2nd QUARTER REPORT 2023

2nd QUARTER REPORT 2023

1 April - 30 June

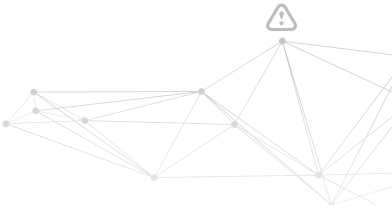
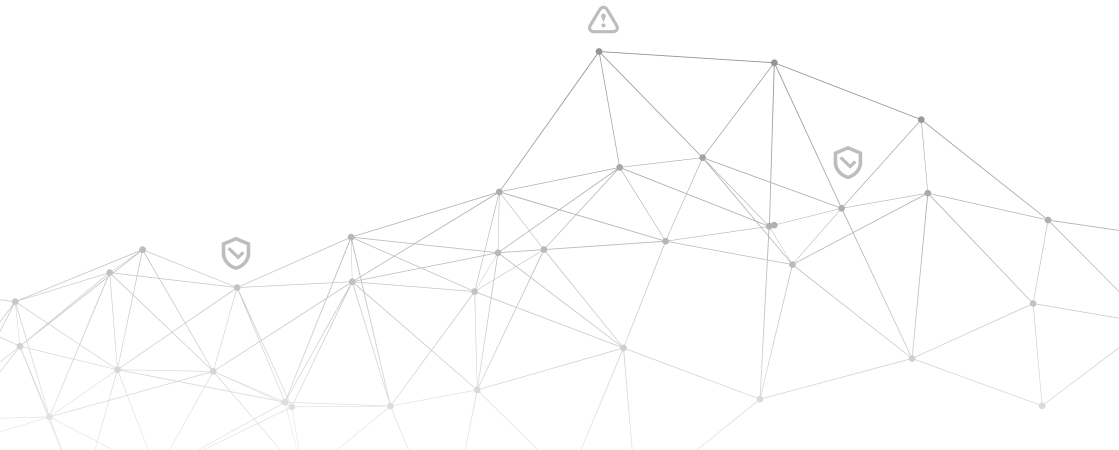


Table of Contents



Executive Summary

The second quarter of 2023 saw a dynamic and challenging cybersecurity landscape marked by emerging threats, significant breaches, and increasing regulatory and compliance requirements. The threat landscape continued to evolve rapidly, with threat actors demonstrating increased sophistication and agility. Ransomware attacks remained a significant concern, targeting both large enterprises and small to medium-sized businesses across various sectors. Advanced persistent threats (APTs) also gained prominence, exploiting zero-day vulnerabilities and leveraging social engineering techniques to infiltrate organizations. This Report provides an overview of the key cybersecurity trends and events that occurred during this period, outlining the significant challenges faced by organizations and highlighting the recommended strategies for risk mitigation.

01/Regional Cyber Threat Landscape

The second quarter of 2023 witnessed a complex regional cyber threat landscape with distinct challenges and trends across different parts of the world. Ransomware attacks, supply chain compromises, and nation-state activities were common themes, underscoring the need for enhanced cybersecurity measures, robust incident response capabilities, and international collaboration. As cyber threats evolve, stakeholders must remain vigilant and proactive in mitigating risks to ensure a secure digital environment for individuals, businesses, and governments.

1.1/CVE-2023-34362: CL0P Ransomware Exploits MOVEit Transfer SQLi Vulnerability

Beginning May 27, 2023, the CL0P Ransomware Gang, also known as TA505, started exploiting a previously unutilised SQL injection flaw (CVE-2023-34362) in MOVEit Transfer, Progress Software's managed file transfer (MFT) technology. A web shell called LEMURLOOT was used to infect publicly accessible MOVEit Transfer web apps and steal data from the underlying MOVEit Transfer databases. A similar surge of activity was launched by TA505 in early 2023 targeting Fortra/Linoma GoAnywhere MFT servers and Accellion File Transfer Appliance (FTA) devices in the form of zero-day exploit-driven attacks. Large-scale spear-phishing efforts that employed validated and digitally signed malware to get past system defenses, exploited CL0P as Ransomware as a Service (RaaS). Previously, CL0P became notorious for adopting a "double extortion" strategy for stealing and encrypting victim data, refusing to provide victim access back, and posting exfiltrated material on Tor via the CL0P_-LEAKS website. The CL0P's toolbox includes a variety of viruses for gathering information, among which are the following:

- To facilitate the download of new malware components [T1071], [T1105], the FlawedAmmyy/FlawedGrace Remote Access Trojan (RAT) gathers data and initiates interaction with the Command and Control (C2) server.
- SDBot RAT spreads the infection [T1105] by taking advantage of flaws and dropping copies of itself in network shares and portable drives. It can also spread when exchanged over peer-to-peer (P2P) networks.

- Truebot is a first-stage downloader module created and credited to the Silence hacking collective that can record screenshots and gather system data [T1113]. After connecting to C2 infrastructure, Truebot may be directed to load shell code [T1055] or DLLs [T1574.002], download further modules [T1129], execute those modules, or erase itself [T1070].
- After acquiring access to the Active Directory (AD) server, Cobalt Strike is used to increase network access [T1018].
- Data from the infected device is stolen via DEWMODE, a web shell written in PHP that targets Accellion FTA devices and communicates with the underlying MySQL database [1505.003].
- LEMURLOOT is a C# web shell made specifically for the MOVEit Transfer platform.

File transfer activities in different organisations are often managed using MOVEit which offers a web application that supports MySQL, Microsoft SQL Server, and Azure SQL database engines. The MOVEit Transfer web apps [T1190] were compromised in May 2023 by the CL0P ransomware gang which installed a web shell called LEMURLOOT using the SQL injection zero-day vulnerability CVE-2023-34362. To pass for a genuine human.aspx file that is a component of the MOVEit Transfer program, the web shell was first noticed under the name human2.aspx. When installed, the web shell generates a random 36-character password that may be used for authentication. The X-siLock-Comment header field, which must be provided a value equal to the password created upon the installation of the web shell, is used by the web shell to communicate with its operators. The web shell watches for HTTP requests containing this header field. Operators send instructions to the web shell after authenticating with it that can:

- Enumerate the underlying SQL databases and retrieve Microsoft Azure system parameters.
- Save a string supplied by the operator, then retrieve a file from the MOVEit Transfer system with a name that matches the string.
- Create a brand-new administrator account with Administrator privileges and the LoginName and RealName values set to “Health Check Service.” The username is most likely selected at random.
- Delete a user account whose RealName and LoginName values are both ‘Health Check Service.’

1.2/New Campaigns of Killnet with Other Hacktivist Groups

After Russia invaded Ukraine in 2022, many hacktivist groups emerged and started to back one side or the other. One of the most notorious groups, Killnet, conducted many campaigns, though limited to DDoS, they had an impact on various infrastructure objects in numerous countries around the world. After many successful attacks, Killnet slowed down and narrowed down to disinformation campaigns. It seemed as if the group was slowly fizzling out when their leader "Killmilk" announced he was leaving the group, but they came back with a new wave of campaigns in thecourse of 2023, especially Q2.

On May 9, 2023, KillNet's founder and de facto leader KillMilk, aka Killmilk, refered to the entire plan as a "mistake" on the t.me/killnet_reservs Telegram channel. Killmilk wrote another post on May 18, 2023, announcing that KillNet "goes global." On May 24, 2023, the actor asserted that the KillNet organization was terminated. He claimed that the organization consisted of 50 factions with a total of 1,250 members, but because their primary focus was not hacktivism, KillMilk chose to operate independently. On June 12, 2023, the actor asserted that KillNet's staff changed.On June 14, the actor KillMilk reposted a video and a news report on the @killmilk_rus Telegram channel of the recently dormant REvil ransomware gang, KillNet, and Anonymous Sudan hack-

