NATIONAL CYBER SECURITY CENTRE UNDER THE MINISTRY OF NATIONAL DEFENCE

NCSC CERT-LT REPORT FOR THE 1st HALF OF 2021

TLP: WHITE

26-07-2021
Vilnius

CONTENTS

I. SUMMARY

According to the National Cyber Security Centre under the Ministry of National Defence (NCSC), the number of cyber incidents registered in Lithuania in the first half of 2021 was similar to the previous year. There were 1,780 cyber incidents, an increase of 2% compared to the same period in 2020. Of these, applying the approved criteria for classifying the impact of such incidents[1], 55 cyber incidents were classified as moderate, half of which (27 incidents) were recorded in the communication and information systems of legal entities[2]. Attempts have also been made to affect the public sector (10 incidents) and internet service providers (4 incidents).

For all 1,780 registered cyber incidents during the half-year, the biggest change was identified in the hacking category. During the first half of the year, 77 incidents of this type were registered, which is 129% more than in the same period in 2020. This significant increase in hacking is due to two main reasons: zero-day vulnerabilities in Microsoft Exchange Server that affected entities worldwide and several major personal data leaks that occurred in Lithuania this spring. Companies providing information technology services have been the main victims of the hacking.

The most significant cyber incidents in Lithuania in the first half of the year were related to the disclosure of the zero-day vulnerabilities in Microsoft Exchange servers. At the beginning of the year, after 1,300 IP addresses were checked, at least 99 email servers in Lithuania had these vulnerabilities, two more were added in the summer, and at the beginning of August 8 email servers still had these vulnerabilities.

The first half of 2021 is also exceptional due to recurring personal data leaks (CityBee, LieMSIS, Kilobaitas, and so on). During these, the personal data of hundreds of thousands of Lithuanian consumers became accessible to persons with malicious intent.

Risk was also posed by 186 websites in the Lithuanian domain which were infected with malicious code, about which the NCSC was informed by a Lithuanian cyber security expert. Corrective action was taken in three-quarters of the sites, but site owners had still not removed the malicious code at 26% of the websites by the end of the first half of the year.

As in previous years, information-cyberattacks were also registered, in which fake news was distributed. At the beginning of 2021, distributed denial-of-service attacks against distance learning

[1] List of criteria for classifying cyber incidents: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[2] Companies registered in Lithuania that are not covered by the definition of Cybersecurity Entities

in schools were registered, and cases of distribution of Emotet malicious code continued to be recorded until February, when such distribution was interrupted by a successful international operation by law enforcement and judicial authorities.[3]

[3] https://policija.lrv.lt/lt/naujienos/tarptautines-operacijos-metu-uzkirstas-kelias-vienos-pavojingiausiu-kenkejisku-programu-emotet-plitimui-visame-pasaulyje

II. CYBER INCIDENTS REGISTERED BY CERT-LT

1. In the first half of 2021, 1,780 cyber incidents were registered, a 2% increase compared to the same period in 2020.

2. The biggest threat was posed by the discovery of zero-day vulnerabilities in Microsoft Exchange service and the identification of potential cyber incidents.

3. An increasing number of leaks of personal data and information-cyberattacks led to media coverage and public concern.

In the first half of 2021, the NCSC by automated means registered and processed more than 215,000 unique Lithuanian IP addresses related to cyber events, i.e. 4% less than in 2020 (when 225,000 were registered). However, it should be noted that this sample also includes addresses of Lithuanian internet service providers with an IP from other countries (Lithuanian service providers that rent IP addresses to entities from other countries). Considering only Lithuanian IP addresses, a 7% increase was recorded: 136,000 IP addresses connected with cyber events were registered in 2021 and 126,000 IP addresses in 2020. In summary, the number of events recorded and processed in the first half of this year is similar to that observed in the first half of last year.

