Threats of Commercialized Malware: Knotweed

Published: 2022-07-28 · Archived: 2026-04-02 10:37:11 UTC

Microsoft associates the private sector offensive actor (PSOA) **Knotweed** with the Austrian spyware distributor **DSIRF**. DSIRF, founded in 2016, advertises itself as an information research company that performs security and analysis tasks for the red team while offering hacking tools and services.

Now it conducts **hack-for-hire** operations worldwide, especially against targets in Europe and Central America, while using and distributing the malware toolset **Subzero**. The company was also seen conducting some attacks using its own infrastructure.

> DSIRF conducting hack-for-hire operations using malware toolset Subzero

It is worth noting that during the 2016 US presidential election, when Russia was accused of hack operations in the election campaign, DSIRF began advertising **Subzero** as a state trojan analyzing hacking operations and exposing warfare tactics.

Subzero Malware Deployed in Windows and Adobe Zero Day Exploits

Devices and network infrastructures can both be hack targets for Subzero. **MSTIC** and **MSRC** believe that DSIRF is responsible for the zero-day attack that took advantage of a recently fixed flaw in **csrss[.]exe**, CVE-2022-22047. Other zero-day exploits led to deploying Subzero: **Adobe Reader RCE vulnerability** (CVE-2021-28550) and exploits involving privilege escalation (CVE-2021-31199 and CVE-2021-31201).

Microsoft stated about commercialized threats such as Knotweed: “Allowing private sector offensive actors, or **PSOAs**, to develop and sell surveillance and intrusion capabilities to unscrupulous governments and business interests endangers basic human rights.”

Microsoft advises customers to deploy **July 2022** security updates to guard their systems from vulnerabilities that could be exploited.

How is the Malware Deployed?

There are two stages of Subzero deployment: **Corelump** and **Jumplump**. Both sections are heavily obfuscated with a complicated control flow. Corelump is loaded into memory by Jumplump, a persistent malware loader. It loads Corelump from a **JPEG** file in the **%TEMP%** directory. The malware’s main payload is Corelump. It can avoid detection because it operates in memory.

An unusually large JPEG file downloaded from an unknown source might indicate compromise. This query looks for those JPEG files.

Keylogging, capturing screenshots, data exfiltration, running remote shells, and arbitrary plugins downloaded from Knotweed’s C2 server are all capabilities of Corelump.

Corelump integrates **malicious code** while copying legitimate Windows DLLs and disables Control Flow Guard. In Microsoft's security advisory, it is said: "As part of this process, Corelump also modifies the fields in the PE header to accommodate the nefarious changes, such as adding new exported functions, disabling Control Flow Guard, and modifying the image file checksum with a computed value from **CheckSumMappedFile**. These trojanized binaries (Jumplump) are dropped to disk in **C:WindowsSystem32spooldriverscolor**, and COM registry keys are modified for persistence."

Microsoft observed the following post-compromise actions in attacks:

- UseLogonCredential set to "1" for enabling plain text credentials:

reg add HKLMSYSTEMCurrentControlSetControlSecurityProvidersWDigest /v UseLogonCredential /t REG_DWORD /d 1 /f

- Dumping the credentials by **comsvcs[.]dll**:

rundll32[.]exe C:WindowsSystem32comsvcs[.]dll, MiniDump

- Access try from a Knotweed IP address to emails with dumped credentials
- Use of Curl to download Knotweed tools from public shared files such as **vultrobjects[.]com**
- Running PowerShell scripts from a GitHub gist that is associated with DSIRF

Previous Attacks by Knotweed

Subzero was deployed due to an exploit chain that included the Adobe Reader RCE exploit CVE-2021-28550 and Windows privilege escalation exploits CVE-2021-31199 and CVE-2021-31201. These vulnerabilities were all fixed in June 2021 updates. Later, it was discovered that a vulnerability in the Windows Update Medic Service (CVE-2021-36948) was also connected to the exploit chain. It enabled an attacker to force-load a DLL.

An Excel file posing as a real estate document was another method for an attacker to deploy Subzero. The file contained obfuscated malicious macro.

Knotweed uses fake Excel file to deploy Subzero

MSTIC found another Adobe Reader RCE and zero-day Windows privilege escalation (CVE-2022-22047) exploit chain used in May 2022. The victim received a PDF file containing the exploits via email. Knotweed used CVE-2022-22047 specifically for privilege escalation. It could also be used in Chromium-based browsers. The vulnerability was patched in July 2022. This vulnerability could allow an attacker to execute arbitrary processes by creating a malicious activation context in the cache (in CSRSS). The exploit enables the escape of a sandbox environment after the attacker writes a malicious DLL to the disk. The next time the system process spawns, the malicious DLL loads in the specified path, allowing the attacker to execute system-level codes.

Knotweed TTPs and IOCs

Microsoft Defender (1.371.503.0) can detect the malware's tools:

- Backdoor: O97M/JumplumpDropper

- Trojan: Win32/Jumplump
- Trojan: Win32/Corelump
- HackTool: Win32/Mexlib
- Trojan: Win32/Medcerc
- Behavior: Win32/SuspModuleLoad

Check Microsoft's Security Advisory for all TTPs and IOCs related to Knotweed and security advice.
