Threats of Commercialized Malware: Knotweed

socradar.io/threats-of-commercialized-malware-knotweed/

July 28, 2022

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:

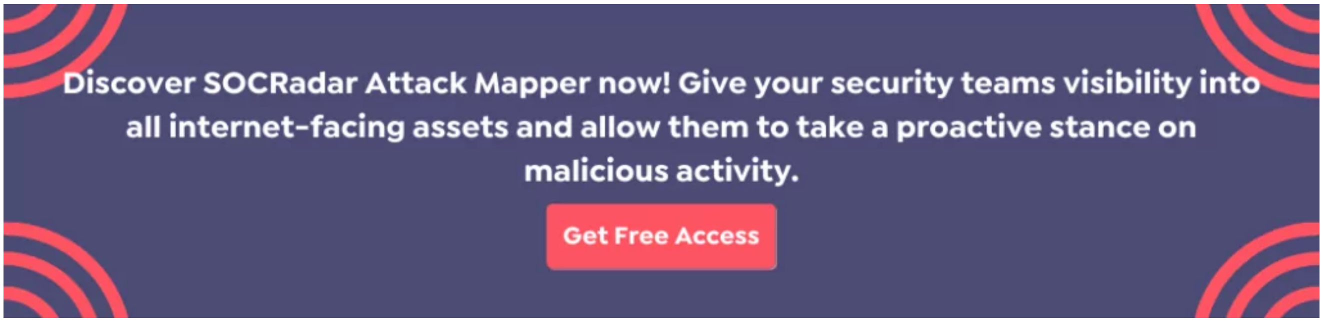
UseLogonCredential set to “1” for enabling plain text credentials:

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

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

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

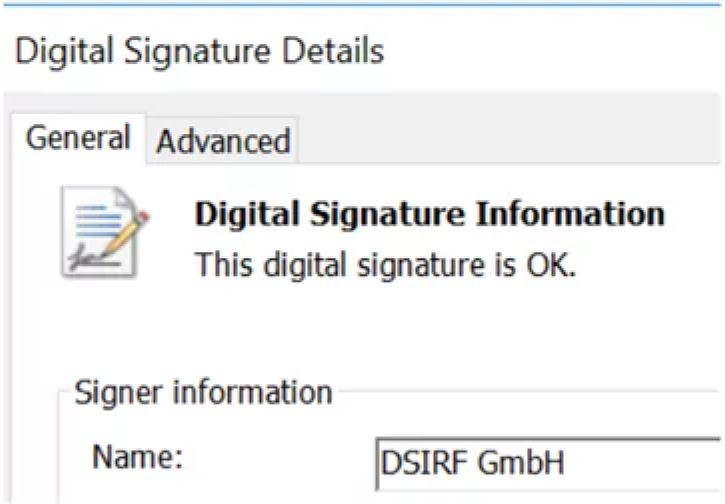
- Access try from a Knotweed IP address to emails with dumped credentials
- Use of Curl to download Knotweed tools from public shared files such as **vultrobjects[.]com**
- Running PowerShell scripts from a GitHub gist that is associated with DSIRF



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.



Digital Signature Information
This digital signature is OK.

Name: DSIRF GmbH

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.

PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site (www.socradar.com). This Cookie Usage Policy (“Policy”) explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,
- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,
- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

3. TYPES OF COOKIES USED ON OUR INTERNET SITE 3.1. Session Cookies

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

3.2. Persistent Cookies

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser’s subfolders until deleted from your browser’s settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

3.3. Mandatory/Technical Cookies

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

3.4. Analytical Cookies

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

3.5. Functional Cookies

Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user’s password on each page visited by the site user.

3.6. Targeting/Advertising Cookies

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors’ navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

4. HOW TO MANAGE COOKIE PREFERENCES?

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website (www.socradar.com) and made accessible to relevant individuals upon request.

SOCRadar
Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA
Phone: +1 (571) 249-4598
Email: [email protected]
Website: www.socradar.com