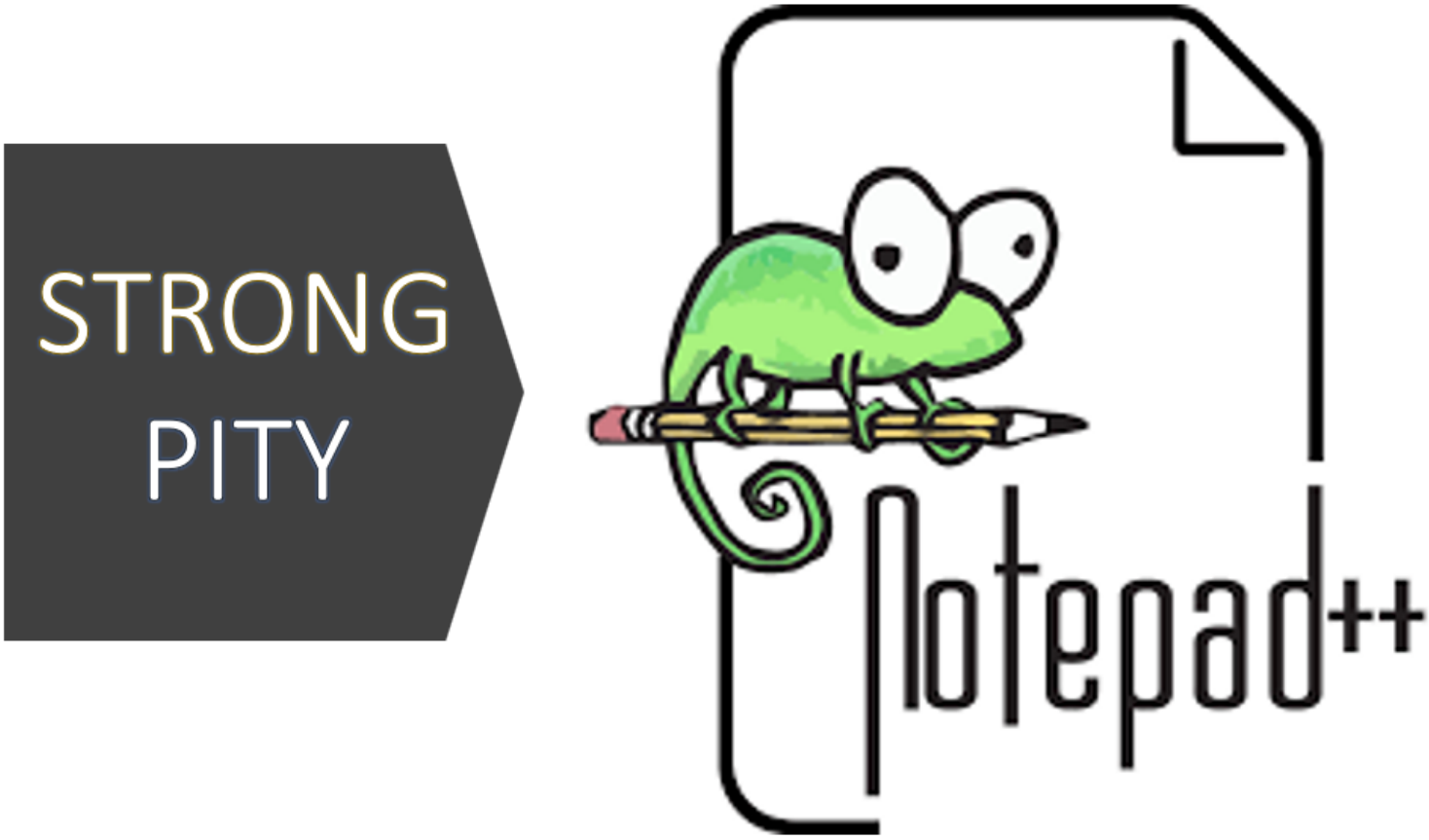
A new StrongPity variant hides behind Notepad++ installation

blog.minerva-labs.com/a-new-strongpity-variant-hides-behind-notepad-installation



The StrongPity actor group has been around since 2012 and employs the same tactics, namely adding backdoors to legitimate software used by specific users, a technique also known as water holing. The group is also referred to as APT-C-41 and PROMETHIUM. In 2016, StrongPity was detected by Kaspersky in a campaign that targeted specific users in Belgium and Italy who were interested in Truecrypt and Winrar software. These APT groups' campaigns are not commonly seen but different research groups have detected several StrongPity campaigns over the years.

