CDN have increased in popularity and usage across all sectors in our partner organizations and nations. RCDC has contributed to the overall awareness of cyber threats and methods of mitigation. Additionally RCDC as an organization has grown and expanded its activities with various projects and initiatives over the last 3 months and is approaching a successful completion by the 2022.

The most notable highlights during this period were the following:

Poland officially joined the RCDC

On October 10 Poland became the 5th nation to officially join the Regional Cyber Defence Centre. During the Board of Directors meeting Poland was formally voted to be accepted and therefore become a full member of the Centre. It is expected that Polish specialists will begin working on a rotational basis starting 2023. Poland's accession and signature of all documents will be completed by the end of the year with Polish representatives starting the work at the unit in Kaunas shortly afterwards. Poland indicated in the formal letter of request to become a member sent this summer that it would post cyber security experts from the Office of the Prime Minister of Poland and the Ministry of National Defence of Poland.

Figure 1. CTAC Board of Directors meeting took place on October 10

The Counter Ransomware Initiative reached a new phase

The Second International Counter Ransomware Initiative (CRI) Summit, with participation of 36 nations and the EU from October 31 to November 1, 2022, was organized by the White House. Throughout the Summit, the CRI and its partners from the commercial sector deliberated on and came up with practical, coordinated strategies for stopping the global spread and effects of ransomware. The Biden-Harris Administration's efforts to stop ransomware assaults are anchored by the CRI Summit which is also a key component of our global cybersecurity strategy.

Figure 2. Officers of CRI countries meeting vice-president Harris

The RCDC will be releasing semi-annual public reports on ransomware trends and defenses. Through this endeavor, CRI countries aim to reach a wide range of stakeholders with the technical information about ransomware (tools, tactics, and procedures), as well as to combine and summarize the data provided by the participating members.

National exercise Cyber Shield 2022 took place in Lithuania

The main cybersecurity exercise in Lithuania, Cyber Shield, took place October 18-20. 116 organizations representing various spheres were among the participants making it the largest number in the history of this exercise. As annually, the exercise was hosted by the National Cyber Security Centre (NCSC) of Lithuania in partnership with Kaunas University of Technology (KTU). The exercise iteration this year also used new NCSC capabilities which include the Cyber Range (CR) and the Phishing Simulation Platform.

02/Regional Cyber Threat Landscape

Sensor data that covers Lithuania's public and government sector shows a slowdown in the overall reconnaissance and scanning events by foreign actors.

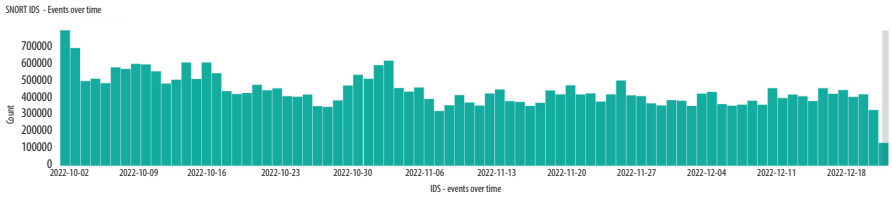


Figure 3. Snort IDS event triggers over time

The graph above presents all events originating in Russia and China recorded by Snort IDS

02.1/ Killnet Operational Slowdown

This quarter we have observed a slowdown in the operation of the previously very active Killnet pro-Russian hacktivist group and of other groups associated with it. Every once in a while these groups conduct DDoS campaigns against various countries that proactively support Ukraine. One of the most high-profile DDoS campaigns Killnet launched was against the US aerospace, defense, and security company Lockheed Martin but it did not seem to impact their infrastructure. In October, allegations that Killnet had adopted Chaos (Yashma) ransomware came to light. Killnet hackers are not asking for any ransom at all as a result of the attacks their real primary goal being to encrypt the victims' data. Not surprisingly, Ukraine's infrastructure, private or public sectors remained their main target. The Killnet ransomware encrypts system files and folders and then delivers a ransom message, just like other malware. However, Killnet uses a bizarre ransom demand method, it does not provide any information about the ransom demand in the message as enemies do, instead, the ransom message includes a link to a pro-Russian Telegram group and its propagandist posts regarding the conflict in Ukraine. The Telegram channel's idea is fundraising for the budget of the Russian Federation. Two ransomware samples have been made publicly available and are tracked under the file hashes:

- b1c8ddcdfea93031a565001366ffa9fdb41a689bddab46aec7611a46bb4dc50
- dfcb800f74b602edc3dfd3fad3bdbedc981fbff895dc3b907decd8b4b889fdc4

The ransomware appends the infected files with ".killnet" extension and leaves the following ransom note ("Ru.txt"), translated from Russian as: "You are under attack from Killnet_reservs." Based on open-source reporting and analysis, both ransomware samples return positive detections for Chaos ransomware.

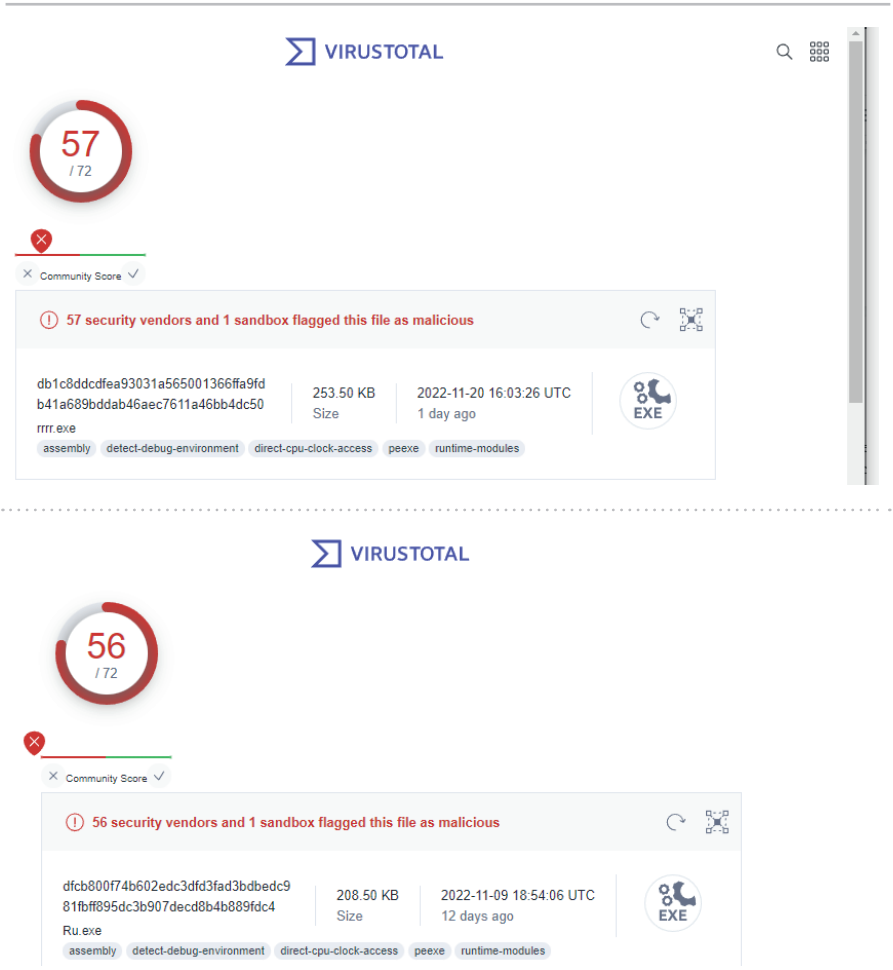


Figure 4. VirusTotal file hash analysis

02.2/ Zoho ManageEngine Unauthenticated Remote Code Execution Vulnerability Causes Multiple Breaches Across Fintech Companies

Zoho has at least 80 million customers worldwide, including big companies like Netflix, Amazon, Fortinet, Facebook, KPMG, Renault, HP, and Tesla. CISA issued a warning "based on evidence of active exploitation". Zoho Corporation is an Indian multinational technology company that makes computer software and web-based business tools. It is best known for its online office suite offering Zoho Office Suite. The company was founded in 1996 by Sridhar Vembu and Tony Thomas and had presence in seven locations with the global headquarters based in Chennai, Tamil Nadu, India, and corporate headquarters outside of Austin in Del Valle, Texas.