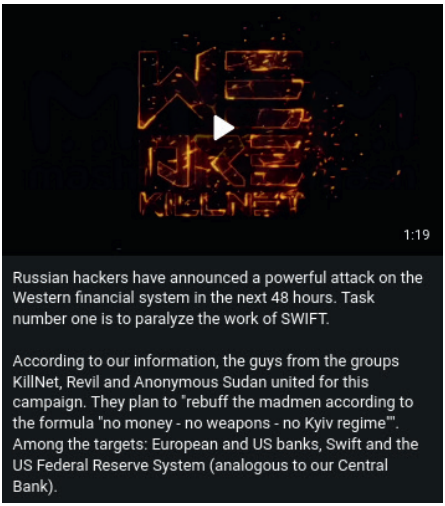


Figure 1. / Telegram message regarding attack on Western financial systems

tivist groups announcing a planned significant attack on the European banking system within the following 48 hours. A distributed denial-of-service (DDoS) attack, according to the KillNet representative, would not be used in the campaign. Although the claims were absent from the original video, the reposted piece of news stated that "the European and American banks, SWIFT, and the U.S. Federal Reserve System" were the main targets. During the indicated 48-hour gap, the groups were silent, did not boast about their "attack on the Western financial system" and, to our knowledge, no systems were affected. But on June 16, 72 hours after the original video was shared, Killnet came back with a message and announced that they, together with other groups from Russia and Sudan, impose sanctions against "the European banking transfer systems SEPA, IBAN, WIRE, SWIFT, WISE". They did not specify what the sanctions would entail. On June 18, Killnet shared another message regarding the campaign against the banking sector: "Tomorrow is a working banking day, which means the beginning of the great work!". According to the group, the destructive campaign was going to start with attacks against the European banking sector, more specifically, the European Investment Bank (EIB). Later, on June 19, Killnet posted an image of what seemed to be an irresponsive EIB web page. On the same day, EIB posted an update on their Twitter page saying, "We are currently facing a cyber attack which affects the availability of http://eib.org and http://eif.org. We are responding to the incident." Despite claiming that they would not be conducting DDoS before the attack, it seems that that is exactly what the group employed, as the attack had no long-term impact. Damage was repaired already next day and the web page of EIB has been up and running.

Figure 2. / Image of allegedly not responding EIB webpage

As of the completion of this Report, no further attacks had conducted and the Killnet group seems to have switched their focus to Ukraine, even if for a short period of time. It is tough to assess the credibility of the claimed attacks because members of the group typically post screenshots of check-host.net or just plain text with claims about successful attacks as proof. That said, Killnet and the groups working in coordination with them have proven in the past that they are capable of conducting massive DDoS attacks and so their claims should be taken both seriously and with a grain of salt.

02/Categories of Attacks Against RCDC Partners

Lithuania:

Most cyber events that took place in Lithuania in the second quarter of 2023, were DDoS attacks from Russian hacking groups, such as KillNet and NoName057(06). Their main focus was disruption of work in the public and private sectors. CTAC analysts witnessed that most of the time when the Russians used DDoS attacks against Lithuania, there was political activity between Ukraine and Lithuania regarding the Russia-Ukraine war. Whether Lithuania was involved in donating military hardware or cash to Ukraine, it was always done with a cautious eye upon Russia. The most notorious cyber events took place on May 30, when NoName057(16) started their DDoS venture against Lithuanian companies.

United States of America:

In the second quarter of 2023, the United States saw increased cyber activities from Dragon Breath APT, Lazarus Subgroup, and Iranian hackers. As we indicated in the previous Quarterly Report, ChatGPT is on the rise and US researchers disclosed a campaign distributing a malicious fake ChatGPT browser extension. The campaign advertised quick access to ChatGPT functionality but was found to be hijacking Facebook accounts and installing hidden account backdoors instead. Particularly noticeable was the use of a malevolent, silently forced Facebook app "backdoor" that gives threat actors super-admin permissions. The campaign also used a sophisticated worm-like approach to propagation. Although it was not the only backdoor, it became known when Iranian hackers started deploying an updated version of a Windows backdoor called PowerLess. In the

overall, many campaigns deliver malware through phishing emails, which shows that threat actors do not change their tactics much, therefore it is essential to educate employees and minimize the risk of potential compromise through phishing campaigns, which are becoming even more popular as Phishing-as-a-Service is on the rise.

