

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

×

https://www.fireeye.com/blog/threat-research/2018/03/sanny-malware-delivery-method-updated-in-recently-observed-attacks.r

Go

FEB

MAR

MAY

31

2018

2019

2017

2018

2019

?

×

f

t

About this capture

24 captures

31 Mar 2018 - 17 Jul 2024



24 captures

31 Mar 2018 - 17 Jul 2024

FEB

MAR

MAY

31

2017

2018

2019

About this capture

up for e

f

t

advanced threats from the lea
advanced threat prevention.

Attacks

March 23, 2018 | by [Sudeep Singh](#), [Yijie Sui](#)

Introduction

In the third week of March 2018, through FireEye's Dynamic Threat Intelligence, FireEye discovered malicious macro-based Microsoft Word documents distributing SANNY malware to multiple governments worldwide. Each malicious document lure was crafted in regard to relevant regional geopolitical issues. FireEye has tracked the SANNY malware family since 2012 and believes that it is unique to a group focused on Korean Peninsula issues. This group has consistently targeted diplomatic entities worldwide, primarily using lure documents written in English and Russian.

As part of these recently observed attacks, the threat actor has made significant changes to their usual malware delivery method. The attack is now carried out in multiple stages, with each stage being downloaded from the attacker's server. Command line evasion techniques, the capability to infect systems running Windows 10, and use of recent User Account Control (UAC) bypass techniques have also been added.

Document Details

The following two documents, detailed below, have been observed in the latest round of attacks:

MD5 hash: c538b2b2628bba25d68ad601e00ad150

SHA256 hash: b0f30741a2449f4d8d5ffe4b029a6d3959775818bf2e85bab7fea29bd5acafa4

Original Filename: РГНФ 2018-2019.doc

The document shown in Figure 1 discusses Eurasian geopolitics as they relate to China, as well as Russia's security.

Углубление евразийской геополитики Китая и интересы безопасности России: транспортный аспект.

Тип проекта: а

Область знания: 07

Код классификатора РГНФ: 07-140

Код ГРНТИ: 73.01.17

Приоритетное направление развития науки, технологий и техники в Российской Федерации, критическая технология|

7. Транспортные и космические системы.

Фамилия, имя, отчество руководителя проекта:

Аристова Людмила Борисовна Телефон руководителя проекта:
+7 9858269051

Объем финансирования проекта

на 2017 г.: 500 000 (пятьсот тысяч) рублей Год начала проекта 2018

Год окончания проекта 2019

Фамилии, имена, отчества основных исполнителей Семенова Н.К.

Название проекта

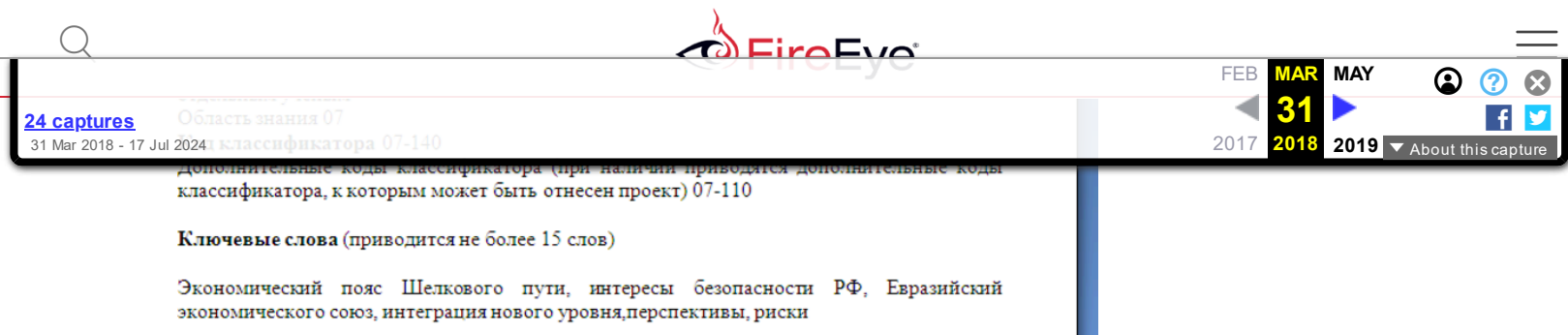


Figure 1: Sample document written in Russian

MD5 hash: 7b0f14d8cd370625aeb8a6af66af28ac

SHA256 hash: e29fad201feba8bd9385893d3c3db42bba094483a51d17e0217ceb7d3a7c08f1

Original Filename: Copy of communication from Security Council Committee (1718).doc

The document shown in Figure 2 discusses sanctions on humanitarian operations in the Democratic People's Republic of Korea (DPRK).

