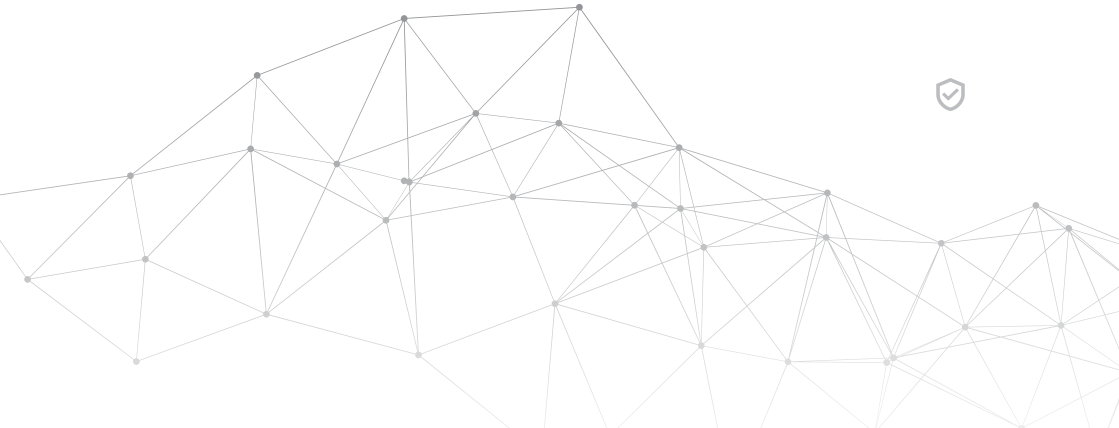
REGIONAL CYBER DEFENCE CENTRE

2022 1st QUARTER REPORT



2022 1st QUARTER REPORT

1 January - 31 March

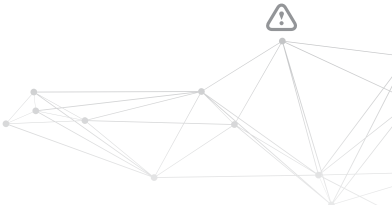
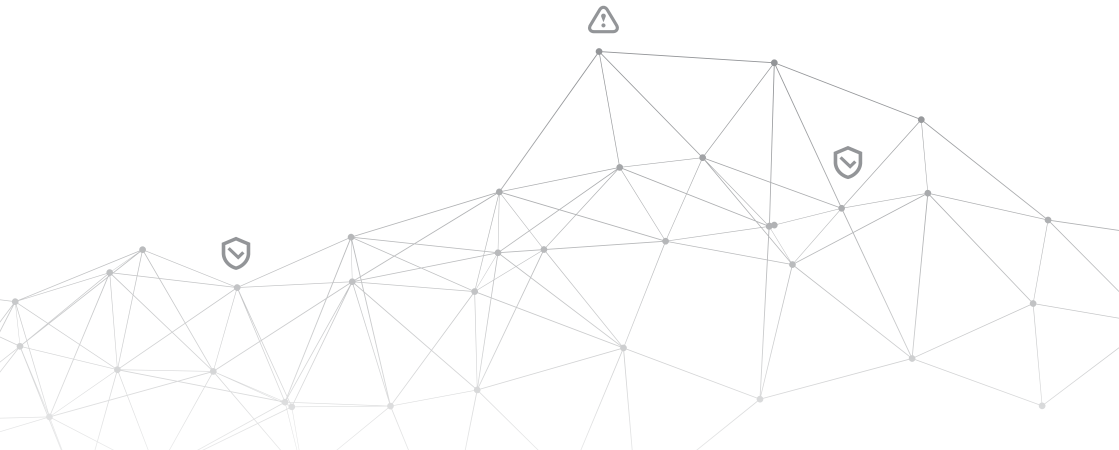


Table of Contents



Col. Romualdas Petkevičius,
Regional Cyber Defence Centre, Director

Director's Message

Cyber defence and resilience are vital for the stability and prosperity of the region.

From the start of this year it was evident that the cyber field would be the battleground of today's modern conflicts. Unfortunately, the entire world was shocked and unprepared for what unfolded on 24 February. Looking back on the three months prior, the signs were visible.

Steadily increasing cyber-attacks against Ukraine, Georgia and the Baltic States were an early indication of increased tensions in the region.