The company provides a variety of tools for small to medium fintech companies, thus the list of disclosed CVE's has caused some reputational damage. This Report will look into the Lithuanian-based company called BankigLAB (officially, BALTIC AMBER SOLUTIONS, UAB) that underwent a data breach facilitated by a Zoho ManageEngine Password Manager Pro vulnerability.

Zoho ManageEngine Password Manager Pro until 12101, and PAM360 until 5510, are vulnerable to unauthenticated remote code execution (this also affects ManageEngine Access Manager Plus until 4303 with authentication.) It has CVE-2022-35405 designation and vulnerability score 9.8 critical. This vulnerability is heavily exploited in the wild.

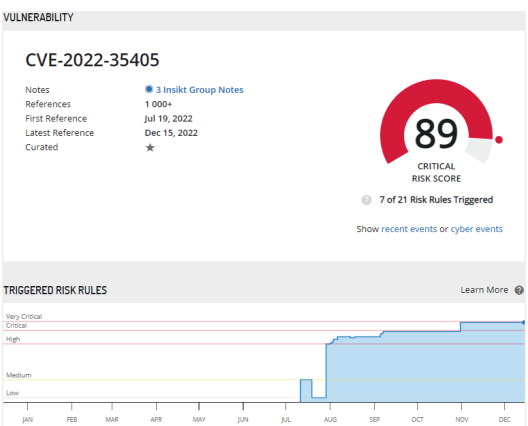


Figure 5. CVE-2022-35405 Risk score

According to BankingLab, hackers managed to leak data of several individuals and legal entities during the attack. According to the company, customer money is safe and the affected customers have been informed. To prevent possible attacks in the future, the company temporarily restricted payment, electronic and mobile banking and other services, implemented additional measures and bolstered cyber security.

As Narimantas Bloznelis, CEO of BankingLAB stated, "All cyberattacks are more complex than being just about one vulnerable product. The cyberattack was large-scale and sophisticated. It is obvious that threat actors have been preparing for it for a long time and in different ways." Bloznelis said he did not want to share any more information about the attack while the investigation was still pending but would elaborate once it was over, adding that he had informed all affected clients. BankingLab also informed the Lithuanian State Data Protection Inspectorate.

It is speculated that the threat actor hacked into the BankingLab software-as-a-service (SaaS) banking platform. It is possible that BankingLab relied on ManageEngine to protect its network. During the investigation of leaked data, the last database entry was found to had taken place on 25/09/2022.

