IXESHE Derivative IHEATE Targets Users in America

blog.trendmicro.com/trendlabs-security-intelligence/ixeshe-derivative-iheate-targets-users-america/

by Razor Huang and CH Lei

Since 2012, we've been keeping an eye on the IXESHE targeted attack campaign. Since its inception in 2009, the campaign has primarily targeted governments and companies in East Asia and Germany. However, the campaign appears to have shifted tactics and is once again targeting users in the United States.

We also noticed that there were some changes to the underlying behavior of the malware used. While there were some incremental improvements in the observed behavior of the new sample, the underlying pattern of behavior is similar to what we observed earlier from IXESHE.

These attacks targeting users in the United States used a variant of IXESHE which has been seen in Taiwan since 2009 named IHEATE. These showed some differences from known IXESHE variants: they had a different command-and-control (C&C) communication model and encryption methods.

One IHEATE sample we found contains the string "EMC112" as part of the C&C traffic. Such strings are frequently used to identify different campaigns. In this particular case, the 112 part of the string matched the malware sample's compilation date of January 12.

The sample we acquired connects to a C&C server whose domain was first registered in 2004, but whose information was modified in December 2015. This suggests that threat actors were able to pose as the original registrant and modify the information for their own needs.

Technical Analysis

IXESHE is a well-known targeted attack campaign which has mainly targeted East Asian governments, electronics manufacturers, and a telecommunications company in Germany. Other targets include G20 government officials as well as the *New York Times*. The campaign is known for targeting users with fake documents using exploits and right-to-left override (RTLO) techniques.

The particular sample we found has a SHA1 hash of 3de8ef34fb98ce5d5d0ec0f46ff92319a5976e63. We detect it as BKDR_IHEATE. Unlike common IXESHE variants which usually communicate with C&C servers via HTTP and a customized Base64-ecoded payload, IHEATE communicates with C&C servers in the TCP layer. (HEATE is a command that is sent by some members of this family to servers that acts as a notice that it's still online; we derived the name IHEATE from this command and its ties to the IXESHE family.)

We have learned from IXESHE variants that even though the encryption routine changed in different variants but the decrypted messages are almost similar.

Information gathering

Once the backdoor is installed, it collects information on the victim's system and sends it to C&C server with the following format :

> *| [Computer name] | [User name] | [IP] | [OS version] | [Process ID or Tag]*

Not all samples include a tag in their message. This tag could be a process ID, victim information, or the date when the malware was compiled. In this IHEATE sample, the tag is “EMC112”. The 112 portion may refer to when the malware was compiled, as its compile date/time is 2016/01/12 03:22:27.

The threat actors behind IHEATE could use these tags to manage victims. The traffic back to their C&C servers could easily be sorted using these tags.

Sometime they slightly change the feedback format, such as

- Removing spaces:“[Computer name]|[User name]|[IP]|[OS version]|[Tag]”
- Changing the delimiter:“* [Computer name] * [User name] * [IP] * [OS version] * [Tag]”

Backdoor instructions

IHEATE provides a similar set of commands as most IXESHE variants. Note that the following list is case insensitive:

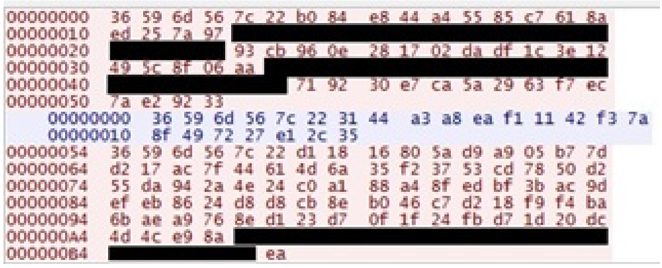
- /WINCMD %s – Launch command and get the output
- /GETCMD %s – copy cmd.exe and rename
- /DISK – List all disks
- /CD – get current directory
- /CD %s – change directory
- /DIR %s – browse directory
- /DEL %s – delete file
- /GETFILE %s – upload file
- /PUTFILE %s – download file
- /TASKLIST – list running processes
- /TASKKILL %s – kill a running process
- /SHUTDOWN – shut down the malware
- /SLEEP %s – sleep for specific period

Encryption

While IXESHE variants have fairly similar phone-home and backdoor routines, they have a wide variety of encryption routines. IHEATE is no different, and has its own unique behavior.

