SORINTSEC

THREAT HUNTING

LAB

ClickFix to StealC: ResiLoader weaponizes pcdhost.sys BYOVD driver to achieve ring-0 code execution.

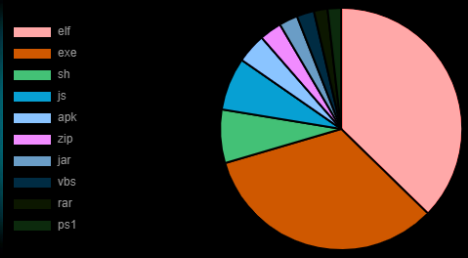
PUBLIC

Index

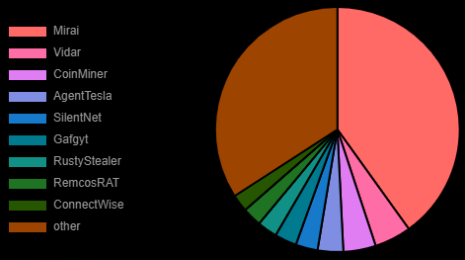
Global Weekly Threat Overview

Threat actors are abusing Microsoft Teams voice calls by impersonating corporate IT support staff to trick employees into installing the EtherRAT malware, giving attackers initial access to corporate networks. After convincing the victim to grant remote control via Microsoft Teams' built-in screen-sharing feature, the attacker guided them through installing legitimate remote-access tools, including HopToDesk and AnyDesk. After establishing remote access, they downloaded and executed a malicious MSI installer (v7.msi) from camorreado[.]click. The MSI acts as a malware loader, downloading a legitimate Node.js runtime, decrypting embedded payloads, and ultimately launching EtherRAT. EtherRAT is a cross-platform remote access trojan written in Node.js that gives attackers full control over compromised systems.

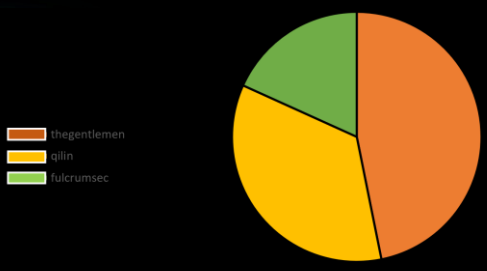
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Researchers identified what they believe is the first documented case of a ransomware operation, JadePuffer, conducted entirely by a large language model (LLM) agent. According researchers, JadePuffer used an autonomous AI agent for reconnaissance on the target, to steal credentials, move laterally, establish persistence, escalate privileges, and to encrypt data. After obtaining code execution through CVE-2025-3248, the AI agent dumped Langflow's PostgreSQL database, collected host information, searched for environment variables and sensitive files, retrieved credentials, and enumerated a MinIO object store.

Global Weekly Notable One

Defense Evasion: Impair Defenses

Last ClickFix campaign observed utilizes sophisticated social engineering to trick users into infecting their own devices through fake Google and Cloudflare verification pages. Attackers employ various lures, such as fake reCAPTCHAs, Google Meet "audio fix" prompts, and unauthorized login alerts. These pages often use countdown timers to create a sense of urgency, pressuring victims into copying and pasting a malicious PowerShell command into their terminal to "verify" themselves.

Once executed, the command downloads payloads from Cloudflare R2 buckets or direct IPs, delivering various malware families like StealC, Remus, and ResiLoader. Notably, ResiLoader weaponizes the legitimate pcdhost.sys (OPSWAT AppRemover) driver in a Bring Your Own Vulnerable Driver (BYOVD) attack. This driver is used to terminate over 140 security-related processes, effectively stripping the system of defenses before deploying the final infostealer payload.

