TURLA LIGHTNEURON

One email away from remote code execution

Mario Leonardo Salinas

UniPi - ICT Risk Assessment

Table of contents

Table of Contents

Turla

- Turla, aka *Snake*, is Russian-based threat group active since 2004. [4]
- Victims in over 45 countries since 2004:
  - industries
  - goverments
  - military
  - education
  - research
- The group owns a large arsenal of malware and backdoors

LightNeuron

- LightNeuron [2] is a malware specifically designed to target Micrsoft Exchange servers.
- It can *spy* on emails and act as a *fully featured backdoor*
- The attack can only happen if an Exchange server is already fundamentally compromised, *e.g. root permissions*
- Hard to detect at the network level (no standard HTTP(s) communications)

Table of Contents

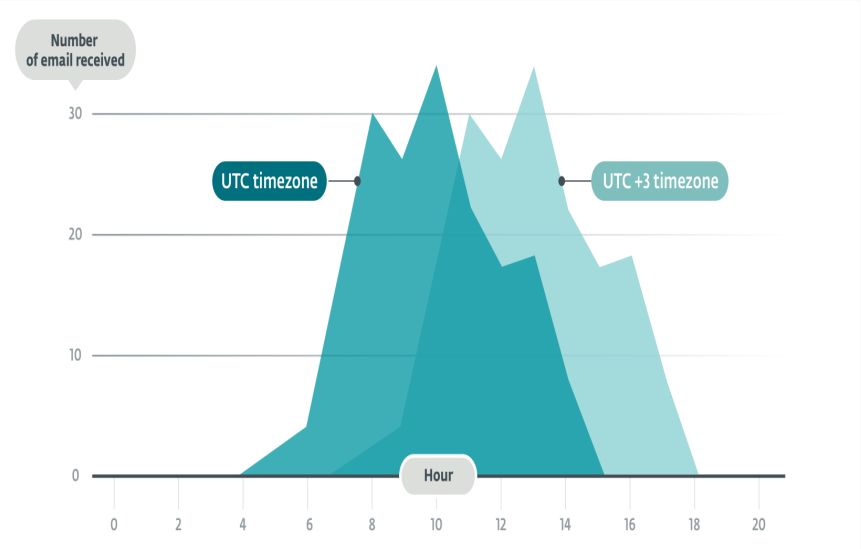
Attacker Profile

- Turla is well known for its advanced custom tools and its ability to run highly targeted operations.
- The group is interested in collecting information from strategic people or organizations.

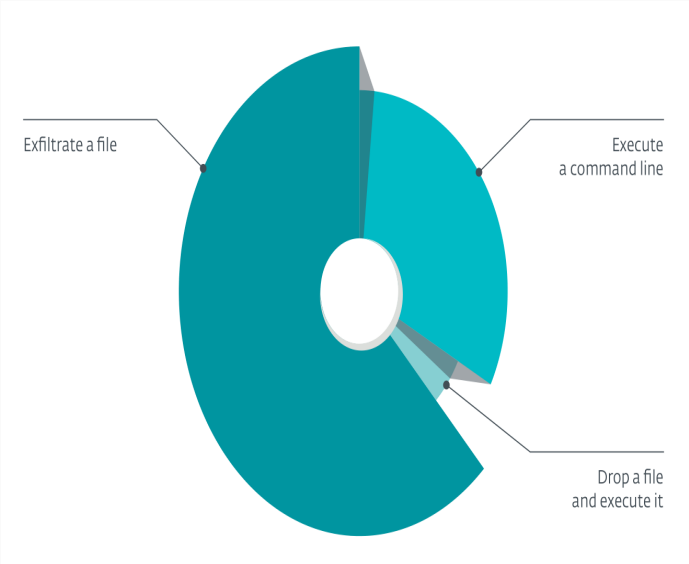
Figure 1: Timeline of important attacks attributed to Turla

Attacker Profile condt

- The operators activity matches a typical 9-to-5 workday in the UTC+3 time zone
- LightNeuron is used mostly to exfiltrate data. The remaining activity is most likely dropping and executing tools to perform lateral movements across the local network



(a) Operators working hours



(b) Distribution of the backdoor commands used by the operators

Victimology

According to ESET, LightNeuron development started before 2014; even if the development occurred several years ago, LightNeuron is still used in recent compromises. These targets are in line with traditional Turla targets:

