Magniber Ransomware Attempts to Bypass MOTW (Mark of the Web)

asec.ahnlab.com/en/41889/

November 11, 2022

The ASEC analysis team uploaded a post on October 25th to inform the users of the changes that have been made to the Magniber ransomware. Magniber, which is still actively being distributed, has undergone many changes to evade the detection of anti-malware software. Out of these changes, this blog will cover the script format found from September 8th to September 29th, 2022, which bypassed Mark of the Web (MOTW), a feature offered by Microsoft that identifies the source of files.

Date	Extension	Execution Process	Encryption Process	Recovery Environment Deactivation Process	Recovery Environment Deactivation (UAC Bypassing)
2022-05-07	msi	msiexec.exe	msiexec.exe	regsvr32.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**ms-settings**\shell\open\command)
6/14/2022	msi	msiexec.exe	Running Process	regsvr32.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)
7/20/2022	cpl	rundll32.exe	rundll32.exe	X	X

Date	Extension	Execution Process	Encryption Process	Recovery Environment Deactivation Process	Recovery Environment Deactivation (UAC Bypassing)
8/8/2022	cpl	rundll32.exe	Running Process	wscript.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)
9/8/2022	jse	wscript.exe	Running Process	wscript.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)
9/16/2022	js	wscript.exe	Running Process	wscript.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)
9/28/2022	wsf	wscript.exe	Running Process	wscript.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)
9/30/2022	msi	msiexec.exe	Running Process	wscript.exe	Modifies reference registry upon execution of fodhelper.exe (HKCU:\Software\Classes**(custom progID)**\shell\open\command)

Table 1. Major characteristics of Magniber ransomware by date (https://asec.ahnlab.com/en/40422/)

Table 1 shows the content of the ASEC blog post which covers the evolution of the Magniber ransomware. Among these changes, the threat operator used scripts as the distribution method during the period from September 8th to September 29th, 2022. Magniber was downloaded through the typosquatting method, which exploits typos made by the user when accessing domains (See Figure 1).

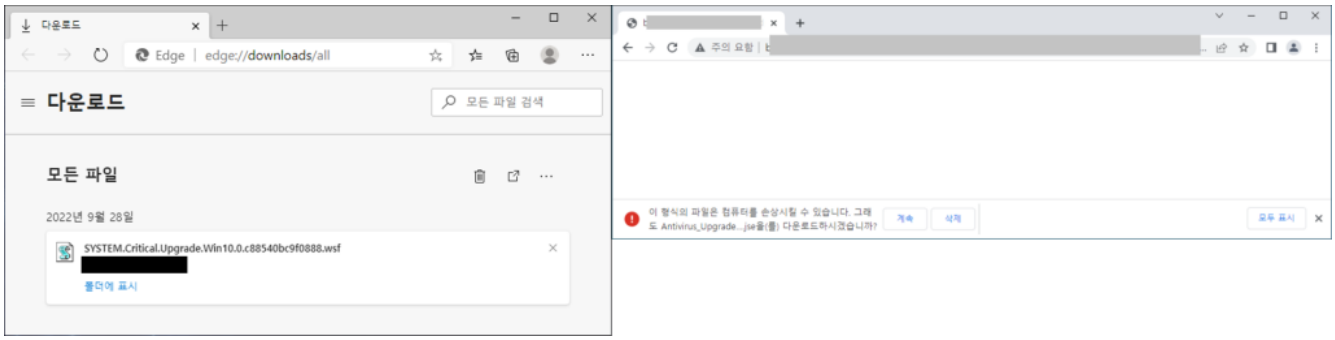

Figure 1. Typosquatting distribution method of Magniber

The downloaded file is identified to be from an external source by the Windows Mark of the Web (MOTW) feature.[2] MOTW operates on New Technology File System (NTFS). The download URL is recorded in a stream in Windows of NTFS.[3] The stream where the URL is saved is created in the file path in the format of “File Name:Zone.Identifier:$DATA” and can be easily viewed with Notepad. When the downloaded files identified by MOTW are executed, a warning message is displayed.

