Tel. 1805
Email: cert@nksc.lt
https://www.nksc.lt/en/

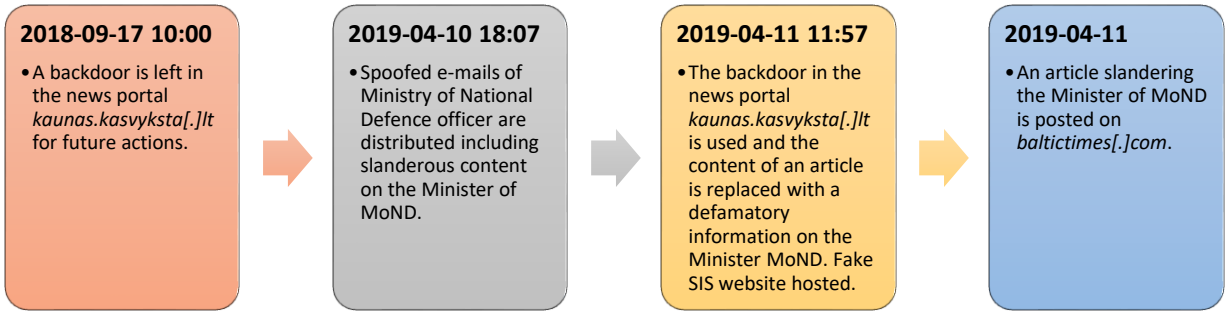
NATIONAL CYBER SECURITY CENTRE
UNDER THE MINISTRY OF NATIONAL DEFENCE REPUBLIC OF LITHUANIA

BRIEF REVIEW OF THE CYBER INCIDENT ANALYSIS
No. 163811

30 April 2019

TLP: WHITE

The object of cyber-incident investigation: The distribution of spoofed e-mails to the targeted audience on 10-04-2019, defacement of the news portal *kaunas.kasvyksta[.]lt* for dissemination of slanderous information.

