THREAT HUNTING

LAB

WEEK 28/07/2025 - 01/08/2025

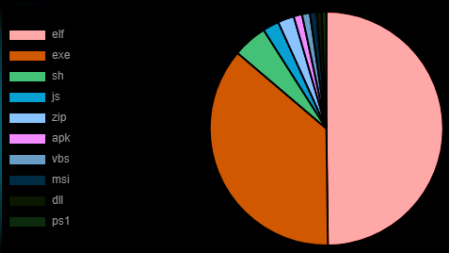
PUBLIC

Index

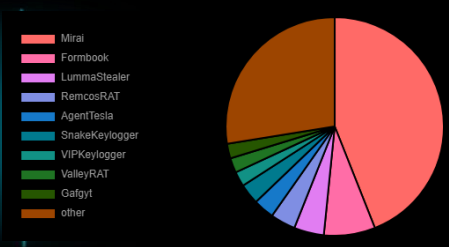
Global Weekly Threat Overview

Scattered Spider hackers have been aggressively targeting virtualized environments by attacking VMware ESXi hypervisors at U.S. companies in the retail, airline, transportation, and insurance sectors. According to the Google Threat Intelligence Group (GITG), the attackers keep employing their usual tactics that do not include vulnerability exploits but rely on perfectly executed social engineering "to bypass even mature security programs. “Scattered Spider (also known as UNC3944, Octo Tempest, 0ktapus) is a financially motivated threat group specialized in social engineering to a level that it can impersonate company employees using the appropriate vocabulary and accent.

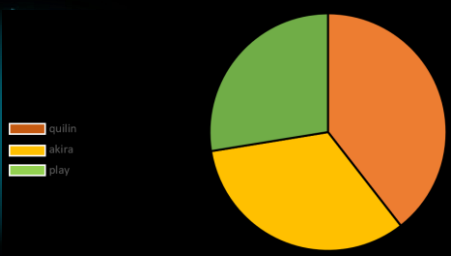
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Aeroflot, Russia's flag carrier, has suffered a cyberattack that resulted in the cancellation of more than 60 flights and severe delays on additional flights. Although official sources from Russia, like the General Prosecutor's Office, did not attribute the attack to specific threat groups or even origin, responsibility was taken by Ukrainian and Belarusian hacktivist collectives 'Silent Crow' and 'Cyberpartisans BY.'According to announcements made on X and on Telegram, the hackers claimed to have infiltrated Aeroflot's IT infrastructure for over a year, mapped it extensively to pinpoint all valuable resources, and then "destroyed" it.

Global Weekly Notable One

Masquerading: Defense Evasion

In a Remcos malware campaign observed in June 2025, attackers used a specialized trick to make their files look like they belonged to official Windows system folders. Specifically, they created fake directories like C:\Windows[] \SysWOW64 (with extra space) and used the \\?\ NT Object Manager path prefix. This allowed them to bypass normal security checks and hide their files as if they were genuine Windows folders.

After the initial infection steps, the malware ensures it stays on the system by creating scheduled tasks and weakening User Account Control (UAC) through changes in the registry. It then injects itself into other processes and communicates with its C2 server using an unusual network port. This method gives attackers complete control over the infected system, enabling them to steal data and record keystrokes while making it difficult to distinguish their activity from normal system operations.