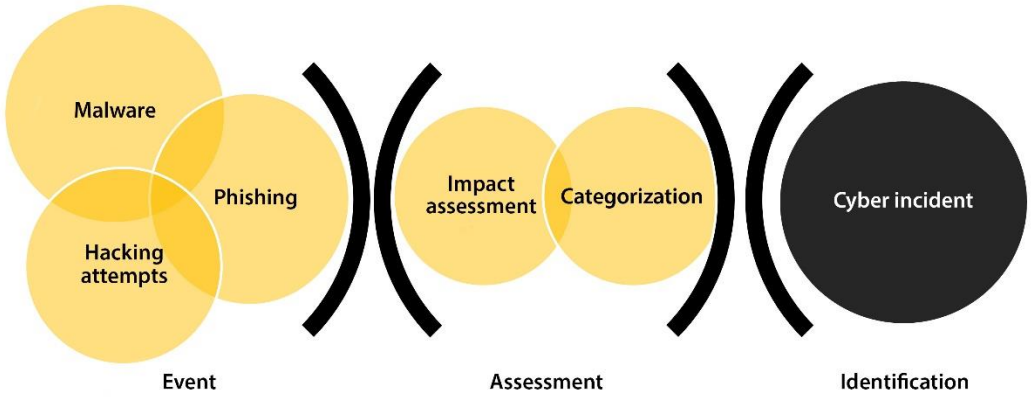

Figure 1: Cyber Incident Assignment Process

The NCSC Incident Management Unit (CERT-LT) registered a 2% increase in cyber incidents in the first half of 2021 compared to a total of 1,780 cyber incidents in the same period in 2020 (Figure 2).

No.	Group	Quantity	Change from 1st half of 2020
1.	Distribution of spam, misleading information	94	- 26%
2.	Malware	891	+ 13%
3.	Information gathering (phishing)	510	- 8%
4.	Hacking attempt	75	- 32%
5.	Successful hacking	77	+ 129%
6.	Service Disruption (DDoS)	25	- 56%
7.	Illegal activity, fraud	58	+ 9%
8.	Other incidents (individual, not matching the descriptions of any of the above-mentioned categories)	50	+ 138%
	Total:	1,780	+ 2%

Figure 2: Cyber incidents in the 1st half of 2021 and change from the same period in 2020

Of a total of 1,780 cyber incidents, applying the impact criteria, 55 were moderate cyber incidents in terms of impact, half of which (49%) were registered in the communication and information systems of legal entities. Attempts were also made to affect the public sector (10 incidents) and internet service providers (4 incidents) (Figure 3).

No.	Group	Quantity
1.	Legal entities	27
2.	Government administration sector	10
3.	Internet service providers	4
4.	Hosting service providers	3
5.	Health care sector	3
6.	Education sector	3
7.	Culture sector	1
8.	Transport and postal sector	1
9.	Information technology and electronic communications sector	1
10.	Digital service provider	1
11.	Social services sector	1
	Total:	55

Figure 3: Moderate-impact cyber incidents by sector in the first half of 2021

Most of the incidents registered in the first half of the year were of negligible impact and were mostly registered in the communication and information systems of hosting services and internet service providers (Figure 4).

No.	Group	Quantity
1.	Hosting service providers	736
2.	Internet service providers	444
3.	Legal entities	120
4.	Natural persons	99

5.	Digital service provider	69
6.	Government administration sector	61
7.	Foreign entities	53
8.	Energy sector	32
9.	Health care sector	27
10.	Other	84
	Total:	1,725

Figure 4: Minor cyber incidents by sector in the first half of 2021

NCSC notes that the exponential increase in the number of successful hacks in the first half of 2021 is due to the identification of zero-day vulnerabilities in Microsoft Exchange email service and in several major personal data leaks that took place in Lithuania this spring.

