

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

By Anton Cherepanov

Archived: 2026-04-02 12:34:32 UTC

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.

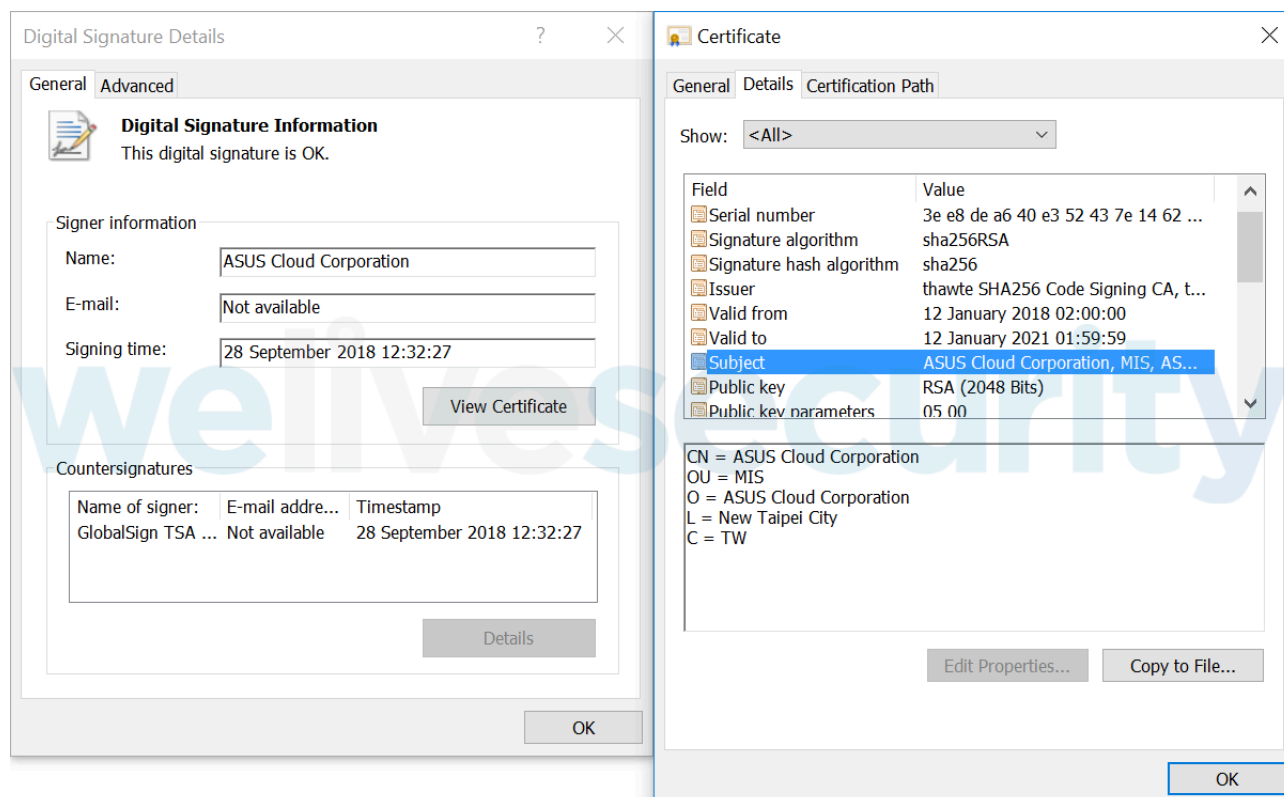


Figure 1. The AsusWSPanel.exe code-signing certificate

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 NewVerUr1, 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.

