PS1Bot: Multi-Stage Malware Framework Targeting Windows Systems - Ag

Data: 2025-08-14 18:38:35

Autor: Inteligência Against Invaders

Cisco Talos researchers have uncovered an aggressive malware campaign active since early 2025,

deploying a sophisticated multi-stage framework dubbed PS1Bot, primarily implemented in

PowerShell and C#.

This threat actor leverages malvertising and SEO poisoning to distribute compressed archives with file names mimicking legitimate search queries, such as “chapter 8 medicare benefit policy manual.zip” or “pambu panchangam 2024-25 pdf.zip.”

Upon extraction, victims encounter a JavaScript file named “FULL DOCUMENT.js,” which contains obfuscated VBScript acting as a downloader.

This script fetches a JScript scriptlet from an attacker-controlled server, initiating environmental setup by writing a PowerShell script to C:ProgramData (e.g., ntu.ps1) and executing it to poll a command-and-control (C2) server.

The polling mechanism derives a unique URL from the system’s C drive serial number, repeatedly invoking Invoke-Expression (IEX) to run retrieved PowerShell content in-memory, minimizing disk artifacts and enhancing stealth.

This modular design echoes prior threats like AHK Bot and overlaps with Skitnet infrastructure, including shared C2 domains and code patterns, suggesting evolutionary ties to these families without direct binary delivery observed in analyzed chains.

Advanced Modules for Espionage and Theft

PS1Bot’s flexibility stems from its array of deployable modules, each tailored for specific malicious functions while incorporating runtime logging via HTTP GET requests with URL parameters for status updates.

An antivirus detection module queries Windows Management Instrumentation (WMI) to enumerate installed security products like Windows Defender, relaying results to the C2 for reconnaissance.

Following this, a screen capture module dynamically compiles C# code using PowerShell’s Add-Type cmdlet, generating in-memory assemblies to produce bitmap screenshots stored temporarily in %TEMP% and %APPDATA%, then Base64-encoded and exfiltrated via HTTP POST, with files promptly deleted to evade detection.

The “grabber” module, a potent information stealer, targets browser data from over 40 variants including Chrome, Edge, and Brave, alongside cryptocurrency extensions like MetaMask and Ledger, staging files in %TEMP% for compression and upload.

It extends to local wallet applications such as Exodus and Electrum, employing embedded wordlists spanning English, Czech, and crypto-specific seed phrases to scan file systems for sensitive documents matching criteria like extensions (.txt, .pdf) and sizes under 100KB, identifying passwords or wallet seeds for separate exfiltration.

Keylogging functionality mirrors this approach, compiling C# for SetWindowsHookEx() hooks to capture keystrokes, mouse events, and clipboard data, transmitting logs in HTTP POST bodies.

A system survey module, “WMIComputerCSHARP,” gathers domain details via WMI queries and environment variables, aiding in targeting high-value networks.

Persistence is achieved by creating randomized directories in %PROGRAMDATA%, housing obfuscated PowerShell scripts fetched from C2 paths like /transform, linked via LNK files in the Startup folder for reboot survival, complete with mutex handling to prevent duplicate executions.

Evolving Threat Landscape

Throughout 2025, PS1Bot has demonstrated rapid evolution, with frequent new samples and module updates observed, indicating active development.

Its in-memory execution and minimal persistence artifacts complicate forensic analysis, while overlaps with AHK Bot’s C2 derivation and modular polling, plus Skitnet’s PowerShell similarities, point to a maturing ecosystem of Windows-targeted threats.

According to the report, Talos assesses high confidence in additional undisclosed modules, enabling adversaries to adapt swiftly for espionage, financial theft, or lateral movement.

Organizations should monitor for anomalous PowerShell activity, unusual WMI queries, and malvertising lures to mitigate this persistent campaign.