Ukraine:

The initial efforts of Russian cyber threat actors (APT28, Sandworm, Gamaredon, Ghostwriter, Killnet, etc.) against Ukraine in June 2023 were primarily focused on conducting cyber reconnaissance. Destructive attacks against the information and telecommunication infrastructure of Ukrainian organizations and institutions were mostly carried out by hacker groups affiliated with the intelligence agency of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation.

In the context of the ongoing counteroffensive of the Armed Forces of Ukraine, information and communication systems of the Armed Forces, the Security Service of Ukraine (including its intelligence capabilities), Ukrainian telecommunications service providers and the media remain Russian cyber threat actors' priority cyber attack targets. Military personnel of the Armed Forces of Ukraine who have access to military situational awareness systems and internal document management systems continues to be a particular interest of the Russian hackers as well.

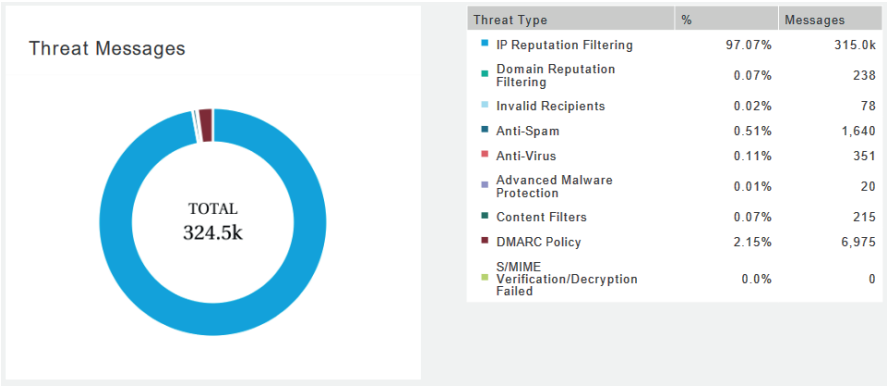
Phishing remains the primary initial access tool in targeting automated systems. However, certain Russian groups, such as APT28, have attempted to exploit the existing software vulnerabilities in email services (CVE-2020-35730, CVE-2020-12641, and CVE-2021-44026) used by the Ukrainian Government and private institutions. During phishing campaigns, compromised accounts of security and defense sector organizations (companies) employees continue to be actively exploited.

The activities of pro-Russian hacktivists, including those targeting Ukraine, were predominantly aimed at establishing their presence in the information space of the Russian Federation and European countries. DDoS attacks remains to be the main form of cyber aggression for most pro-Russian hacktivist groups (KillNet, NoName57(16), Anonymous Sudan, etc.). Certain hacktivist groups or individual members with a highly probably engaged by Russian special services to carry out cyber attacks against Ukrainian military command structures.

There have been attempts by certain pro-Russian hacktivist groups (KillNet, Anonymous Sudan) to seek support from Turkish hacker groups (Devils Sec, TurkHackTeam) in conducting cyber attacks against Ukraine and Israel. However, the likelihood of their success in it is low at the moment.

Georgia:

In the 2nd quarter, there was no significant cyber activity as far as Georgia is concerned. Due to its officially neutral posture, Georgia remains in the radar of main Russian hacker groups or hacktivists. Statistical data of the 2nd quarter indicates that the Georgian governmental sector was subjected to regular scanning and phishing attempts. However, these were not specifically targeted and can be considered as background noise.