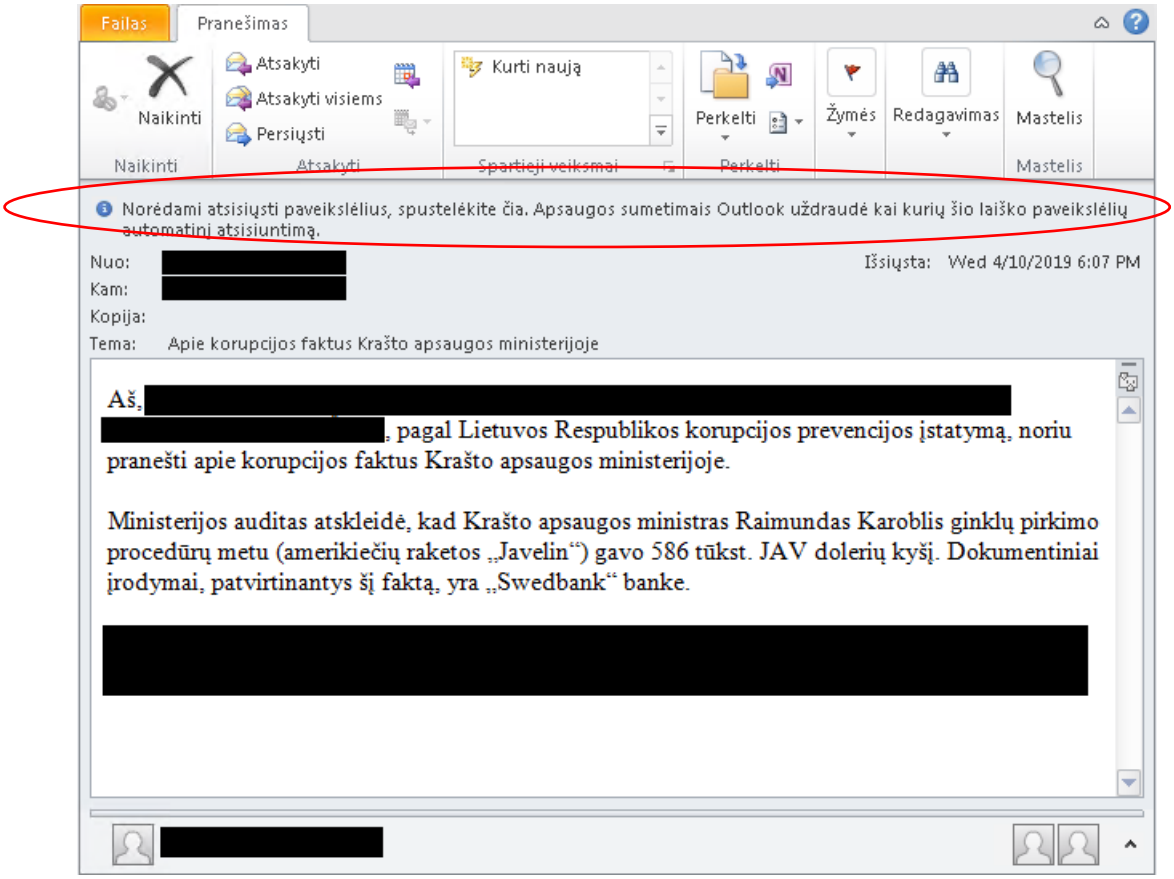


Timeline

2019 April 10 In the evening, spoofed e-mails of Ministry of National Defence officer are distributed including slanderous content on the Minister of MoND. Letters are distributed to the targeted audience: representatives of state institutions of the Republic of Lithuania, politicians. The content of the letter is written in a smooth, correct, formalized Lithuanian language, with a clear understanding of the legal basis and internal organizational structure of the Republic of Lithuania.

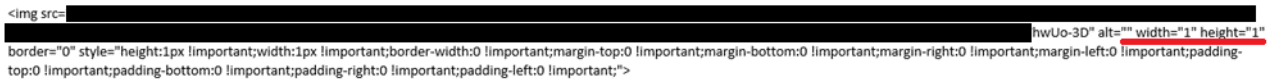
After checking the header of the e-mail, it was sent from an IP address 94.103.82[.]136, which is using email / news distribution service providers. This is to hide the original header of the message and thus circumvent the various mail server protections

Tel. 1805
Email: cert@nksc.lt
https://www.nksc.lt/en/



Content of the spoofed email

After the analysis of the email, it was found that a link was inserted in the message content: one pixel size, invisible to the user. The purpose of the inserted image is that the sender of the message can identify who and how many times he read the sent message.



1 pixel size picture inserted in the e-mail

The study found that using a publicly available software code after modifying it, was placed in the news portal *kaunas.kasvyksta[.]lt* **2018-09-17 10:00:05**. Such software code sets are used by web administrators, but in some cases also conducting malicious activity by hacking into the website system and leaving the set file as a backdoor for future attacks. It is possible that such actions were also performed during this incident. Due to the lack of the event logs, there cannot be a determination on how the file was uploaded to the system.

On **April 11, 2019 11:57** the backdoor was used to deface the news portal *kaunas.kasvyksta[.]lt*, publishing a fake news article on the Minister of MoND. Based on the received information, it was found that the attack was performed using TOR network services, from the IP address **38.117.96[.]154**. TOR directs Internet traffic through a free, worldwide, volunteer overlay to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. The logical IP addresses of the nodes that were captured and used during hacking are associated with malicious Internet activity.

After checking the content of the updated article on **April 11, 2019** on the site *kaunas.kasvyksta[.]lt* it was found that the content of the article matches with the fake letter.

A hyperlink "**notify SIS**" has been inserted in the fake article, which redirects to the same *kaunas.kasvyksta[.]lt* site, which falsifies the website of the Special Investigation Service of the Republic of Lithuania. The hyperlink consisted of the same style, design and pictures of a real website with the same fake news article slandering the Minister of MoND.

Fake SIS page is placed in the *kaunas.kasvyksta[.]lt* website

On **2019-04-11** NCSC received information that the news portal *baltictimes[.]com* was hacked and an article in English had been placed on the site, the content is supposedly based on a fake news article posted by the *kaunas.kasvyksta[.]lt*, regarding the same slanderous information on Minister of MoND. The website displays article upload date of 2019-04-10, which shows the possibility that the news portal *baltictimes[.]com* has a similar backdoor as the *kaunas.kasvyksta[.]lt* portal.

THE BALTIC Times

ESTONIA LATVIA LITHUANIA BUSINESS ANALYSIS OPINION CULTURE EU AFFAIRS

Lithuanian Minister of Defence Karoblis is suspected of corruption

2019-04-10 BNS/TBT Staff

VILNIUS – Lithuanian Special Investigation Service on Wednesday announced opening an investigation into the Lithuanian Minister of National Defence for suspected bribery.

The Special Investigation Service is carrying out an extraordinary pre-trial investigation into alleged large-scale bribery, trading in influence and abuse of powers in the Ministry of National Defence of the Republic of Lithuania.