Nonetheless, a tweet from blackorbird caught our eye. Here, a StrongPity APT hides its three-stage attack behind a Notepad++ installation.

This attack method is highly efficient since the malware 'hides' itself inside a legitimate tool that is commonly found within organizations. Accordingly, when downloaded from an unofficial URL, the common tool can be exploited– as in this case.

In the first stage, the victim downloads a "Notepad++" setup file and executes it. To make the malicious file more trustable to the victim, the threat actor adds an Original Notepad++ icon:

Figure 1 - Notepad++ icon

When executed, the malicious file creates a new folder named “WindowsData“ under C:\ProgramData\Microsoft and drops three different files on the infected station:

1. npp.8.1.7.Installer.x64.exe – the original Notepad++ installation file under C:\Users\Username\AppData\Local\Temp\ folder.
2. winpickr.exe - a malicious file under C:\Windows\System32 folder.
3. ntuis32.exe – malicious keylogger under C:\ProgramData\Microsoft\WindowsData folder.

After the file drop, the first stage executable runs the legitimate Notepad++ installation, whilst the victim is oblivious to the two malicious files being installed in the background.

In the last phase of the setup.exe stage, it runs winpickr.exe with an “update” argument.

In its first execution by setup.exe, winpickr.exe (with the “update” argument) creates a new service named “PickerSrv” (Display name: FilePicker UI Server) whose purpose is to execute itself at startup and stay persistent on the endpoint.

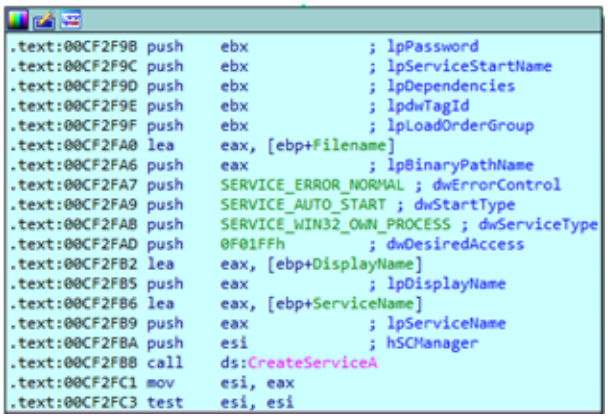


Figure 2 - Service Creation

Figure 3 - New Service Created

A malicious file with such parameters can easily bypass the sandbox, given the fact that it is only creating a service.

When executed as a service (without any parameters), winpickr.exe uncovers its real purpose. Firstly, it immediately executes ntuis32.exe. This malicious file is a simple keylogger that saves users’ keystrokes to a file. The file name follows an inf_loc_ky_%u_v1.0.0_.tbl pattern when %u is a file serial number. These

files are created as hidden system files with read-only attributes and saved in the C:\ProgramData\Microsoft\WindowsData folder that was previously created by the first stage setup.exe file. To remain hidden, the keylogger runs as an overlapped windows (using WS_MINIMIZEBOX style). A new mutex called “Local\WinLoginWait” is also created during the execution process.

While the keylogger runs in the background, winpickr.exe repeatedly checks C:\ProgramData\Microsoft\WindowsData folder for .tbl files. When a file is found containing the attributes of the log files created by ntuis32.exe (hidden, system, and read-only), it connects to its C&C server (https[:]//advancedtoenableplatform[.]com/contact[.]php) for file transfer. After sending the file to the C&C, winpickr.exe deletes the file on the endpoint.

This attack’s pattern is identical to StrongPity’s usual attack flow. The setup.exe and winpickr.exe code is mostly identical to the code from previous campaigns.

This kind of attack is preventable using Minerva Lab’s DLP module.

IOC’s:

Hashes:

- 18107fa059cf457b0b351b683e08e01a3b029ba277f5ca4583a4e3322df21622 - npp.8.1.7.Installer.x64.exe – legitimate notepad++ installer
- 7d3192cad53f934173187f91d8555065d69e09b4f127275a1d47f9f1f9405c5c – setup.exe
- 1380160229604c7d499372dd8192024451291d8bf54e87f19c9e2077b1f165c6 - winpickr.exe
- ed2eae7c0a6cd81d108d71289a49e4a187078a9a6af8400c6a3253d802a7ac95 - ntuis32.exe

Domains:

https://advancedtoenableplatform[.]com – C&C server

Resources:

https://anchorednarratives.substack.com/p/recover-your-files-with-strongpity