THREAT RESEARCH

APT10 Targeting Japanese Corporations Using Updated

AYAKO MATSUDA, IRSHAD MUHAMMAD

SEP 13, 2018 | 6 MIN READ | LAST UPDATED: AUG 10, 2023

#ADVANCED PERSISTENT THREATS (APTS) #TTPS #THREAT RESEARCH #MALWARE

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 docume

REPORT

Company

to the installation of the UPPERCUT backdoor. This backdoor is well-known in the se community as ANEL, and it used to come in beta or RC (release candidate) until recently. Part of this blog post will discuss the updates and differences we have observed across multiple versions of this backdoor.

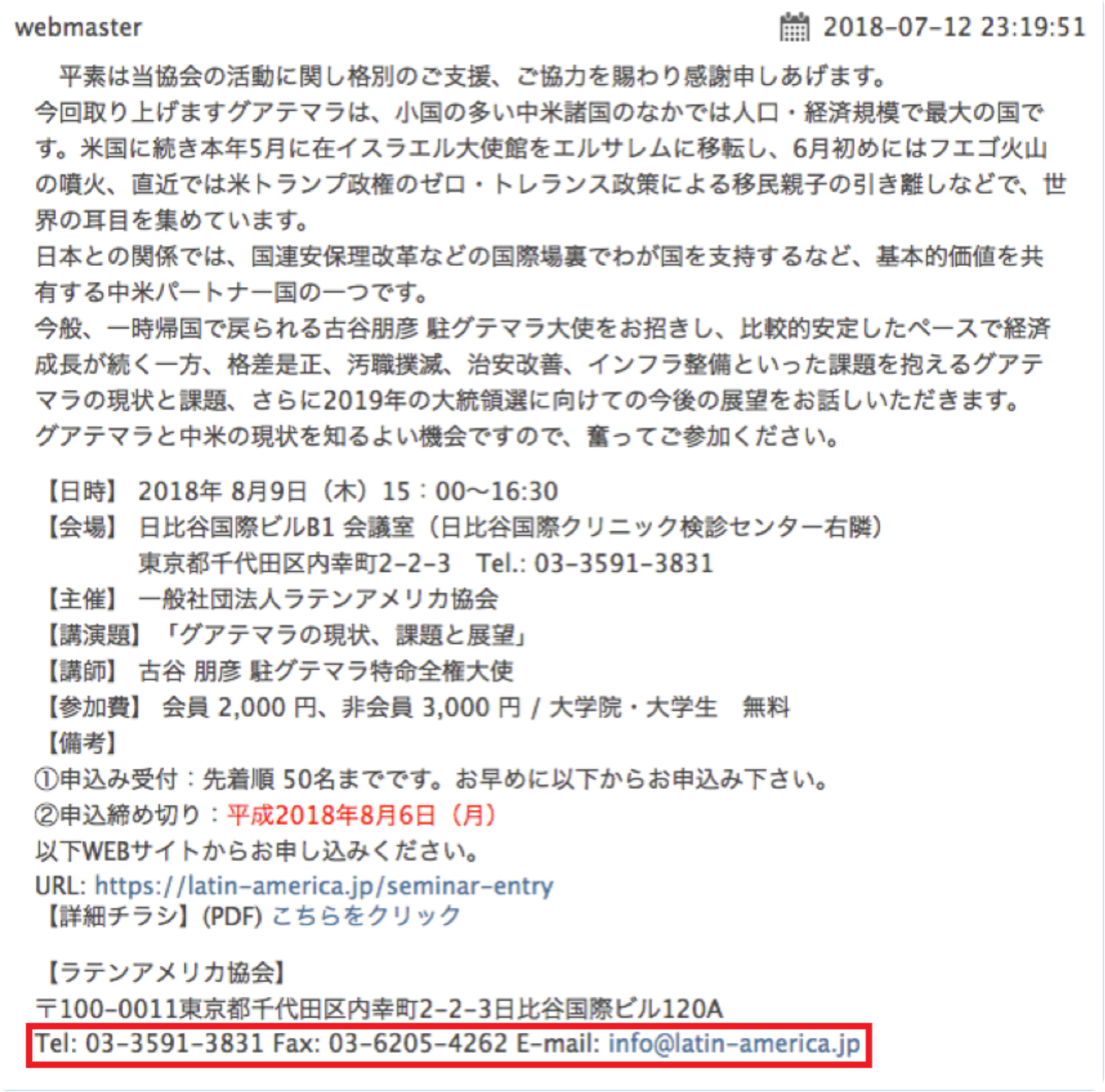
Attack Overview

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	Size	C2
自民党海洋総合戦略小委員 Maritime Subcommittee			
グテマラ大使講演会案内状.doc Invitation to Lecture by Guatemalan Ambassador	f188936d2c8423cf064d6b8160769f21	720384	eservake.jetos[.]com 151.106.53.147 153.92.210.208
米国接近に揺れる北朝鮮内部.doc North Korean interior swayed by the approach of the United States	cca227f70a64e1e7fcf5bccdc6cc25dd	733184	eservake.jetos[.]com 153.92.210.208 167.99.121.203

Table 1: UPPERCUT IoCs

For the North Korean lure, a news article with an identical title was readily available online. It's also worth noting that 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.