Threat Type	%	Messages
IP Reputation Filtering	97.07%	315.0k
Domain Reputation Filtering	0.07%	238
Invalid Recipients	0.02%	78
Anti-Spam	0.51%	1,640
Anti-Virus	0.11%	351
Advanced Malware Protection	0.01%	20
Content Filters	0.07%	215
DMARC Policy	2.15%	6,975
S/MIME Verification/Decryption Failed	0.0%	0

Figure 3. / Activity of cyber attacks in Georgia

Poland:

On April 18, 2023, CSIRT of the Ministry of National Defense (CSIRT MON) observed a wide disinformation campaign distributing information about a potential recruitment to the Great Hetman Konstanty Ostrogski Lithuanian-Polish-Ukrainian Brigade. Analysis:
SMS and Telegram messages with the infomration were sent to many citizens of the Republic of Poland. In addition, the false information was also sent via e-mail, for which purpose the adversary used a newly registered mon-gov[.]com domain.
Example sender addresses:

- info@mon-gov[.]com
- informacja@mon-gov[.]com
- infolinia@mon-gov[.]com
- kontakt@mon-gov[.]com

Based on the characteristics of the mon-gov[.]com domains registered by the attacker, CSIRT MON analysts identified additional newly registered domains highly likely to be used in the same operation.

- gov-mon[.]com
- government-mon[.]com
- mon-government[.]com

The operation in question bears the hallmarks of being based on previously prepared information. The incident in question corresponded to the propaganda operation carried out for several dozen hours - suggesting the participation of the brigade (LITPOLUKRBRIG) in military operations on the territory of Ukraine. The process of shaping the information background was orchestrated by subjects permanently involved in Russian disinformation operations. This is yet another incident in which the adversary combines operations in the information and psychological domain with technical activities to carry out the assigned tasks. CSIRT MON team indicates that the threat posed by the incident in question is not of a short-term nature and the operation can be continued.

In March 2023, another disinformation campaign of sending e-mails was carried agaisnt Polish citizens targeting them with disinformation about potential terrorist attacks in Poland. Messages were sent from mailboxes in domains whose structure suggests an attempt to impersonate the Police:

- p0licja[.]eu
- policja-pl[.]info
- p0licja[.]info
- p0licja[.]pw
- policja.in[.]net
- policja[.]pw
- policja-pl[.]com
- p0licja-pl[.]info
- p0licja[.]com
- poli-cja[.]com
- policia[.]pw

CSIRT MON Assessment

CSIRT MON analysts indicate that the described disinformation operations were highly probably carried out by the Belarusian UNC1151 group. Based on several years of constant observation of the activity of UNC1151, CSIRT of the Ministry of National Defense made a quick attribution because of the use of TTPs, which fits into the modus operandi of the said adversary. It is a continuation of the Ghostwriter disinformation campaign.

The Ghostwriter disinformation campaign run by the UNC1151 group aims to:

- Undermine Poland's bilateral relations with the US and other NATO Allies;
- Disrupt the Polish-Ukrainian relations;
- Discredit the aid provided to Ukraine by Poland and other NATO Allies;
- Create conditions for social unrest among the Polish citizens;
- Obtain information for intelligence purposes, including information and psychological operations;
- Support the Russian-Belarusian information operations against NATO.

In addition, it should be kept in mind that the UNC1151 group conducts disinformation campaigns, and constantly conducts phishing campaigns involving e-mail login credential theft. The concrete adversary also compromises websites and conducts campaigns aimed at distributing malware. In 2023, CSIRT of the Ministry of National Defense identified two attempts to deliver malware from the UNC1151 group to entities supervised by the Minister of National Defence.

Since the Russian invasion of Ukraine, CSIRT MON of Poland has been observing a significant increase in UNC1151 activity against Poland and Ukraine.

03/Cyber Activity in the Region: Chronological Order

2023

1. **April 3, Winter Vivern launch attacks against government entities in Europe.**
The recent wave of assaults on European governments was attributed to a lesser-known Russian hacking organization, Winter Vivern. Since February, a campaign has been up and running attempting to steal emails and other sensitive data from NATO officials, governments, military personnel, and diplomats involved in the Russia-Ukraine war. Their strategy uses unpatched Zimbra endpoints. Proofpoint has discovered that the Winter Vivern APT group (TA473) targets webmail accounts of NATO-aligned governments in Europe by taking advantage of a cross-site scripting vulnerability (CVE-2022-27926) in Zimbra Collaboration Suite.