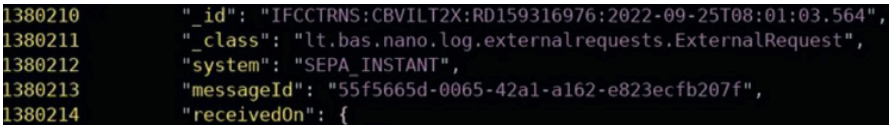


Figure 6. Leaked database content

The threat actor made the 108MG-strong database publicly available for free, it contained a PostgreSQL dump with extensive log data and other sensitive information, such as mail account settings, all user mail settings, agent installation, mobile authorization keys, bank account numbers, clients names, surnames, citizenship and personal identification number (equivalent of the Social Security Number used in the USA and the National Insurance Number used in the UK) that was found to be exfiltrated. During the initial analysis of leaked data, there were no indications of any possible malware placement in the archive. The tar.gz file contained mainly BSON MongoDB files. 86264 transactions are found to have been performed as shown by the number of transactions IODS. Further analysis still needs to be conducted to identify the list of affected users. Most of the leaked files contained system information and metadata. The CTAC was unable to find any unhashed or clear passwords in the leaked files.

```
{
        "_id": "LT[redacted]:EUR:7d10e16a-54a4-41a1-a236-53c468361996",
        "_class": "lt.bas.nano.query.accountant.vmi.model.SaskaitaT",
        "savininkas": {
                "partyId": "543dd5b7-c7f0-45cc-a6c8-ce5e64e3c529",
                "tip": "F",
                "kod": "[redacted]",
                "vard": "[redacted]",
                "pav": "[redacted]",
                "pil": "LT"
        },
        "refId": "S:CA:[redacted]:EUR:130",
        "data": {
                "$date": {
                        "$numberLong": "1617840000000"
                }
        },
        "bnkod": "30200",
        "typ": {
                "$numberInt": "1"
        },
        "nr": "LT[redacted]",
        "vkod": "EUR",
        "adat": {
                "$date": {
                        "$numberLong": "1452211200000"
                }
        },
        "kdata": {
                "$date": {
                        "$numberLong": "1452261117811"
                }
        },
        "dependantParties": [
                "543dd5b7-c7f0-45cc-a6c8-ce5e64e3c529"
        ],
        "pending": false,
        "errors": "",
        "reportRefId": "67b8797c-49e7-49bc-a1fa-b85852f1d44c",
        "source": {
                "accountType": "CURRENT_ACCOUNT",
                "accountNumber": "LT[redacted]"
        }
```


Figure 7. Leaked database content (anonymized)

At the time of writing the Report, the investigation was still ongoing and no further information was available. On a positive note, all vulnerabilities relating to ZOHO ManageEngine Password Manager Pro and PAM 360 have been fixed and this particularly vulnerability should no longer become a security threat.

Severity : Critical

CVE ID : CVE-2022-35405

This document explains the remote code execution vulnerability identified in the following ManageEngine products,

1. Unauthenticated remote code execution in ManageEngine Password Manager Pro and PAM360.
2. Authenticated remote code execution in ManageEngine Access Manager Plus.

The complete fix for this is now available in the below versions,

Product Name	Affected Version(s)	Fixed Version(s)	Fixed On
Access Manager Plus	4302 and below	4303	24-06-2022
Password Manager Pro	12100 and below	12101	24-06-2022
PAM360	5500 and below	5510	23-06-2022

Figure 8. CVE-2022-35405 patch dates

02.3/ Analysis of a Remote Code Execution (RCE) Vulnerability in Cobalt Strike 4.7.1

To address the problem found in Cobalt Strike version 4.7, HelpSystems released an out-of-band update. Cross-Site Scripting (XSS) was the designation given to the vulnerability by identification number CVE-2022-39197. Red Team operations address the fine balance between command and control (C2) structures. The Red Team will frequently hold a position of great privilege on the target network, therefore a compromise of the C2 framework could result in a compromise of the Red Team operator's system, as well as control established on the target systems over beacons. As a result, threat actors and Counterintelligence (CI) operations have given a high priority to C2 framework vulnerabilities. At that time, it was considered a critical vulnerability. A client-side UI input field manipulation, a check-in simulation of a Cobalt Strike implant, or hooking an active Cobalt Strike implant on a host might all result in a successful exploitation of the XSS vulnerability.

The research was conducted because of the disclosure of the release notes that this vulnerability could result in RCE. Threat actors could exploit the flaw by leveraging an HTML <object> tag to load a malicious payload hosted on a remote server and inject it within the note field or the graphical file explorer menu in the post-exploitation platform UI. The screenshot below shows

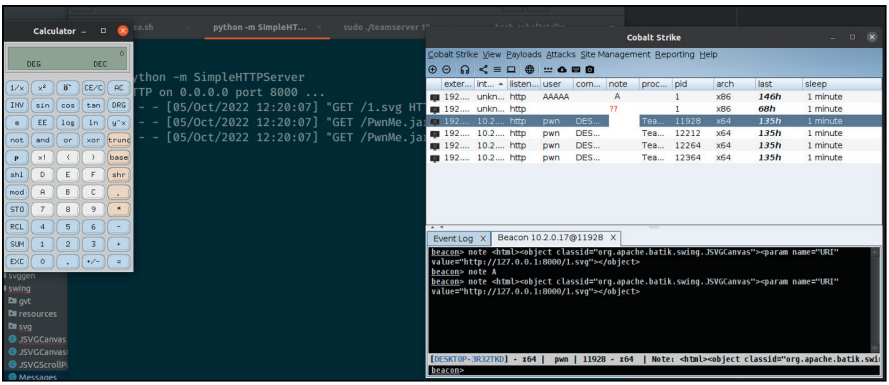


Figure 9. Successfully executed Cobalt-Strike

how IBM researchers successfully exploited the flaw and executed /usr/bin/xcalc.

