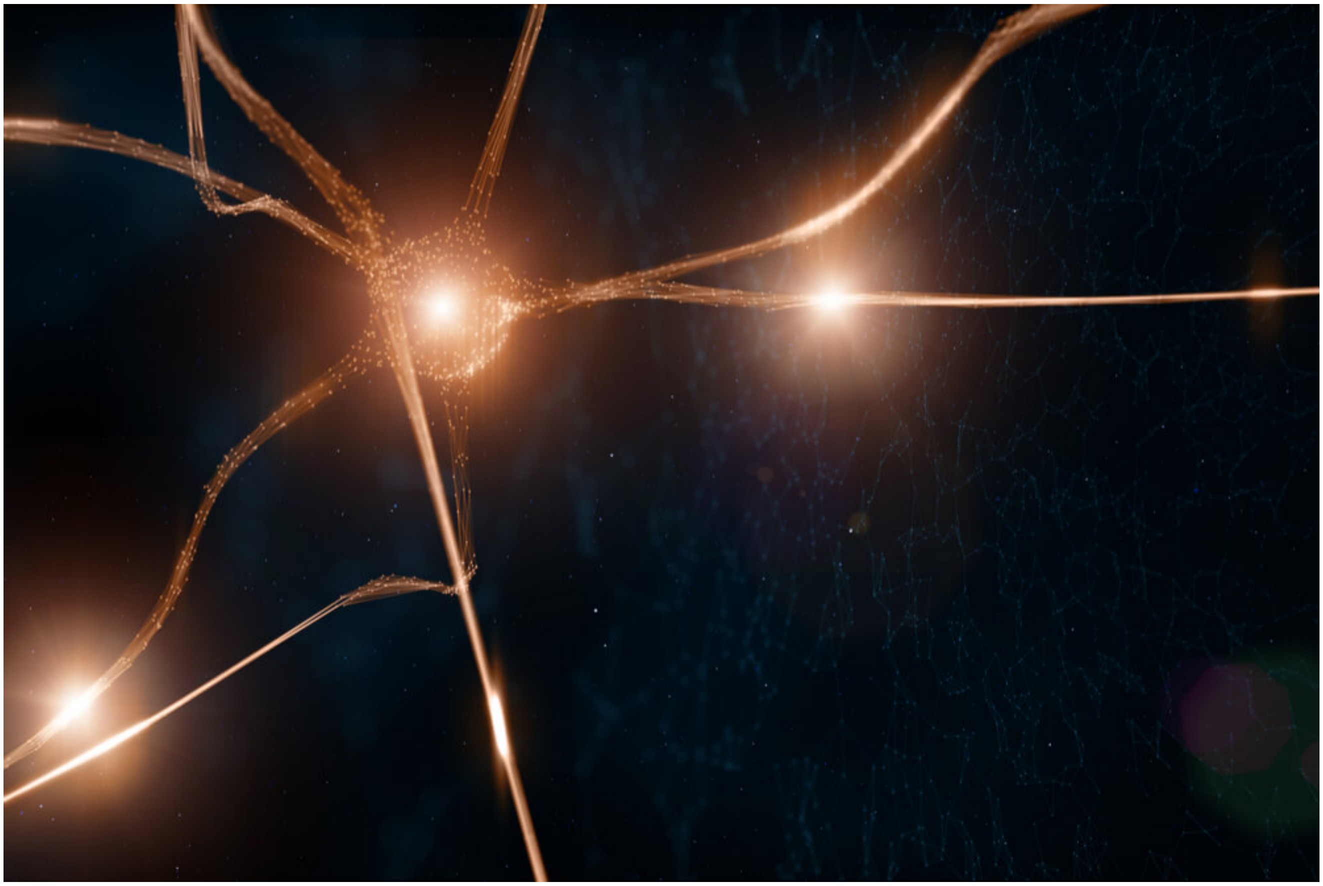
Turla LightNeuron: An email too far

welivesecurity.com/2019/05/07/turla-lightneuron-email-too-far/

May 7, 2019



ESET research uncovers Microsoft Exchange malware remotely controlled via steganographic PDF and JPG email attachments

Matthieu Faou
7 May 2019 - 02:00PM

ESET research uncovers Microsoft Exchange malware remotely controlled via steganographic PDF and JPG email attachments

Due to security improvements in operating systems, rootkit usage has been in constant decline for several years. As such, malware developers – especially those working in espionage groups – have been busy developing new stealthy userland malware.

