‘Purple Fox’ Malware Can Rootkit and Abuse PowerShell

Published: 2019-09-09 · Archived: 2026-04-05 13:10:26 UTC

Exploit kits may no longer be as prolific as it was back when their activities were detected in the millions, but their recurring activities in the first half of 2019 indicate that they won’t be going away any time soon. The Rig exploit kit, for instance, is known for delivering various payloads — such as downloader trojans, ransomware, cryptocurrency-mining malware, and information stealers — whose arrival and delivery techniques are also constantly fine-tuned.

The Purple Fox fileless downloader malware, which was reported to have at least affected 30,000 users last year, is a recent example. Also delivered by the Rig exploit kit, Purple Fox previously used the Nullsoft Scriptable Install System (NSIS) tool to retrieve and execute its payload. We’ve also previously seen Purple Fox downloading and executing cryptocurrency-mining malware.

This new iteration of Purple Fox that we came across, also being delivered by Rig, has a few new tricks up its sleeve. It retains its rootkit component by abusing publicly available code. It now also eschews its use of NSIS in favor of abusing PowerShell, making Purple Fox capable of fileless infection. It also incorporated additional exploits to its infection chain, most likely as a foolproof mechanism to ensure that it can still infect the system. Purple Fox is a downloader malware; besides retrieving and executing cryptocurrency-mining threats, it can also deliver other kinds of malware.

 Figure 1. Purple Fox’s infection chain that abuses PowerShell

Purple Fox’s Infection Chain

Here’s an overview of the infection chain of this new version of Purple Fox:

- Once the user accesses a malicious site hosting one of Rig’s landing pages, there are three methods used to ultimately redirect the user to a malicious PowerShell script that will, in turn, either directly execute Purple Fox’s main component or escalate privileges in order to download and execute a file that would lead to Purple Fox:
  -
  - Through a Flash (.swf) file that exploits CVE-2018-15982, which would lead to a malicious PowerShell script
  - Two .htm files that exploit CVE-2014-6332, a vulnerability in Internet Explorer’s VBScript engine; and CVE-2018-8174, a remote code execution (RCE) vulnerability in VBScript engine affecting various Windows versions (note that these vulnerabilities have long been patched). The .htm file containing an exploit for CVE-2018-8174 redirects to an HTML application (.hta) file.
  - The .hta file, which redirects to a malicious PowerShell script
- If the current user account in the affected system has administrative access, the malicious PowerShell script, posing as an image (.jpg) file, will abuse the application programming interface (API) of *msi.dll* — a dynamic-link library (DLL) that contains functions for installing Microsoft Installer (.msi) packages — in

order to execute and install Purple Fox's main component, which also poses as a randomly named image file.

- If the current user account does not have administration access, the PowerShell script would instead abuse a PowerSploit module (normally used by penetration testers) that will, in turn, exploit two vulnerabilities: CVE-2015-1701 and CVE-2018-8120. Both of these are privilege escalation flaws in Win32k, a multiuser driver in Windows.
- Once the script successfully exploits CVE-2015-1701 and CVE-2018-8120, it will gain elevated privileges, used to abuse *msiexec.exe* (an executable that enables the installation or modification of .msi files via command line) to download and execute Purple Fox's main component.

 Figure 2. Snapshots of code showing: the .hta file, which leads to the malicious PowerShell script (top); how msi.dll is abused (center); and how msiexec.exe is abused to download and execute Purple Fox's main component (bottom)

Purple Fox's Payload Delivery and Rootkit Component

The malware uses *msi.dll*'s MsiInstallProductA function to download and execute its payload — an .msi file that contains an encrypted shellcode as well as 32-bit and 64-bit versions of the payload. Once executed, the malware restarts the system and uses the *PendingFileRenameOperations* registry (responsible for storing names of files that the OS will rename when it restarts) to rename its components.

It would then use its rootkit capability (hiding its files and registry entries) after the system is restarted. It creates a suspended *svchost* process and injects a DLL that will then create a driver with the rootkit capability. Before proceeding further to the payload, it sets up the following in the injected DLL: a driver file (*dump_{random hex}.sys*), which is responsible for the rootkit capability; and its main component in the form of a DLL file (*Ms{random hex}App.dll*).

Unlike the previous version of Purple Fox, however, this new iteration abuses an open-source code to enable its rootkit components, which includes hiding and protecting its files and registry entries. Also of note is the way this new version of Purple Fox abuses a file utility software to hide its DLL component, which deters reverse engineering or cracking attempts.

 Figure 3. Snapshot of code showing how Purple Fox abuses an open-source code to hide and protect its components and registry entries

Best practices and Trend Micro solutions

Purple Fox exemplifies what we're seeing in this year's threat landscape: a multilayered approach to how it "lives off the land." Purple Fox's emphasis on leaving a small footprint is also notable, with its abuse of legitimate tools and use of fileless techniques (e.g., DLL injection). Purple Fox also uses exploits for vulnerabilities with available patches. Its attack chain, for instance, exploits a vulnerability that was disclosed and patched five years ago. This

highlights the significance of patching, especially for enterprises. And given how Purple Fox can deliver virtually any kind of threat, a defense-in-depth approach to securing online infrastructures is important. Here are some best practices that users and organizations can adopt:

- Enforce the principle of least privilege by restricting and securing the use of tools reserved for system administrators.
- Regularly patch and update (or employ virtual patching for legacy or embedded systems or software).
- Deploy additional mechanisms that provide additional layers of security, such as behavior monitoring, which thwarts malware-related routines from being executed in the system; sandboxes, which can quarantine malicious files and further analyze suspicious behaviors; and firewalls and intrusion prevention and detection systems that can deter incursions or flag data exfiltration attempts.
- Cultivate cybersecurity awareness at home and in the workplace, especially against email-borne threats that fileless threats could use as attack vectors or entry points.

Trend Micro endpoint solutions such as the Smart Protection Suites and Worry-Free Business Security solutions, which have behavior monitoring capabilities, can protect users and businesses from these types of threats by detecting malicious files, scripts, and messages as well as blocking all related malicious URLs. Trend Micro Apex One™ protection employs a variety of threat detection capabilities, notably behavioral analysis, which protect against malicious scripts, injection, ransomware, memory and browser attacks related to fileless threats.

The Trend Micro™ Deep Discovery Inspector solution protects customers from Rig exploit kit and Purple Fox via these DDI rules:

- 3286: RIG - Exploit Kit - HTTP (Request)
- 4220: RIG - Exploit Kit - HTTP (Request)

The indicators of compromise (IoCs) are in this ***appendix***.