Businesses can identify and stop the attempts to exploit RCE vulnerabilities through injection or buffer overflow attacks with Check Point firewalls that can significantly lower the danger they pose to the enterprise. Additionally, Check Point can assist organizations trying to fix an RCE vulnerability or already a victim of an RCE assault.

03/ Categories of Attacks Against RCDC Partners

Most of the attacks/campaigns in the course of the 4th quarter of 2022 were aimed at Ukraine and its infrastructure, which is not surprising as Russia is using all ways possible - including cyber - to achieve its goals.

Phishing campaigns keep affecting cyber infrastructure in Ukraine. CERT-UA discovered a mass mailing of phishing emails allegedly on behalf of the press service of the General Staff of the Armed Forces of Ukraine and the State Service for Special Communications and Information Protection of Ukraine. The emails contained malicious attachments and links that, when activated, infected the victim's computer and gave the attackers access to the data. There are also phishing campaigns aimed to compromise user accounts (stealing credentials, widespread phishing, attempts to dump hashes, accessing data, etc.) on email services and specific software (for example, military software Delta - situational awareness system).

There is also an increase in DDoS attacks not only on state institutions of Ukraine but also on its partners who provide assistance. When Members of the European Parliament designated Russia as a state sponsor of terrorism on November 23 the institutions official website was down for several hours due to a denial-of-service attack by pro-Kremlin hackers. In addition, due to the failures on the battlefield, defacement-type attacks are carried out against web pages of private organizations in Ukraine with a call to lay down arms and over throw the leadership.

In Georgia, the Cybersecurity Bureau (CSB) has recorded several of campaigns targeting their infrastructure:

- **FormBook Spear-phishing**
  A spear-phishing attack against the Ministry of Defense of Georgia and 6 of its critical information system entities was carried out by sending emails with a malicious attachment in an attempt to gain access to the target systems. In such attacks, the adversary attaches a file to the spear-phishing email and usually relies upon user execution to gain further access. Upon further analysis the CSB found that the final stage of the malware was the infamous Formbook infostealer.
- **Raspberry Robin worm**
  In October 2022, the Cybersecurity Bureau observed the Raspberry Robin worm, malware is installed via USB drive. The CSB took action to prevent malware execution tin its first stage.
- **BumbleBee campaign**
  In the BumbleBee campaign, the CSB sighted users being targeted with phishing emails, prompting them to download, extract and run an archive. They were provided with a password and an archive, which in the end resulted in unpacking an ISO file with malicious DLL and ultimately the bat file and launcher shortcut infecting the victim with the payload. No user was affected thanks to the mail security systems that were able to detect it as a malicious campaign in which emails were spread by utilizing hijacked threads.
- **DDoS attacks**
  On November 5 and 10 the Cybersecurity Bureau observed substantial amounts of DDoS on the website of the Ministry of Defence. Some services were down for approximately 5 minutes as a result of the first attack, however, the second one was successfully prevented and no services were affected.

04 /Cyber Activity in the Region: Chronological Order

2022

1. **October 10, DDoS attacks conducted by pro-Russian hackers took down websites of US airports.**
   Websites of numerous major airports in the United States were reportedly targeted by large distributed denial-of-service (DDoS) attacks, according to the pro-Russian hacktivist organization KillNet. Travelers were said to have been unable to log in and receive information about their booked flights or make airport service reservations because the servers hosting the sites were overloaded with spurious requests as a result of the DDoS attacks.

