

Introducing DevOpt: A Multifunctional Backdoor Arsenal

 zscaler.com/blogs/security-research/introducing-devopt-multifunctional-backdoor-arsenal

Summary

In recent years, malware attacks have become increasingly sophisticated, and attackers are always finding new ways to exploit vulnerabilities and steal sensitive data. To stay ahead of these threats, security researchers must constantly monitor the landscape and identify new threats as they emerge. In this article, we'll take a closer look at the findings of a recent study conducted by Zscaler's ThreatLabz team, which uncovered a new backdoor built using Free Pascal that has the ability to steal data from infected systems. We'll explore the techniques used by this malware, as well as the tactics employed by cybercriminals to entice users into downloading malicious payloads. By understanding these threats, we can take steps to protect ourselves and our systems from the dangers of malware attacks.

Introduction

Zscaler ThreatLabz has recently unearthed a new backdoor called '**Devopt**'. It utilizes hard-coded names for persistence and offers several functionalities, including keylogging, stealing browser credentials, clipper, and more. Multiple versions of the backdoor have surfaced in just the last few days, indicating that it is still in development. In this blog post, we will delve into the specifics of this new backdoor and its workings. Additionally, we will offer tips on how to safeguard yourself against such attacks.

Key Takeaways:

- Zscaler ThreatLabz uncovered a new backdoor and named it DevOpt based on the name of the persistence malware
- Discovered on a Russian website promising monetary rewards, victims are lured into downloading malicious payloads containing DevOpt malware
- The malware is currently still in development and is receiving continuous improvement updates designed to make it a more potent and effective tool for attackers and threat for defenders
- DevOpt has advanced capabilities to function as a keylogger, stealer, grabber, and a clipper along with persistence mechanisms.

Campaign:

While on the hunt for new malware, the ThreatLabz research team at Zscaler came across a newly discovered backdoor that was created using Free Pascal. This backdoor is particularly dangerous as it has the ability to steal data from infected systems.

Zscaler's ThreatLabz research team remains vigilant in tracking new malware threats. During a recent investigation, we discovered a backdoor that uses Free Pascal and is capable of stealing data from infected systems. Additionally, we came across a Russian website where users were offered financial rewards for completing a task that unwittingly involved downloading malware. Further analysis revealed that the downloaded malware had an archive icon, giving the impression of a compressed file and luring users into double-clicking it, which then executed the malware. This discovery underscores the lengths to which cybercriminals will go to lure users into downloading malicious payloads, using tactics such as offering financial incentives. It's worth noting that the malware's downloading URL pattern generally follows this structure: **wdfiles-download[.]siteme[.]org/axiv[digit].exe**.