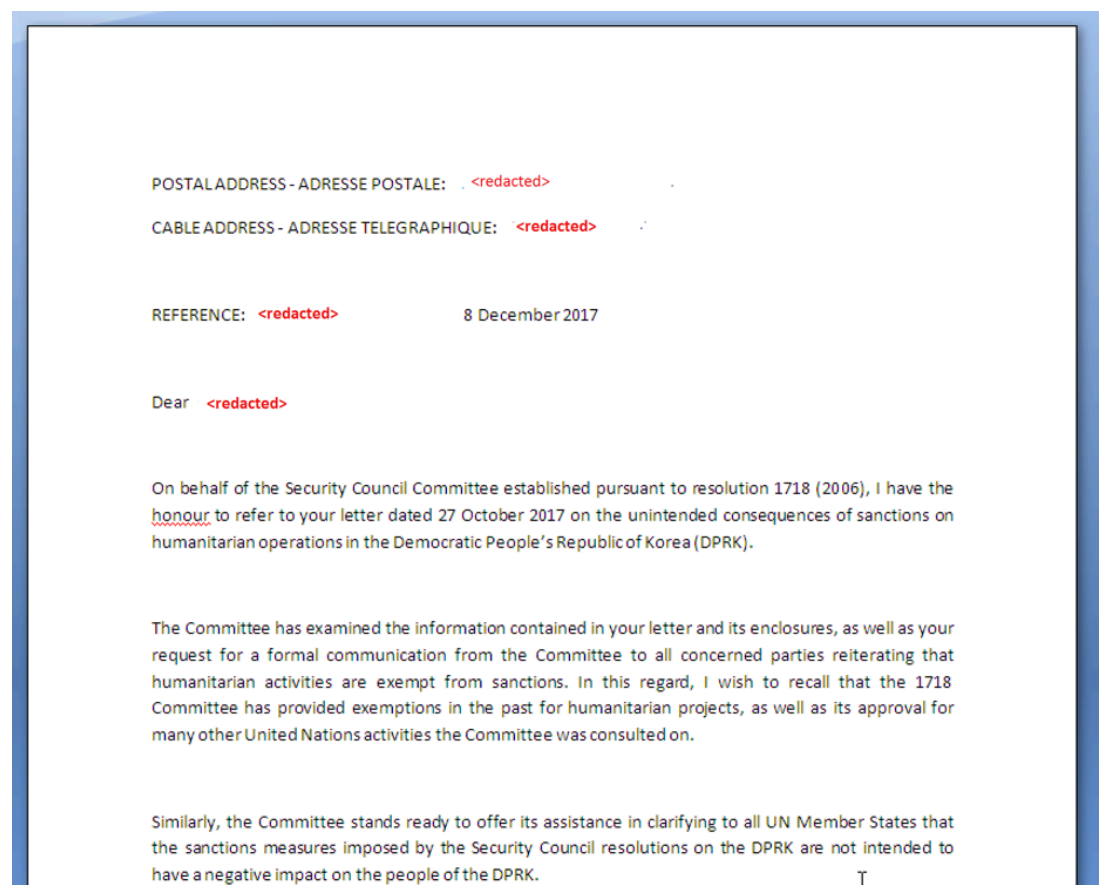


Figure 2: Sample document written in English

Macro Analysis

In both documents, an embedded macro stores the malicious command line to be executed in the TextBox property (TextBox1.Text) of the document. This TextBox property is first accessed by the macro to execute the command on the system and is then overwritten to delete evidence of the command line.



24 captures

In Stage 1, the macro leverages the legitimate Microsoft Windows certutil.exe utility to download an encoded file from the following URL: [http://more.1apps\[.\]com/1.txt](http://more.1apps[.]com/1.txt). The macro then decodes the encoded file and drops it in the %temp% directory with the name: 1.bat.

There were a few interesting observations in the command line:

1. The macro copies the Microsoft Windows certutil.exe utility to the %temp% directory with the name: ct.exe. One of the reasons for this is to evade detection by security products. Recently, FireEye has observed other threat actors using certutil.exe for malicious purposes. By renaming "certutil.exe" before execution, the malware authors are attempting to evade simple file-name based heuristic detections.
2. The malicious BAT file is stored as the contents of a fake PEM encoded SSL certificate (with the BEGIN and END markers) on the Stage 1 URL, as shown in Figure 3. The "certutil.exe" utility is then leveraged to both strip the BEGIN/END markers and decode the Base64 contents of the file. FireEye has not previously observed the malware authors use this technique in past campaigns.

Figure 3: Malicious BAT file stored as an encoded file to appear as an SSL certificate

BAT File Analysis

Once decoded and executed, the BAT file from Stage 1 will download an encoded CAB file from the base URL: [http://more.1apps\[.\]com/](http://more.1apps[.]com/). The exact file name downloaded is based on the architecture of the operating system.