Recently, ESET researchers have investigated a sophisticated backdoor used by the infamous espionage group Turla, also known as Snake. This backdoor, dubbed LightNeuron, has been specifically targeting Microsoft Exchange mail servers since at least 2014. Although no samples were available for analysis, code artefacts in the Windows version lead us to believe that a Linux variant exists.

Turla LightNeuron: One email away from remote code execution

Download Research Paper

Victimology

During the course of our investigation, we were able to identify at least three different victim organizations, as shown in Figure 1.

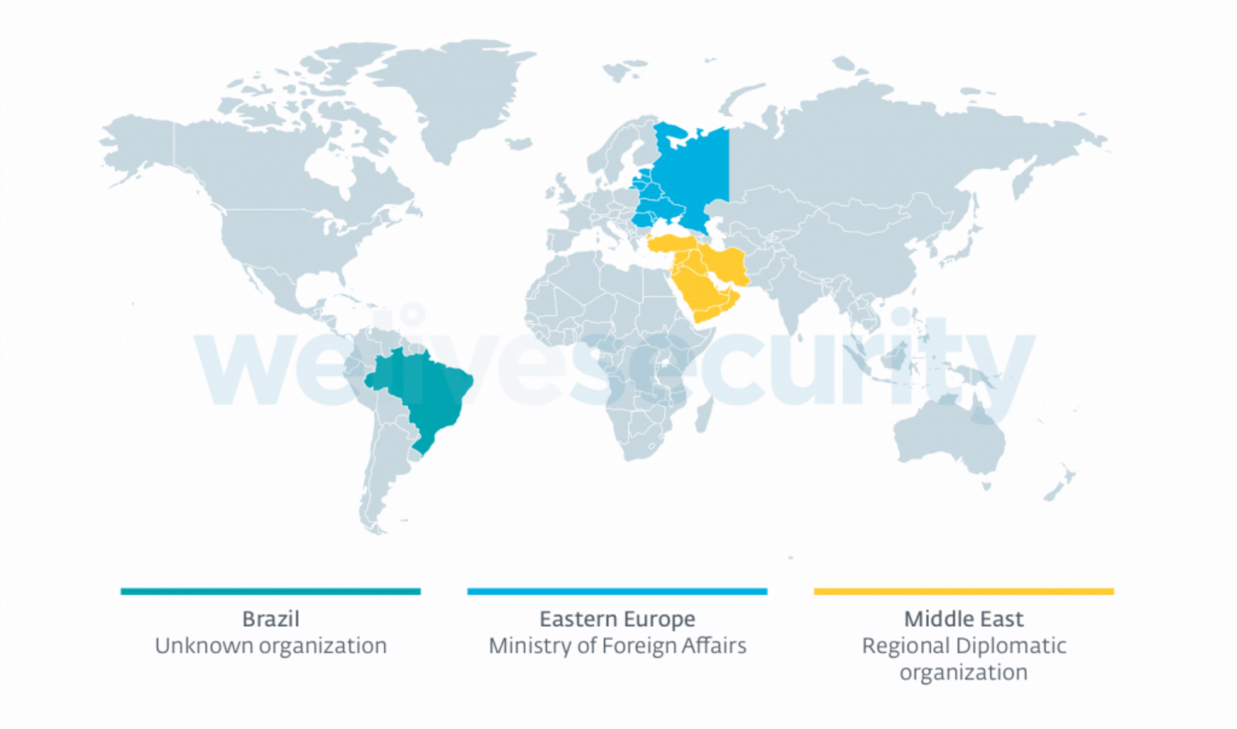


Figure 1 – Map of known LightNeuron victims

Two of the victims – a ministry of foreign affairs and a regional diplomatic organization – are in line with recent Turla campaigns we have analyzed.

As we noticed the victim in Brazil thanks to a sample uploaded to the popular multi-scanner *VirusTotal*, we were not able to determine the nature of the victim organization.