2. **October 11, Internet disruptions and cyberattacks hit Ukraine following Russian missile strikes.**
   Internet services and mobile communications were disrupted in Ukraine right after the Russian missile strikes caused widespread power outages. Cloudflare data shows that Internet availability in the country was 35% below the usual on Monday, October 11. The next day Ukraine was still experiencing Internet disruptions as Russia continued to attack the country's critical infrastructure, but most regions have restored connections, according to Cloudflare.

3. **October 14, the new Prestige ransomware campaign targeted Ukraine and Poland.**
   A coordinated ransomware campaign targeted the Ukrainian and Polish transportation and logistics sectors with a previously unknown payload. The company's Threat Intelligence Center said it tracked malware—which called itself "the Prestige ransomware" in the ransom note left on victim devices— deployed Tuesday in "attacks occurring within an hour of each other across all victims".

4. **October 15, a cyber-attack disrupted Bulgarian government websites over 'betrayal of Russia'.**
   Killnet, a pro-Russian activist group, took credit for a DDoS attack on Bulgaria's government organizations. On its Telegram channel, Killnet declared that it had targeted the websites of the Bulgarian Government, including those of the Defense Ministry, Interior Ministry, Justice Ministry, Constitutional Court, and the Office of the President.

5. **October 21, a cyber-attack on state organizations of Ukraine took place using RomCom malware.**
   CERT-UA, the Government's Computer Emergency Response Team of Ukraine, tracked down a campaign that was disseminating emails pretending to come from the Press Service of the General Staff of the Armed Forces of Ukraine and including a link to an unofficial web page where an alleged "order" could be downloaded.

6 **October 24, Killnet conducted yet another DDoS attack, this time targeting the Polish financial sector.**

The pro-Russian hacktivist group Killnet claimed responsibility for another DDoS attack against yet one more EU and NATO member state. Killnet announced on its Telegram channel that it had targeted the Polish financial sector, specifically, the following domains: 4bondnet.bondspot.pl, a Polish company that specializes in trading in treasury bonds and bills; Giełda Papierów Wartościowych w Warszawie SA(gpw.pl, the Warsaw Stock Exchange); 4brokernet.gpw.pl, an official member's portal for Giełda Papierów Wartościowych w Warszawie SA.

7 **October 26, Russian hackers targeted the Knesset website.**

A group of Kremlin-affiliated Russian hackers recently targeted the Knesset, Israeli Parliament's website, according to a Wednesday report. The website was brought down overnight, between Sunday and Monday, by a Russian group of hackers called Xaknet, briefly rendering the site unavailable for users in Israel and abroad, according to Channel 12 reporting.

8 **November 1, a phishing campaign targeted Ukraine's private sector.**

A phishing email targeting the Ukrainian private sector was detected. The email had an HTML attachment with a malicious LNK file leading to download a malicious *.rtf file. The email content stated "10/21/2022.rar""Regarding the execution of instructions on the use of the electronic document management system in wartime.lnk" and pointed to HTTP address https://hilr[.]ru/21.10/debate.rtf. The sender address was spoofed to look like it was coming from mail.gov.ua.

9 **November 7, Ukrainian hacktivists claimed to have leaked a trove of documents from Russia's Central Bank.**

Ukrainian hacktivists claimed to have breached the Central Bank of Russia, stealing thousands of internal documents. A 2.6 GB folder released publicly and partially reviewed by The Record contains 27,000 allegedly stolen files detailing the bank's operations, its security policies, and personal data of some of its current and former employees.

10 **November 8, the UAC-0010 group mounted a cyber-attack sending spoofed emails imitating the State Special Communications Service.**

A phishing email targeting the Ukrainian government sector was detected. The email included a link to hXXp://tzi.info-cip[.]org/07_11_2022.xhtml, an HTML file that contains JavaScript code which creates a RAR archive on the victim's computer, such as"08.11.2022.rar".

11 **November 11, the Ukrainian CERT detected and investigated a case Somnia malware use.**

The Computer Emergency Response Team of Ukraine (CERT-UA) took measures to in-

vestigate an information security incident that involved Somnia malware and violated integrity and availability of information. FRwL (aka Z-Team), whose activity is monitored by CERT-UA under identifier UAC-0118, took responsibility for the unauthorized intervention in target automated systems and computer equipment. An investigation found that the initial compromise occurred as a result of downloading and running a file containing Vidar malware that mimicked Advanced IP Scanner software.