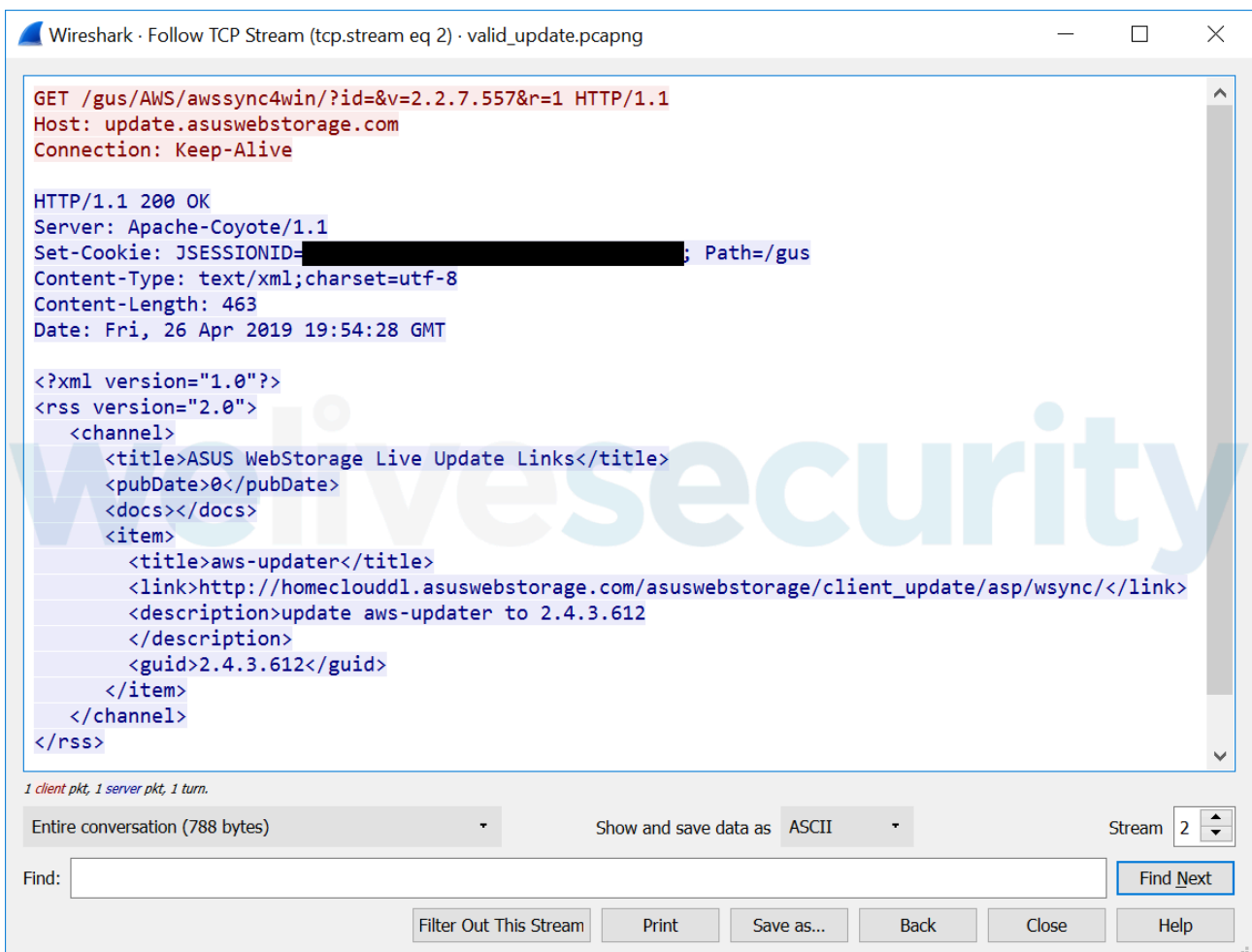


Figure 3. A legitimate communication during an update check of the ASUS WebStorage software

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.