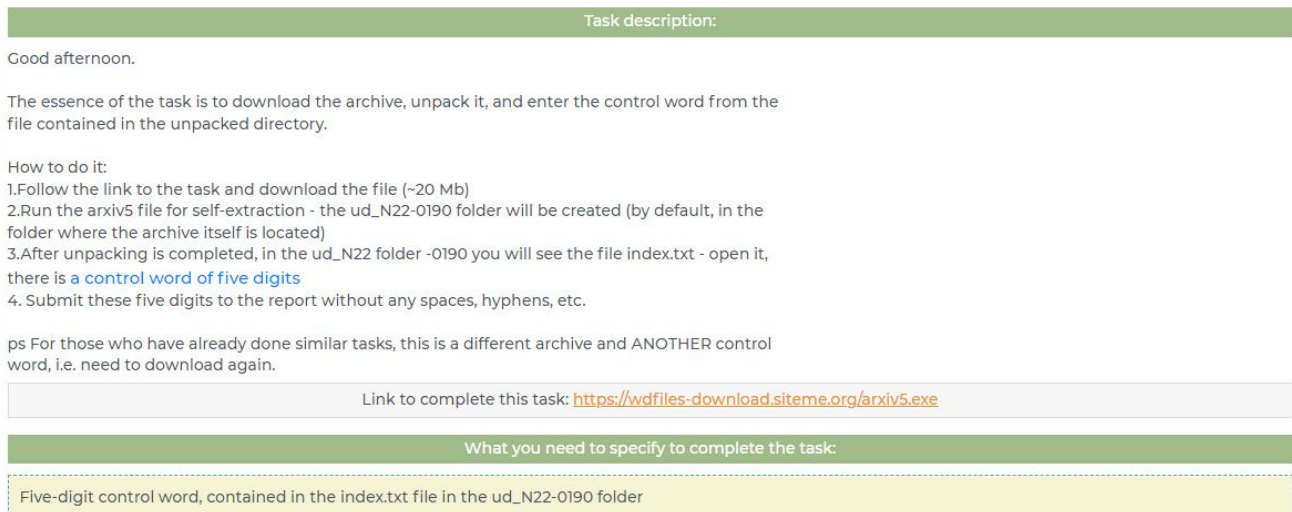


Fig 1. - Russian Website(Translated to english) enticing users into downloading malicious payloads.

Technical Analysis:

Two versions of the backdoor have been discovered in the development stage. The first version, which lacks obfuscation to hide its strings, is roughly 20 MB in size and contains a Graphic User Interface not found in the newer variant, which is approximately 2 MB in size. The second version uses encoded integer-based strings for its functionality.

The older version uses plain text HTTP protocol, while the newer variant searches for OpenSSH DLLs in the infected system to establish encrypted HTTPS connections to its command and control. To establish network connections, the backdoor requires several

DLLs: **libcrypto-1_1.dll**, **libeay32.dll**, **libssl-1_1.dll**, **libssl32.dll**, and **ssleay32.dll**. If the malware is unable to locate these DLLs, it becomes inactive and will not infect the system further.

Encoded String	Decoded Strings	Description
5494-4756-7544-6970-9430-8282-9348-9430-7544	C:\\Users\\	String to access infected system Users Directory
7544-5576-8282-9430-8774-9512-9102-9184-7544	\\Desktop\\	String to access infected system Desktop Directory
7544-5576-9102-8118-9594-8938-8282-9020-9512-9430-7544	\\Documents\\	String to access infected system Documents Directory
7544-5576-9102-9758-9020-8856-9102-7954-8200-9430-7544	\\Downloads\\	String to access Infected system Downloads Directory
8200-8282-9676-9102-9184-9512-3444-3772-8282-9840-8282	devopt*.exe	Create a copy of itself in the Startup folder with devopt(random 2 digit).exe name.

7544-7134-8610-9020-8774-8282-9922-6068-8282-9512-3772-8610-9020-8610	\\WinkeyJet.ini	Create configuration file with WinkeyJet.ini name.
8528-9512-9512-9184-9430-4756-3854-3854-8938-9676-8200-3690-8774-3690-9512-9594-8856-7954-3772-9430-8610-9512-8282-8938-8282-3772-9102-9348-8446-3854	https://mvd-k-tula[.]siteme[.]org/	Command and Control domain.
7544-5330-9184-9184-5576-7954-9512-7954-7544-6724-9102-7954-8938-8610-9020-8446-7544-6314-8610-8118-9348-9102-9430-9102-8364-9512-7544-7134-8610-9020-8200-9102-9758-9430-7544-6806-9512-7954-9348-9512-2624-6314-8282-9020-9594-7544-6560-9348-9102-8446-9348-7954-8938-9430-7544-6806-9512-7954-9348-9512-9594-9184-7544	\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\	Startup directory path.

6314-9102-10004-8610-8856-8856-7954-3854-4346-3772-3936-2624-3280-7134-8610-9020-8200-9102-9758-9430-2624-6396-6888-2624-4428-3772-4100-4838-2624-9348-9676-4756-4018-3936-4264-3772-3936-3362-2624-5822-8282-8118-8774-9102-3854-4100-3936-4018-3936-3936-4018-3936-4018-2624-5740-8610-9348-8282-8364-9102-9840-3854-4018-3936-4264-3772-3936	Mozilla/5.0 (Windows NT 6.2; rv:104.0) Gecko/20100101 Firefox/104.0	User Agent used for network requests.
8856-8610-9430-9512-8282-9020-8282-9348-3772-9184-8528-9184	listener.php	Send collected data as listener.php

The earlier version of the backdoor required user interaction by clicking on the Extract button, whereas newer versions run silently in the background without any need for user interaction.