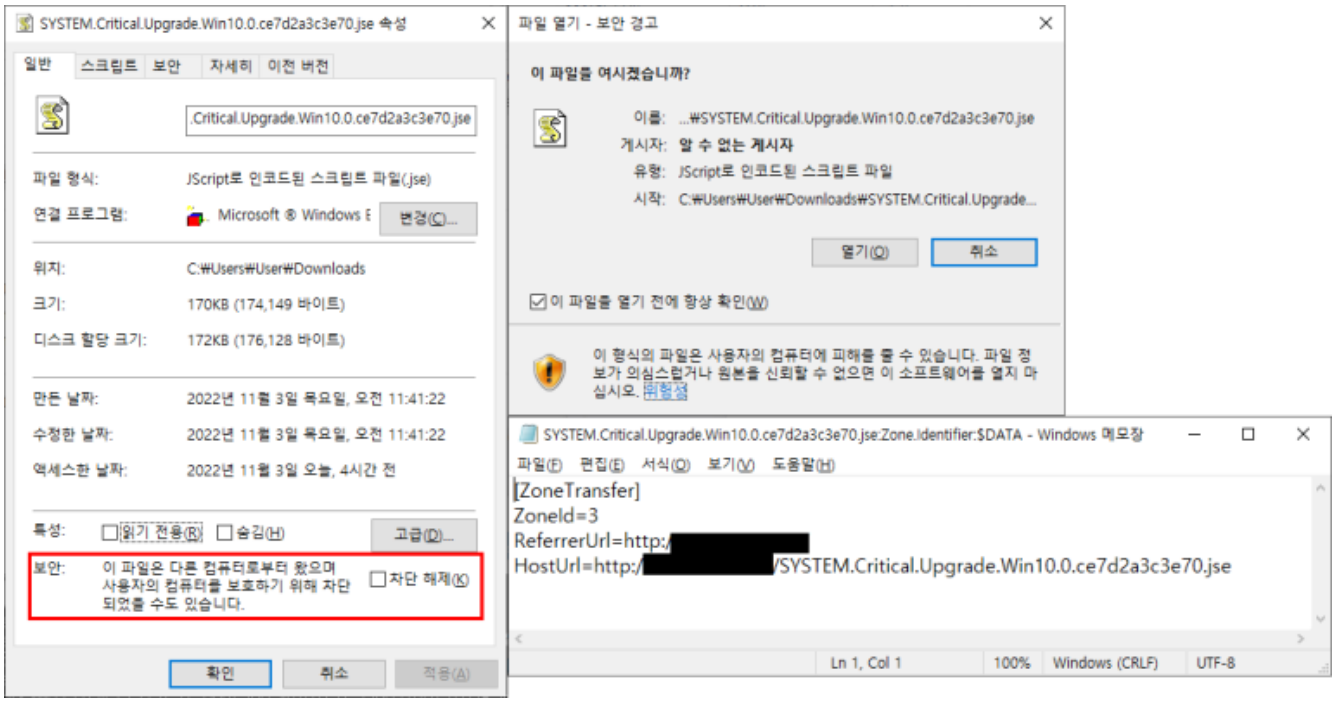

Figure 2. File recorded by MOTW

In order to bypass such execution blocks by MOTW, Magniber used a digital signature at the end of the script during the period between September 8th and September 29th, 2022. Through signing after the script is compiled, a digital signature on the script[4] guarantees that the script has not been modified, and provides a way to identify the author of the script. According to a post published on Bleeping Computer,[1] the digital signature at the end of the Magniber ransomware script is added to bypass MOTW.

Figure 3. Magniber distribution script (wsf, js, jse)

Currently, Magniber is being distributed with an MSI file extension instead of a script format. However, user vigilance is still required as it goes through frequent changes in its technique to bypass detection. Additionally, users must be careful when executing files downloaded from untrusted websites.

Currently, AhnLab is responding to the Magniber ransomware with not only file detection but also with various detection methods. Thus, it is recommended that users activate the **Process Memory Scan** and the **Malicious Script Detection (AMSI) options** in **[V3 Preferences] – [PC Scan Settings]**.

[IOC]

b8e94ffbfc560d56e28c10073b911d50
ba7a32f15227c5d30b648ba407e73c80
2da51943a0ea7699b01436eaa01f7a59

Script File Detection
Ransomware/JS.Magniber (2022.09.08.02)
Ransomware/WSF.Magniber (2022.09.28.02)

Process Memory Detection
Ransomware/Win.Magniber.XM153 (2022.09.15.03)
AMSI Detection (.NET DLL)
Ransomware/Win.Magniber.R519329 (2022.09.15.02)

Reference
[1]Exploited Windows zero-day lets JavaScript files bypass security warnings
[2]Macros from the internet will be blocked by default in Office
[3]5.1 NTFS Streams
[4]Digitally Signing Scripts

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:malware, Ransomware