Threat Hunting Activity

TACTIC

Defense Evasion

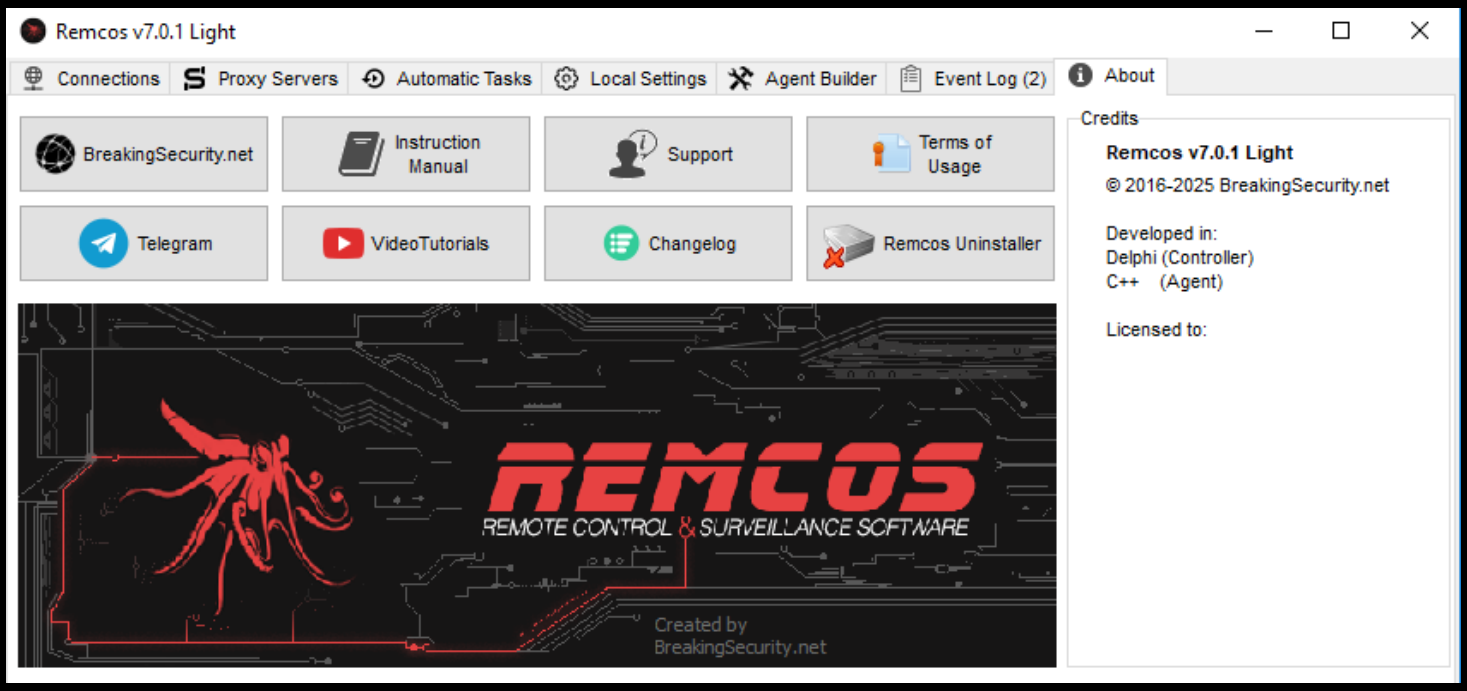
TECHNIQUES

T1036 – Masquerading

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

Threat Hunting Activity

Remcos is a remote access trojan (RAT) designed to infect Windows systems and provide attackers with extensive control over compromised devices. Typically distributed through phishing emails, Remcos facilitates unauthorized activities including password theft, keystroke logging, screen and webcam capture and file manipulation. The malware employs advanced evasion techniques, such as process injection and persistent installation, to avoid detection. Newer variants may operate solely in memory, further enhancing their stealth and making identification and removal significantly more challenging.