2. **April 3, Use of unlicensed Microsoft Office programs as vector of primary ICS compromise.**
The Computer Emergency Response Team of Ukraine (CERT-UA) published results of an investigation into yet another cyberattack on a government infrastructure facility. CERT-UA found out that the initial compromise took place using unlicensed Microsoft Office 2019 software. This software was downloaded on a computer as a BitTorrent file from hxxps://toloka[.]to/t661196.

3 **April 5, Ukraine targeted by another DDoS attack.**
Several Ukrainian governmental institutions experienced a DDoS attack with minimal harm. The arising damage was minitigated with standard anti-DDoS techniques, like geolocation blocking, and content delivery network (CDN) services. This attack is suspected to have originated from a Russian Federation APT.

4 **April 10, Pro-Russian hacktivist group claims access to Ukraine's troop movement data.**
According to a hacktivist collective working with Russia, it compromised the Ukrainian battlefield management system (BMS) DELTA. The Donetsk People's Republic is the name of the separatist organization in eastern Ukraine that calls itself Joker DPR, in the group's own words, its goal is to "destroy the clowns" running the country's government. It also asserted that it had real-time access to DELTA, the Ukrainian military's battlefield management system (BMS), in November, which seems to support the agenda.

5 **April 11, Malware disguised as document from Ukraine's Energoatom delivers Havoc Demon backdoor.**
A faked document with malicious load posing as sent by Energoatom, a state-owned firm in Ukraine that manages its nuclear power reactors, was discovered by FortiGuard Labs. "Zatverdzhenniy spisok osib na otrim", which roughly translates as "Authorized list of individuals to receive" in Ukrainian, is the name of the macro-enabled document. A file with the same name is sent inside an ISO image archive.

6 **April 11, Russian hackers target security cameras inside Ukraine's coffee shops.**
The Guardian published an article "Russian Hackers target security cameras inside Ukraine coffee shops". Russian hacking groups reportedly have access to surveillance cameras in different establishments and stores. The compromised cameras enable surveillance of public roads: constant monitoring of sections of roads allow the hackers to collect intelligence on military equipment and humanitarian aid movement.

7 **April 19, Disinformation operation against RP underway, UNC1151 misinforms about recruitment to LitPolUkrBrig.**
The Computer Security Incident Response Team of the Polish Ministry of Defense (CSIRT MON) published a report on a new cyber attack. The cyberattack has been linked to a Belarusian hacking group known as Ghostwriter. As part of the campaign, the hackers (also refered to as UNC1151 by cybersecurity experts) sent fake messages to Polish citizens about potential recruitment to the Lithuanian-Polish-Ukrainian Brigade, a multinational military unit for peacekeeping and humanitarian operations. The hackers falsely claimed that the Brigade would participate in Ukraine's military operations.

8 **April 24, Russian hackers use Tomiris to target Central Asia in intelligence gathering.**
New research from Kaspersky showed that a Russian-speaking threat actor, Tomiris, is focused on gathering intelligence in Central Asia. Tomiris initially came to light in September 2021 when Kaspersky pointed out its possible ties to Nobelium, the Russian nation-state

9 group responsible for the SolarWinds supply chain assault (also known as APT29, Cozy Bear, or Midnight Blizzard). The criminal group has used a "polyglot toolset" of low-tech "burner" implants to launch repeated spear-phishing operations against the same targets.

10 **April 28, APT28 phishing campaign targets the Ukrainian government.**
The Ukraine Computer Emergency Response Team (CERT-UA) warned of a phishing attack by APT28 (Fancy Bear) intended to target the Ukrainian Government. To trick victims into interaction with the malicious Windows Update, APT28 pretended to be system administrators of Ukrainian government organizations. APT28 targeted victims with emails that contained malicious Windows update phish lures using fictitious outlook[.]com email accounts forged using names of actual Ukrainian Government personnel.