That is why cyber defence is now relevant more than ever. Lessons learned, tactics observed and decisions made. The Regional Cyber Defence Centre is committed to defending our region by providing vital cyber intelligence and training against the current and emerging threats. We have partnered with countries and organizations in order to share our knowledge, expertise and to collaborate in making the region safe.

01/Q1 Highlights

The first quarter of 2022 was quite eventful inside and outside of the cyber field. Geopolitical tensions have risen and have culminated in the war in Ukraine. We have observed an increased vulnerability scan traffic from various countries that peaked on 24 February 2022. After the invasion of Ukraine, the load decreased, thus pointing to the obvious threat actor. Georgia and Ukraine have confirmed similar observations.

Most notable highlights during this period:

DDoS and Malware Campaign Against Ukraine

During these three months, we have observed a number of various cyber-attacks against the Ukrainian Government, financial and public sectors. These campaigns were coordinated and were a prelude to war.

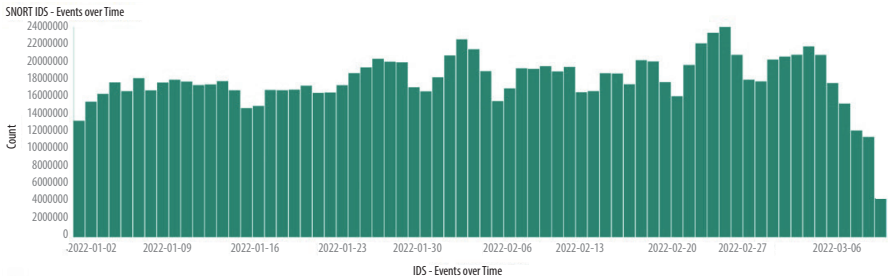


Figure 1. / Scans against Lithuanian governmental websites

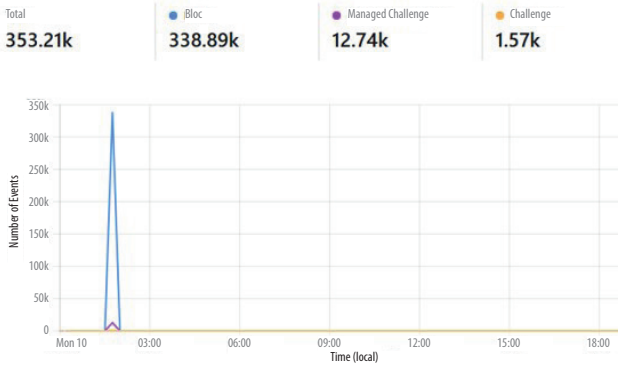


Figure 2. / Georgia MoD DDoS attempt

DDoS Attack Against Georgia and Mitigation

Georgia has reported an increased DDoS activity from the Russian Federation. A number of IP addresses were identified and decimated via MISP. Georgia has avoided any disruptions due to the CDN protection and utilization.

Overspill of Malware from Ukraine to the Baltic states

It has been reported that some Lithuanian and Latvian companies faced the Hermetic Wiper malware due to sharing a VPN and LAN with the Ukrainian-based branches. However, no significant damage was reported.

Invasion of Ukraine and Ripple Effect in Cyberspace

The Russian-announced "Special Military Operation", which is a full-scale war against Ukraine, had a ripple effect on the entire cyberspace. A large number of white hats and black hats and even computer-illiterate people have started DDoS campaigns on Russian media outlets, web pages, government and financial sectors, even OT systems were attacked. This crippled numerous Russian websites, including the Kremlin, the government website and many others. The ongoing information war pushed the Kremlin towards isolating itself in an information bubble, claiming that there is an immense amount of western disinformation about the "Special Operation" in Ukraine. That led to the ban on nearly all social media in Russia.

Ukraine Joins CCDCOE

On a more pleasant note, Ukraine is now part of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn as a Contributing Participant. This has been achieved with all 27 contributing countries agreeing on the decision. It is a huge benefit for the Ukrainians to be able to exchange practice and expertise with the Centre, as Ukraine is fighting a cyber-war too.

