SORINT SEC

THREAT HUNTING

LAB

The Diagnostic Loophole: Extract Secure Credentials from Windows Kernel Live Dumps

PUBLIC

Index

Global Weekly Threat Overview

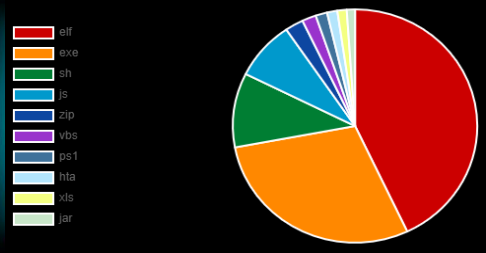
Global Weekly Notable One

Threat Hunting Activity

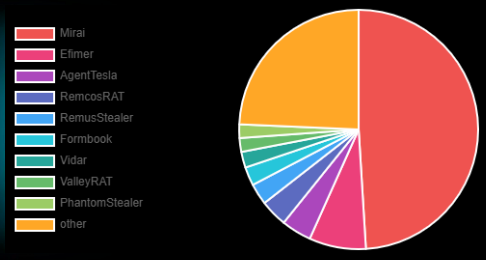
Global Weekly Threat Overview

A new ClickFix variant dubbed TerminalFix uses fake Cloudflare CAPTCHA prompts on compromised websites to trick victims into executing malicious PowerShell commands in Windows Terminal. Unlike typical ClickFix attacks that often lead to infostealer malware infections, this campaign uses a multi-stage intrusion chain that ultimately gives attackers a reverse tunnel into the victim's internal network. TerminalFix differs from normal ClickFix attacks in that it directs users to Windows Terminal or PowerShell, which enables successful execution of more complex, multi-line scripts.

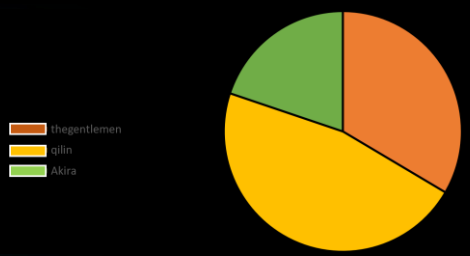
Top 10 file types



Top 10 malware family

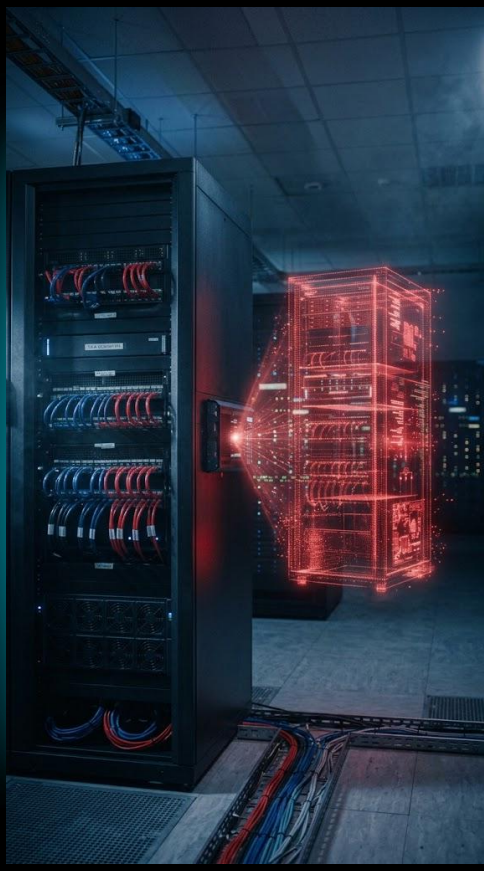


Top 3 Ransomware Group



Phishing actors are abusing the legitimate Faronics Deploy endpoint-management platform to gain remote administrative control over victim computers and install the ScreenConnect remote support software. In activity observed between July 21 and August 20, Faronics-themed lures reached more than 457 endpoints via emails disguised as invoices, tax documents, or other business files. Faronics Deploy is a cloud-based endpoint management platform that allows IT administrators to remotely enroll and manage computers, deploy software, and execute scripts.

Global Weekly Notable One



Credential Access: OS Credential Dumping

An LSASS memory dump captures a snapshot of the LSASS process to extract cached credentials like NTLM hashes or Kerberos tickets. Because LSASS requires administrative or SYSTEM privileges to access, attackers use post-exploitation tools to generate these files for safer offline analysis. Built-in methods include using Task Manager, running the MiniDump function in comsvcs.dll via rundll32, or abusing silent process exit mechanisms via WerFault.exe.

Adversaries also leverage Sysinternals ProcDump or offensive tools like Mimikatz and LaZagne to obtain these dumps. Notably, on Windows 11 and Server 2025, attackers can bypass direct process protections by running a PowerShell command to trigger a kernel live dump, extracting the LSASS process memory from the resulting diagnostic file without ever touching the active process directly.

Threat Hunting Activity

TACTIC

Credential Access

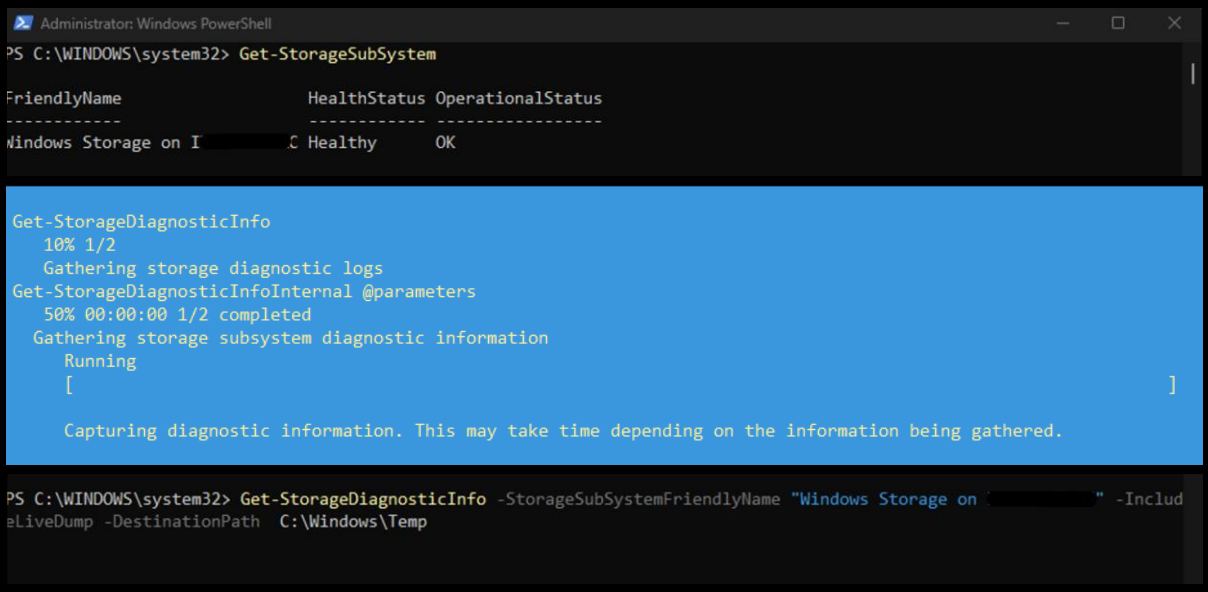
TECHNIQUES

T1003 – OS Credential Dumping

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password. Credentials can be obtained from OS caches, memory, or structures.[1] Credentials can then be used to perform Lateral Movement and access restricted information.

Threat Hunting Activity

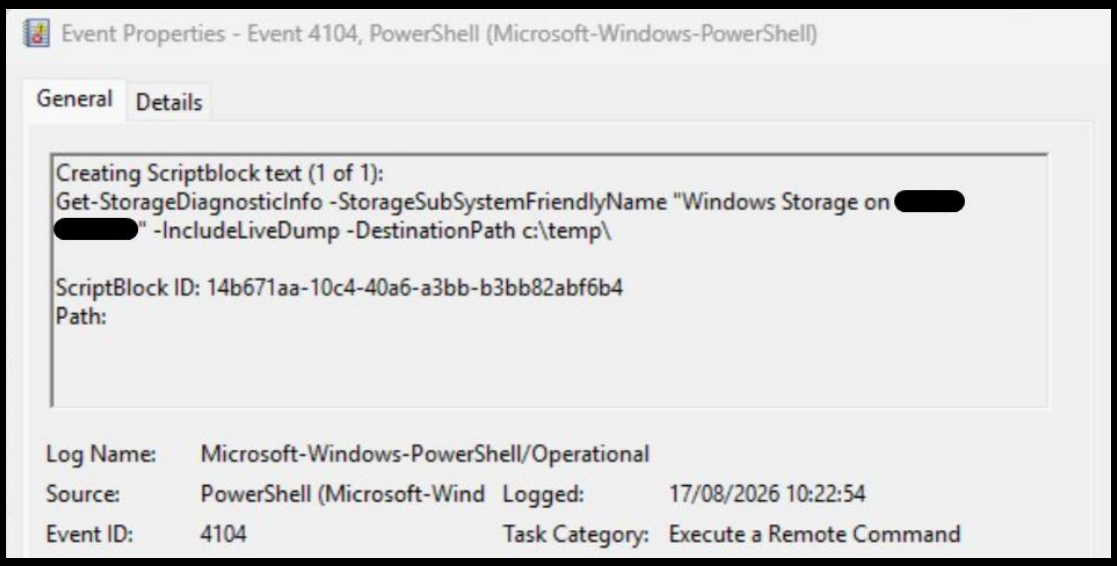
To extract credentials on Windows 11 or Server 2025 without directly touching the LSASS process, attackers can trigger a Windows kernel live dump. Unlike a traditional bug check, a live dump creates a consistent snapshot of kernel memory without resetting the operating system.



Using an elevated PowerShell prompt, an attacker can manually trigger this dump by retrieving the storage subsystem name via Get-StorageSubSystem and running Get-StorageDiagnosticInfo with the -IncludeLiveDump parameter. Because these dumps are saved to disk and can contain user-mode process pages, the attacker can subsequently read and parse the LSASS memory from the resulting LiveDump.dmp file offline. This effectively bypasses protections that restrict direct access to the active LSASS process.

Threat Hunting Activity

Detection can be made monitoring also Powershell Operational Logs, by intercepting the command used to perform a kernel dump.



PUBLIC