Fig 2. - Earlier version of malware requiring user interaction

Based on the aforementioned observation, it can be concluded that the Threat Actor is adding more features to the backdoor and making it stealthier.

Additional Analysis:

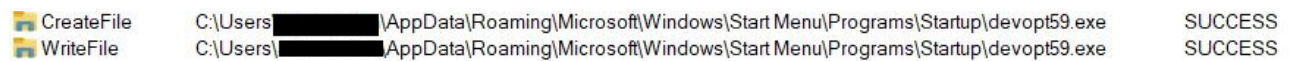
After analyzing the malware, our observations revealed that it contains numerous capabilities. The following functionalities were observed:

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.



CreateFile	C:\Users\████████\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\devopt59.exe	SUCCESS
WriteFile	C:\Users\████████\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\devopt59.exe	SUCCESS

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.



```
1 [Data]
2 explorer.exe=[SPACE]
3 Procmon64.exe=[SPACE]C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\devopt59.exe [SPACE]
```

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]

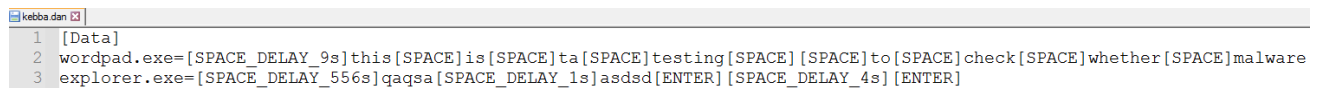
2. Yandex data collected from infected system:

- [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.



```

1 [Data]
2 wordpad.exe=[SPACE_DELAY_9s]this[SPACE]is[SPACE]ta[SPACE]testing[SPACE][SPACE]to[SPACE]check[SPACE]whether[SPACE]malware
3 explorer.exe=[SPACE_DELAY_556s]qagsa[SPACE_DELAY_1s]asdsd[ENTER][SPACE_DELAY_4s][ENTER]

```

Fig 5. - Keylogger logging keystrokes

Grabber:

```

QueryDirectory C:\Users\[redacted]\Desktop\*.doc
QueryDirectory C:\Users\[redacted]\Desktop\*.docx
QueryDirectory C:\Users\[redacted]\Desktop\*.rtf
QueryDirectory C:\Users\[redacted]\Desktop\*.xls
QueryDirectory C:\Users\[redacted]\Desktop\*.xlsx
QueryDirectory C:\Users\[redacted]\Documents\*.txt
QueryDirectory C:\Users\[redacted]\Documents\*.doc
QueryDirectory C:\Users\[redacted]\Documents\*.docx
QueryDirectory C:\Users\[redacted]\Documents\*.rtf
QueryDirectory C:\Users\[redacted]\Documents\*.xls
QueryDirectory C:\Users\[redacted]\Documents\*.xlsx
QueryDirectory C:\Users\[redacted]\Downloads\*.txt
QueryDirectory C:\Users\[redacted]\Downloads\*.doc
QueryDirectory C:\Users\[redacted]\Downloads\*.docx
QueryDirectory C:\Users\[redacted]\Downloads\*.rtf
QueryDirectory C:\Users\[redacted]\Downloads\*.xls
QueryDirectory C:\Users\[redacted]\Downloads\*.xlsx

```

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.

```

grb bin
1 [C:\Users\User\Desktop\0.txt]
2 yAIQBRxQqCEnriT4XgntNOWtzoVP5k6E2mPXM9RRYtNNSwMG8IDA9xWLw7ptgbmJsdz92kC0BdCnWTGrmCrTH74YFEFadm8KjBmkz3rDZX7EcD.
3
4 [C:\Users\User\Desktop\test.txt]
5 This is a text document to check whether grabber is logging files in Desktop directory.
6
7 [C:\Users\User\Documents\test3.txt]
8 This is a text document to check whether grabber is logging files in Documents directory.
9
10 [C:\Users\User\Downloads\test2.txt]
11 This is a text document to check whether grabber is logging files in Downloads directory.
12

```

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.