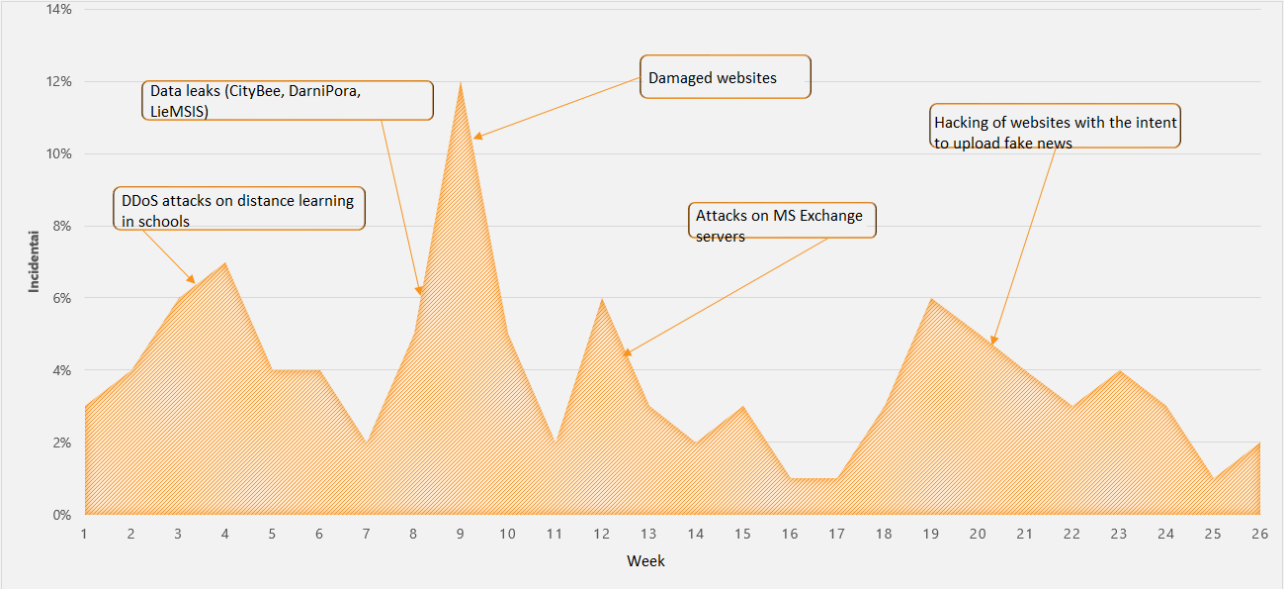

Figure 3: Cyber incidents in the first half of 2021

In the first half of 2021, NCSC specialists responsible for management of vulnerabilities coordinated the patching of vulnerabilities in the Microsoft Exchange email service in the communication and information systems of Lithuanian cyber security entities (Figure 4). At the beginning of the year, after 1,300 IP addresses were checked, at least 99 email servers in Lithuania had Microsoft Exchange vulnerabilities; at the beginning of summer, two more with such vulnerabilities were identified, and at the beginning of August, 8 email servers still had such vulnerabilities.

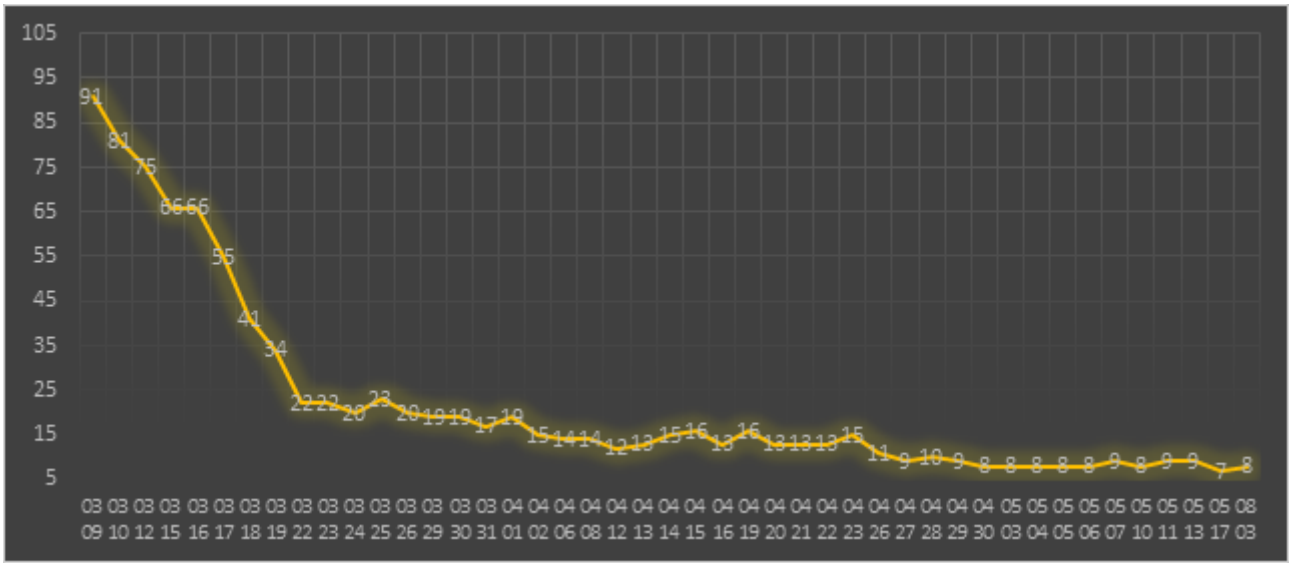

Figure 4: The scope of Microsoft Exchange vulnerabilities through 3 August 2021

In the first half of 2021, the NCSC registered a significant increase in the number of leaks of personal data. It should be noted that this type of incident has occurred in the past, but the increased interest in the personal data of users suggests that the value of personal data of Lithuanian users is increasing. The NCSC was involved in investigating data leak incidents related to CityBee, DarniPora, LieMSIS, and Kilobaitas. The NCSC believes that access was mostly obtained through unsophisticated methods, as the affected entities had not applied sufficient risk control measures.

Risk was also posed by 186 websites in the Lithuanian domain that were infected with malicious code, about which the NCSC was informed by a Lithuanian cyber security expert. The removal of malicious code from websites on which a user was redirected from search engines to a malicious website (hoax) was coordinated by the NCSC together with the website administrators. NCSC notes that not all website owners have removed the malicious code from their websites; 26% of the affected websites (49 of 186) were still infected at the end of the first half of the year. For this reason, in order to protect users, the NCSC additionally, within its remit, once again contacted the website owners, hosting service providers and the Lithuanian police regarding the possible commission of a criminal offence.

At the beginning of the year, a trend in DDoS cyberattacks was observed. Some of these attacks were targeted at online lessons, i.e. when the IP addresses of teachers' computers were discovered, they were targeted by attacks, thereby disrupting distance learning. Given that this type

of activity is considered to be criminal, it is appropriate to initiate criminal proceedings in such cases and, having identified the perpetrators of such attacks, to apply criminal liability.[4]

Until February, cases of distribution of Emotet malicious code, which had started at the end of 2020, continued to be registered, but such incidents were brought to an end by a successful international operation by law enforcement and judicial authorities. As part of international coordinated measures taking place around the world, law enforcement authorities took control of malware infrastructure, in this way stopping the mass distribution of the malicious code.[5] NCSC notes that polymorphic malicious code, due to frequent changes in attributes, continues to be a threat vector for cyber incidents in Lithuanian communication and information systems. In essence, this concerns the relatively limited ability of cybersecurity entities to quickly and efficiently detect this type of malicious code.

In 2021, the dissemination of fake news continued to be monitored, with the dissemination using elements of cyber incidents such as simulating websites and hacking. Such cyber-information attacks aim to mislead internet users, discredit and influence strategic processes or international relations. It should be noted that the activities of cyber-information operations are not limited to the territory of the state of Lithuania.[6] In 2021, the NCSC, for its part, registered information attacks directed exclusively against processes taking place in Lithuania, namely, the National Certificate for COVID-19. It should be noted that the impact of the cyber incident in this particular case was not identified and the dissemination of the simulated websites for the National Certificate for COVID-19 was limited. The NCSC believes that the dissemination of fake news using elements of cyber incidents will continue in 2021.

[4] https://www.etaplius.lt/hakeris-is-alytaus-bausmes-isvenge-tik-per-plauka
[5] https://policija.lrv.lt/lt/naujienos/tarptautines-operacijos-metu-uzkirstas-kelias-vienos-pavojingiausiu-kenkejisku-programu-emotet-plitimui-visame-pasaulyje
[6] https://www.fireeye.com/blog/threat-research/2021/04/espionage-group-unc1151-likely-conducts-ghostwriter-influence-activity.html

2.1 CERT-LT CYBER INCIDENT INVESTIGATIONS AND ANALYSES

2.1.1 CityBee data leak

On 15 February 2021, CityBee user data was published in an online forum with limited access: email address, password SHA-1 checksum, first name, surname and national identification number. During the night, from 15 February to 16 February, a record of additional available data was placed on the same online forum, that is, the full CityBee database, including driving licence numbers, residential addresses, telephone numbers. Following the investigation of the cyber incident, the NCSC identified the following circumstances:

- Also among the leaked data of the 110,000 CityBee clients was included passwords for their accounts, which had been stored in an unsafe SHA-1 algorithm without additional security measures (salt).
- The national identification numbers of clients had been stored in plaintext.
- From the data provided, it is not possible to determine precisely at what time the backup database of CityBee customers was misappropriated. It is also impossible to determine precisely when the ongoing vulnerability was blocked.

