Further Updates in LODEINFO Malware - JPCERT/CC Eyes

By 喜野 孝太(Kota Kino)

Published: 2021-02-17 · Archived: 2026-04-05 23:06:55 UTC

February 18, 2021

- LODEINFO

The functions and evolution of malware LODEINFO have been described in our past articles in February 2020 and June 2020. Yet in 2021, JPCERT/CC continues to observe activities related to this malware. Its functions have been expanding with some new commands implemented or actually used in attacks. This article introduces the details of the updated functions and recent attack trends.

LODEINFO versions

At the time of the last blog update, the latest version of LODEINFO was v.0.3.6, and currently v0.4.8 is being used. Figure 1 shows the transition of LODEINFO versions based on JPCERT/CC's observation.

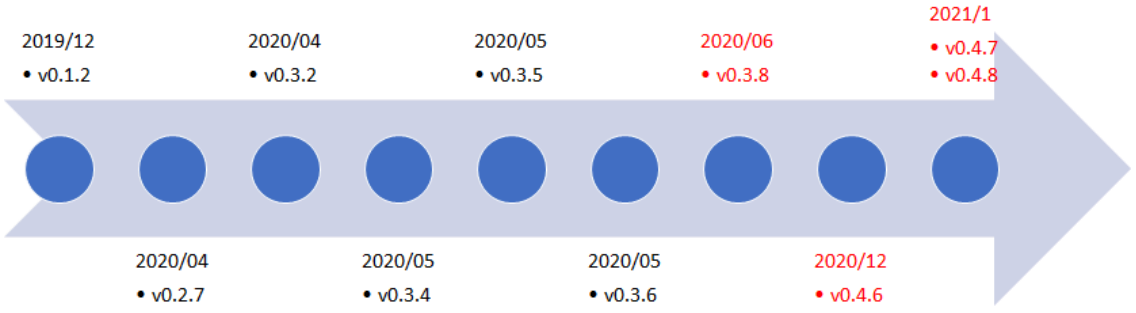


Figure 1：LODEINFO versions

Decoy document

As we previously explained, LODEINFO infection spreads once a user enables the macro in a Word or Excel file attached to a spear phishing email. In some recent cases, these document files are protected with a password, which is specified in the email body. The Word document convinces the user to enable the macro as in Figure 2. (The statement in the yellow box is roughly translated as follows: In case Word application cannot open the

document properly, you may be able to open it with Word premium mode. To proceed, please click the button in the yellow message bar above.)