According to Kasvyksta.lt, Raimundas Karoblis received large amounts of money for promoting the U.S. interests in Lithuania. More than $500,000 and €120,000 have been found during search for evidence.

Public procurement audit revealed serious violations in the Ministry of Defence. Mr.Karoblis received $586,000 from the U.S. to support the procurement of additional missiles for the US-made Javelin anti-tank defence systems in February 2019.

The Ministry of National Defence did not disclose the number of systems acquired, ostensibly for security reasons.

Thanks to his efforts, in April the United States and Lithuania signed a plan of cooperation in the field of defence for the period up to 2024, which is detrimental to the national interests of Lithuania.

Thus, according to the U.S. DoD report, since 2014, the United States has invested only $80 million for defence security cooperation in Lithuania, and Lithuania has committed more than $200 million in national funds to purchase U.S. defense articles.

In addition to this, in January 2017 Lithuanian Minister of National Defence Raimundas Karoblis and U.S. Ambassador Anne Hall in Vilnius signed an agreement on the status of U.S. troops in the country. The agreement gives the U.S. jurisdiction over crimes committed by its military personnel in Lithuania.

According to the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania, Raimundas Karoblis with 356 thousand euros of assets is in the list of the richest ministers in the country. However, his personal debt is 79 thousand euros, and a loan is about 120 thousand euros.

According to the preliminary investigation, Mr. Karoblis and his wife purchased expensive pieces of real estate and cars. Their daughters Guoda and Justina live a luxury lifestyle and study at prestigious educational institutions in Belgium and the United Kingdom. By the way, trading in influence, Raimundas Karoblis in the Seimas supported the idea not to introduce compulsory military service for girls (probably, in order to avoid speculations about his own daughters).

The investigation suggests that it was debt that forced Karoblis to accept a bribe.

The Ministry of Defence declined to comment on the information to the media.

MOBILE VERSION

Subscribe Advertise Log In

Related Articles


Lithuanian defense minister visiting


Russia's taking revenge on


Lithuanian president, EU leaders to


Lithuanian presidential candidates

Defaced news portal *baltictimes[.]com*

Tel. 1805
Email: cert@nksc.lt
https://www.nksc.lt/en/

Conclusions

- Spoofed e-mails of Ministry of National Defence officer are distributed including slanderous content on the Minister of MoND. Letters are distributed to the targeted audience: representatives of state institutions of the Republic of Lithuania, politicians. The content of the letter is written in a smooth, correct, formalized Lithuanian language, with a clear understanding of the legal basis and internal organizational structure of the Republic of Lithuania. A link was inserted in the message content: one pixel size, invisible to the user. The purpose of the inserted image is that the sender of the message can identify who and how many times he read the sent message.
- The backdoor in the news portal *kaunas.kasvyksta[.]lt* is used and the content of an article is replaced with a defamatory information on the Minister MoND. Fake SIS website hosted.
- NCSC received information that the news portal *baltictimes[.]com* was hacked and an article in English had been placed on the site, the content is supposedly based on a fake news article posted by the *kaunas.kasvyksta[.]lt*

Indicators of compromise

94.103.82.136		
Type **IP**	Date **2019-04-10** IP address of the server used to distribute the e-mails.	Threat level High (3/5) Confidence level (70/100)
38.117.96.154		
Type **IP**	Date **2019-04-11** IP address, from which an article was changed in *kaunas.kasvyksta[.]lt* website.	Threat level High (4/5) Confidence level (70/100)

Recommendations

- Since the most popular method to deceive users is social engineering (compelling or frightening information, manipulation of emotions), constant education to boost the cyber-awareness of the personnel is vital: information on possible threats, arrangement of cyber-security exercises, recommendations on how to treat suspicious e-mails and documents.
- After receiving an e-mail with suspicious content from a known person or organization, always check the headers of the e-mail that shows what the actual sender is in the field “From”. During the analysis of the header, you should look at the first "Received" parameter from the bottom. This attribute will show from which server the e-mail was sent. If the "From" field is *sender@organization.lt*, then in the "Received" field you will usually see the domain name "organization.lt".
- Deactivate automatic download of images of the e-mail content. Do not initiate image downloads in suspicious emails.
- In order to protect publicly available systems, software used on the servers should be regularly patched, access to administration interface restricted (e.g., by access control lists), additional security measures (e.g., web application firewalls) used, accounts with admin rights strictly controlled, complex and regularly changed passwords used, and logs regularly audited, perform timely audit of logs, regularly scan your website for vulnerabilities.