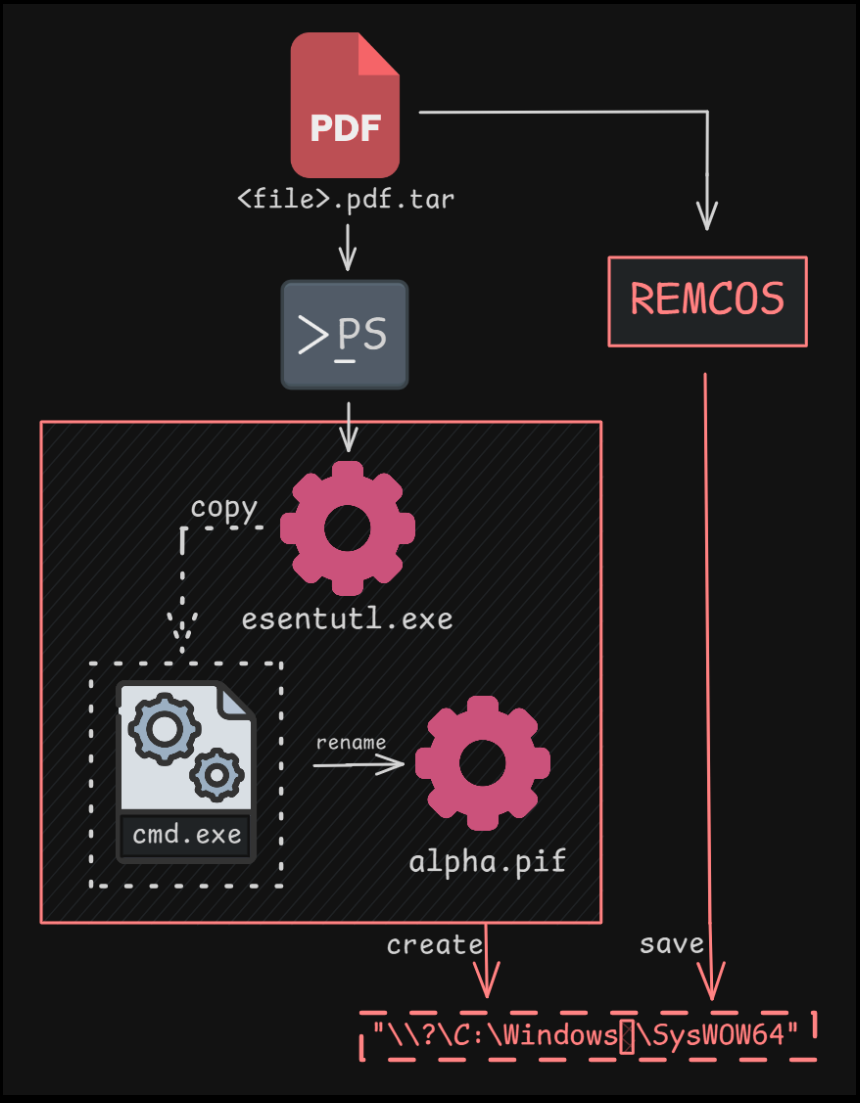


Remcos GUI

Remcos can be used legitimately by IT administrators for authorized remote monitoring and management of company-owned devices in accordance with organizational policies and legal requirements. Conversely, cybercriminals illicitly exploit Remcos for clandestine surveillance, data theft, unauthorized system access and the deployment of further malware.

Threat Hunting Activity

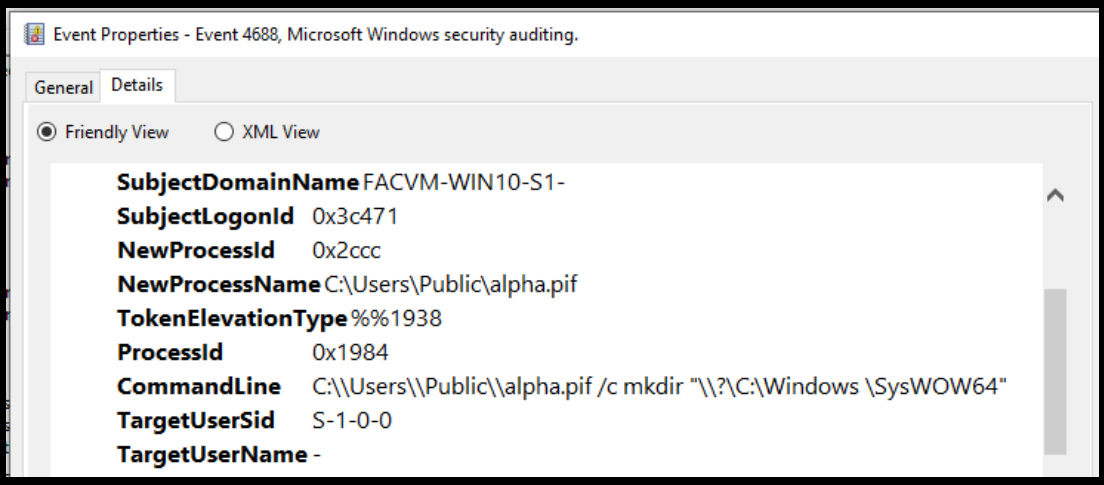
After the first stagers, malware enable the creation of a counterfeit Windows directory by exploiting path-parsing bypass methods, including the use of the NT namespace prefix “\\?\”. The image shows part of the simplified execution chain: the malware exploit a Microsoft-signed application to copy the legitimate cmd.exe instance to a different folder, renaming it in order to be used to generate the target spoofed folder. Once created this folder the malware will hide in it and perform process injection to executing.



Simplified infection chain

Threat Hunting Activity

Detection can be made on EID 4688 looking for relates behavioral patterns linked to this campaign.



EID 4688

PUBLIC