12 **November 14, the pro-Russian hacktivist group Killnet carried out disruptive activities using Malware-as-a-Service model.**

New information was made public regarding Russian cyber operations in a Cyble Research Labs report which stated that data-destructive ransomware linked to the pro-Russian hacktivist group known as Killnet had been used to target Ukraine and its partners. The researchers posit that the new Killnet ransomware is a rebrand of the infamous Chaos Ransomware, a Malware-as-a-Service (MaaS) program advertised on the top-tier Russian-language forum XSS before a cracked version was published on Telegram by the Arvin Club ransomware gang on or around May 2, 2022.

13 **November 23, the European Parliament faced a cyberattack from a pro-Russian group after the declaration on support to terrorism.**

The official website of the European Parliament was down for about an hour as a result of a distributed denial-of-service (DDoS) attack mounted by a pro-Russian hacking group. The attack came just hours after the European Parliament designated Russia a state sponsor of terrorism. The declaration argued that Russia's attacks on the Ukrainian infrastructure, schools, and hospitals violated international law.

14 **November 28, RansomBoggs Attacks linked to Russian hackers took place against Ukraine.**

According to ESET experts, multiple Ukrainian businesses' networks were targeted by a brand-new malware named RansomBoggs. Based on similarities with earlier operations carried out by the same group, researchers linked the RansomBoggs attacks to the Sandworm APT actor.

15 **December 4, a newly discovered wiper CryWiper posed as ransomware while targeting Russian entities.**

CryWiper, a previously unidentified data wiper was discovered by researchers as it targeted Russian mayors' offices and courts in a series of destructive attacks. The malware poses as ransomware but analysis of the code shows that it destroys data in the compromised system rather than encrypting it.

16 **December 8, Cyber-attacks were held against government organizations exploiting the theme of the Iranian Shahed-136 kamikaze drones and deploying DolphinCape malware.**

The Government Computer Emergency Response Team of Ukraine CERT-UA was informed by specialists of the cyber security unit of JSC Ukrzaliznytsia about distribution of emails with the subject line saying "How to recognize a kamikaze drone." The email

attachments contained malicious files used for spying on the target, list and exfiltrate files, and create and exfiltrate screenshots.

17 **December 12, DolphinCape malware allegedly targeted the Ukrainian Railways and other government agencies.**

Ukraine's Computer Emergency Response Team (CERT-UA) disclosed announced that the state railway and various government agencies in the country were targeted by a wave of phishing attacks.

18 **December 16, cyberattacks targeted Ukrainian government entities using a Trojanized Windows 10 installer.**

Several government organizations in Ukraine were compromised by trojanized installer files for Windows 10. The files were used to carry out post-exploitation operations. The malicious ISO files were distributed via Ukrainian and Russian-language Torrent websites.

19 **December 17, a cyber-attack targeted DELTA system users with FateGrab/StealDeal malware.**

The Government Computer Emergency Response Team of Ukraine CERT-UA received information from the Center for Innovations and Development of Defense Technologies of the Ministry of Defense of Ukraine regarding distribution of malicious e-mails and messenger messages calling to update certificates in the DELTA system.

20 **December 21, the Russian Killnet hackers claim FBI data theft.**

Killnet published a text file on Telegram that contained login information of 10,000 people claiming them to be FBI agents. Like in most of their attacks, the pro-Kremlin gang also appeared to be driven by political motivations in this alleged strike.

05/ Recommendations

Planning of cybersecurity defenses and mitigation techniques draws considerable benefits from awareness of trends of threat actors, their objectives, and their targets. It is a crucial component of the overall threat assessment because it enables prioritization of security measures and development of a focused strategy based on the potential consequences and the likelihood that the threats will occur. Lack of awareness in terms of threat actors and the results of their method is a severe knowledge gap in cybersecurity since analyzing threats without considering the motivations and objectives may result in ineffective defenses or, in certain situations, the inability to protect at all.