Threat Hunting Activity

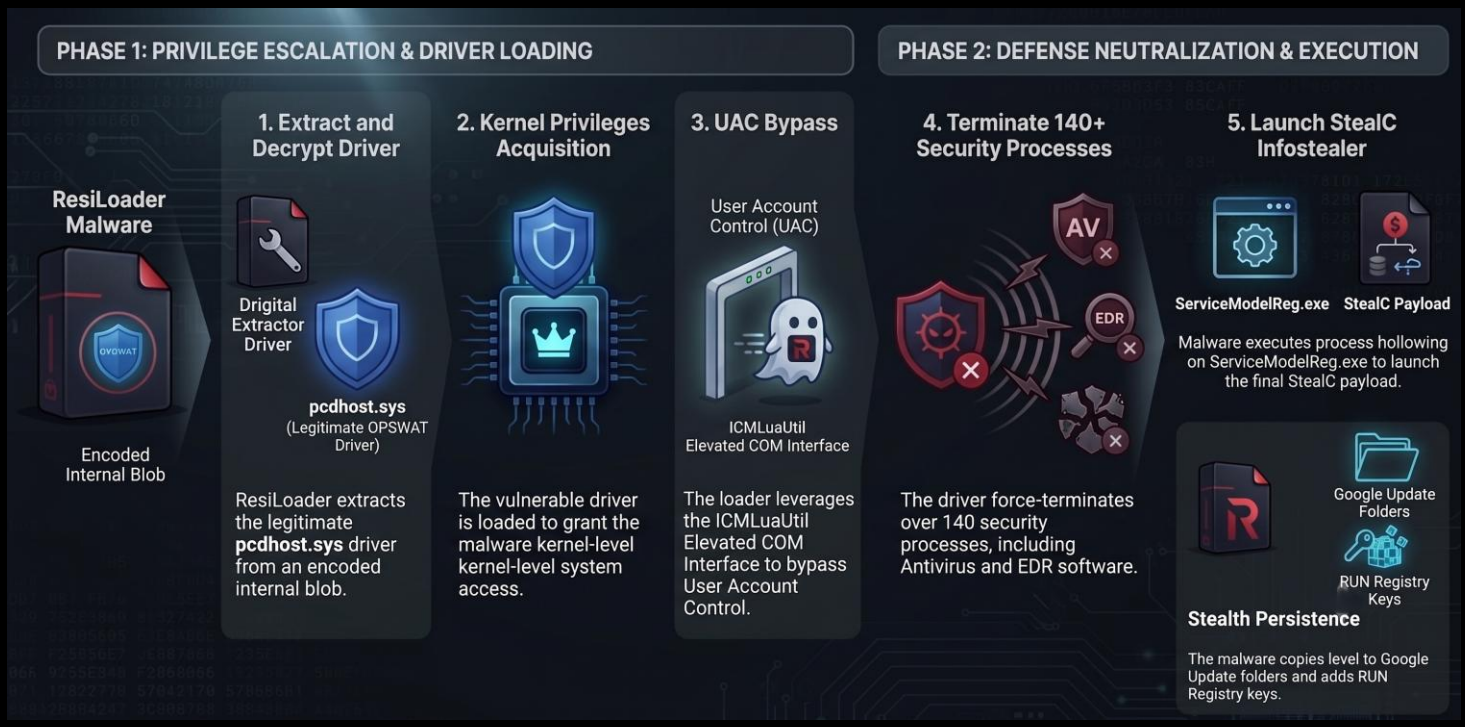
TACTIC Defense Evasion

TECHNIQUES T1629 – Impair Defenses

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may span both native defenses as well as supplemental capabilities installed by users or mobile endpoint administrators.