Attribution to Turla

We believe with high confidence that Turla operates LightNeuron. The following artefacts, collected during our investigation, back this:

- On one compromised Exchange server:
  - a PowerShell script containing malware previously attributed to Turla was dropped 44 minutes before a PowerShell script used to install LightNeuron, and
  - both scripts were located in C:\windows\system32.
- The script used to install LightNeuron has a filename – msinp.ps1 – that looks like typical filenames used by Turla.
- On another compromised server, IntelliAdmin – a remote administration tool, packed with a packer used only by Turla – was dropped by LightNeuron.
- For each LightNeuron attack, there were several other instances of Turla malware on the same network.
- The email address used by the attackers was registered at GMX and was impersonating an employee of the targeted organization. The same provider was used for the Outlook backdoor and for an undocumented PowerShell backdoor we named PowerStallion.

Further, in an earlier APT trends report, Kaspersky Labs researchers attributed LightNeuron with medium confidence to Turla.

Operator activity

While analyzing a compromised asset, we were able to retrace part of the attackers' activities. In particular, we were able to map the working hours of the operators, using the time at which the compromised Exchange server received emails containing commands for the backdoor.

Our first observation is that the activity aligns well with a typical 9-to-5 workday in the UTC+3 time zone, as shown in Figure 2.

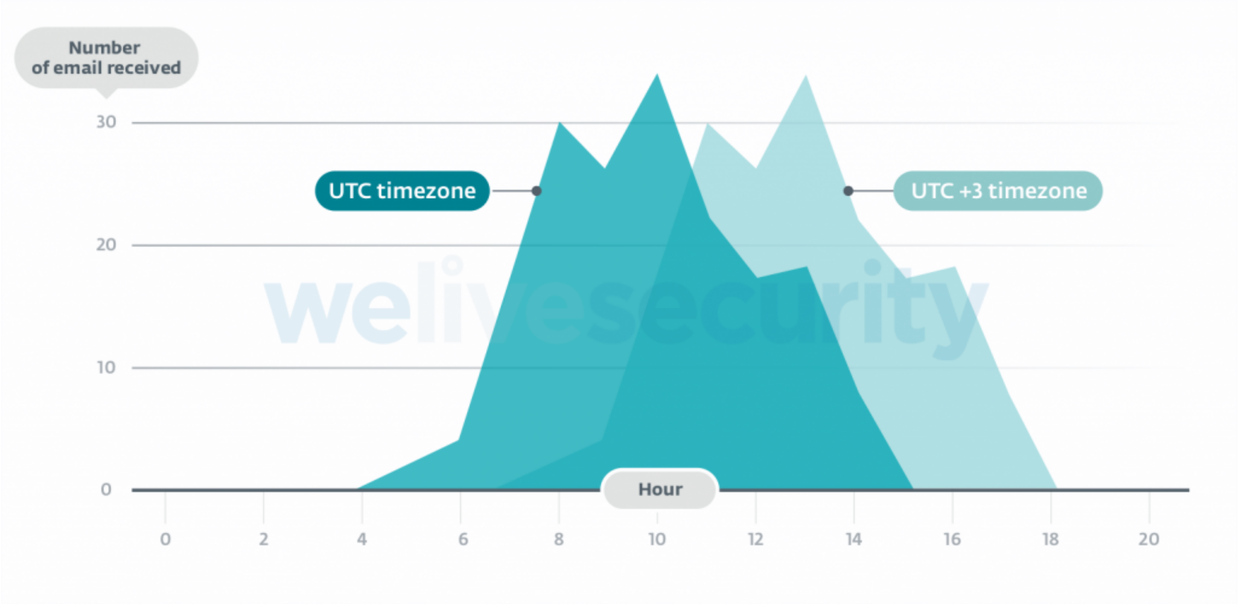


Figure 2 – LightNeuron operators' working hours

Our second observation is that no activity was observed between December 28, 2018 and January 14, 2019, while previously and afterwards, the attackers sent several emails per week. This break in activities corresponds to holidays around the Eastern Orthodox Christmas.

Even if it is not sufficient for a strong attribution, you can correlate these two observations with other elements you might have at your disposal.

Main characteristics

LightNeuron is, to our knowledge, the first malware specifically targeting Microsoft Exchange email servers. It uses a persistence technique never before seen: a Transport Agent. In the mail server architecture, it operates at the same level of trust as security products such as spam filters. Figure 3 summarizes how LightNeuron operates.