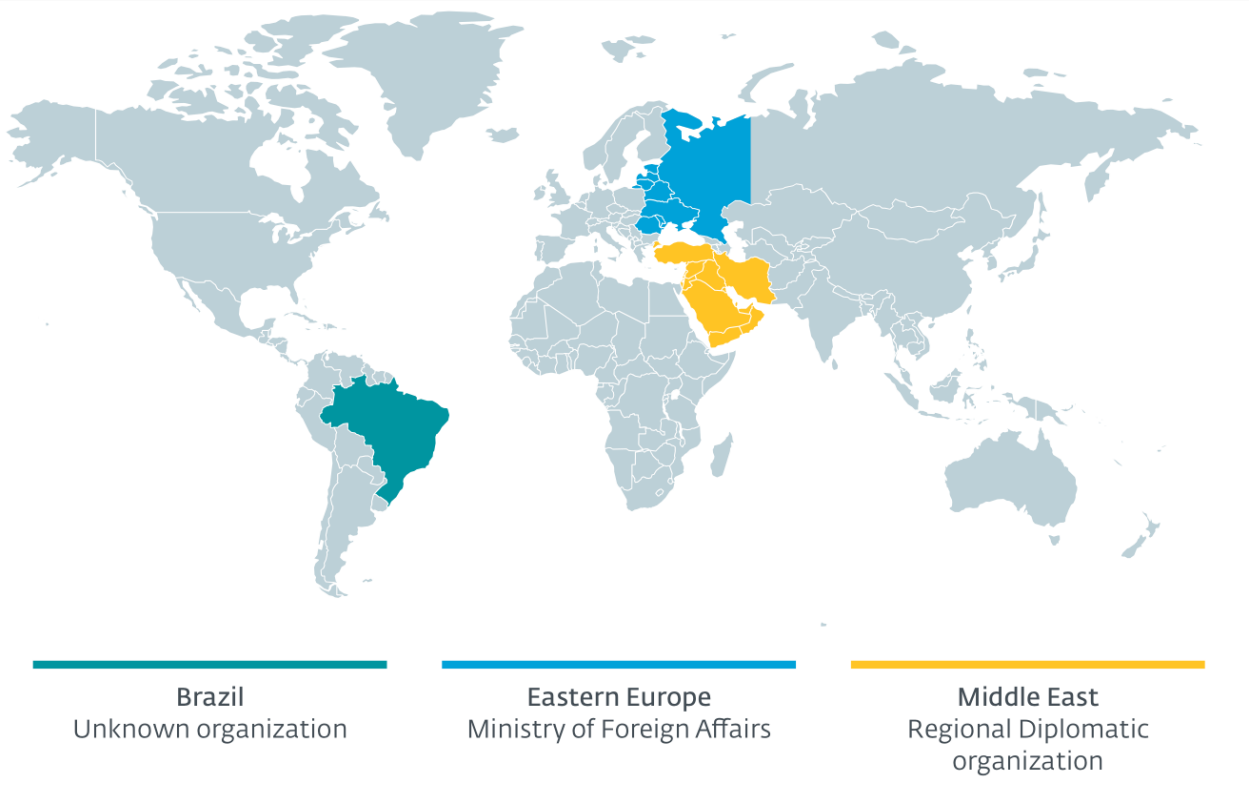


Figure 2: Map of known LightNeuron victims

Table of Contents

Microsoft Exchange Transport Agent

- Transport agents let you install custom software that is created by Microsoft, by third-party vendors, or by your organization, on an Exchange server [3]
- This software can then process email messages that pass through the transport pipeline
- Having a single pipeline means that you can have confidence that every message goes is processed in the same way; however it also means that if an attacker can introduce a transport agent, they have access to *every message*
- LightNeuron it's the first malware that uses a Transport Agent for malicious purposes

LightNeuron components

Two main components comprise LightNeuron:

- a *Transport Agent* that can process and modify all email messages going through the mail server
- a companion 64-bit *Dynamic Link Library (DLL)* containing most of the malicious code.

Turla modus operandi

A tipical Turla attack chain involves:

1. **Initial Reconnissance**, usually a basic first-stage malware or a more powerful one if they deem the victim interesting (Metasploit, Carbon or Gazer). Very specific targets
2. **Credential Gathering**, they move laterally on the network to collect accounts, using stealthy communications and periodically creating new accounts for persistence
3. **Exfiltration**, using an HTTP/email C&C channel and SATCOM IP addresses to obfuscate the traffic content and destination.

LightNeuron Attack Chain (MITRE ATT&CK)

1. **Initial Acces & Privilege Escalation**: Valid Accounts using MITM, spreadpishing emails and watering-hole attacks
2. **Execution**: PowerShell script to install Lightneuron components

3a. **Collection**: Automated Collection of both emails and files

3b. **Command & Control**: email communication using cryptography and steganography

4. **Exfiltration**: Automated and Encrypted exfiltration via C&C interface with optional night scheduling

Initial Access & Privilege Escalation

- Valid Accounts T1078: adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier through social engineering [1]
- The attackers must have privileged administrative access to the server in order to start the attack chain

Execution

- PowerShell T1086: a powershell script is executed
- The malicious Transport Agent is a 32-bit Windows DLL developed in .NET
- The attackers drop this executable in the Exchange folder located in the Program Files folder.