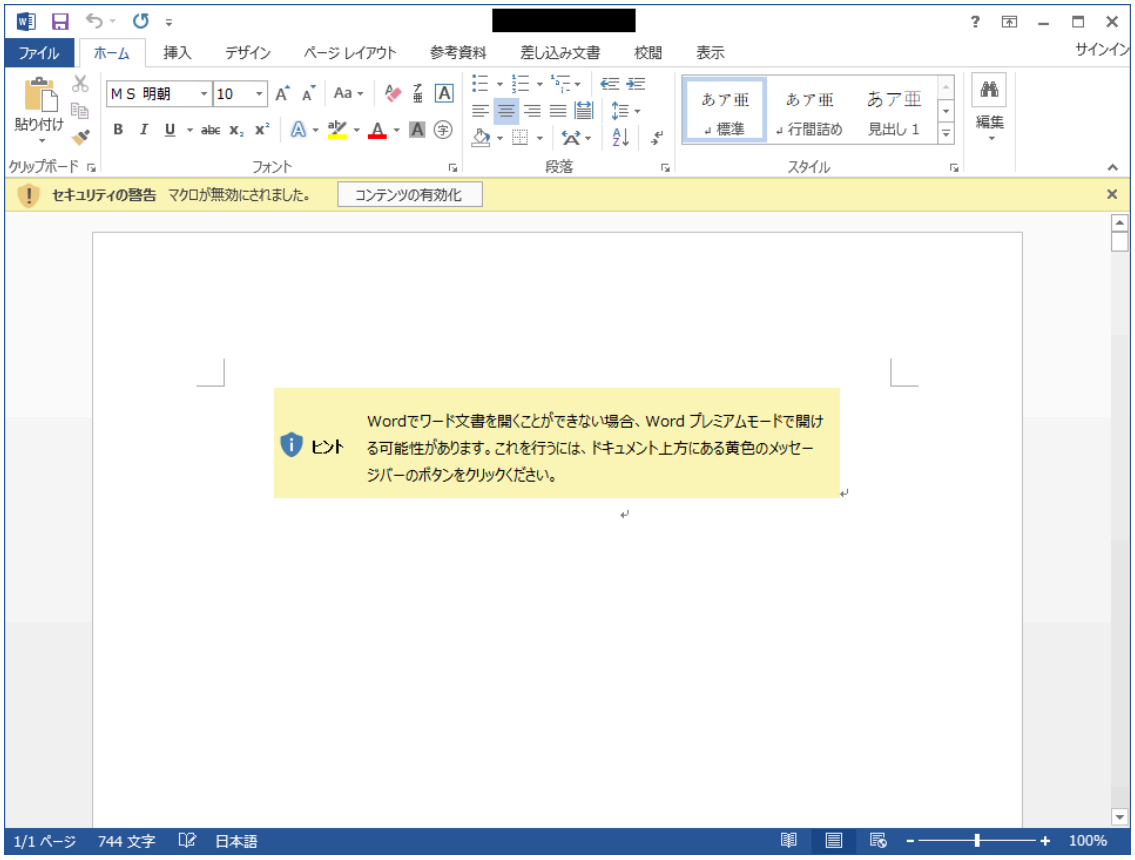


Figure 2： Word document content sample

The document appears to be empty, however, there are hidden letters in small and white fonts, containing macro configuration values and BASE64-encoded strings of a zip file which stores LODEINFO.

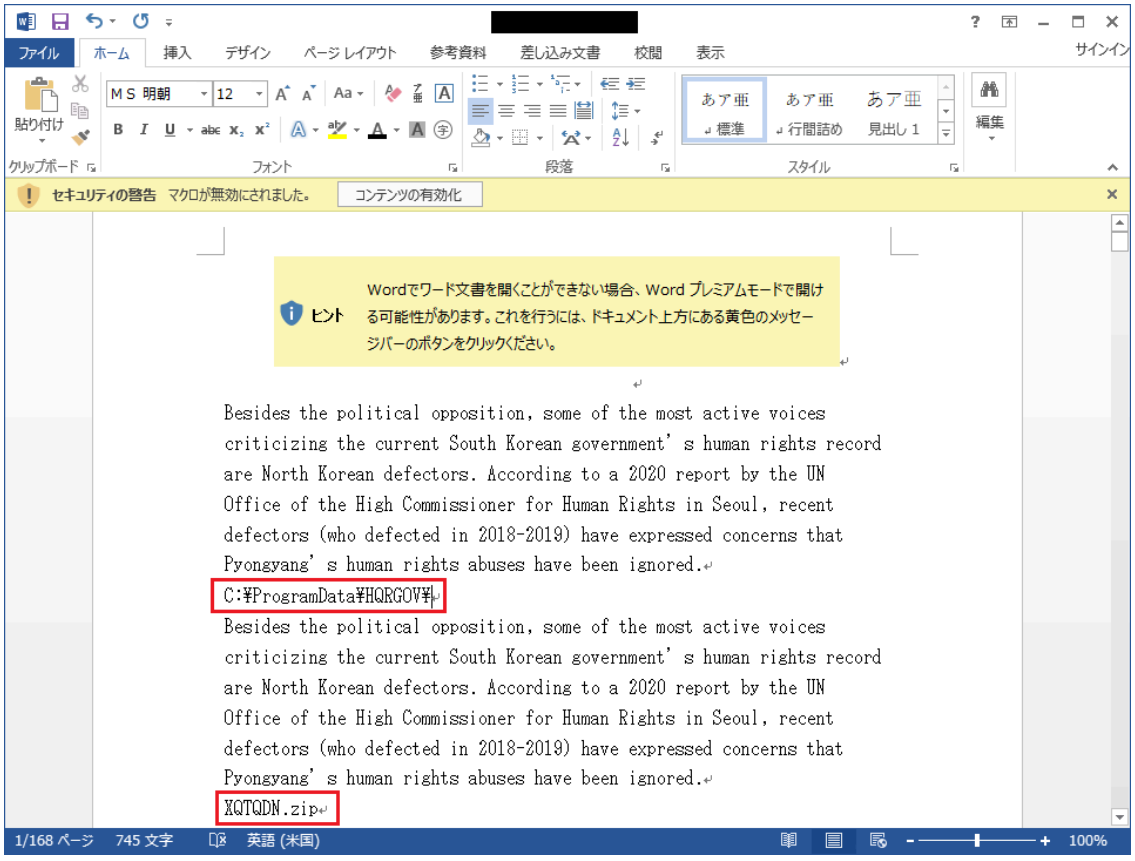


Figure 3： Word document contents sample (after changing the font)

The macro uses a method called LOLBAS to execute LODEINFO. Below is the command for executing a file created.

```
rundll32.exe advpack.dll,RegisterOCX
```

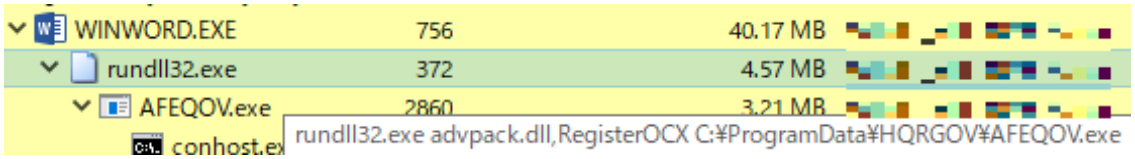


Figure 4： Process after enabling macro

The code of the macro contained in the documents shows sentences in public articles related to the diplomatic relations between South Korea and Japan or North Korea in the comments.

```
Private Sub Form_Close()
'原告は賠償金確保手段として南朝鮮内にある日本政府の資産の差し押さえ・売却を進めることが可能になった。
Dim QDN() As Byte
'22日に控訴期限を迎えたが、日本政府が訴訟参加を拒み控訴しなかったため、判決は23日0時に確定した。
'22日に控訴期限を迎えたが、日本政府が訴訟参加を拒み控訴しなかったため、判決は23日0時に確定した。
If Len(ActiveDocument.Content) < 100 Then GoTo QPO
'日本政府に原告1人当たり1億ウォン(約950万円)の損害賠償を命じる判決を出した。
```

Figure 5： Comments in the macro

New commands

The latest LODEINFO v0.4.8 has the following additional commands compared to v.0.3.6. (See Appendix A for details.)

- ransom (implemented)
- keylog (implemented)
- mv
- cp
- mkdir
- ps
- pkill

The following sections describe some of the new features that are available in the newer versions.

Ransomware function

“ransom” command has been implemented in v.0.3.8 and after. The encryption algorithm is a combination of AES and RSA. The files are first encrypted with an AES key generated for each fille. The key is then encrypted with the RSA public key embedded in the malware. After that, the message `“WOW! THIS FILE HAS BEEN ENCRYPTED...”` is inserted in the beginning of the file.