- For a 32-bit operating system: [http://more.1apps\[.\]com/2.txt](http://more.1apps[.]com/2.txt)
- For a 64-bit operating system: [http://more.1apps\[.\]com/3.txt](http://more.1apps[.]com/3.txt)

Similarly, based on Windows operating system version and architecture, the CAB file is installed using different techniques. For Windows 10, the BAT file uses rundll32 to invoke the appropriate function from update.dll (component inside setup.cab).

- For a 32-bit operating system: `rundll32 update.dll _EntryPoint@16`
- For a 64-bit operating system: `rundll32 update.dll EntryPoint`

For other versions of Windows, the CAB file is extracted using the legitimate Windows Update Standalone Installer (wusa.exe) directly into the system directory:

The BAT file also checks for the presence of Kaspersky Lab Antivirus software on the machine. If found, CAB installation is changed accordingly in an attempt to bypass detection:

Stage 2: CAB File Analysis

As described in the previous section, the BAT file will download the CAB file based on the architecture of the underlying operating system. The rest of the malicious activities are performed by the downloaded CAB file.





FEB

MAR

MAY

31

2017

2018

2019



24 captures

et.dll – Main component that we refer to as SANNY malware.

31 Mar 2018 - 17 Jul 2024

Config file used by SANNY malware

About this capture

- NTWDBLIB.dll – Performs UAC bypass on Windows 7 (32-bit and 64-bit).
- update.dll – Performs UAC bypass on Windows 10.

install.bat will perform the following essential activities:

1. Checks the current execution directory of the BAT file. If it is not the Windows system directory, then it will first copy the necessary components (ipnet.dll and ipnet.ini) to the Windows system directory before continuing execution:
2. Hijacks a legitimate Windows system service, COMSysApp (COM+ System Application) by first stopping this service, and then modifying the appropriate Windows service registry keys to ensure that the malicious ipnet.dll will be loaded when the COMSysApp service is started:
3. After the hijacked COMSysApp service is started, it will delete all remaining components of the CAB file:

ipnet.dll is the main component inside the CAB file that is used for performing malicious activities. This DLL exports the following two functions:

1. ServiceMain – Invoked when the hijacked system service, COMSysApp, is started.
2. Post – Used to perform data exfiltration to the command and control (C2) server using FTP protocol.

The ServiceMain function first performs a check to see if it is being run in the context of svchost.exe or rundll32.exe. If it is being run in the context of svchost.exe, then it will first start the system service before proceeding with the malicious activities. If it is being run in the context of rundll32.exe, then it performs the following activities:

1. Deletes the module NTWDBLIB.DLL from the disk using the following command:

```
cmd /c taskkill /im cliconfg.exe /f /t && del /f /q NTWDBLIB.DLL
```

2. Sets the code page on the system to 65001, which corresponds to UTF-8:

```
cmd /c REG ADD HKCU\Console /v CodePage /t REG_DWORD /d 65001 /f
```

Command and Control (C2) Communication

SANNY malware uses the FTP protocol as the C2 communication channel.

FTP Config File

The FTP configuration information used by SANNY malware is encoded and stored inside ipnet.ini.



FEB

MAR

MAY

2017

2018

2019

31

31

31

24 captures

31 Mar 2018 - 17 Jul 2024

?

?

?

f

t

About this capture

- FTP Server: ftp.capnix[.]com
- Username: cnix_21072852
- Password: vlasimir2017

It then continues to perform the connection to the FTP server decoded from the aforementioned config file, and sets the current directory on the FTP server as “htdocs” using the FtpSetCurrentDirectoryW function.

System Information Collection

For reconnaissance purposes, SANNY malware executes commands on the system to collect information, which is sent to the C2 server.

System information is gathered from the machine using the following command:

The list of running tasks on the system is gathered by executing the following command:

C2 Commands

After successful connection to the FTP server decoded from the configuration file, the malware searches for a file containing the substring “to everyone” in the “htdocs” directory. This file will contain C2 commands to be executed by the malware.

Upon discovery of the file with the “to everyone” substring, the malware will download the file and then performs actions based on the following command names:

- chip command: This command deletes the existing ipnet.ini configuration file from the file system and creates a new ipnet.ini file with a specified configuration string. The chip commands allows the attacker to migrate malware to a new FTP C2 server. The command has the following syntax:
- pull command: This command is used for the purpose of data exfiltration. It has the ability to upload an arbitrary file from the local filesystem to the attacker’s FTP server. The command has the following syntax:

The uploaded file is compressed and encrypted using the routine described later in the Compression and Encoding Data section.

- put command: This command is used to copy an existing file on the system to a new location and delete the file from the original location. The command has the following syntax:
- default command: If the command begins with the substring “cmd /c”, but it is not followed by



FEB MAR MAY
2017 2018 2019
About this capture

24 captures

following steps:

1. Enumerates the running processes on the system to search for the explorer.exe process and obtain the process ID of explorer.exe.
2. Obtains the access token for the explorer.exe process with the access flags set to 0x000F01FF.
3. Starts the application (defined in the C2 command) on the system by calling the CreateProcessAsUser function and using the access token obtained in Step 2.

C2 Command	Purpose
chip	Update the FTP server config file
pull	Upload a file from the machine
put	Copy an existing file to a new destination
/user	Create a new process with explorer.exe access token
default command	Execute a program on the machine using WinExec()

Compression and Encoding Data

SANNY malware uses an interesting mechanism for compressing the contents of data collected from the system and encoding it before exfiltration. Instead of using an archiving utility, the malware leverages Shell.Application COM object and calls the CopyHere method of the IShellDispatch interface to perform compression as follows:

1. Creates an empty ZIP file with the name: temp.zip in the %temp% directory.
2. Writes the first 16 bytes of the PK header to the ZIP file.
3. Calls the CopyHere method of IShellDispatch interface to compress the collected data and write to temp.zip.
4. Reads the contents of temp.zip to memory.
5. Deletes temp.zip from the disk.
6. Creates an empty file, post.txt, in the %temp% directory.
7. The temp.zip file contents are Base64 encoded (using the same custom character set mentioned in the previous FTP Config File section) and written to the file: %temp%\post.txt.
8. Calls the FtpPutFileW function to write the contents of post.txt to the remote file with the format:
"from <computer_name timestamp>.txt"

Execution on Windows 7 and User Account Control (UAC) Bypass

NTWDBLIB.dll – This component from the CAB file will be extracted to the %windir%\system32 directory.



Execution on Windows 10 and UAC Bypass

Update.dll – This component from the CAB file is used to perform UAC bypass on Windows 10. As described in the BAT File Analysis section, if the underlying operating system is Windows 10, then it uses update.dll to begin the execution of code instead of invoking the install.bat file directly.

The main actions performed by update.dll are as follows:

1. Executes the following commands to setup the Windows registry for UAC bypass:
2. Leverages a [UAC bypass technique](#) that uses the legitimate Windows binary, fodhelper.exe, to perform the UAC bypass on Windows 10 so that the install.bat file is executed with elevated privileges:
3. Creates an additional BAT file, kill.bat, in the current directory to delete evidence of the UAC bypass. The BAT file kills the current process and deletes the components update.dll and kill.bat from the file system:

Conclusion

This activity shows us that the threat actors using SANNY malware are evolving their malware delivery methods, notably by incorporating UAC bypasses and endpoint evasion techniques. By using a multi-stage attack with a modular architecture, the malware authors increase the difficulty of reverse engineering and potentially evade security solutions.

Users can protect themselves from such attacks by disabling Office macros in their settings and practicing vigilance when enabling macros (especially when prompted) in documents, even if such documents are from seemingly trusted sources.

Indicators of Compromise

SHA256 Hash	Original Filename
b0f30741a2449f4d8d5ffe4b029a6d3959775818bf2e85bab7fea29bd5acafa4	РГНФ 2018-2019.doc
e29fad201feba8bd9385893d3c3db42bba094483a51d17e0217ceb7d3a7c08f1	Copy of communication

FireEye

FEB

MAR

MAY

31

2018

2019

About this capture

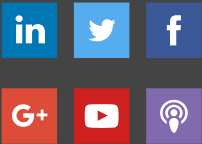
24 captures

31 Mar 2018 - 17 Jul 2024

eb394523df31fc83aefa402f8015c4a46f534c0a1f224151c47e80513ceea46f	1.bat
a2e897c03f313a097dc0f3c5245071fbaeee316cfb3f07785932605046697170	Setup.cab (64-bit)
a3b2c4746f471b4eabc3d91e2d0547c6f3e7a10a92ce119d92fa70a6d7d3a113	Setup.cab (32-bit)

This entry was posted on Fri Mar 23 11:00 EDT 2018 and filed under [Malware](#), [TTPs](#), [Yijie Sui](#), [tactics](#), [techniques and procedures](#), and [Sudeep Singh](#).

Stay Connected



Contact Us
+1 877-347-3393

Company

- About FireEye
- Customer Stories
- Careers
- Partners
- Investor Relations
- Supplier Documents

News & Events

- Newsroom
- Press Releases
- Webinars
- Events
- Blogs
- Communication Preferences

Technical Support

- Incident?
- Report Security Issue
- Contact Support
- Customer Portal
- Communities
- Documentation Portal

Cyber Threat Map