11 **April 29, Russian hackers use WinRAR to wipe Ukrainisn state agency's data.**
The Computer Emergency Response Team of Ukraine (CERT-UA) published an article about an attack using WinRar against government resources. Machines with installed Windows OS were attacked by RoarBat, a BAT script that recursively searches for files (on disks and in specific directories) according to a defined list of extensions (.doc, .docx, .rtf, .txt, .xls, .xlsx , .ppt, .pptx, .vsd, .vsdx, .pdf, .png, .jpeg, .jpg, .zip, .rar, .7z, .mp4, .sql, .php, .vbk, .vib, . vrb, .p7s and .sys, .dll, .exe, .bin, .dat) for their further archiving with WinRAR program with "-df" option which provides for deletion of the source file, as well as subsequent deletion of the created archives.

12 **May 2, Polish healthcare industry targeted by Vidar Infostealer likely linked to Djvu ransomware.**
Researchers from EclecticIQ detected a spearphishing email sent to Poland's healthcare sector. A malicious Microsoft Excel XLL attachment in the counterfeit email that claimed to be received from a Polish Government organization downloads and runs the Vidar infostealer virus. Vidar can gather private data from compromised devices and launch ransomware, putting the Polish healthcare sector in danger of losing crucial data and experiencing system interruption.

13 **May 17, APT28 leverage multiple phishing techniques to target Ukrainian civil society.**
The Russian GRU-affiliated APT28 intrusion suite, also known as Sofacy, PawnStorm, and Fancy Bear, is notorious for its cyberespionage and sabotage efforts and has been seen utilizing a variety of phishing methods to target the Ukrainian civil society. Their methods include compromising Ubiquiti routers to obtain victims' credentials and exploiting HTTP webhook services, like Pipedream and Webhook. In one case, APT28 was observed displaying a phony login page to a victim that was meant to decode a document using the "Browser in the Browser" approach.

14 **May 20, Mustang Panda hijack TP-Link routers of European foreign affairs entities.**
TP-Link routers fell victim to many targeted assaults believed to had been carried out by the Chinese state-sponsored APT organization Mustang Panda. Aimed at organizations involved

in European foreign affairs, the campaign has been running since January. A proprietary backdoor called Horse Shell and numerous other malicious components are included in the implants, thus allowing attackers to maintain permanent access, create anonymous infrastructure, and move laterally through infected networks.

15 **May 23, A spying campaign targets Ukraine, Israel, India, and Kazakhstan.** Ukraine's CERT-UA identified a cyber-espionage campaign targeting an undisclosed government agency in Ukraine. A threat actor identified by researchers as UAC-0063 "has also shown interest" in targeting Mongolia, Kazakhstan, Kyrgyzstan, Israel, and India. Researchers initially detected activity associated with UAC-0063 in 2021, but the group's origins remain unclear. The goal of its attacks, according to CERT-UA, is gathering intelligence.

16 **May 29, Threat actors continue targeting Ukrainian infrastructure with SmokeLoader.** The Government Computer Emergency Response Team of Ukraine CERT-UA detected another SmokeLoader distribution campaign. Legitimate compromised mailboxes were used to send e-mails, and SmokeLoader malware is delivered to computers within several ways. Over that time, probably due to the attackers' mistake, one of the VHDX files, the executable file "Declaration fraudulent operation SIRION.scr", which is the Cobalt Strike Beacon malware, was detected.

17 **May 29, Lithuania witnesses DDoS attacks in both government and private sectors.** At around 11:30, the Russian hacker group NoName057(16) DDoS'ed the Lithuanian Government's website www.lrs.lt rendering it not reachable (the issue was subsequently fixed by the IT department). At around 13:40, Litgrid (www.litgrid.eu), Lithuania's electricity transmission operator's website went down. At 14:50 a Lithuanian agricultural company, Linas Agro fell victim next. The website web server was fixed quickly after the attacks and operational since. Other victims of the NoName057(16) hacking group in the same surge of attacks were Kauno Energija AB and the Lithuanian Riflemen's Union.

