Sednit Espionage Group Attacking Air-Gapped Networks

By Joan Calvet

Archived: 2026-04-05 14:10:31 UTC

Malware

The Sednit espionage group, also known as the Sofacy group, APT28 or “Fancy Bear”, has been targeting various institutions for many years. We recently discovered a component the group employed to reach physically isolated computer networks -- “air-gapped” networks -- and exfiltrate sensitive files from them through removable drives.

11 Nov 2014 • , 9 min. read

The Sednit espionage group, also known as the Sofacy group, APT28 or “Fancy Bear”, has been targeting various institutions for many years. We recently discovered a component the group employed to reach physically isolated computer networks -- “air-gapped” networks -- and exfiltrate sensitive files from them through removable drives.

Introduction

Last month ESET discovered that the Sednit group was performing watering-hole attacks using a custom-built exploit kit. Over the last few weeks several pieces of intelligence have been shared on this group, including the Operation Pawn Storm report from Trend Micro and the APT28 report from FireEye.

In this blog post, we are sharing knowledge of a tool employed to extract sensitive information from air-gapped networks. ESET detects it as Win32/USBStealer.

We believe the Sednit group has been using this tool at least since 2005, and is still using it today against their usual types of target, namely governmental institutions in Eastern Europe. Several versions of the tool have been employed over the past few years, with various degrees of complexity.

Win32/USBStealer strategy

A common security measure for sensitive computer networks is to have them totally isolated from the outside world via an “air gap”. As the name implies, these networks do not possess any direct, outside connections to the Internet.

However, the use of removable drives can create paths to the outside world. This is particularly true when the same removable drive is repeatedly plugged into both Internet-connected machines and air-gapped machines, such as when transferring files.

This is the scenario that is exploited by Win32/USBStealer in order to reach air-gapped networks. The following image presents a high-level overview of this strategy in the simple case of just two computers. Computer A is connected to the Internet and is initially infected with the Win32/USBStealer dropper, whereas Computer B is physically isolated and becomes infected with Win32/USBStealer during the attack.

