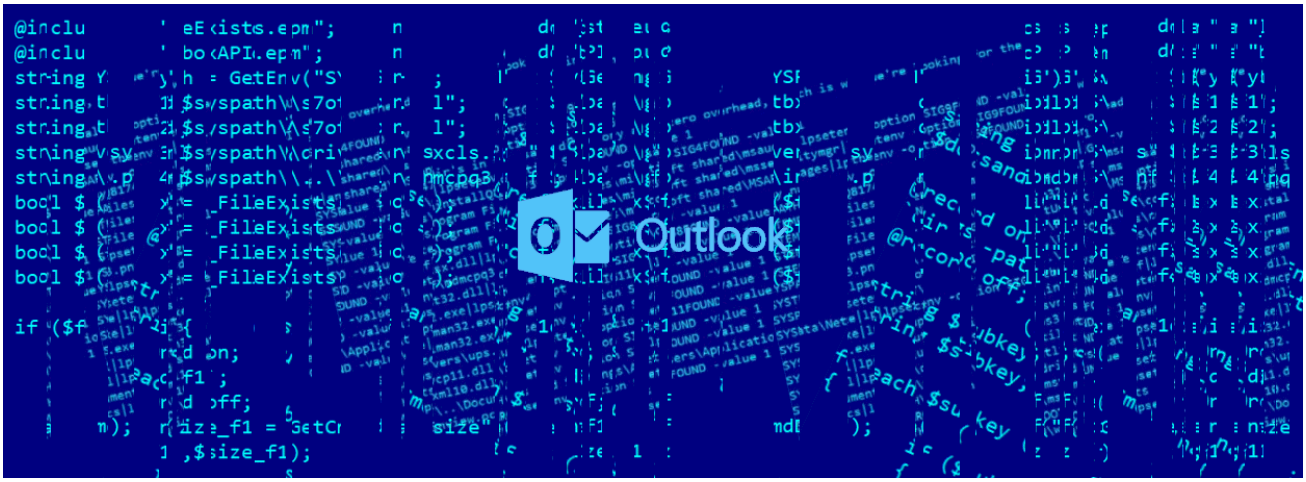
Turla Outlook Backdoor Uses Clever Tactics for Stealth and Persistence

bleepingcomputer.com/news/security/turla-outlook-backdoor-uses-clever-tactics-for-stealth-and-persistence/

Ionut Ilascu

By
Ionut Ilascu

- August 22, 2018
- 05:15 PM
- 0



The Outlook backdoor used by Turla APT group for its espionage operations is an unusual beast built for stealth and persistence, capable to survive in highly restricted networks.

The malware does not connect to a command and control server and can receive updates and instructions via PDF files delivered to the victim's email address. Its control depends only on an email exchange that can originate from any address the attacker chooses.

Security researchers from ESET analyzed the functionality of the utility and managed to learn how it can exfiltrate data without triggering the alarm.

The Turla group counts on this backdoor since at least 2013 and has developed it from a basic utility that only dumped email content to a tool that can execute PowerShell commands with the help of Empire PSInject open-source kit.

In its most recent reiterations, the backdoor is a standalone DLL (dynamic link library) that can install itself and interact with Outlook and The Bat! email clients. It can do this regardless of its location on the disk.

For persistence, Turla developers use COM object hijacking - a common, but effective technique they're well versed in. The method allows the malicious DLL to load each time Outlook loads the COM object. The researchers noticed that this happens when the email client starts.

Stealth is achieved by relying on the legitimate Messaging Application Programming Interface (MAPI) to interact with Outlook and get access to the target's inboxes.

The researchers say that the operator uses the email transport layer to deliver specially crafted PDF documents containing commands for data exfiltration or for downloading additional files. Information is extracted in the same way, by generating a PDF with the data demanded by the attacker, like outgoing emails and message metadata.