2.1.2 Copy of vatesi.lt page

On 17 March 2021, NCSC detected a registered domain, vatesl.lt, the purpose of which was to simulate the real website of the State Nuclear Power Safety Inspectorate (VATESI), *vatesi.lt*. The forged website contained information that did not correspond to reality. Almost at the same time, a hack took place on the website of the Polish National Atomic Energy Agency, *paa.gov.pl.* This website also contained information that did not correspond to reality, which quoted fake news from the fake vatesl.lt website. Information that did not correspond to reality spread further through the Polish website *www.zdrowie.gov.pl,* where links were provided to the fake news uploaded to vatesl.lt and *paa.gov.pl*. The dissemination of fake news also benefited from the use of social media and the possibly hijacked Facebook and Twitter accounts of Polish officials connected with the energy sector.

The circumstances of the cyber incident as established by the NCSC have been forwarded to the Polish authorities.

2.1.3 Vilniaus kolegija/University of Applied Sciences students' data leak

On 11 March 2021, the personal data of students at Vilniaus kolegija/University of Applied Sciences was published in an online forum with limited access: first name, surname, gender, national identification number, home address, city, school, year of school graduation, date of birth, ethnicity, field of study, code of study programme, date of study start, date of graduation, faculty and name of academic institution. At some point in time, the data had previously been misappropriated, stolen or accessed as a result of a cyber incident. It was also announced in the forum that the malicious person also has data from other educational institutions related to the *www.liemsis.lt* information system.

Following the investigation of the cyber incident, the NCSC identified the following circumstances:

- The illegal misappropriation of the personal data of students at Vilniaus kolegija/University of Applied Sciences possibly occurred due to unrestricted access to the system via the internet and the improperly organized cybersecurity of *www.liemsis.lt*. The investigation identified that the cause of the incident could also have been unrestricted access to other information resources via the internet.
- From the limited information available during the investigation, it was not possible to determine precisely when and from which system the student database of Vilniaus kolegija/University of Applied Sciences was misappropriated. This could not be determined because of the uncontrolled expansion of the information resources of higher education institutions, system sprawl.
- Potentially inappropriate processing of personal data has been identified. Among the leaked data of 7,000 students of Vilniaus kolegija/University of Applied Sciences, the national identification numbers had been stored in plaintext.

2.1.4 Websites infected by malicious software

In March 2021, information was received from a natural person about 186 websites in the Lithuanian IP domain **.lt* that were infected with malicious code. After checking the information received, it was found that visitors to the websites could be redirected to other websites of poor repute where criminal activity was potentially committed: attempts were made to lure login credentials as well as payment card details and other data from visitors, to infect visitors' devices with malicious code, and website visitors were encouraged to take part in various lotteries allegedly organised by Google, Apple, Samsung or other well-known companies.

In order to protect visitors to the websites, this information was communicated in writing to hosting service providers and measures were recommended to prevent cyber incidents at the source:

1. to contact the responsible persons on whose behalf the services were used and to inform them about the involvement of their websites in malicious and potentially criminal activities;
2. in the absence of action by service owners, to limit the services provided to users until the malicious code on the websites had been removed;
3. to inform the NCSC by 18 March 2021 of the actions taken to remove the malicious code.

A review of the sites performed on 22-23 March 2021 revealed that 84 sites were still infected with malicious code and involved in malicious activities. In accordance with Article 14 of the Law on Cyber Security of the Republic of Lithuania ("Interinstitutional Cooperation in the Investigation of Cyber Incidents"), information on recent continuing cyber incidents in which the hosting service users or hosting service providers providing services to such users were informed of the fact that they cause and participate in cyber incidents, but did not take measures to eliminate the causes of these incidents, was submitted to the 5th Board (in Lithuanian, *valdyba*) for the Investigation of Serious and Organised Crime of the Lithuanian Criminal Police Bureau (hereinafter, the Police). Cooperation with the Police succeeded in closing or compelling the majority of hosting service users (site owners) to remove the malicious code.