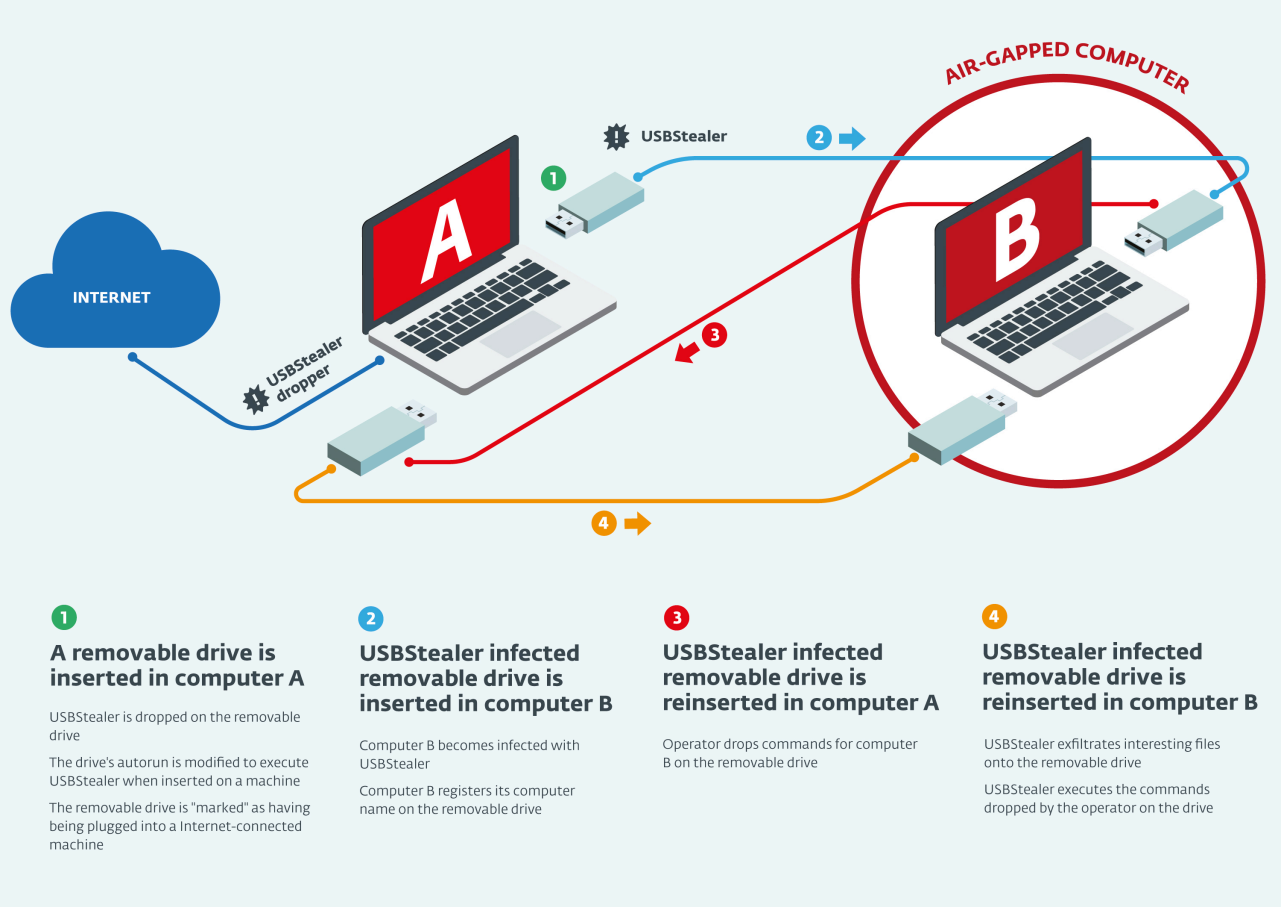


Figure 1 - Attack Scenario

In this scenario a same removable drive goes back and forth between the Internet-connected Computer A and the air-gapped Computer B. We are now going to explain each step of this attack in more detail. We focus here on the most complex version of Win32/USBStealer observed.

Step 1: First insertion in Computer A

Computer A is initially infected with the Win32/USBStealer dropper, detected as Win32/USBStealer.D by ESET. The dropper file name is USBSRService.exe, and it tries to mimic a legitimate Russian program called USB Disk Security, as shown below.

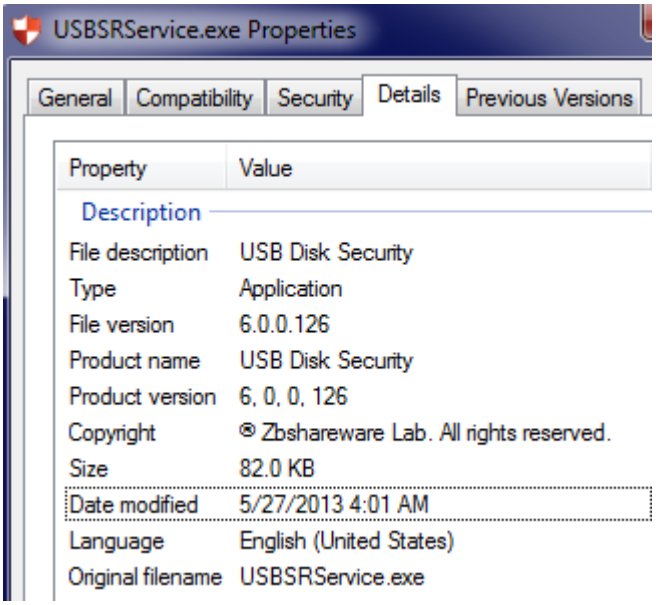


Figure 2 - Win32/USBStealer Dropper Metadata

The main logic of the dropper is as follows:

- It monitors the insertion of removable drives into the machine by creating a window with a callback that will be notified when such events occur.
- Once a removable drive is inserted, the dropper decrypts two of its resources in memory. The first one drops the program Win32/USBStealer onto the removable drive under the name “USBGuard.exe”. The second resource is an AUTORUN.INF file whose content is shown below.

[autorun]

open=

shell\open=Explore

shell\open\command="System Volume Information\USBGuard.exe" install

shell\open\Default=1

- This file is dropped onto the removable drive root. It ensures that double-clicking on the drive executes USBGuard.exe, as well as clicking on the first right-click option (renamed “*Explore*” instead of “*Open*”). This will only work on computers with Windows AutoRun feature enabled, which was deactivated by the Windows update KB971029 in August 2009. It may seem a long time ago, but we believe Win32/USBStealer started to propagate at least four years before that period. Moreover, it is common for machines in air-gapped networks to be out-to-date, because they can be hard to update and they are assumed to be unreachable by attackers.