The image shows a debugger window with assembly code on the left and a memory dump on the right. Annotations include:

- Red arrows pointing to assembly instructions: `CALL Mv_RANDSTR` (labeled "Function to generate alphanumeric Random Strings") and `CALL Mv_PUTFILE` (labeled "Dropped unpacked.dt file in data folder").
- A red arrow pointing to a memory dump entry: `0042AC34` (labeled "Dropped unpacked.dt file in data folder").

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 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.

```
[Windows]
DEVICE_ID=oz [REDACTED]
Version=10.0
OwnVer=4.0

[Server]
Address=https://mvd-k-tula.siteme.org/
```

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

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



Fig 10. - MsgBox displayed in underdeveloped versions of malware

Network Communication:

Establishing a connection with the Command and Control (CnC) starts with the malware sending a "create" request. Upon recognizing the request, the CnC responds with a "200 OK" message.

After establishing the connection, the malware sends a command request to the CnC, which in turn responds with a SYNC command. Upon receiving the SYNC command, the malware executes the given command and sends a "SYNCRONIZED" response back to the CnC to indicate successful completion.



Fig 11. - Network communication steps

Commands:

Below are the encoded string commands used by the observed malware:

Encoded String	Decoded Strings	Description
----------------	-----------------	-------------

6806-7298-6396-5494	SYNC	Command to check connection between CnC and Malware. We observed in some variants malware send the 'SYNCRONIZED' response along with the version of the malware.
5576-5986-6724	DIR	Command to collect file information of the given directory. It can collect file name, directory name, size and modified date.
6560-6970-6888	PUT	Command to write collected information in file. It will give the response 'HAD WRITTEN' if the file is already present else 'NOT WRITTEN'.
6724-5658-5330-5576	READ	Command to read collected information from stored files and send data to CnC.
5658-7216-5658-5494	EXEC	To execute commands sent from CnC and after successful execution it sends 'EXECUTED' response.
5576-6724-6232-6806	DRLS	Command to collect Drive information (HDD, CDROM, RAMDISK, Network and Removable) of the infected system.
6560-6724-6232-6806	PRLS	Command to collect the Process list of infected systems.

The previous version of the malware did not include the DRLS and PRLS commands for gathering drive and process information, respectively.

Conclusion

Based on the observations made during the malware analysis, it is evident that the malware in question is a sophisticated and multifunctional threat. The malware is capable of performing various malicious activities such as stealing confidential information, logging keystrokes, stealing files, and establishing persistent access to the victim's system.

It is also evident that the threat actor behind the malware is continuously improving the malware by adding new features, making it stealthier, and using various techniques to evade detection. The malware uses encoded strings for its commands and drops files with misleading names to deceive malware analysts.

Furthermore, the malware communicates with a Command and Control server to receive instructions and send stolen data. The server's IP address and other details are hardcoded into the malware.

Overall, the findings highlight the need for robust security measures to protect against advanced and evolving malware threats. It also emphasizes the importance of regular updates and security patches to mitigate the risks associated with these threats.

As cyber threats continue to evolve and become increasingly complex, it is critical to remain alert and take proactive measures to protect against them. The discovery of this new backdoor is a testament to the ever-changing tactics of attackers and underscores the importance of ongoing monitoring and research. Zscaler's ThreatLabz team is dedicated to staying on top of these threats and sharing their findings with the wider community. It is essential to stay informed and take necessary precautions to safeguard against malware attacks. Remember to keep your software up-to-date, use strong passwords, and be wary of suspicious emails or messages.

Zscaler Sandbox Coverage

Zscaler's multilayered cloud security platform detects indicators, as shown below:

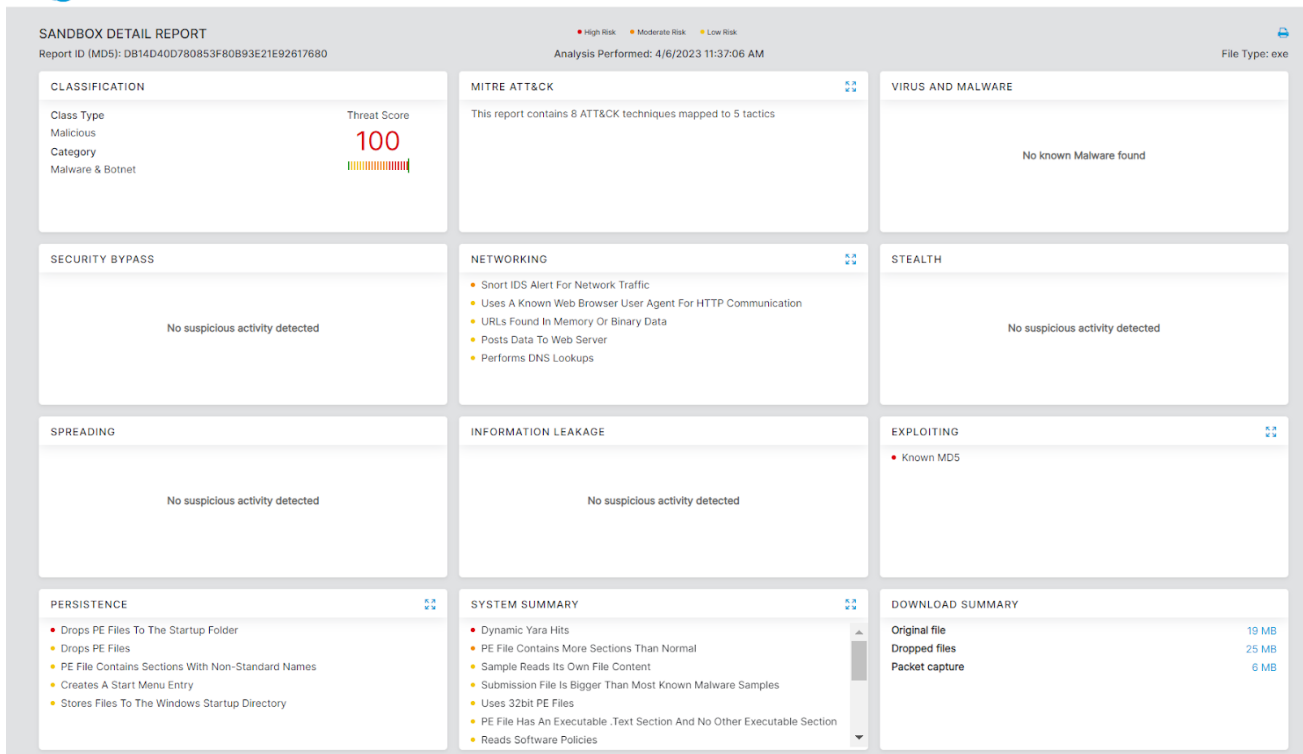


Fig 12. - DevOpt Backdoor Zscaler sandbox report

The following threat names are detected by Zscaler's multilayered cloud security platform for identifying malicious payloads:

Win32.Backdoor.DevOpt

MITRE ATT&CK Techniques:

Tactic	Technique ID	Technique Name
Execution	<u>T1129</u>	Shared Modules
Defense Evasion	<u>T1027</u>	Obfuscated Files or Information
Persistence	<u>T1037.005</u>	Startup Items
	<u>T1547.001</u>	Registry Run Keys / Startup Folder

Discovery	<u>T1057</u>	Process Discovery
	<u>T1082</u>	System Information Discovery
	<u>T1083</u>	File and Directory Discovery
Collection	<u>T1005</u>	Data from Local System
	<u>T1115</u>	Clipboard Data
Credential Access	<u>T1003</u>	OS Credential Dumping
	<u>T1555.003</u>	Credentials from Web Browsers
	<u>T1539</u>	Steal Web Session Cookie
	<u>T1056.001</u>	Keylogging
Command and Control	<u>T1095</u>	Non-Application Layer Protocol
	<u>T1071</u>	Application Layer Protocol

Indicators of Compromise (IOCs):

db14d40d780853f80b93e21e92617680	Old Variant
94df2e4aa0f432ef992893d7b994ce84	
391c894616dd0e8b372b801cbbc0a790	New Variant
e42198e7c0647238b999a2b2133daac2	
mvd-k-tula[.]siteme[.]org	Command and Control Domain
mvd-k-tula[.]ru	
wdfiles-download[.]siteme[.]org/axiv5.exe	Malicious Source Url used for distribution