Scranos

Threat: **Rootkit**

Author: **Jeffrey Farnan** Date Originally Published: **February 22th, 2021**

1. SUMMARY

- A new rootkit was found in 2019 called Scranos, first detected in China but now being pushed out to other parts of the world. This rootkit steals user passwords and account payment methods which are stored in the victim's browser. Scranos poses as legitimate software such as ebook readers, video players or anti-malware products. Scranos infects Windows computers gaining persistent access even after a restart. The aim of this rootkit is to infect as many devices as possible, steal victim information, perform advertising abuse and also be used as a platform for third party malware.

2. MALWARE FAMILY

- **Type** = Rootkit.
- **Sub-type** = Spyware.

- A rootkit can be thought of as special software with built-in tools to create a second administrator on a targeted system, while hiding itself from other admins. In most cases, rootkits don't do much damage, apart from modifying the operating system. The main function of the rootkit is to keep the malware that it's linked to from being discovered. The malware does the actual damage.

- The primary functions of rootkits are:
  - To remain undetected, making it hard for security analysts to detect.
  - For the rootkit to remain persistence, surviving removal attempts and reboots.
  - Hide malware linked to the rootkit, which may be part of a larger sustained attack.
  - Provide the attacker access to the machine, often via backdoors.
  - The rootkit can escalate the privilege level which the malware operates.
  - The compromised machine can be used as a member of a bot.

- The four main types of rootkits are Kernel rootkits, User mode rootkits, Memory rootkits and Bootloader rootkits. Scranos is a kernel mode and cross platform rootkit, it injects the system with high level malicious payloads known for spying and stealing user data.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = China.
- **First seen date/period** = 2019.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = January 23th, 2021.

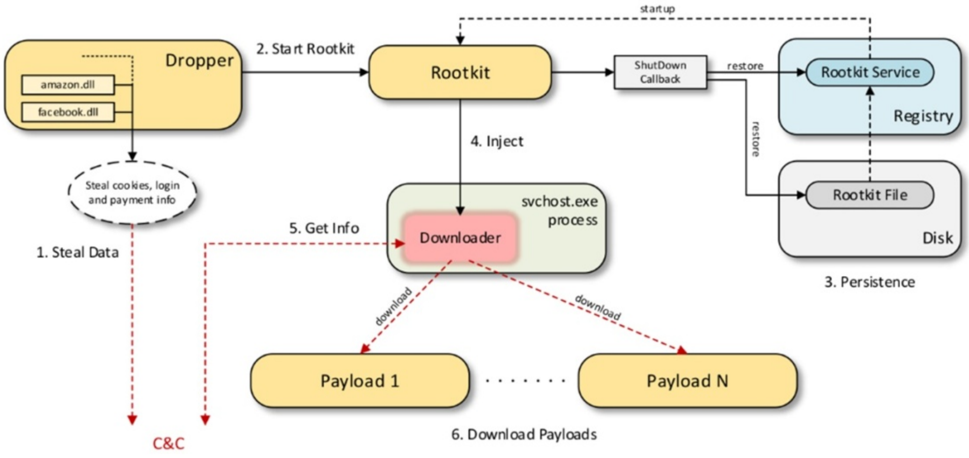
4. MALWARE HISTORY

- Scranos was first seen in 2019, it comes from a long rootkit history, which began by first been theorized in the early 80's before eventually coming into existence in UNIX systems. Windows rootkits came much later in the late 90's, the first seen was NTRootkit developed by security researcher Greg Hoglund to see what a rootkit could do on a windows system. Other rootkits followed He4Hook, Hacker Defender and Vanquish improving on what rootkits could do.
- Attempts have been made in the past to stop the infiltration of rootkits onto a system. In 2006 Microsoft made a major change, introducing Kernel Patch Protection (KPP) where every 3rd party vender had to have digitally sign drivers. This reduced rootkit infections for many years. Rootkits such as Scranos have evolved over time and able to overcome these security challenges, by gaining fraudulent signed drivers, and bypassing these security measures.
- Rootkits of today are known for accomplishing stealth and persistence, they are a modular design and can be linked to other types of malware such as bots and are used in wider cyberattacks.