02/Regional Cyber Threat Landscape

The first quarter of 2022 has shown a gradual increase in malicious cyber activity. The activity can be categorized into several tactics and procedures targeting to disrupt and damage infrastructure, leak sensitive information and extort financial gain by utilizing cryptolockers. We also have noticed additional goals that have only become clear in recent days – to cause reputational damage, spread fear, uncertainty and doubt. As well as to perform aggressive misinformation campaigns against the public and government sectors. The cyber threat situation in the region and the world was pretty intense in general. In mid-February, when Russia invaded Ukraine, it turned for the worse and a full-on cyber warfare began. The world split in two parts: the first being on Ukraine's side and the other – on Russia's. As of now, people all around the world have decided to be either with Ukraine or Russia.

When the invasion started, Ukraine began a campaign for recruiting people to what they call an "IT army" with at least some background and knowledge in IT to put pressure on Russia's cyber infrastructure. The goal of this army organization is to use any vectors of cyber and DDoS attacks

on a variety of Russian targets, mainly in the public sector: military, FSB, Kremlin and a variety of news pages spreading propaganda about Russia's invasion of Ukraine.

In this report, we will not be covering the attacks against the Russian Federation. It is not part of the RCDC region and it is currently considered an aggressor. The Russian activity will be covered in a separate report.

03/Categories of Attacks Against RCDC Partners:

Phishing Campaigns Against Ukraine, Georgia and Lithuania. A phishing campaign is an email scam designed to steal personal information from victims.

DDoS and DoS Attacks Against Georgia and Ukraine. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. A DDoS attack uses more than one unique IP address or devices, often from thousands of hosts infected with malware.

Data Wiper Attacks Against Ukraine. In computer security, a wiper is a class of malware intended to erase (wipe) the hard drive of the computer it infects, maliciously deleting data and programs. Observed wipers overwrite data with a single value to prevent recovery using undelete tools. Also, those particular wipers corrupted and wiped the Master Boot Record of the affected systems rendering them unbootable and inoperable.

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or altogether block access to it unless a ransom is paid.

Defacement Attacks Against Ukraine's Government and Public Sector.
Website defacement is an attack on a website that changes the visual appearance of a website or a web page. These are typically the work of defacers who break into a web server and replace the hosted website with one of their own. Like other forms of vandalism, it is used to spread messages by politically motivated "cyber protesters" or hacktivists.

04/Pilot Project "Securing Our Cyberspace Together"

Since July 2021, when the Regional Cyber Defence Centre (RCDC) was established, it has proven its worth in building a better cyber threat picture in the region. Our Cyber Threat Analysis Cell (CTAC) focuses on gathering information from partner countries, analyzing it and finally generating a very actionable tactical level data, as well as operational level reports.

Since the cyber domain in our region has become "hot", we have decided to take it a step further and enhance our capabilities by seeking new partners. To benefit a wide range of countries and organizations, the RCDC proposed to them to join the RCDC on a pilot basis to share information on cyber events and receive cyber threat intelligence reports generated by CTAC. As of right now, RCDC partner organizations include the National Cyber Security Centre of Lithuania (Lithuania), Mil-CERT of Ukraine, Georgia's Cyber Security Bureau (CSB), and the USA Pennsylvania National Guard. CTAC is sharing information not only with partners mentioned above but also with the following organizations: the Ukrainian Defence Intelligence, US EUCOM, CISA, and the US Embassy in Lithuania. As of this date, Poland has successfully joined our Centre's activity on the pilot basis. The Cyber Threat Analysis Cell is currently in talks with a couple of EU countries. Any partner organization can be fully incorporated into CTAC's workflow and receive our reports via email, and as a full-fledged member can help shape the RCDC policy to benefit all involved parties.

As mentioned before, any interested parties are welcome to start a dialogue and get involved in CTAC activity. This can be anything, from information sharing via PGP-encrypted emails to having their representatives here in Kaunas. It is important to emphasize that CTAC is flexible and can adapt to different countries' requirements, needs and possibilities.