The traffic below simulates the traffic between a IHEATE-affected machine and its C&C server. Traffic from the client to the server is in red; traffic from the server to the client is in blue. The C&C server has sent a /DISK command to the machine.

Figure 1. Captured IHEATE network traffic



```
00000000  36 59 6d 56 7c 22 b0 84  e8 44 a4 55 85 c7 61 8a
00000010  ed 25 7a 97 [redacted]
00000020  [redacted] 93 cb 96 0e  28 17 02 da df 1c 3e 12
00000030  49 5c 8f 06 aa [redacted]
00000040  [redacted] 71 92  30 e7 ca 5a 29 63 f7 ec
00000050  7a e2 92 33
    00000000  36 59 6d 56 7c 22 31 44  a3 a8 ea f1 11 42 f3 7a
    00000010  8f 49 72 27 e1 2c 35
00000054  36 59 6d 56 7c 22 d1 18  16 80 5a d9 a9 05 b7 7d
00000064  d2 17 ac 7f 44 61 4d 6a  35 f2 37 53 cd 78 50 d2
00000074  55 da 94 2a 4e 24 c0 a1  88 a4 8f ed bf 3b ac 9d
00000084  ef eb 86 24 d8 d8 cb 8e  b0 46 c7 d2 18 f9 f4 ba
00000094  6b ae a9 76 8e d1 23 d7  0f 1f 24 fb d7 1d 20 dc
000000A4  4d 4c e9 8a [redacted]
00000084  [redacted] ea
```

The first part of the network traffic is from the client to the C&C server. It is as follows:

1. The first six bytes make up the hardcoded portion of the encryption key. In this case, it is “36 59 6d 56 7c 22”. We have seen different encryption keys in other IHEATE variants; in some variants this part is ten bytes long.

2. The following eight bytes make up the randomly generated portion of the encryption key. Here it is “b0 84 e8 44 a4 55 85 c7”. In some samples, this portion is ten bytes long.
3. The next two bytes say how long the encrypted data is, here it is “61 8a”. The contents are encrypted with RC4, using the randomly generated encryption key.
4. Last is the data itself. This is also encrypted using RC4, with the hardcoded and randomly generated portions of the encryption key concatenated together.

The second part is the response of the server to the client. It is described as follows:

1. The encryption procedure is identical to that used by the client to talk to the server.
2. The six-bit hardcoded portion of the encryption key *must* be identical to the one used by the client earlier. Otherwise, if the keys do not match, the connection is dropped.

However, some newer IHEATE samples use yet another technique. These use asymmetric encryption:

1. Before communicating with C&C server, the malware client generates a random session key.
2. The client encrypts the session key using RSA-1024, using a public key hardcoded inside of malware.
3. The client encrypts the data to be sent using a custom encryption routine.
4. On top of this, the data sent to the C&C server is encrypted with RC4, using the previously generated session key,