Threat Hunting Activity

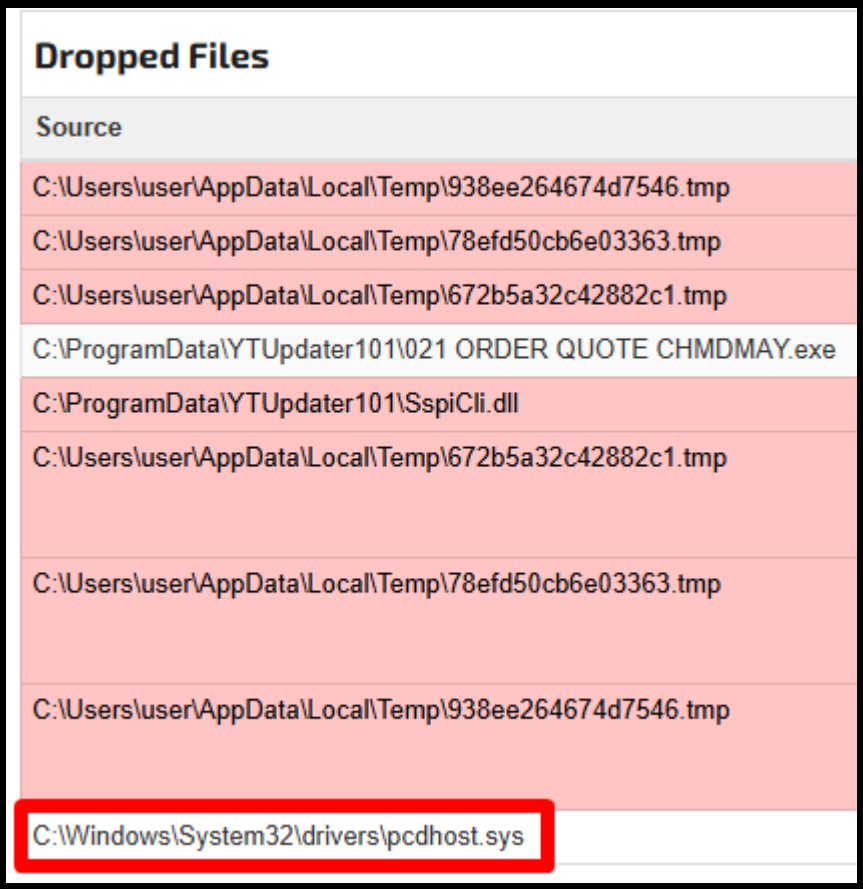
ResiLoader employs a Bring Your Own Vulnerable Driver (BYOVD) technique to neutralize endpoint defenses. The loader extracts and decrypts a legitimate but vulnerable driver called pcdhost.sys, which belongs to the OPSWAT AppRemover utility (now the CleanUp Module).



Because this driver is natively designed to terminate and uninstall software that is otherwise difficult to remove, ResiLoader weaponizes these capabilities.
Once the driver is loaded, ResiLoader leverages its kernel-level privileges to terminate more than 140 processes associated with antivirus (AV) and endpoint detection and response (EDR) software. This surgical removal of security products ensures the malware can operate without interference. With the system's defenses effectively stripped, the loader proceeds to its final stage: performing process hollowing on ServiceModelReg.exe to execute the StealC infostealer payload.

Threat Hunting Activity

BYOVD hunting matters because attackers load legitimately signed but vulnerable kernel drivers to gain ring-0 code execution, bypassing kernel-mode code signing enforcement. Once loaded, these drivers expose IOCTLs that let userland processes perform arbitrary kernel memory read/write, terminate protected processes to blind EDR and AV, or escalate token privileges.



Dropped Files

Source
C:\Users\user\AppData\Local\Temp\938ee264674d7546.tmp
C:\Users\user\AppData\Local\Temp\78efd50cb6e03363.tmp
C:\Users\user\AppData\Local\Temp\672b5a32c42882c1.tmp
C:\ProgramData\YTUpdater101\021 ORDER QUOTE CHMDMAY.exe
C:\ProgramData\YTUpdater101\SspiCli.dll
C:\Users\user\AppData\Local\Temp\672b5a32c42882c1.tmp
C:\Users\user\AppData\Local\Temp\78efd50cb6e03363.tmp
C:\Users\user\AppData\Local\Temp\938ee264674d7546.tmp
C:\Windows\System32\drivers\pcdhost.sys

PUBLIC