5. MALWARE DESCRIPTION

Scranos was first detected in China in 2019 by security researchers from Bitdefender, who now see it spreading to other countries making it a global cyberattack. The researchers call this attack a work in process, which seems to be evolving, new components being developed and minor improvements being made.

- The main component of Scranos is the dropper which executes the malicious software to install the rootkit. This rootkit is a digitally-signed rootkit driver, issued by a Chinese company. Cybercriminals may have obtained the original digital code-signing certificate or may have illegally compromised it. When the dropper is installed, it tries to communicate with its Command and Control (C&C) server and downloads other malicious payloads.



The main targets are the popular browsers such as Internet explorer, Chrome and apps like Facebook, Amazon and YouTube. The Data gathered are cookies, login credentials, payment information are all collected and sent back to the C&C server and then waits for additional instructions.

- The payloads carry other malicious modules:
  - It has been observed this malware aggressively promoting four different YouTube videos on different channels to users, in a bid to generate video revenue.
  - Another downloadable component sends friend requests to other users, and also spams contacts with links to malicious Android apps.
- The main functions of Scranos are:
  - Injects adware into browsers and infiltrating browser history.
  - Install browser extensions, launching malicious adware.
  - Steals user credentials for the users account on Steam.
  - Sends friend requests from the users Facebook account to other accounts.
  - Display ads or muted YouTube videos to users via Chrome browser.
  - Install and run other malicious payloads.

6. POTENTIAL CUSTOMER DEFENSE

Scranos is unlike many other rootkits very complex and persistent, and notoriously difficult to detect. Here is helpful information to prevent, detect and remove rootkits:

- **Prevent a rootkit malware attack.** There are many ways of preventing rootkit malware being installed on your system:
  - Update your software, Windows and other companies release regular updates to fix bugs and vulnerabilities. Older programs may be exploited by cybercriminals taking advantage of vulnerabilities.
  - Ensure you have stricter policies in place which only allow 3rd party drivers which are signed and verified.
  - Use next-gen antivirus scanners, which can leverage modern security techniques like machine learning-based anomaly detection and behavioural heuristics.
- **Detect rootkits:** Scan your systems with antivirus software, these can detect and remove application level rootkits. Other signs to look out for:
  - Rootkits are very hard to detect, one way attackers communicate is via the internet, so one place to start is reviewing is the TCP/IP packets travelling to and from that device. You should have a logging solution which alerts you to any usual traffic. If a system is misbehaving such as excessive CPU or internet bandwidth usage could be an indicator of a rootkit infection.
  - One of the things that make Scranos stand out is its use in social activity. A user who notices strange activity from Facebook or YouTube that they didn’t initiate, may be a sign of someone controlling their account.

  - Scan your systems with antivirus software, these can detect and remove application level rootkits, but ineffective against kernel, bootloader, or firmware rootkits.

- **Removal Tools:** There is a manual method which can be time consuming and usually a specialist dealing in computer forensics is needed. Another option, considered the automatic method uses rootkit removals tools and Kernel level scanners. Malicious code can only be detected by kernel level scanners when the rootkit is inactive, this means all system processes have to be stopped. The most effective method is to reboot the computer in safe mode and scan with a variety of kernel level scanners, which should detect and remove any infections.

Research Sources:

https://blog.malwarebytes.com/how-tos-2/2020/01/how-to-prevent-a-rootkit-attack/

- https://heimdalsecurity.com/blog/scranos-malware-rootkit/
- https://www.pcrisk.com/removal-guides/14887-scranos-rootkit

Disclaimer: All opinions expressed in this article are the opinions solely of the author.