NATIONAL CYBER SECURITY CENTRE
UNDER THE MINISTRY OF NATIONAL DEFENCE

CYBER-ATTACK AND FAKE NEWS DISSEMINATION CAMPAIGN ANALYSIS

14 January 2020

On the 9th of December 2020, after exploiting authentication vulnerability of the website content management system, a large number of public-sector websites were hacked and three different pieces of fake news were posted.

The attack was conducted on the 9th of December 2020, between 17:00 and 21:00 EET. It is known that the attackers were successfully authorized to 22 public-sector websites, most of which belong to municipal administrations. Having gained access, hackers posted three different pieces of fake news: “Polish Diplomat Detained while Entering Lithuania”, “Šiauliai Airport Infrastructure Modernization is FAKE”, “Military Conscription and Recruitment Service’s Regional Units Revise Lists of Conscripts”.

LENKIJOS DIPLOMATAS SULAIKYTAS ĮVAŽIUOJANT Į LIETUVĄ

2020-12-09

Lenkijos ambasados Lietuvoje trečiasis sekretorius ponas Paweł Tadeusz Purski buvo sulaikytas įvažiuojant į Lietuvą.

Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos pareigūnai, specialios operacijos metu, pas sulaikytąjį rado daug pinigų, narkotikų ir ginklų.

Remiantis operatyvine informacija, Lenkijos diplomatas žinojo, kad muitinėje pareigūnai netikrina automobilių su diplomatiniais numeriais, nes jie turi imunitetą. Jis ne kartą per Lietuvos Respublikos valstybės sieną gabenęs pinigus, šaunamuosius ginklus, šaudmenis, sprogstamąsias medžiagas, stipriai veikiančias, narkotines, psichotropines medžiagas (4,5 kg), radikalaus ir ekstremistinio turinio literatūrą, skirta Lenkijos piliečiams, vykdantiems ekstremistinę veiklą Lietuvos teritorijoje.

Užsienio reikalų ministerija įteikė protesto notą Lenkijos ambasadai Vilniuje.

NAUJIENOS

Karo prievolės ir komplektavimo tarnybos regioniniai padaliniai patikslina karo prievolininkų (šauktinių) sąrašus
2020-12-09

Vadovaujantis Lietuvos Respublikos Krašto apsaugos ministerijos sprendimu, Karo prievolės ir komplektavimo tarnybos regioniniai padaliniai patikslina karo prievolininkų (šauktinių) sąrašus.

Prašome užtikrinti organizacijos karo prievolininkų (šauktinių) į Karo prievolės ir komplektavimo tarnybos regioninį padalinį atvykimą.

Surinkimo laikas - 2020 m. gruodžio 10 d.

Atvykdami į Karo prievolės ir komplektavimo tarnybos regioninį padalinį su savimi turėkite:

Asmens tapatybę patvirtinantį dokumentą (asmens tapatybės kortelė arba pasas).

Išsilavinimą ir (arba) kvalifikaciją patvirtinančius dokumentus, kad galėtume Jums pasiūlyti tinkamiausią tarnybos vietą ir pareigas.

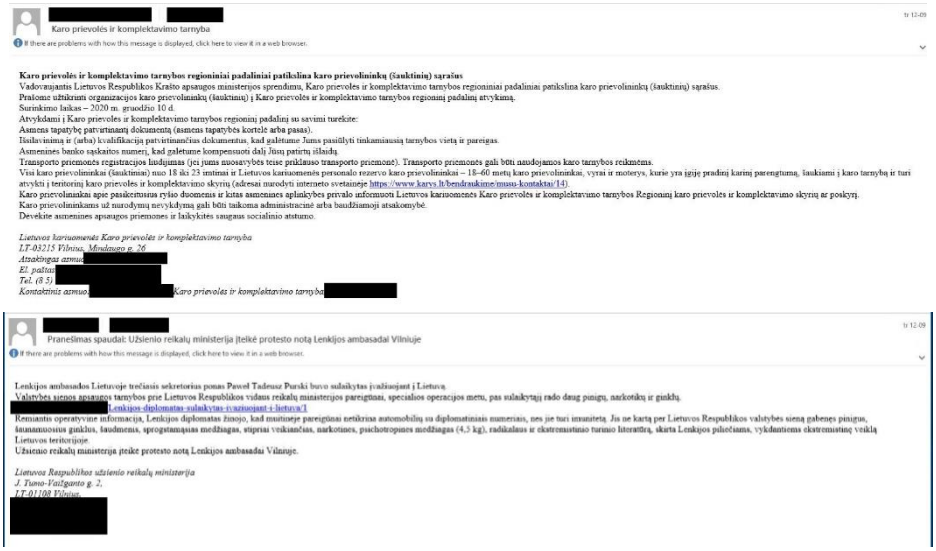
Asmeninės banko sąskaitos numerį, kad galėtume kompensuoti dalį Jūsų patirtų išlaidų.