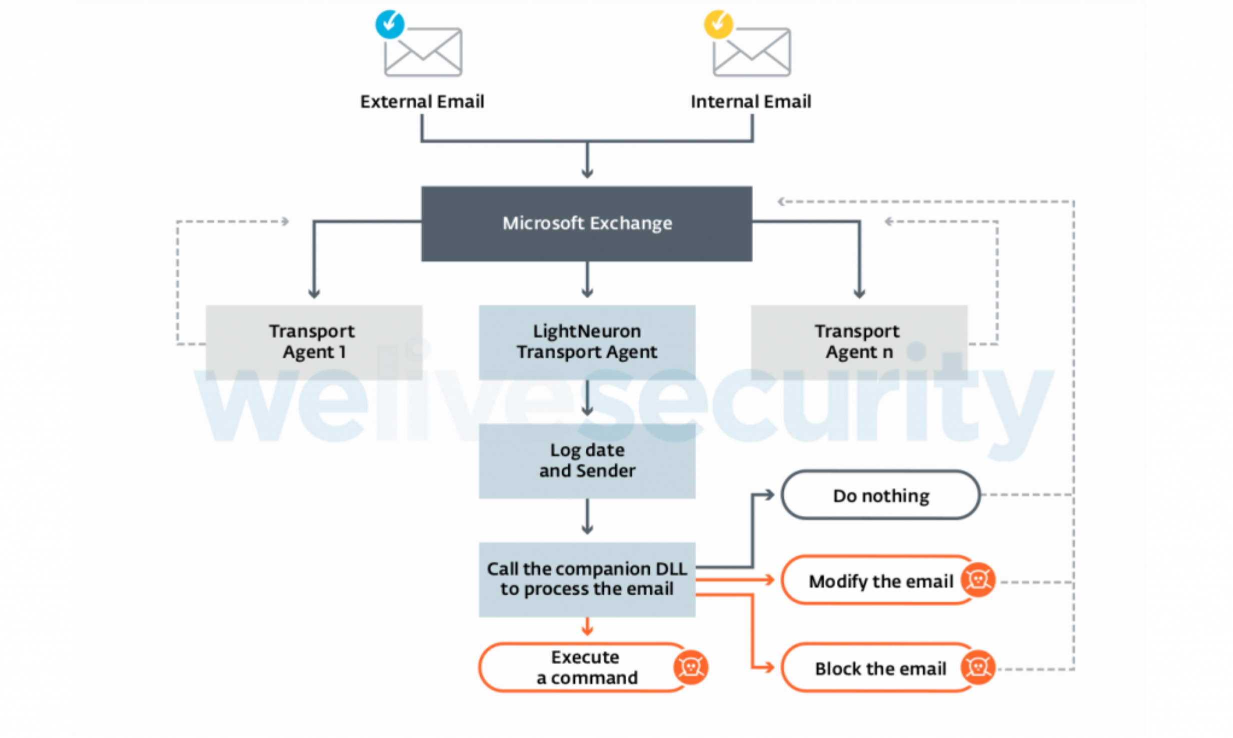


Figure 3 – LightNeuron Transport Agent

By leveraging the Transport Agent accesses, LightNeuron is able to:

- Read and modify any email going through the mail server.
- Compose and send new emails.
- Block any email. The original recipient will not receive the email.

A flexible set of XML rules drives these functions, as shown in Figure 4.

JavaScript

```
<class name="zip" metric="30" id="1" dllName="ZipMe" type="dll" include="1">
    <rule metric="10" id="1" include="1">
        <and>
            <or>
                <To condition="cnt" value="email1@[redacted]" />
                <From condition="cnt" value="email1@[redacted]" />
                <To condition="cnt" value="email2@[redacted]" />
                <From condition="cnt" value="email2@[redacted]" />
                [...]
            </or>
            <and>
                <To condition="!cnt" value="email3@[redacted]" />
                <From condition="!cnt" value="email3@[redacted]" />
               [...]
            </and>
        </and>
    </rule>
</class>
<class name="command" metric="40" id="1" dllName="ZipMe" type="dll" include="1">
    <rule metric="10" id="1" include="1">
        <attachment_Content-Type condition="cnt" value="image/jpeg" />
    </rule>
</class>
log:logHandler
zip:zipHandler
changeSubject:changeSubjectHandler
changeBody:changeBodyHandler
create:createHandler
command:commandHandler
block:blockHandler
replace:replaceHandler
stat:statHandler
```

Figure 4 – Redacted example of a rule file

The email addresses used in these rules are customized for each victim in order to target the most interesting people.