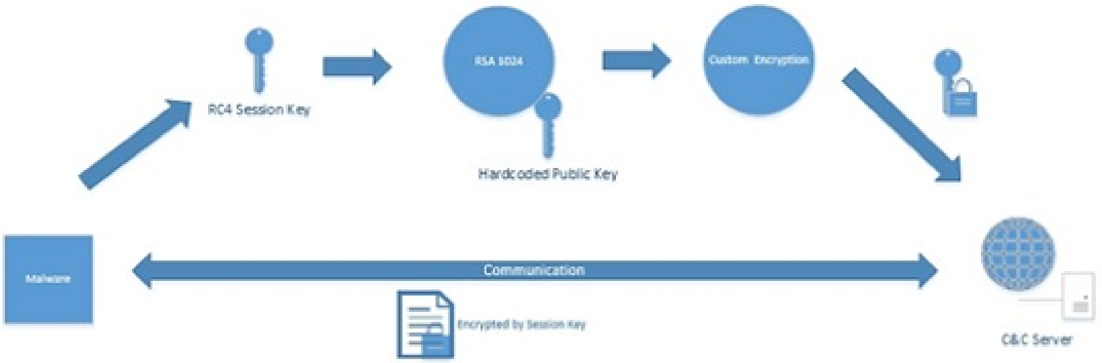
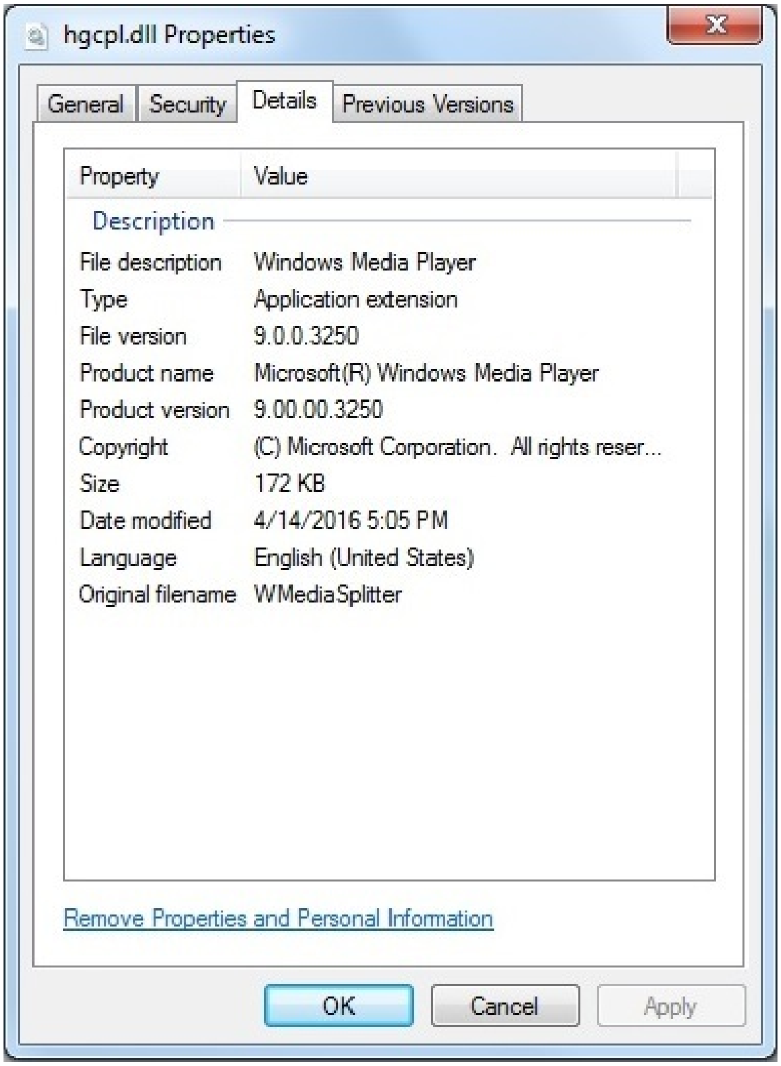


Figure 2. Asymmetric encryption as used by IHEATE

File properties

The IHEATE sample with the “EMC112” identifier passes itself off as legitimate Media Player-related .DLL file, as can be seen below:



Property	Value
Description	
File description	Windows Media Player
Type	Application extension
File version	9.0.0.3250
Product name	Microsoft(R) Windows Media Player
Product version	9.00.00.3250
Copyright	(C) Microsoft Corporation. All rights reser...
Size	172 KB
Date modified	4/14/2016 5:05 PM
Language	English (United States)
Original filename	WMediaSplitter