- Finally, an empty file named “destktop.in” is dropped onto the removable drive. It will serve as a sign for other infected machines that this drive has been connected to an Internet-connected machine at some point. In other words, the drive is a potential path to the outside world for air-gapped machines.

Overall, the dropper takes great care not to attract attention. For example, both the AUTORUN.INF and USBGuard.exe files have their last-access and last-write timestamps set to those of a standard Windows library chosen on the system. Also, the two decrypted resources are immediately re-encrypted in memory after having been dropped on the removable drive. Finally, all dropped files are set with hidden and system file attributes, to help ensure that they will remain undetected by casual users.

Step 2: First insertion in Computer B

When the USB drive is inserted in Computer B, which has AutoRun enabled, Win32/USBStealer installs itself. It then enumerates all drives connected to the machine and, depending on the drive's type, it executes a different logic:

- If the drive is removable and has been marked as having being connected to an Internet-capable machine (thanks to the dropped desktop.in file in step 1), Computer B registers itself on the drive by creating a folder with its computer name. This registration will allow the operators to map the reachable machines when the drive comes back to Computer A.

Computer B also keeps track of the drive locally by recording its hardware ID. Thus even if desktop.in is removed by the user from the drive, Computer B will remember that this drive can be used as a path to the outside.

- If the drive is non-removable, or can be removed without any sign of having been connected to an Internet-connected machine, Win32/USBStealer executes an automatic exfiltration procedure (in opposition to the manual procedure we will describe later).

The purpose of this step is to group interesting files from all these drives in the same local directory. The actual exfiltration will happen the next time the "marked" removable drive gets inserted into Computer B. "Interesting files" are here defined as:

- Files whose extension is ".skr",".pkr" or ".key". The first two correspond to the default extensions for the "keyrings" of the PGP Desktop cryptographic application. These files are storage for private and public keys respectively. The ".key" extension is often used by cryptographic tools for files storing generated keys.

- Files whose name belongs to a hardcoded list. We have observed two different lists in the wild, described in the table array below.

*	**List 1**	**List 2**
Possible period of use	2005	2011-2014

*	List 1	List 2
File names searched for	Win32Negah.dll Ssers.dat Settings.dat Negah2.exe DtInt.dat Audit.dat	key.in key.out z_box.exe talgar.exe

The possible period of use corresponds to the compilation timestamps of the files containing these lists.

We found very few references for most of these file names on Internet, probably because they belong to private software. Interestingly, Talgar (from “talgar.exe”) is a town in the Almaty Province of southeastern Kazakhstan.

The malware searches for these files everywhere on the machine, except in folders matching the following antivirus names: Symantec, Norton, McAfee, ESET Smart Security, AVG9, Kaspersky Lab and Doctor Web.

Step 3: Second insertion in Computer A

The malware operators collect the computer name that has been registered by Computer B from the drive. As the dropper running on Computer A does not implement anything more than we previously described, the operators should have another malicious component running on Computer A in order to achieve that step.

Then, the operators drop commands for Computer B onto the removable drive, in an encrypted file named “COMPUTER_NAME.in”.

Step 4: Second insertion in Computer B

When the removable drive comes back in Computer B, Win32/USBStealer drops onto it the files grouped during the automatic exfiltration procedure described in step 2, above. The next time the removable drive gets connected to Computer A, the operators will be able to grab these “air-gapped” files.

Win32/USBStealer then decrypts the command files dropped by the operators for Computer B. It gives a series of commands that will be executed consecutively. Each command is a two-byte number followed by parameter.

Command Number	Parameter	Purpose
0x0001	Windows path	Copies files matching the path to the removable drive
0x0002	Root = Path = Day	Copies files whose path matches “Root \Path*” to the removable drive, but only if they have been modified less than Day days ago
0x0003	Root = Path = Day	Same as command 0x0002, but the parameter is also written in the startup monitoring file (see paragraph below)

Command Number	Parameter	Purpose
0x0004	Should be set to “!”	Launch the automatic exfiltration function (see step 2) on all connected drives
0x0005	None	Removes startup monitoring file (see paragraph below)
0x0006	Windows path	Executes a copy of the file pointed by the parameter under the name “taskrel.exe”
0x0007	None	Removes file named “taskrel.exe”
0x0008	Root = Path = Day	Writes filenames matching “Root \Path*” to the removable drive, but only if they have been modified less than Day days ago, in a file named “inres.in”
0x0009	None	Removes file named “inres.in”

Commands 0x0003 and 0x0005 refer to the startup monitoring file, which is a file stored locally on Computer B containing file patterns in the format “Root = Path = Day”. Each time the machine boots up, command 0x0002 will be executed on these patterns. This allows long-term monitoring for files of interest.