webmaster 2018-07-12 23:19:51

　平素は当協会の活動に関し格別のご支援、ご協力を賜わり感謝申しあげます。
今回取り上げますグアテマラは、小国の多い中米諸国のなかでは人口・経済規模で最大の国です。米国に続き本年5月に在イスラエル大使館をエルサレムに移転し、6月初めにはフエゴ火山の噴火、直近では米トランプ政権のゼロ・トレランス政策による移民親子の引き離しなどで、世界の耳目を集めています。
日本との関係では、国連安保理改革などの国際場裏でわが国を支持するなど、基本的価値を共有する中米パートナー国の一つです。
今般、一時帰国で戻られる古谷朋彦 駐グテマラ大使をお招きし、比較的安定したペースで経済成長が続く一方、格差是正、汚職撲滅、治安改善、インフラ整備といった課題を抱えるグアテマラの現状と課題、さらに2019年の大統領選に向けての今後の展望をお話しいただきます。
グアテマラと中米の現状を知るよい機会ですので、奮ってご参加ください。

【日時】 2018年 8月9日（木）15：00～16:30
【会場】 日比谷国際ビルB1 会議室（日比谷国際クリニック検診センター右隣）
　　　　東京都千代田区内幸町2-2-3　Tel.: 03-3591-3831
【主催】 一般社団法人ラテンアメリカ協会
【講演題】「グアテマラの現状、課題と展望」
【講師】 古谷 朋彦 駐グテマラ特命全権大使
【参加費】 会員 2,000 円、非会員 3,000 円 / 大学院・大学生　無料
【備考】
①申込み受付：先着順 50名までです。お早めに以下からお申込み下さい。
②申込締め切り：平成2018年8月6日（月）
以下WEBサイトからお申し込みください。
URL: https://latin-america.jp/seminar-entry
【詳細チラシ】(PDF) こちらをクリック

【ラテンアメリカ協会】
〒100-0011東京都千代田区内幸町2-2-3日比谷国際ビル120A
Tel: 03-3591-3831 Fax: 03-6205-4262 E-mail: info@latin-america.jp

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 3: Lure document

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
C:\ProgramData\\3F2E3AB9
```

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\esentutl.exe" /y C:\ProgramData\\GUP.txt /d C:\ProgramData\GUP.exe /o
```

```
C:\Windows\System32\esentutl.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.

- The executable sideloads the malicious DLL (libcurl.dll), which decrypts and runs shellcode (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

Figure 8 shows the timeline of updates for UPPERCUT. The PE compile time of loaders and the create time of 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	Import Hash	Exported Funct
aa3f303c3319b14b4829fe2faa5999c1	322164	182ee99b4f0803628c30411b1faa9992	I7MF25T96n45c
126067d634d94c45084cbe1d9873d895	330804	5f45532f947501cf024d84c36e3a19a1	hJvTJcdAU3mN
fce54b4886cac5c61eda1e7605483ca3	345812	c1942a0ca397b627019dace26eca78d8	WcuH

Table 2: Static characteristics of UPPERCUT

Another new feature in the latest UPPERCUT sample is that the malware sends an error code in the Cookie 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.

C2	**MD5**	**Blowfish Key**
hxxp[:]//151.106.53[.]147/VxQG	f613846eb5bed227ec1a5f8df7e678d0	bdc4b9f5af9868e028dd0adc100
hxxp[:]//153.92.210[.]208/wBNh1	50c60f37922ff2ff8733aaeaa9802da5	fb9f7fb3c709373523ff27824ed6a
hxxp[:]//eservake.jetos[.]com/qIDj	c500dae1ca41236830b59f1467ee96c1	d3450966ceb2eba93282aace7d7
Default	Default	f12df6984bb65d18e2561bd017df2

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.

Table 4: URL parameters

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 received buffer is executed via cmd.exe and 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

Link to RSS feed

Mandiant Advantage Platform

Platform Overview

Security Validation

Attack Surface Management

Threat Intelligence

Digital Threat Monitoring

Managed Defense

Solutions

Proactive Exposure Management

Ransomware

Industrial Controls & OT

Cyber Risk Management

Digital Risk Protection

Insider Threats

Cyber Security Skills Gap

Election Security

Government Cyber Security

Manufacturing

Cyber Threat Visibility

Attack Surface Visibility

Cyber Preparedness

Detection and Response

Financial Services Cyber Security

Services

Services Overview

Incident Response

Strategic Readiness

Cyber Security Transformation

Technical Assurance

View all Services (48)

Expertise on Demand

Mandiant Academy

Overview

Education Formats

Upcoming Courses

On-Demand Courses

Certifications

ThreatSpace Cyber Range

Free Course Sneak Peaks

Resources

Resource Center

Blog

Podcasts

Company

About Us

Careers

Events

Partners

Partners Overview

Technology Partners

Cyber Risk Partners

Connect with Mandiant

Contact Us

Report an Incident

Customer Support

Customer Stories

Reports

Webinars

Insights

eBooks

Infographics

White Papers

Datasheets

Media Center

Service Partners

Partner Portal

Customer Success

Media Inquiries

Website Privacy Policy Terms & Conditions Compliance

Site Map