At the end of the rules, there is the list of the handlers implemented by LightNeuron. These functions are used in the rules to process the emails. Table 1 describes the eleven different handlers.

Handler name	Description
block	Block the email
changeBody	Change the body of the email
changeTo	Change the recipient of the email
changeSubject	Change the subject of the email
command	Parse the jpg/pdf attachment, decrypt and execute the commands.
create	Create a new email
log	Log email attachment in LOG_OUTPUT
replace	Replace the attachment
spam	Re-create and re-send the email from the exchange server to bypass the spam filter
stat	Log the From, Date, To, and Subject headers in CSV format in STAT_PATH
zip	Encrypt the email with RSA and store it in the path specified by ZIP_FILE_NAME.

Table 1 – Description of the handlers implemented in the DLL

Backdoor

The *command* handler is different from the others that perform modifications on the emails. It is actually a backdoor controlled by emails. The commands are hidden in PDF or JPG attachments using steganography.

The attackers just have to send an email containing a specially crafted PDF document or JPG image to any email address of the compromised organization. It allows full control over the Exchange server by using the commands shown in Table 2.

Instruction Code	Description	Argument 1	Argument 2	Argument 3
0x01	Write an executable. Execute it if it is an executable.	Exe path	N/A	File data

Instruction Code	Description	Argument 1	Argument 2	Argument 3
0x02	Delete a file	File path	N/A	N/A
0x03	Exfiltrate a file	File path	Set to “1” to delete the file	N/A
0x04	Execute a process (CreateProcess)	Command line	N/A	N/A
0x05	Execute a command line (cmd.exe /c)	Command line	N/A	N/A
0x06	Return 0	N/A	N/A	N/A
0x07	Disable backdoor for x minutes.	Minutes	N/A	N/A
0x09	Exfiltrate a file	File path	Set to “1” to delete the file	N/A
0x65	Return 0	N/A	N/A	N/A

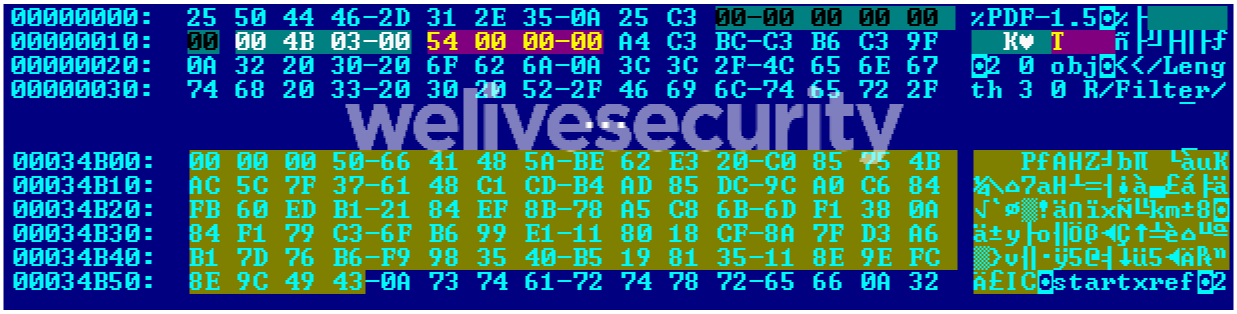
Table 2 – List of instruction codes

Once an email is recognized as a command email, the command is executed and the email is blocked directly on the Exchange server. Thus, it is very stealthy and the original recipient will not be able to view it.

Steganography

LightNeuron uses steganography to hide its commands inside a PDF document or a JPG image. Thus, even if the email is intercepted, it might look legitimate, as it contains a valid attachment.

In the case of a PDF, the command data can be anywhere in the document. LightNeuron operators just add a header at the beginning of the PDF to specify the offset at which the data is located, as shown in Figure 5.