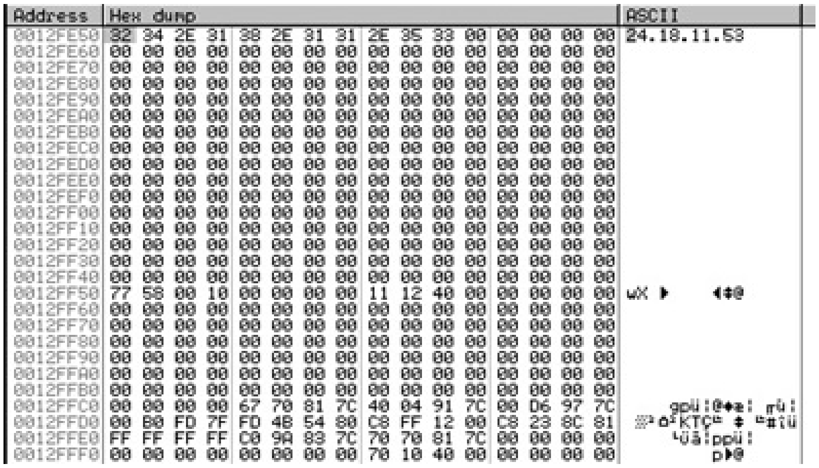
Figure 3. IHEATE pretending to be a Media Player .DLL file

C&C Servers

IXESHE was known for using compromised hosts for its C&C servers, and IHEATE behaves similarly.

The IHEATE sample with the “EMC112” identifier used the subdomain *cknew[.]{abused domain}[.]com* as the location of its C&C server. This domain appears to contain the personal blog of the original registrant, who has been using it since the domain was registered in 2004. We do not believe that the registrant is tied to IHEATE; instead we believe that his credentials were compromised so that threat actors could set up subdomains. This site was active briefly in the middle of 2015, but came back online at the start of 2016.

Other IHEATE samples showed interesting behavior as well. In one case, the attackers planted a fake C&C server address in the code:



```
Address  Hex dump                                         ASCII
0012FE50 32 34 2E 31 38 2E 31 31 2E 35 33 00 00 00 00 00 24.18.11.53
0012FE60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FE70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FE80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FE90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FEA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FEB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FEC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FED0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FEE0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FEF0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF50 77 58 00 10 00 00 00 00 11 12 40 00 00 00 00 00 wX ►    ◄‡@
0012FF60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FF90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FFA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FFB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0012FFC0 00 00 00 00 67 70 81 7C 40 04 91 7C 00 D6 97 7C     gpü¦@♦æ¦ ╓ù¦
0012FFD0 00 B0 FD 7F FD 4B 54 80 C8 FF 12 00 C8 23 8C 81  ░²⌂²KTÇ╚ ‡ ╚#îü
0012FFE0 FF FF FF FF C0 9A 83 7C 70 70 81 7C 00 00 00 00     └Üâ¦ppü¦
0012FFF0 00 00 00 00 00 00 00 00 70 10 40 00 00 00 00 00         p►@
```

Figure 4. Fake C&C server in code

The address here is not an actual C&C address; instead it is used to calculate the port that the client will use (in this case, 443: (24*18)+11.) Other attacks are known to have used similar tactics as well.

Other domains used by IHEATE also overlapped with servers used by IXESHE. Two domains (*ipv6pro[.]root[.]sx* and *gimeover[.]psp-moscow[.]com*) were used by IHEATE and resolved to the IP address *200[.]93[.]193[.]163*. At approximately the same time, IXESHE also used the same server – except it did so by accessing the domain *skype[.]silksky[.]com*.

Conclusions

IXESHE and associated threats like IHEATE have not gone away, and they continue to evolve and change with the times. We will continue to monitor this threat and apprise our readers of any future developments.