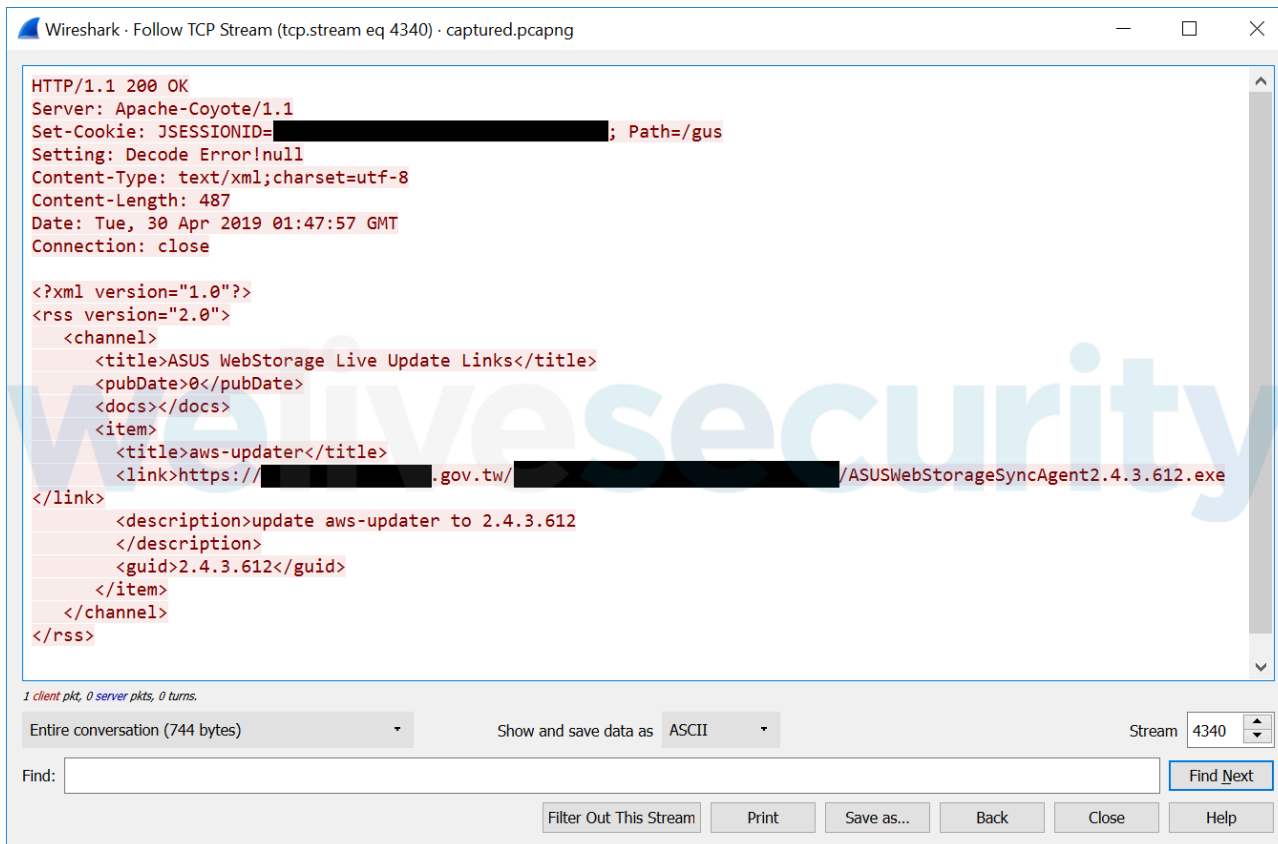
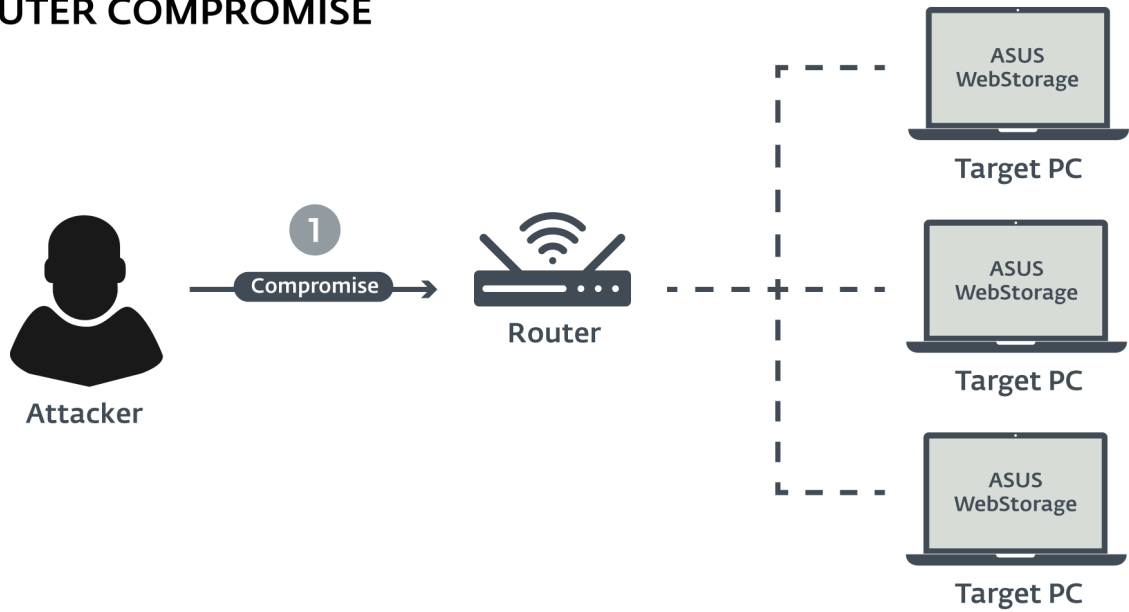