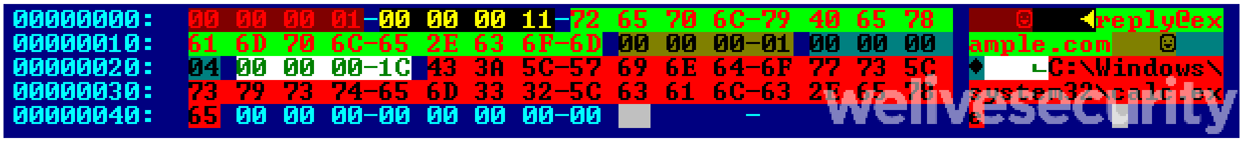


```
00000000:  25 50 44 46-2D 31 2E 35-0A 25 C3 00-00 00 00 00  %PDF-1.5◙%├
00000010:  00 00 4B 03-00 54 00 00-00 A4 C3 BC-C3 B6 C3 9F    K♥ T   ñ├╝├╢├ƒ
00000020:  0A 32 20 30-20 6F 62 6A-0A 3C 3C 2F-4C 65 6E 67  ◙2 0 obj◙<</Leng
00000030:  74 68 20 33-20 30 20 52-2F 46 69 6C-74 65 72 2F  th 3 0 R/Filter/

00034B00:  00 00 00 50-66 41 48 5A-BE 62 E3 20-C0 85 75 4B     PfAHZ╛bπ └àuK
00034B10:  AC 5C 7F 37-61 48 C1 CD-B4 AD 85 DC-9C A0 C6 84  ¼\⌂7aH┴═┤¡à▄£á╞ä
00034B20:  FB 60 ED B1-21 84 EF 8B-78 A5 C8 6B-6D F1 38 0A  √`φ▒!ä∩ïxÑ╚km±8◙
00034B30:  84 F1 79 C3-6F B6 99 E1-11 80 18 CF-8A 7F D3 A6  ä±y├o╢Öß◄Ç↑╧è⌂╙ª
00034B40:  B1 7D 76 B6-F9 98 35 40-B5 19 81 35-11 8E 9E FC  ▒}v╢·ÿ5@╡↓ü5◄ÄR₧ⁿ
00034B50:  8E 9C 49 43-0A 73 74 61-72 74 78 72-65 66 0A 32  Ä£IC◙startxref◙2
```

Figure 5 – Representation in hexadecimal of a PDF containing a LightNeuron command container

Once this blob of data has been decrypted with AES-256, it reveals a custom structure shown in Figure 6.



```
00000000:  00 00 00 01-00 00 00 11-72 65 70 6C-79 40 65 78   ☺    ◄reply@ex
00000010:  61 6D 70 6C-65 2E 63 6F-6D 00 00 00-01 00 00 00  ample.com   ☺
00000020:  04 00 00 00-1C 43 3A 5C-57 69 6E 64-6F 77 73 5C  ♦   ∟C:\Windows\
00000030:  73 79 73 74-65 6D 33 32-5C 63 61 6C-63 2E 65 78  system32\calc.ex
00000040:  65 00 00 00-00 00 00 00-00                       e
```

Figure 6 – Hexadecimal dump of a decrypted command container

The most interesting fields are:

- Offset 0x08, the email address to which the result of the command is sent.
- Offset 0x1D, the instruction code. It corresponds to one of the function described above.
- Offset 0x25, the first argument. It will be passed to the function represented by the instruction code.

If an email containing such a command container, embedded in a JPG or in a PDF, is sent to a server compromised by LightNeuron, a calculator will be executed on the Microsoft Exchange server.

Cleaning

The cleaning of LightNeuron is not an easy task. **Simply removing the two malicious files will break Microsoft Exchange**, preventing everybody in the organization from sending and receiving emails. Before actually removing the files, the malicious Transport Agent should be disabled. We encourage you to read the full white paper before implementing a cleaning mechanism.

In conclusion

Over the past years, we have published numerous blogposts and white papers detailing the activities of the Turla group, including man-in-the-middle attacks against adobe.com or sophisticated userland malware. However, for now it seems that LightNeuron has taken up the mantle of the most advanced known malware in Turla's arsenal.

By leveraging a previously unseen persistence mechanism, a Microsoft Exchange Transport Agent, LightNeuron allows its operators to stay under the radar for months or years. It allows them to exfiltrate sensitive documents and control other local machines via a C&C mechanism that is very hard to detect and block.

We will continue to track Turla activities closely to help defenders protect their networks.

A full and comprehensive list of Indicators of Compromise (IoCs) and samples can be found in the full white paper and on GitHub.

For a detailed analysis of the backdoor, refer to our white paper *Turla LightNeuron: One email away from remote code execution. For any inquiries, or to make sample submissions related to the subject, contact us at threatintel@eset.com.*

7 May 2019 - 02:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion