DevOpt | ThreatLabz

By Shatak Jain, Meghraj Nandanwar

Published: 2023-04-18 · Archived: 2026-04-05 22:44:01 UTC

Additional Analysis

After analyzing the malware, our observations revealed that it contains numerous capabilities. The following functionalities were observed:

Persistence

Persistence refers to a malware's capability to remain active on a system even after a reboot or shutdown. This can be achieved by adding entries to the Windows Registry or by creating scheduled tasks. Once a malware establishes persistence, it can continue to operate in the background and carry out malicious activities undetected by the user.

Upon closer observation, researchers noticed that the malware replicated itself in the Startup folder, enabling it to initiate automatically whenever the computer is powered on. Further observations of different versions revealed that it duplicates itself with a name **devopt[random 2 digits].exe** under the following path: **C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup.**

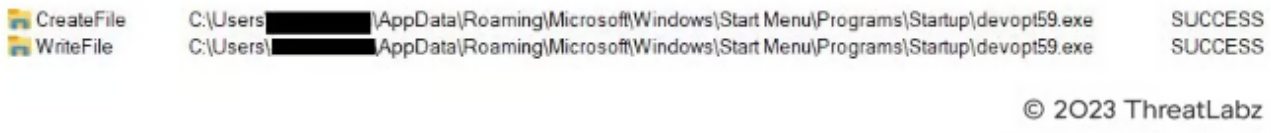

Fig 3. - Persistence mechanism

Clipper

A clipper malware is created to pilfer confidential data from victims. Once it is installed on a victim's device, it can record the clipboard data, which can potentially be used to steal other sensitive information like login credentials, credit card numbers, or other financial data.

Researchers noticed that the malware generates a file called '**clippa.dan**' in the **C:\User\[User]** directory, which logs all the information copied to the clipboard.

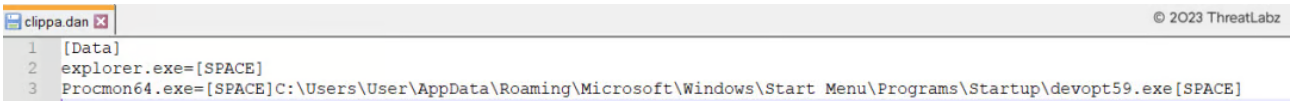

Fig 4. - Clipper logging data from the system

Stealer

A stealer malware is created to pilfer sensitive information, such as login credentials, credit card details, and other personal data. Once it is installed on a victim's device, it can monitor the user's activity and steal sensitive information.

The malware generates two files, namely '**cdck.bin**' and '**bdck.bin**,' in the **C:\User\[User]** directory, which steal the credentials, cookies, history, and version information of the two specific browsers, respectively.

1. Chrome browser data collected from infected system:

- [C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies]
- [C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\History]
- [C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Login Data]
- [C:\Users\User\AppData\Local\Google\Chrome\User Data\Last Version]

2. Yandex data collected from infected system:

- [C:\Users\User\AppData\Local\Yandex\YandexBrowser\User Data\Default\Network\Cookies]
- [C:\Users\User\AppData\Local\Yandex\YandexBrowser\User Data\Default\Network\History]
- [C:\Users\User\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Passman Data]
- [C:\Users\User\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Autofill Data]

Keylogger

Keylogger malware is specifically designed to capture every keystroke made by a user on their device. This can be used to steal sensitive information like login credentials, credit card details, and other personal data.

In this case, the malware creates a file named '**Kebba.dan**' in the **C:\User\[User]** directory to log the keystrokes of the user.

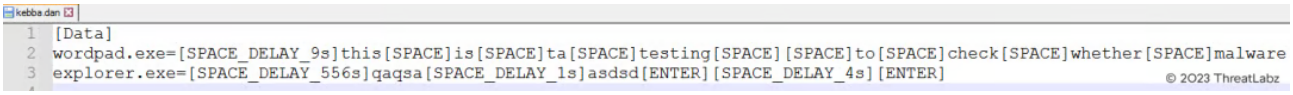

Fig 5. - Keylogger logging keystrokes

Grabber

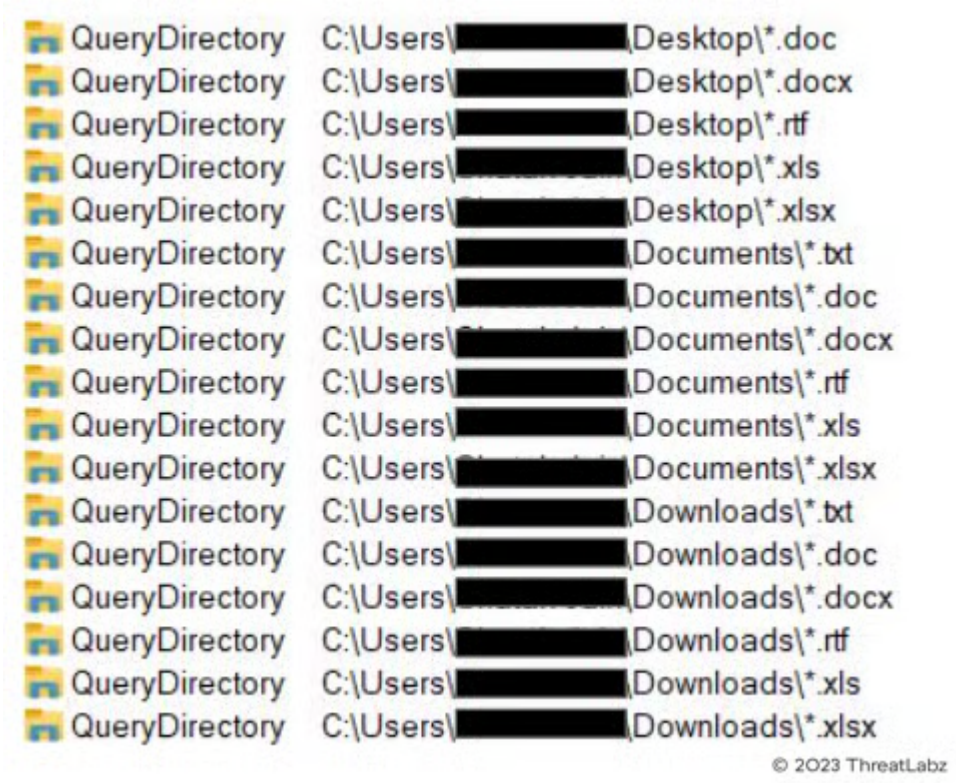

Fig 6. - Grabber enumerating the Directories for stealing file contents

Grabber malware is created to illicitly obtain files and other data from an infected device. It targets text, Word, Excel, and RTF files stored in the Document, Download, or Desktop directories, and saves the stolen data in a file named "**grb.bin**" located at **C:\User\[User]** directory.

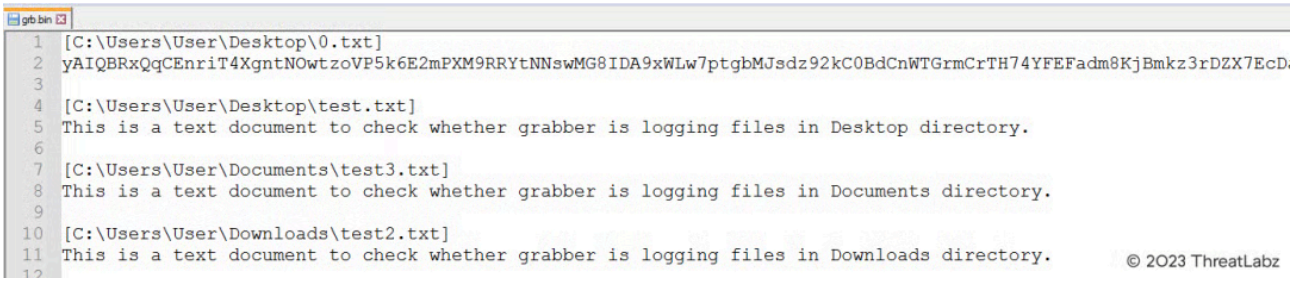

Fig 7. - Grabber File contents stealing data

Dropped text file

In previous versions of this backdoor, researchers observed that it drops a file called '**unpacked.dt**' in the '**data**' folder of the current directory. This file is likely designed to confuse malware analysts because it appears to be an encoded malicious payload, but in reality, it contains randomly generated alphanumeric strings. In newer versions of the backdoor, a similar file named '**0.txt**' is dropped in the current directory, which contains random strings that are hardcoded into the malware itself.