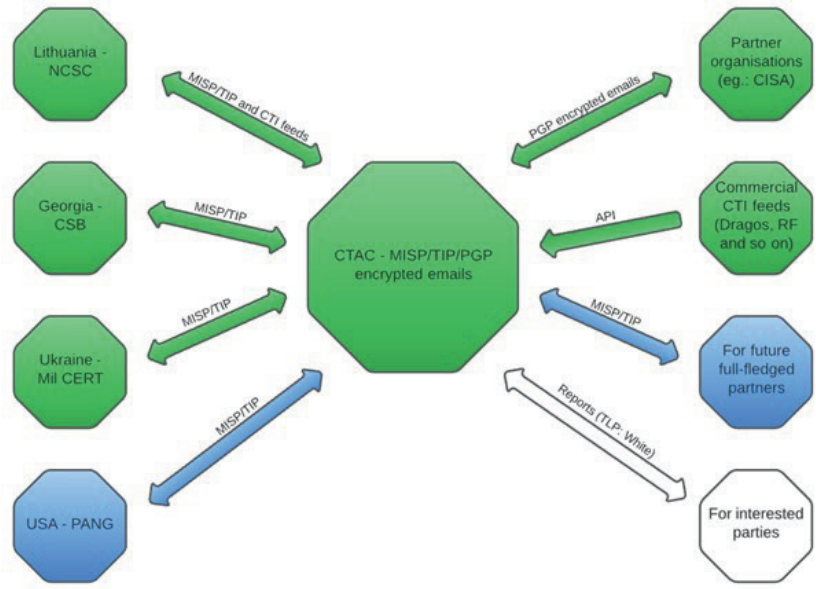


Figure 3. / CTAC Activity model

05/Cyber Activity in the Region: Chronological Order

2022

1. **10-17 January 2022 DDoS Attempts Against Georgian MoD.**
The Georgian CSB registered an anomalous network flow on the official website of the Ministry of Defence and its sub-domains. It was identified as a DDoS attack. Parallel to that, an attempt was made to compromise the web server and web application on the basis of some common vulnerabilities. As Georgia's infrastructure is shielded by CloudFlare, the disruption of the website activity was mitigated. Some of the attacker IP addresses were found also on the Ukrainian and Lithuanian sides.

2. **13 January 2022 WhisperGate Wiper Attacks, Ukraine.**
In mid-2022, Microsoft identified a new destructive malware which was soon dubbed WhisperGate, targeting multiple public sector organizations in Ukraine. This malware is compiled to look like ransomware but it doesn't have a recovery mechanism like ransomware usually does. WhisperGate is intended to be destructive rendering targeted devices inoperable rather than gaining ransom. Multiple government, non-profit and information technology organizations were targeted by this attack were.

3. **14-15 January 2022 Defacement of Government Websites, Ukraine.**
Following the WhisperGate, a defacement attack was launched on Government websites. On 14 January 2022, before going down temporarily, more than 70 Ukrainian websites were defaced by displaying threatening political messages in Russian, Ukrainian and Polish languages. The messages claimed that there was public information stolen and that soon it would become public, however, no evidence of exfiltration followed. The attackers managed to cripple much of the Government's digital infrastructure, including the most widely used site Diia which has a role in Ukraine's coronavirus response. They also managed to cripple the sites of the Cabinet of Ministers and the Ministries of Veteran Affairs, Sports, Energy, Foreign Affairs, Education & Science, Defense, Agriculture and Ecology. The Belarusian group UNC1151 is suspected to stand behind this attack.

4. **15-16 February 2022 DDoS Attacks on Websites, Ukraine.**
In mid-February, Ukraine suffered the most significant DDoS attack to date. A number of Ukrainian websites were affected and taken down. This attack had an impact on bank, military and government websites. Because the scale of this attack was moderate, the sites were recovered within hours from being taken down. It seems that the attack was intended to create chaos and panic which were growing already due to the threat of the Russian invasion. Ukraine believes that Russia was behind this attack.

5. **15 February 2022 SMS Spam/Disinformation Campaign, Ukraine.**
On 15 February, one of the state-owned banks' customers started to receive information via SMS messages that claimed there had been technical ATM malfunctions. The Ukrainian Cyber Police soon debunked these claims as false.

6 **23 February 2022 DDoS Attacks on Websites, Ukraine.**

The websites of several Ukrainian banks and Government departments, including the Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, Security Service (SBU) and the Cabinet of Ministers, became inaccessible as result of a large DDoS attack. Most of the other sites came back online within two hours from the attack but for others latency and outages continued into the following day. Attribution: Nation-State – Russia.

A week after the most significant DDoS attack on Ukraine, it suffered another one. This time websites of Ukrainian banks, and the Government sector, including the Ministry of Internal Affairs and the Ministry of Defense, Cabinet of Ministers and the Security Service (SBU) became inaccessible due to large-scale DDoS attacks. Most of the issues were fixed within a couple of hours after the attack, however, outages and latency continued throughout the following day. Once again, Ukraine blames Russian APTs for this DDoS attack.