Transporto priemonės registracijos liudijimas (jei jums nuosavybės teise priklauso transporto priemonė). Transporto priemonės gali būti naudojamos karo tarnybos reikmėms.

Visi karo prievolininkai (šauktiniai) nuo 18 iki 23 imtinai ir Lietuvos kariuomenės personalo rezervo karo prievolininkai – 18-60 metų karo prievolininkai, vyrai ir moterys, kurie yra įgiję pradinį karinį parengtumą, šaukiami į karo tarnybą ir turi atvykti į teritorinį karo prievolės ir komplektavimo skyrių (adresai nurodyti interneto svetainėje https://www.karys.lt /bendraukime/musu-kontaktai/14).

Examples of fake news

At the same time, fake e-mails were disseminated, by spoofing e-mail addresses of the Ministry of National Defence of the Republic of Lithuania, the Ministry of Foreign Affairs of the Republic of Lithuania and Šiauliai City Municipality Administration. Fake news content was repeated in the e-mails and links to the hacked websites were listed.


[redacted] [redacted]

Karo prievolės ir komplektavimo tarnyba

If there are problems with how this message is displayed, click here to view it in a web browser.

Karo prievolės ir komplektavimo tarnybos regioniniai padaliniai patikslina karo prievolininkų (šauktinių) sąrašus

Vadovaujantis Lietuvos Respublikos Krašto apsaugos ministerijos sprendimu, Karo prievolės ir komplektavimo tarnybos regioniniai padaliniai patikslina karo prievolininkų (šauktinių) sąrašus.
Prašome užtikrinti organizacijos karo prievolininkų (šauktinių) į Karo prievolės ir komplektavimo tarnybos regioninių padalinių atvykimą.
Surinkimo laikas – 2020 m. gruodžio 10 d.
Atvykdami į Karo prievoles ir komplektavimo tarnybos regioninį padalinį su savimi turėkite:
Asmens tapatybę patvirtinantį dokumentą (asmens tapatybės kortelė arba pasas).
Išsilavinimą ir (arba) kvalifikaciją patvirtinančius dokumentus, kad galėtume Jums pasiūlyti tinkamiausią tarnybos vietą ir pareigas.
Asmeninės banko sąskaitos numerį, kad galėtume kompensuoti dalį Jūsų patirtų išlaidų.
Transporto priemonės registracijos liudijimas (jei jums nuosavybės teise priklauso transporto priemonė). Transporto priemonės gali būti naudojamos karo tarnybos reikmėms.
Visi karo prievolininkai (šauktiniai) nuo 18 iki 23 imtinai ir Lietuvos kariuomenės personalo rezervo karo prievolininkai – 18–60 metų karo prievolininkai, vyrai ir moterys, kurie yra įgiję pradinį karinį parengtumą, šaukiami į karo tarnybą ir turi atvykti į teritorinį karo prievolės ir komplektavimo skyrių (adresai nurodyti interneto svetainėje https://www.karys.lt/bendraukime/musu-kontaktai/14).
Karo prievolininkai apie pasikeitusius ryšio duomenis ir kitas asmenines aplinkybes privalo informuoti Lietuvos kariuomenės Karo prievolės ir komplektavimo tarnybos Regioninį karo prievolės ir komplektavimo skyrių ar poskyrį.
Karo prievolininkams už nurodymų nevykdymą gali būti taikoma administracinė arba baudžiamoji atsakomybė.
Devekite asmenines apsaugos priemones ir laikykitės saugaus socialinio atstumo.