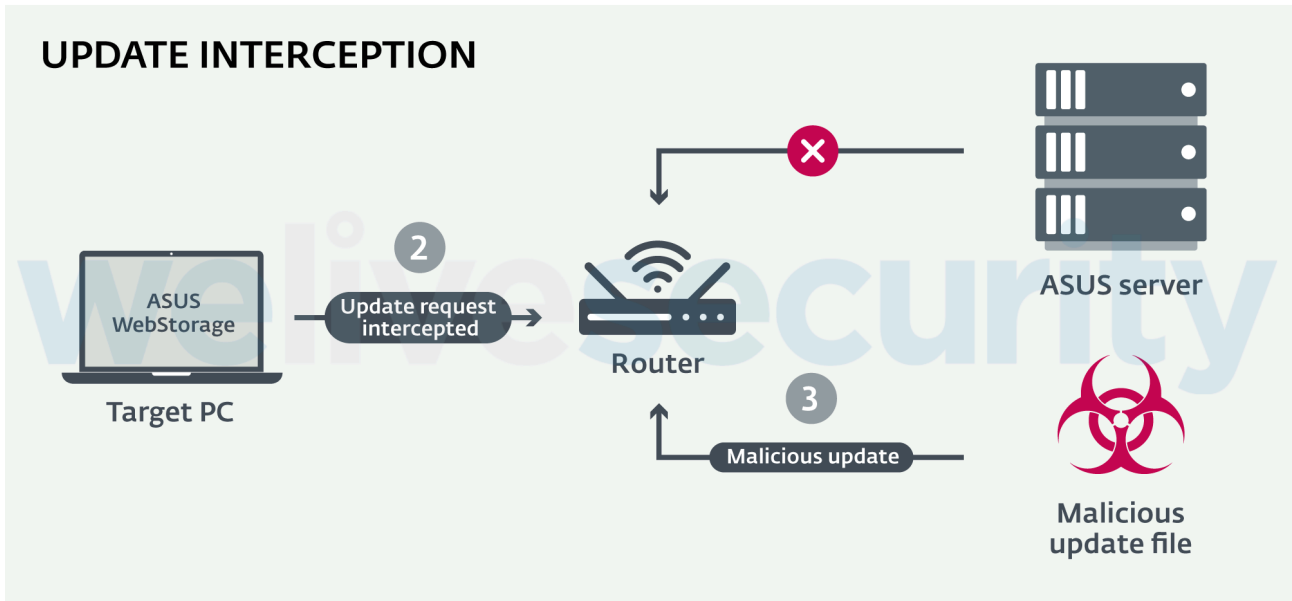
Figure 4. A captured communication during a malicious update of the ASUS WebStorage software

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

ROUTER COMPROMISE



UPDATE INTERCEPTION



PAYLOAD DELIVERY

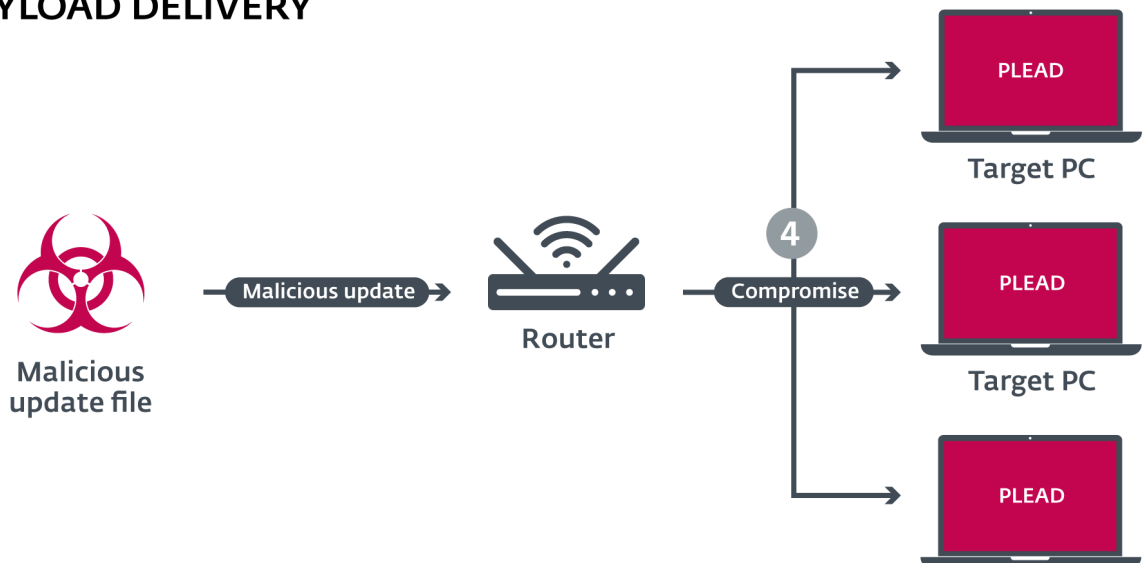


Figure 5. Man-in-the-middle attack scenario

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.