7 **23 February 2022 HermeticWiper Malware Attack, Ukraine, Lithuania, Latvia.**

On the early morning of 24 February 2022, 9 days after the attack of 15 February, when Government websites were hit by a DDOS attack, Ukraine faced yet another cyber-attack against their infrastructure. A number of organizations across Ukraine were hit by a cyber-attack infecting hundreds of computers. This attack contained a new data-wiping malware soon dubbed HermeticWiper – a malware that can corrupt or even delete data on a targeted network or computer. A spillover of this attack has been detected to the Ukrainian companies located in Latvia and Lithuania. Technical analysis indicates the mechanism of the attack was built at least six weeks prior to the attack, indicating that this attack has been coordinated with a military invasion and the full-scale war on Ukraine. A large number of Government's and private sector companies' websites were defaced, and a destructive malware was unleashed. Ukrainian cyber teams are struggling to recover due to conventional military actions. Moreover, priorities have shifted.

8 **24 February 2022 an Attack Takes Down the Internet, Phishing Attack, Ukraine.**

On the morning of 24 February 2022, NetBlocks reported a large-scale disruption to the internet service in the second-largest city in Ukraine – Kharkiv. It is reported that up to 25% of internet users in Kharkiv and its surrounding region were impacted. In total, about 1.8 million people were affected. On the same day, the oldest English-language newspaper in Ukraine, The Kyiv Post, announced that their site had been under a constant cyberattack.

On the same day, a phishing campaign took place. European Government personnel involved in managing the logistics for refugees fleeing for Europe were targeted using possibly compromised accounts of Ukrainian Armed Forces personnel. Like many other attacks, this attack is attributed to UNC1151.

9 **24 February, 2022, IsaacWiper, Ukraine.**

On the same morning as the beginning of the Russian invasion of Ukraine, ESET identified a new wiper. This wiper was dubbed IsaacWiper and it was found to had affected organizations that had not been attacked by HermeticWiper. There was no shared code between these two

wipers found. On February 25, the attackers dropped a new version of IsaacWiper with debug logs, indicating that the attackers were unable to wipe some of the compromised devices. The malware has been developed/deployed at least since 19 October 2021. IsaacWiper enumerates logical drives and wipes the content of each disk using randomly generated bytes. The malware recursively wipes the files in a single thread, though the process could be time-consuming for large disks.

10 **25 February 2022 Cyber-attack on Border Control Station, Ukraine.**

The Ukrainian border control station located at the Ukraine/Romania border reported that they had been struck by a data wiper cyber-attack. This attack slowed down the process of allowing war refugees to cross into Romania.

11 **28 February 2022 Facebook, YouTube and Twitter Remove Disinformation Targeting Ukraine.**

Meta (Facebook parent company) claims that they have uncovered Russian efforts to erode the trust in and image of the Ukrainian Government and a separate attempt to hack the officials and journalists from the Ukrainian military on its platform.

It seems that the two campaigns were small in scale, and Facebook managed to detect them in early stages. The first campaign involved about 40 accounts, groups and pages on Facebook and Instagram from Russia and Ukraine. These accounts, groups and pages were disguised as an independent news source and posted fake claims about Ukraine. Meta also detected an increase in attempted hacks against the Ukrainians. Some hacking attempts were attributed to group that has links in Belarus, Ghostwriter. This group has been making the effort to hack the accounts of high-profile Ukrainians, like military officials, public figures and journalists.

12 **5 March 2022 Phishing Attack by Compromised Accounts**

Ukraine's Computer Emergency Response Team (CERT-UA) disclosed information that a phishing campaign was targeting Ukraine's citizens. According to CERT-UA, such emails are sent from compromised accounts belonging to Indian entities. It seems that the campaign was launched to lure out sensitive information.

13 **7 March 2022 Phishing Campaign Delivering MicroBackdoor Malware**

Ukraine's Computer Emergency Response Team (CERT-UA) confirmed an ongoing phishing campaign against Ukraine's Government. This campaign is used to deliver malware known as MicroBackdoor. CERT-UA discovered dovidka.zip, a file containing a contextual help file, which in turn includes two files: a bait image presenting information on the procedure for frequent artillery shelling and an HTA-file with malicious VBScript. Running the VBScript leads to an infection chain resulting in a MicroBackdoor malware infection. Although tentative, this attack was attributed to UNC1151.