Establishment of in-depth defence should be considered when developing a cybersecurity plan to ensure that management of the current evolving threats and dangers is efficient. That means stacking security instruments. Education is another essential part of maintaining company safety. Employees will know what to watch out for if they are informed about sensitive information security.

The most recent technology is required for today's workforce regarding threat monitoring and emergency communication. Next level organizational resilience can be reached by using cutting-edge emergency communication systems with integrated threat intelligence.

Unfortunately, there is no cyber security plan or defence strategy that can protect an organization or a business completely. So it is vital to have a business continuity and disaster recovery strategy. Business continuity is an organization's ability to maintain essential functions during and after a disaster has occurred. Business continuity planning is important because it establishes risk management processes and procedures that aim to prevent interruptions of mission-critical services and to re-establish the full function of the organization as quickly and smoothly as possible.

Taking care to become ready as described also helps companies to identify the essential functions and allocate the available budget accordingly. The plan should enable the organization to maintain at least the minimal level of operation in the course of a crisis.

1. Empower your team. As more employees are working remotely, companies need to ensure that their workforce can fully leverage the tools available to them. Companies still relying on traditional training methods should integrate modern training practices that create engaging training experiences and thus ensure the employees can be engaged as much as possible when working in a remote scenario.

2. Educate and train your regular and mission-critical staff. One of the most dangerous cyber offenses is a phishing campaign. To mitigate against it, a common and effective training system needs to be incorporated into the organization's strategy. Cyber Hygiene courses and regular refreshers can prevent a disaster as adequately trained personnel know how to quickly react and respond during an attack or disaster.

3. Enhance your reporting. Analytics are critical during a disruption of operations. Data obtained by analyzing different types of incidents can help predict what might happen during a business interruption. It can help to identify an organization's vulnerabilities and propose solutions that allow you to closely monitor daily changes in productivity and absenteeism, improve the well-being of your organization and employees, identify business scenarios and the data needed to monitor and manage the impact on areas of business (e.g. supply chain, production, finance, HR, IT), as well as develop core KPIs (Key Performance Indicators) and design organizational impact dashboards to enable business impact measuring and tracking.

4. Keep communication constant. Your workforce will look for your guidance during these times. Keeping open and transparent communication, addressing their concerns, and regularly so, will help to keep them engaged and maintain business continuity.

5. Automate as much as possible. As more employees are working from home, companies trying to drive operational costs down and maintain service levels should turn to robotics and automation. As we know, RPA (Robotic Process Automation) technologies can take care of repetitive, rule-based tasks through software robots. By turning to robotics and automation, companies can redeploy their workforce into activities that are more critical and add more value to their clients, while the robots take care of simpler tasks. On top of that, RPA technologies are not costly, can deliver significant improvements in a short period of time, and are fairly easy to deploy.

6. Provide the necessary tools. Companies need to ensure that they provide the proper software and have a solid infrastructure to support a seamless and secure transition to a fully remote work model. To do this, companies might need to quickly acquire new software (secure video conferencing, collaboration, digital adoption solutions, and document-sharing tools) or scale their technology capabilities (additional bandwidth and network capacity).

06/ Endnote

It is now rather bold to say that, unfortunately, the last quarter of 2022 ends on the same note as the first quarter started - Ukraine. Throughout the year, Ukraine showed not only to the world but also to themselves that it was possible not only to defend but to fight – and fight back successfully. The Ukrainian cyber army was stood out as an amazing proof of how you can recruit any person to form one fist and cripple the Kremlin's systems. It is safe to predict that 2023 will be still a challenging year nevertheless, but the primary factor in this warfare is to learn from the mistakes you make. Cyber operations adjust to new challenges and innovations brought by Russia's war against Ukraine quickly. Ukraine has showed its strong side by defending itself from various threats quickly. Awareness is the main component in today's cyber field where everyone can be targeted: even the most minor organizations or random people. Financial returns of even a little investment in cybersecurity awareness training are beneficial. The most successful security education initiatives put people first. Increasing participation, training relevance, and eventually, a long-lasting behavior change, enhance cooperation.

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