Lietuvos kariuomenės Karo prievolės ir komplektavimo tarnyba
LT-03215 Vilnius, Mindaugo g. 26
Atsakingas asmuo [redacted]
El. paštas: [redacted]
Tel. (8 5) [redacted]
Kontaktinis asmuo [redacted] *Karo prievolės ir komplektavimo tarnyba* [redacted]

[redacted] [redacted]

Pranešimas spaudai: Užsienio reikalų ministerija įteikė protesto notą Lenkijos ambasadai Vilniuje

If there are problems with how this message is displayed, click here to view it in a web browser.

Lenkijos ambasados Lietuvoje trečiasis sekretorius ponas Paweł Tadeusz Purski buvo sulaikytas įvažiuojant į Lietuvą.
Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos pareigūnai, specialios operacijos metu, pas sulaikytąjį rado daug pinigų, narkotikų ir ginklų.
[redacted] Lenkijos diplomatas sulaikytas tvarkingai - lietuva/3
Remiantis operatyvine informacija, Lenkijos diplomatas žinojo, kad muitinėje pareigūnai netikrina automobilių su diplomatiniais numeriais, nes jie turi imunitetą. Jis ne kartą per Lietuvos Respublikos valstybės sieną gabenęs pinigus, šaunamuosius ginklus, šaudmenis, sprogmenąsias medžiagas, stipriai veikiančias, narkotines, psichotropines medžiagas (4,5 kg), radikalaus ir ekstremistinio turinio literatūrą, skirtą Lenkijos pilečiams, vykdantiems ekstremistinę veiklą Lietuvos teritorijoje.
Užsienio reikalų ministerija įteikė protesto notą Lenkijos ambasadai Vilniuje.

Lietuvos Respublikos užsienio reikalų ministerija
J. Tumo-Vaižganto g. 2,
LT-01108 Vilnius
[redacted]

Examples of spoofed e-mails

The evidence gathered during the forensic analysis revealed that the cyber-attack was carried out with specific objectives in mind. The cyber-attack was planned and prepared in advance. It must be concluded that potential targets and victims of cyber criminals do not pay sufficient attention to cyber security: content management systems are accessible from the public Internet, there is no strict control policy towards behaviour of content management system users, who use insecure passwords and do not tend to change them periodically. These incidents demonstrate that website developers and administrators do not pay adequate attention to cyber security best practices, and recommendations provided by cyber security specialists are insufficiently implemented.

National Cyber Security Centre Recommendations

- Limit access to the content management system to administrators or content managers by whitelisting IP addresses. When a public access is indispensable, it is necessary to reinforce measures for authentication of administrators and users, by applying Two-Factor Authentication (2FA).
- Since the most popular method to deceive users is social engineering (by spreading compelling or frightening information, thus, using emotional manipulation), continuous education in order to increase the cyber-awareness of personnel is of vital importance: providing information on possible threats, organizing cyber-security exercises, making recommendations on how to treat suspicious e-mails, attachments and documents.
- Deactivate automatic download of images of the e-mail content. Do not initiate image downloads in suspicious e-mails.
- Periodically perform a thorough security policy evaluation on website: review all user names and passwords used in the systems; inspect files; prohibit unused functionalities, especially those which enable access from outside to inside.
- In order to protect publicly available systems, software used on the servers should be regularly patched, a restricted access to administration interface should be enabled (e.g., by access control lists), additional security measures should be implemented (e.g., web application firewalls). Moreover, strict control over accounts with administrative rights should be exercised, complex and regularly-changed passwords should be used, regular audits of logs should be carried out. Finally, websites should be regularly scanned for vulnerabilities.