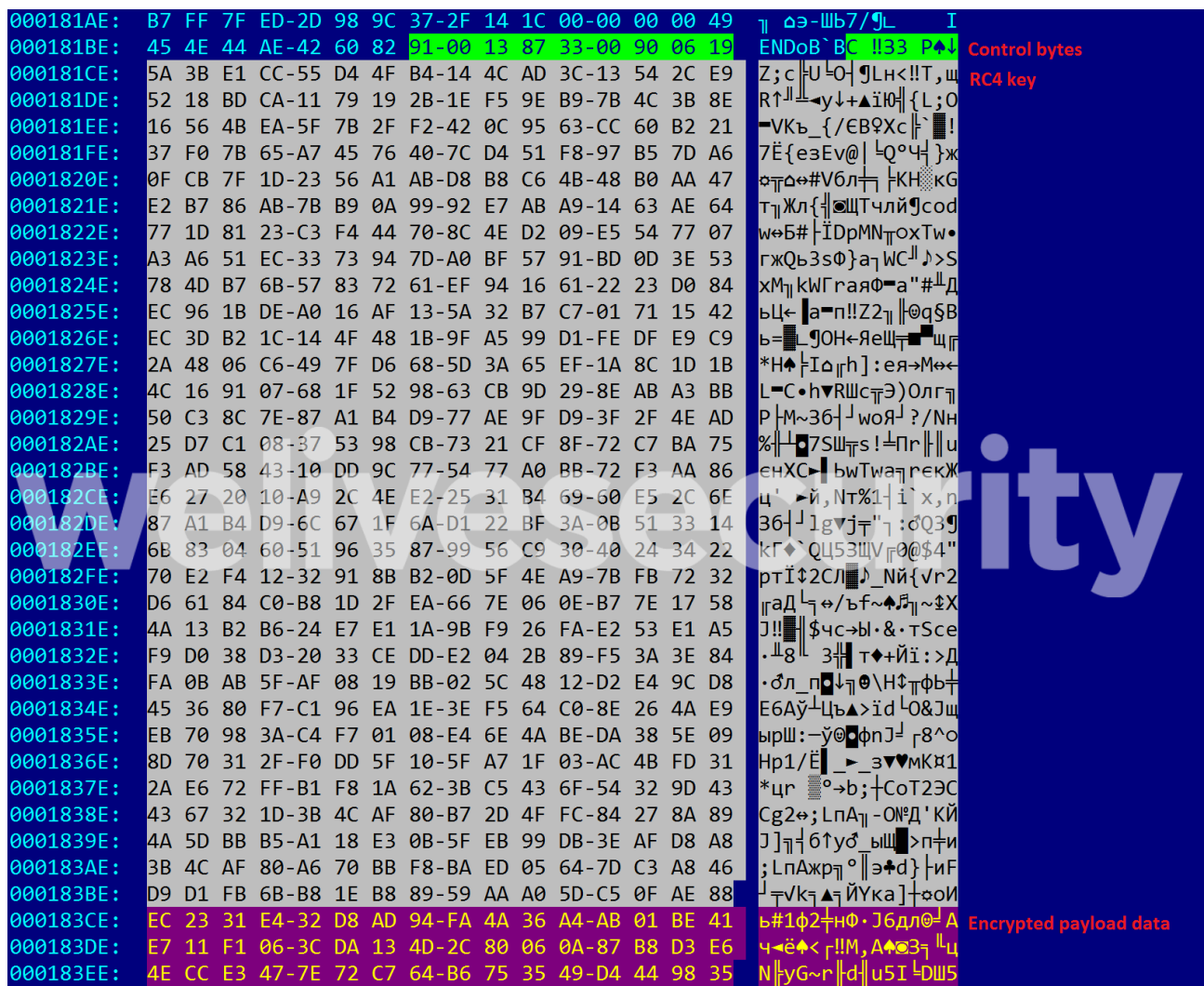


Figure 6. The data used by the Plead malware in the downloaded PNG file

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. |
| 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. |

Source: <https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/>