14 **14 March 2022 Malware CaddyWiper Attacks on Organizations**

New malware, dubbed CaddyWiper, detected on 14 March. This attack focused on limited organizations in Ukraine. No code similarities were detected between CaddyWiper and previously disclosed HermeticWiper or IsaacWiper. There is evidence that threat actors infiltrated the targeted networks prior to wiper execution.

15 **16 March 2022 Disinformation Campaign Against Ukraine's TV Station**

TV station Ukraine24 suffered an attack: the news ticker of the program was hacked to display messages allegedly announced by the President. The messages claimed that the Ukrainian President urged the Ukrainians to stop fighting and give up their weapons. Since then, the TV station confirmed that they had been hacked and that the displayed messages were fake.

16 **17 March 2022 State Authorities Suffer a Phishing Campaign**

The Ukrainian Ministry of Defence notified CERT-UA that emails containing malicious files were distributed targeting Ukraine's state authorities. In case of a successful attack, a victim's computer would be infected with SPECTR malware as a result. CERT-UA attributes this attack to VERMIN / UAC-0020 Ukraine Hacking Collective.

17 **17 March 2022 Wiper DoubleZero Attack Against Ukraine's Enterprises**

In mid-March, Ukraine's enterprises were targeted by a new wiper dubbed DoubleZero. CERT-UA discovered a number of ZIP archives containing the mentioned wiper DoubleZero. The activity is tracked by the UAC-0088 identifier. The purpose of this campaign is believed to be an attempt to disrupt regular operation of information systems of Ukraine's enterprises.

18 **18 March 2022 Phishing Campaign Spreading Backdoor**

CERT-UA reported an ongoing phishing attack targeting Ukraine's organizations with LoadEdge backdoor. The incident was attributed to InvisiMole/ UAC-0035, a hacking group with alleged ties to the Russian Advanced Persistent Threat (APT) Group Gamaredon.

19 **22 March 2022 Chinese APT Scarab Targeting Ukraine**

Ukraine's CERT issued an alert sharing a summary of indicators associated with a recent intrusion attempt through the delivery of a malicious RAR file. Attribution: China APT – Scarab (UAC-0026). Since the invasion, this malicious behavior is one of the first public examples of a Chinese threat actor targeting Ukraine.

06/Recommendations

As cases of DDoS attacks are on a massive increase, the best advice for protecting yourself is following Georgia's example. As it is written above, the MoD of Georgia was targeted by a DDoS attack but they managed to repel it and suffered no harm just by using CloudFlare. So, it is highly recommended to use Content Delivery System (CDS) services to protect from DDoS attacks, either the previously mentioned CloudFlare or any other CDS service, for example CloudFront.

It is important to have up-to-date security and antivirus systems and segregate networks to prevent the spread of malware, as well as working back-up solutions, in order to mitigate phishing attacks. But most importantly - train your personnel to identify these risks, since human factor is the main target of phishing.

When it comes to protection against ransomware, it gets more difficult but surely not impossible. Really, it all comes down to basics, like:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
- Regularly patching and updating software and OSs to the latest available versions.
- It is essential to ensure the devices are properly configured and that security features are enabled. For example, disable ports and protocols not used for a business purpose.
- Furthermore, companies should employ best practices of using RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services – and later propagate ransomware.
- Lastly, disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations.

07/End Note

To sum up, in these challenging times, it is vital to keep your vigilance and to be prepared for a range of different situations. It is hard to tell whether the Russian invasion of Ukraine and the cyber-warfare that came before and after it is the toughest challenge that we will have to face this year. We can see that the attacks are getting less sophisticated, it is just because threat actors seek to spread chaos and not any other reward. The best example of this is the massive DDoS attacks targeting both, Russian and Ukrainian institutions. That being said, there are new wipers discovered mainly in Ukraine, however, there have already been spillovers, so each and every one of us have to be prepared to take action and resolve potential attacks. It is very important to emphasize that which seems to be a very simple matter, like the use of strong passwords and the importance of critical thinking. These, at first sight simple actions, can help prevent brute-force or phishing attacks which may lead to way worse outcomes, like identity theft and financial losses.

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