Execution: Transport Agent Installation

Once admin priviledge have been obtained, a PowerShell script is executed to register the DLL as a Transport Agent

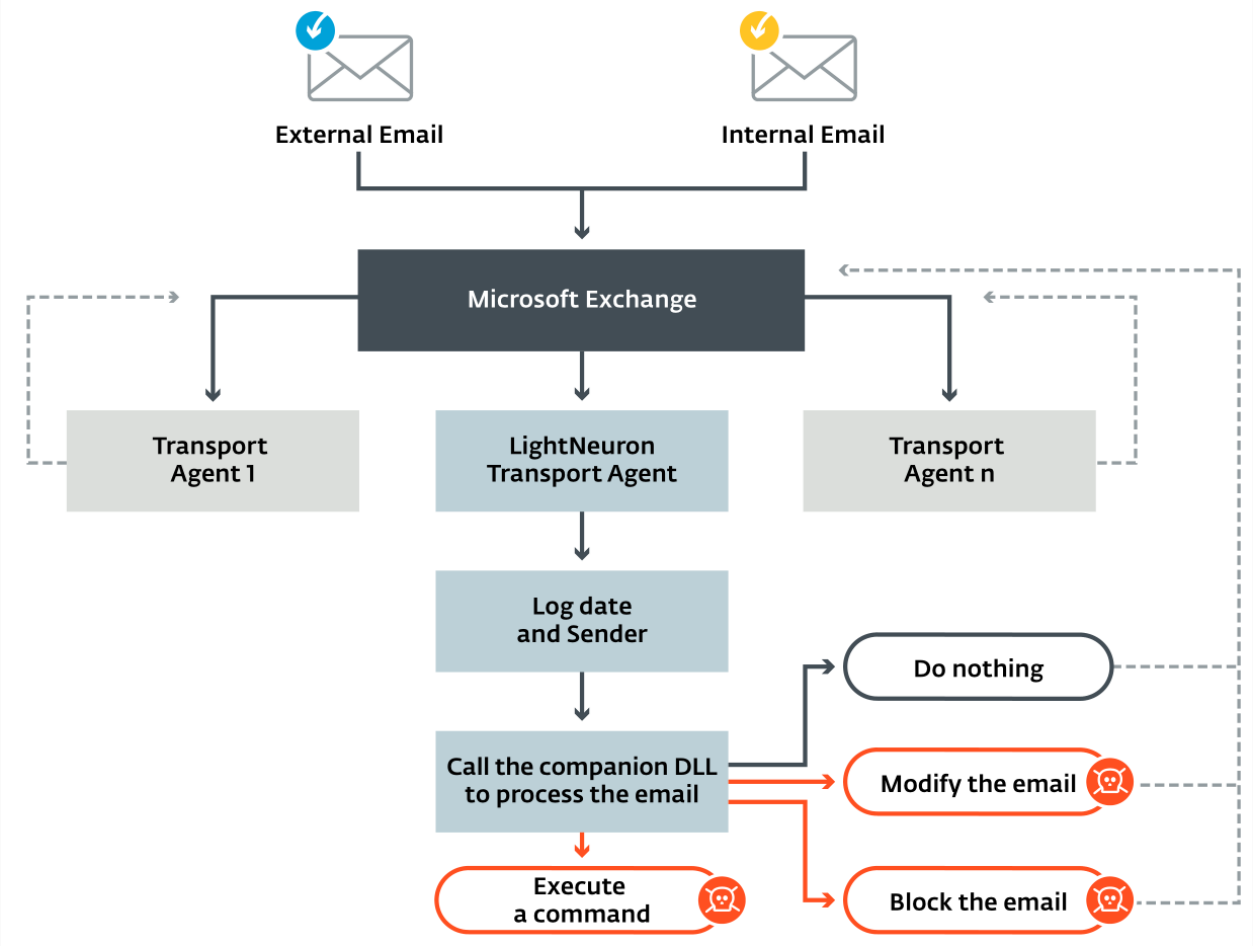


Figure 3: LightNeuron Transport Agent

Execution: Companion Dynamic Link Libray

- The companion DLL is a 64-bit Windows DLL developed in C
- When the Transport Agent loads the DLL, the DLL's main function performs various initialization tasks.
- After initail decription operations, it decrypts the configuration file stored in `%tmp%/winmail.dat`; this filename has been chosen to hide their configuration file in plain sight

The Configuration Files

- The configuration file `winmail.dat` contains various parameters
- An interesting one is `CONFIG_FILE_NAME`
- Once decrypted, this second configuration file contains the rules used to process the emails.

Configuration File Rule System

- The second configuration file contains several class nodes, each one corresponding to a different function (aka handler) implemented in the DLL.
- Each class node contains a set of rules describing conditions using the logical operators AND and OR.
- At the end of the file is the mapping of the class names with the name of the functions in the DLL.

```
<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
```

Configuration File Rule System condt

- These rules are applied to every email processed by the DLL
- This configuration is highly flexible
- There are eleven different handlers implemented in the DLL

Table of Contents

Impact

very high

Table of Contents

Countermeasures

some IoCs are...

Table of Contents

Conclusions

very dangerous rootkit with specific and high profile targets

References i

[1] The MITRE Corporation. MITRE ATT&CK. https://attack.mitre.org/.

[2] Matthieu Faou. Turla LightNeuron, one email away from remote code execution. Technical report, ESET Research.

[3] Microsoft. Transport agents. https://docs.microsoft.com/en-us/exchange/transport-agents-exchange-2013-help.

[4] Edward Millington. Turla. https://attack.mitre.org/groups/G0010/.