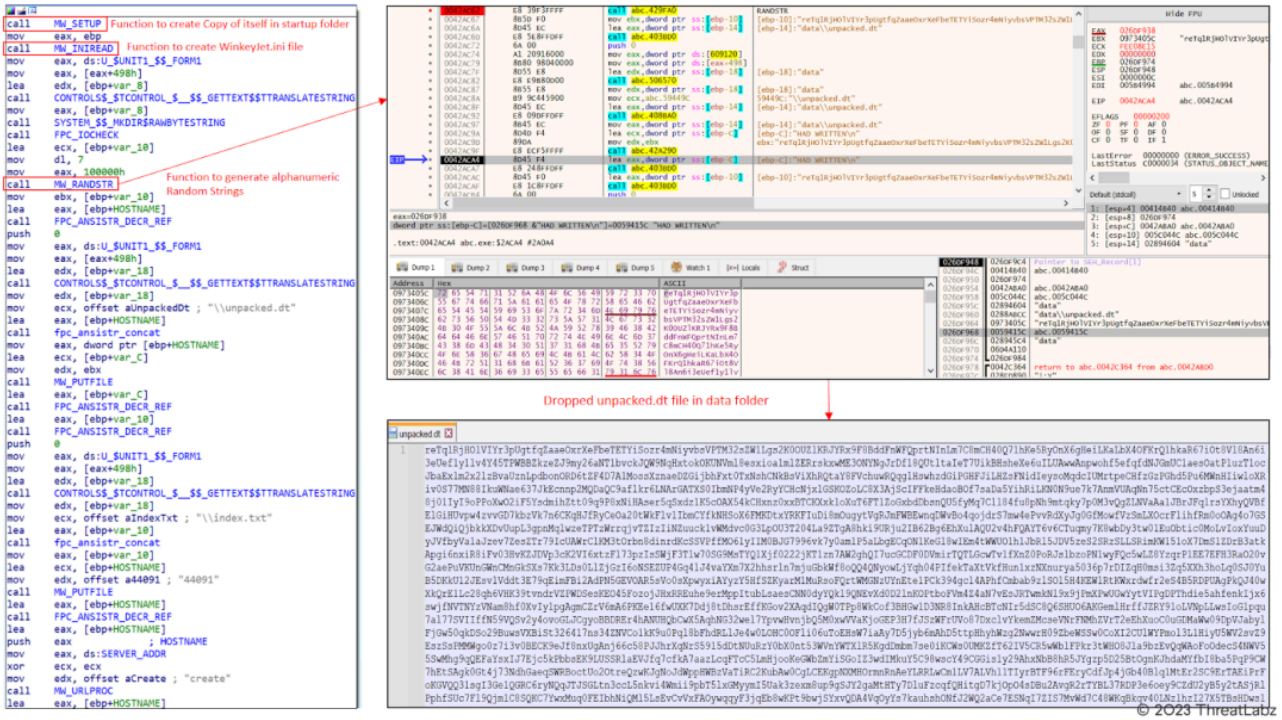

Fig 8. - Generating random alphanumeric strings for unpacked.dt file

Configuration File

The researchers noted the presence of a configuration file named "**Winkeyjet.ini**" that was dropped in the Users directory. This file contains information about the compromised system, such as the name of the operating system, a unique **Device_ID**, and the version number (**Version**) that represents the major version information of the compromised system. Additionally, the file includes the malware's hardcoded own version (**OwnVer**). The configuration file also specifies the Command and Control (CnC) server, which is responsible for providing instructions to the malware once it has been successfully installed.

Fig 9. - Configuration file generated recording the device and version information

Additional investigation has uncovered that certain malwares that are still in the early stages of development are displaying a message box that contains the text "**putin Xyilo**", which is a slogan that ridicules Russian President Vladimir Putin.

Fig 10. - Msgbox displayed in underdeveloped versions of malware

---

Source: https://www.zscaler.com/blogs/security-research/introducing-devopt-multifunctional-backdoor-arsenal