18 **On May 30, Another DDoS attack against various Lithuanian infrastructure.** Lithuanian charter airlines GetJet, Heston Airlines, KlasJet, City Service utility company, Achema and Achemos Grupė manufacturer were slammed by DDoS attacks. Website of the Lithuanian copmany Akropolis Group which engages in building and renting of retail and entertainment complexes, business centers and real estate projects in Lithuania and Latvia, was disrupted and went down. Further, the sizeable Baltic news agency Baltic News Service (BNS) took a hit. DDoS attacks also targeted authorization portal of the Lithuanian airline and the website of the Lithuanian airline Avion Express.

19 **On May 31, Last DDoS attack of May's campaign against Lithuania.** At around 12:20, an attack hit the website of the Lithuanian automotive logistics company Freight. Another attack slammed PST - Panevėžys Construction Trust at 13:30. was another attack for. SBA Group furniture and clothing producer and real estate and investment management copmany took a hit At 14:45.

20 **June 19, Cyberattacks UAC-0036 against UKR.NET service users.**
CERT-UA published information about an ongoing campaign in which emails are sent ostensibly on behalf of UKR.NET technical support with "Suspicious activity observed @UKR.NET" written in the subject line and an attachment "Security warning.pdf". The PDF contained a link to a fraudulent website which imitated an email service webpage.

21 **June 20, Russian APT28 hackers breach Ukrainian Government's email servers.**
Multiple Ukrainian institutions, including government agencies, had their Roundcube email servers compromised by a threat group known as APT28 which is connected to Russia's General Staff Main Intelligence Directorate (GRU). The cyber-espionage group behind the attacks, also known as BlueDelta, Fancy Bear, Sednit, and Sofacy, used information about the ongoing conflict between Russia and Ukraine to dupe recipients into opening malicious emails that would compromise unpatched servers by utilizing Roundcube Webmail vulnerabilities.

22 **June 30, Pro-Russian hackers upgrade DDoSia bot to attack Ukraine and NATO Allies.**
The NoName057(16) group and its followers are actively deploying the tool against government agencies, media, and private companies in Lithuania, Ukraine, Poland, Italy, and other European countries. "This likely stems from the fact that those countries are the most vocal in public declarations against Russia and pro-Ukraine, as well as providing military support and capabilities," the researchers said. Sekoia detected a total of 486 different websites impacted by DDoSia attacks.

03/Recommendations

Given the global nature of cyber threats, international collaboration is essential for combating cybercrime effectively. Organizations should participate in information-sharing initiatives and collaborate with industry peers, government agencies, and cybersecurity organizations at regional and international levels. Sharing threat intelligence and best practices can help identify emerging threats and develop more effective defense strategies. Organizations should prioritize regular software patching and updates to address known vulnerabilities. The exploitation of vulnerabilities, as seen in the case of CVE-2023-34362, can lead to severe consequences. Implementation of a robust patch management process helps to minimize the risk of exploitation by threat actors. Private organizations should establish collaborative relationships with government agencies responsible for cybersecurity. Sharing information and participating in public-private partnerships can enhance overall cybersecurity resilience, enable faster response to emerging threats, and promote a safer digital ecosystem.

04/Endnote

In conclusion, the second quarter of 2023 presented a challenging regional cyber threat landscape characterized by ransomware attacks, supply chain compromises, and nation-state activities. The CL0P Ransomware Gang exploited a SQL injection flaw in MOVEit Transfer, highlighting the importance of secure file transfer practices. The Killnet hacktivist group resurfaced with disinformation and DDoS campaigns, targeting various infrastructure objects worldwide. The United States experienced cyber activities from Dragon Breath APT, Lazarus Subgroup, and Iranian hackers, emphasizing the need for increased vigilance against phishing campaigns. Ukraine faced cyber reconnaissance by Russian threat actors, with phishing and software vulnerabilities as primary entry points. Pro-Russian hacktivist groups conducted DDoS attacks, while attempts to involve Turkish hacker groups were observed. Poland witnessed disinformation campaigns orchestrated by the UNC1151 group, aiming to undermine bilateral relations and create social unrest. The latest developments underscore the importance of enhanced cybersecurity measures, robust incident response capabilities, and international collaboration to ensure a secure digital environment.

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