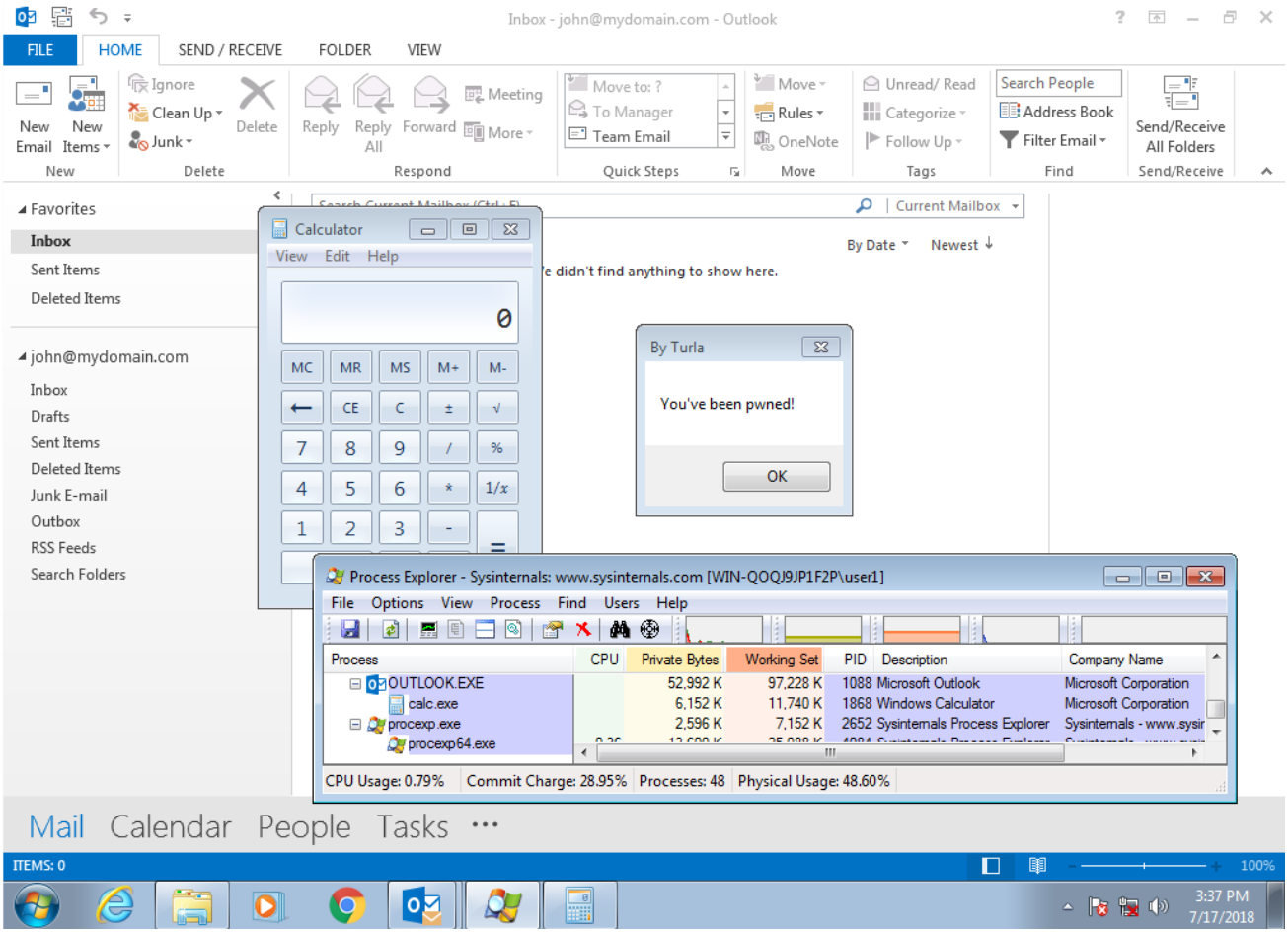
Table 2.	List of backdoor commands
ID	Description
0x10	Not implemented
0x11	Display a MessageBox
0x12	Sleep
0x20	Delete file
0x21	Get file
0x22	Set operator email address (overriding the initial one hardcoded in the DLL)
0x23	Put file
0x24	Run shell command
0x25	Create process
0x26	Delete directory
0x27	Create directory
0x28	Change timeout (interval for emails sent to the operator)
0x29	Run Powershell command (Empire PSInject) – 2018 version of the backdoor
0x2A	Set answer mode – 2018 version of the backdoor

“From the PDF documents, the backdoor is able to recover what attackers call a container in the logs. This is a binary blob with a special format that contains encrypted commands for the backdoor,” ESET analysts explain in a report released today.

“Technically, the attachment does not have to be a valid PDF document. The only requirement is that it includes a container in the right format.”

To hide the email exchanges from the user, the backdoor deletes the messages sent to or received from the attacker. New email notifications may appear for a few seconds, but the message body is not shown to the user, which could pass as a glitch in the client software.

Although they did not get a PDF sample with commands for the backdoor, the researchers were able to create such a document. Once sent to an Outlook inbox controlled by the malware, it recognized the directions and launched the Calculator app in Windows.



The complexity of the Outlook backdoor component is also visible in its encryption algorithm. Just like other tools bearing the Turla signature, the backdoor uses a less common algorithm, which suffered customizations from the developer.

It employs MISTY1 symmetric encryption, created by Mitsubishi Electric in 1995. To the original implementation, Turla added two XOR operations, changed the key generation method. They also shuffled the values in the s7 and s9 non-linear look-up tables, causing all tools that recognize cryptographic algorithms based on the s-table values to break.

With no command and control server to take down, a modus operandi that can pass as legitimate activity to network security components, and modifications to standard functions, Turla's Outlook backdoor proves difficult to fight.

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: