



Google Cloud

Blog

Contact sales

Get started for free

Threat Intelligence

APT10 Targeting Japanese Corporations Using Updated TTPs

September 13, 2018

Mandiant

Written by: Ayako Matsuda, Irshad Muhammad



Introduction

In July 2018, FireEye devices detected and blocked what appears to be APT10 (Menupass) activity targeting the Japanese media sector. APT10 is a Chinese cyber espionage group that FireEye has tracked since 2009, and they have a history of [targeting Japanese entities](#).

In this campaign, the group sent spear phishing emails containing malicious documents that led to the installation of the UPPERCUT backdoor. This backdoor is well-known in the security community as [ANEL](#), and it

and differences we have observed across multiple versions of this backdoor.

Attack Overview

The attack starts with Microsoft Word documents containing a malicious VBA macro being attached to spear phishing emails. Although the contents of the malicious documents are unreadable (see Figure 3), the Japanese titles are related to maritime, diplomatic, and North Korean issues. Table 1 shows the UPPERCUT indicators of compromise (IoCs).

File Name	MD5
-----------	-----

Contact sales

Get started for free

<div>に提言申し入れ.doc</div> <div>Government Recommendations from the Liberal Democratic Party's Comprehensive Strategic Maritime Subcommittee</div>	4f83c01e8f7507d23c67ab085bf7'
<div>グテマラ大使講演会案内状.doc</div> <div>Invitation to Lecture by Guatemalan Ambassador</div>	f188936d2c8423cf064d6b816076
<div>米国接近に揺れる北朝鮮内部.doc</div> <div>North Korean interior swayed by the approach of the United States</div>	cca227f70a64e1e7fcf5bccdc6cc2

Table 1: UPPERCUT IoCs

In the Guatemalan lure, the attacker used an unusual spelling of Guatemala in Japanese. The top result of a Google search using the same spelling led us to the event website for the lecture of the Guatemalan Ambassador, held in August 2018. Figure 1 shows the screenshot of the event page.

Figure 1: Event Website for the Lecture of Guatemala Ambassador

Figure 2 shows the macro function that displays the lure document. At the bottom of this function, we can see the readable text that matches the contact information found in Figure 1. Thus, people who would have an interest in Latin American issues may have been the targets of this campaign.

Figure 2: Macro to display lure document

The initial Word documents were password protected, likely in an effort to bypass detection. Once the password (delivered in the body of the email) is entered, the users are presented with a document that will request users to enable the malicious macro, as shown in Figure 3.

Figure 4 shows what happens when the malicious macro is executed.

Figure 4: Macro to install UPPERCUT

The execution workflow is as follows:

- 1. The macro drops three PEM files, padre1.txt, padre2.txt, and padre3.txt, to the victim's %TEMP% folder and then copies them from %TEMP% to the %AllUserProfile% folder.
- 2. The macro decodes the dropped files using Windows certutil.exe with the following commands (certutil.exe is a legitimate built-in command-line program to manage certificates in Windows):

C:\Windows\System32\cmd.exe" /c certutil -decode C:\ProgramData\padre1.txt C:\ProgramData\GUP.txt
C:\Windows\System32\cmd.exe" /c certutil -decode C:\ProgramData\padre2.txt C:\ProgramData\libcurl.txt
C:\Windows\System32\cmd.exe" /c certutil -decode C:\ProgramData\padre3.txt

3. The macro creates a copy of the files with their proper extensions using Extensible Storage Engine Utilities (esentutil.exe) with the following commands (esentutil.exe is also a legitimate program that is pre-installed in Windows):

```
C:\Windows\System32\esentutil.exe" /y  
C:\ProgramData\GUP.txt /d C:\ProgramData\GUP.exe  
/o
```

```
C:\Windows\System32\esentutil.exe" /y  
C:\ProgramData\libcurl.txt /d  
C:\ProgramData\libcurl.dll /o
```

The dropped files include the following:

- GUP.exe : GUP, a free (LGPL) Generic Updater. GUP is an open source binary used by Notepad++ for software updates. The version used here is version 4.1 digitally signed by Notepad++, as shown in Figure 5.
- libcurl.dll: Malicious Loader DLL
- 3F2E3AB9: Encrypted shellcode

Figure 5: Notepad++ signed updater

4. The macro launches the legitimate executable GUP.exe.

(3F2E3AB9) located in the same folder.

- The shellcode decodes and decompresses another DLL, which is an updated variant of UPPERCUT. Before decoding the DLL, the shellcode uses an anti-debug technique based on `ntdll_NtSetInformationThread` which causes the thread to be detached from the debugger, as shown in Figure 6. The DLL is then loaded into memory and the randomly named exported function is called.

Figure 6: Anti-debug technique used by shellcode

5. The macro deletes the initially dropped .txt files using Windows `esentutl.exe` and changes the document text to an embedded message.

The complete attack overview is shown in Figure 7.

Figure 7: Attack overview

Several threat actors leverage the technique of using [Windows `certutil.exe`](#) for [payload decoding](#), and APT10 continues to employ this technique.

Evolution of UPPERCUT

droppers (word documents) are plotted in the graph. The compile time of loaders in the newer version(s) are not shown here since the timestamps are overwritten and filled with zeroes. We don't have visibility into UPPERCUT 5.2.x series, but it's possible that minor revisions were released every few months between December 2017 and May 2018.

Figure 8: Timeline of UPPERCUT updates

Unlike previous versions, the exported function names are randomized in the latest version (Table 2).

Encoded Payload	Decoded Payload	
MD5	Size	
aa3f303c3319b14b4829fe2faa5999c1	322164	
126067d634d94c45084cbe1d9873d895	330804	
fce54b4886cac5c61eda1e7605483ca3	345812	

Table 2: Static characteristics of UPPERCUT

header if it fails to receive the HTTP response from the command and control (C2) server. The error code is the value returned by the GetLastError function and sent in the next beacon. This was likely included to help the attackers understand the problem if the backdoor is unable to receive a response (Figure 9). This Cookie header is a unique indicator that can be used for network-based detection.

Figure 9: Example of callback

Earlier versions of UPPERCUT used the hard-coded string “this is the encrypt key” for Blowfish encryption when communicating with a C2. However, in the latest version, the keys are hard-coded uniquely for each C2 address and use the C2’s calculated MD5 hash to determine which key to use, as shown in Figure 10.

Figure 10: Blowfish key generation

For instance, Table 3 lists the hard-coded C2 addresses, their MD5 hash, and the corresponding Blowfish key in the decoded payload of 126067d634d94c45084cbe1d9873d895.

hxxp[:]//151.106.53[.]147/VxQG	f613846eb5bed22
hxxp[:]//153.92.210[.]208/wBNh1	50c60f37922ff2ff
hxxp[:]//eservake.jetos[.]com/qlDj	c500dae1ca41236
Default	Default

Table 3: Example of Blowfish keys

In this example, the MD5 hash of hxxp[:]//151.106.53[.]147/VxQG will be f613846eb5bed227ec1a5f8df7e678d0. When the malware interacts with this URL, bdc4b9f5af9868e028dd0adc10099a4e6656e9f0ad12b2e75a30f5ca0e34489d will be selected as a Blowfish key. If the MD5 hash of the URL does not match any of the listed hashes, then the default key f12df6984bb65d18e2561bd017df29ee1cf946efa5e510802005aeee9035dd53 will be used.

Another difference in the network traffic generated from the malware is that the encoded proxy information has been added in the URL query values during the C2 communication. Table 4 shows the parameters sent to C2 server from the backdoor in the newer versions. These are sent via POST request, as shown in Figure 9.

Additionally, the command string is hashed using the same RGPH hashing algorithm as before. Two more commands, 0xD290626C85FB1CE3 and 0x409C7A89CFF0A727, are supported in the newer versions (Table 5).

Commands	Description
0x97A168D9697D40DD	Download and validate file (XXHash comparison) from C2 server
0x7CF812296CCC68D5	Upload file to C2 server
0x652CB1CEFF1C0A00	Load PE file
0x27595F1F74B55278	Download, validate (XXHash comparison), execute file, and send output to C2 server
0xD290626C85FB1CE3	Format the current timestamp
0x409C7A89CFF0A727	Capture the desktop screenshot in PNG format and send it to C2

None of the above	the output is then sent to the C2 server
-------------------	--

Table 5: Supported commands

Conclusion

While APT10 consistently targets the same geolocation and industry, the malware they use is actively evolving. In the newer versions of UPPERCUT, there is a significant change in the way backdoor initializes the Blowfish encryption key, which makes it harder for analysts to detect and decrypt the backdoor’s network communications. This shows that APT10 is very capable of maintaining and updating their malware.

To mitigate the threat, users are advised to disable Office macros in their settings and not to open documents from unknown sources. FireEye Multi-Vector Execution (MVX) engine is able to recognize and block this threat with the following detection names:

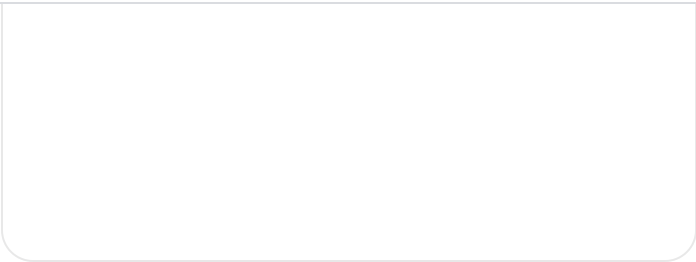
- APT.Backdoor.Win.UPPERCUT
- FE_APT_Backdoor_Win32_UPPERCUT

Posted in [Threat Intelligence](#)—[Security & Identity](#)

Related articles

Contact sales

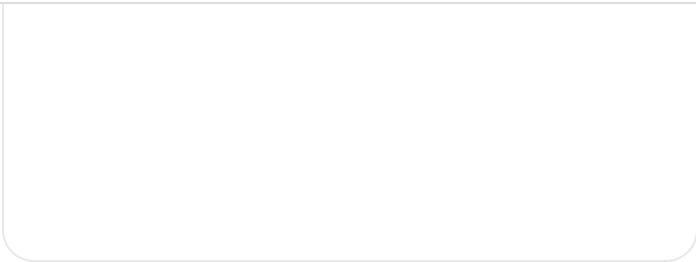
Get started for free



Threat Intelligence

Hybrid Russian Espionage and
Influence Campaign Aims to
Compromise Ukrainian Military Recruits
and Deliver Anti-Mobilization Narratives

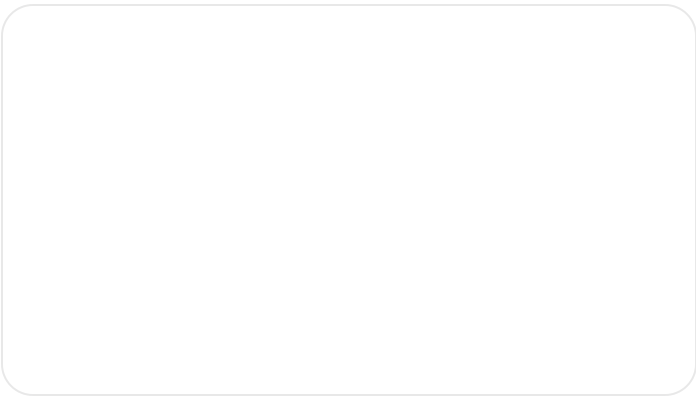
By Google Threat Intelligence Group • 10-minute
read



Threat Intelligence

Investigating FortiManager Zero-Day
Exploitation (CVE-2024-47575)

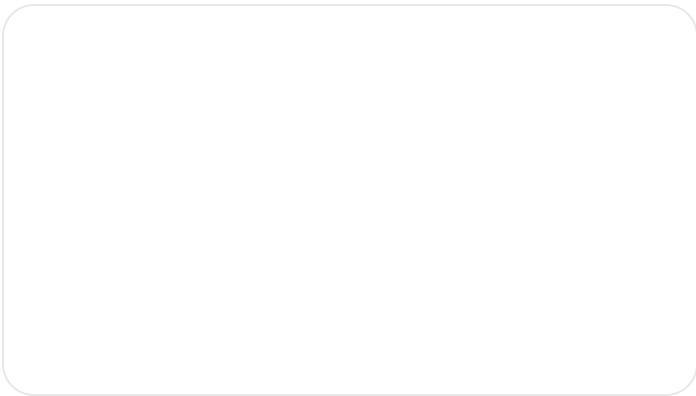
By Mandiant • 19-minute read



Threat Intelligence

How Low Can You Go? An Analysis of
2023 Time-to-Exploit Trends

By Mandiant • 10-minute read



Threat Intelligence

capa Explorer Web: A Web-Based Tool
for Program Capability Analysis

By Mandiant • 6-minute read

Contact sales

Get started for free



Google Cloud

Google Cloud Products

Privacy

Terms

? Help

English ▼