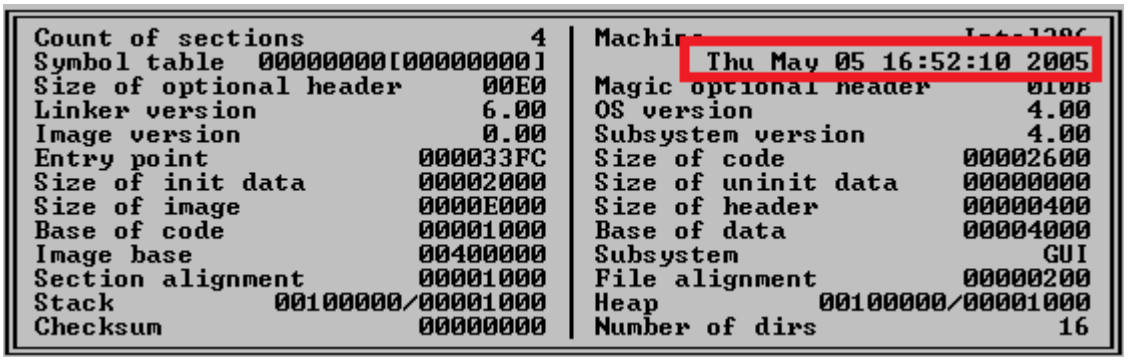
Command 0x0008 serves as a means of discovering possibly interesting files. We can speculate that operators start with command 0x0008, and then run commands 0x0002 or 0x0003 to collect files of possible interest.

For all commands that copy files to removable drives there is a fallback mechanism. In case the copy fails, for example because write access to the drive is not granted, the files will be grouped in a local directory instead. They will be copied onto the next Internet-capable drive that gets connected to the machine.

Conclusion

Win32/USBStealer shows the high level of determination of its operators, the Sednit group. Here are some surprising things discovered during the investigation:

- **Almost 10 years of operation:** The earliest compilation date we found for the Win32/USBStealer payload is May 2005, as shown in the Figure below. As the compiler version that produced this particular binary is consistent with the compilation date, and since other Win32/USBStealer payloads have realistic compilation timestamps (dating from the past few years), we believe this represents the actual date of operation for this program.



- **Precise targeting:** The names of the searched files by the automatic extraction procedure indicate very precise knowledge of the targets.

Some open questions remain; for example it is currently unclear how the initial infection occurred. We can speculate that the classic spear-phishing technique has been used. It should be noted that the recent FireEye report on this group reports a spear phishing campaign using the topic “USB Disk Security is the best software to block threats that can damage your PC or compromise your personal information via USB storage.”

In the attack scenario we described, Computer A has to be already controlled by the miscreants. The Win32/USBStealer dropper does not have the ability to communicate over Internet, so we can speculate there are other malicious components running on this machine.

Indicators of Compromise (IOC)

Dropper

- Registers service named "USB Disk Security" with the description "Provide protection against threats via USB drive".
- Alternatively, registers itself under the “HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\Run” registry key, under the name “USB Disk Security”
- Opens mutex named “ZXCVMutexHello”
- Resources of type “X”:
    - ID=109 for the payload
    - ID=106 for the AUTORUN.INF file

Payload

- Registers service named "USBGuard" with the description " Protects removable media from becoming infected with malware".
- Alternatively, registers itself under the “HKEY_CURRENT_USER Software\Microsoft\Windows\CurrentVersion\Run” registry key, under the name “USBGuard”
- Opens mutex named “USB_Flash”

Hashes

SHA1	Purpose	ESET Detection Name
BB63211E4D47344514A8C79CC8C310352268E731	Dropper (USBSRService.exe)	Win32/USBStealer.D
776C04A10BDEEC9C10F51632A589E2C52AABDF48	Payload (USBGuard.exe)	Win32/USBStealer.A

Source: http://www.welivesecurity.com/2014/11/11/sednit-espionage-group-attacking-air-gapped-networks/