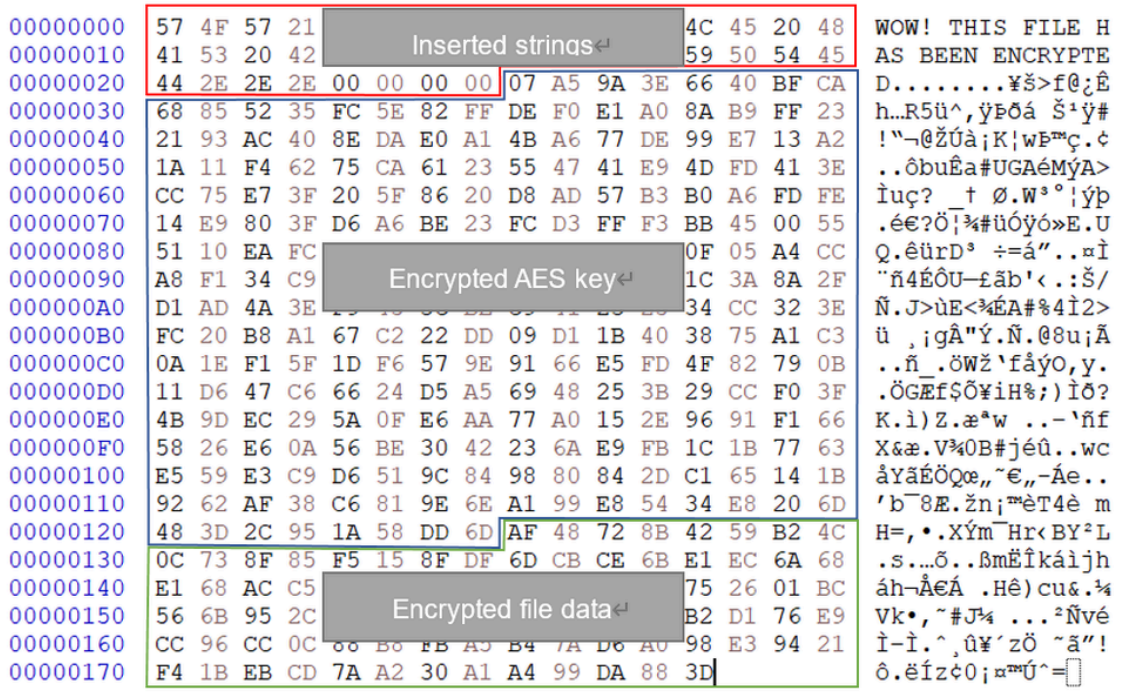


Figure 6： Structure of the encrypted file

This process makes it difficult to decrypt the files. Files and folders to encrypt can be specified with the ransom command, however, those with file extensions and paths in Figure 7 are excluded.

```
65  strcpy(v2 + 272, "WINDOWS");
66  strcpy(v2 + 280, "Program Files");
67  strcpy(v2 + 296, "Program Files (x86)");
68  strcpy(v2 + 316, "ProgramData");
69  strcpy(v2 + 328, "Recovery");
70  strcpy(v2 + 340, "$Recycle.Bin");
71  strcpy(v2 + 356, ".iso");
72  strcpy(v2 + 364, ".exe");
73  strcpy(v2 + 372, ".dll");
74  strcpy(v2 + 380, "NTUSER.");
75  strcpy(v2 + 388, ".dat");
76  strcpy(v2 + 396, ".bin");
```

Figure 7： Files excluded from encryption

In case a folder is selected, its path name is checked against the list, but not the individual files inside the folder. Therefore, files including these names listed above are encrypted in this case. Unlike other types of common ransomware, alteration of file extension, creation of ransom notes and/or change of background image do not occur. JPCERT/CC has not yet observed these features in actual attack cases, but they may be used for the purpose of deleting evidence or exfiltrating data.

Keylog function

“keylog” command has been implemented in v.0.4.6 and after. This command checks the following registry value to see if the option is enabled.

```
7  strcpy(reg, "SOFTWARE\\Microsoft\\Keyboard");
8  strcpy(&reg[28], "Enable");
9  enabled = 0;
10 v3 = 4;
11 aa_check_regvalue(this, HKEY_CURRENT_USER, (int)reg, (int)&reg[28], (int)&enabled, &v3);
12 return enabled;
```

Figure 8： Keylog checks if it is enabled

If it is enabled, a file named `“<NetBIOS name>.tmp”` is created in %TEMP% folder, and stolen key strings are encoded and stored there. An XOR key is used for encoding, which contains the first 1 byte of the SHA512 value of the device’s NetBIOS name. The following is an example of code to decode the keylog file.

```
import os
import hashlib

name = os.getenv("COMPUTERNAME")
keylog_file = os.getenv("TEMP") + "//" + name + ".tmp"
hash_of_name = hashlib.sha512(name.encode("UTF-8")).hexdigest()
xor_key = int(hash_of_name[0:2], 16)

decode_data = bytes()
with open(keylog_file, "rb") as f:
    for ch in f.read():
        decode_data += (ch ^ xor_key).to_bytes(1, byteorder="big", signed=False)
```

```
print(decode_data.decode('shift_jis'))
```

One of the distinctive features of this function is that it checks if the device's keyboard layout is set to Japanese according to the following criteria:

- "OverrideKeyboardIdentifier" value in HKLM\SYSTEM\CurrentControlSet\Service\i8042prt\Parameters is set to "PCAT_106KEY"
- "GetKeyboardLayout" function returns "1041"

If the device uses the Japanese keyboard layout, the key strings are converted accordingly. This fact implies that the attackers using LODEINFO malware target Japanese language users.

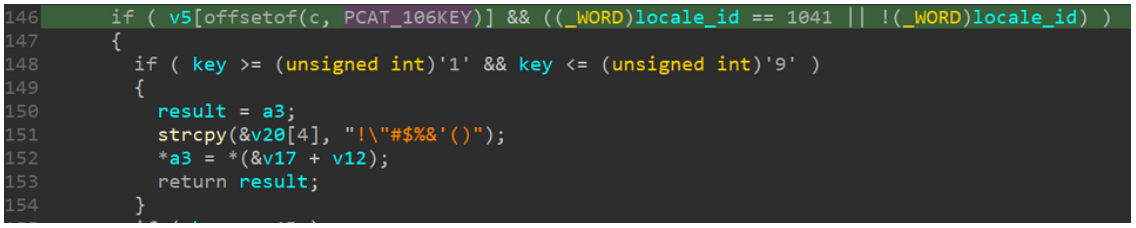


Figure 9： Checking keyboard layout

In closing

Attacks using LODEINFO has been continuously observed, and it is considered as a severe threat. We will keep an eye on this activity as it is yet likely to continue.

The hash value of the sample described in the article is listed in Appendix B, together with some newly confirmed C&C servers in Appendix C. Please make sure that none of your devices is communicating with such hosts.

- Kota Kino
(Translated by Yukako Uchida)

Reference

Appendix A New commands

Value	Contents
ransom	Encrypt files
keylog	Control keylogger
mv	Move files
cp	Copy files

Value	Contents
mkdir	Create directory
ps	List process
pkill	Kill process

Appendix B SHA-256 has value of a sample

- 3fda6fd600b4892bda1d28c1835811a139615db41c99a37747954dcccaebff6e （v0.4.6）

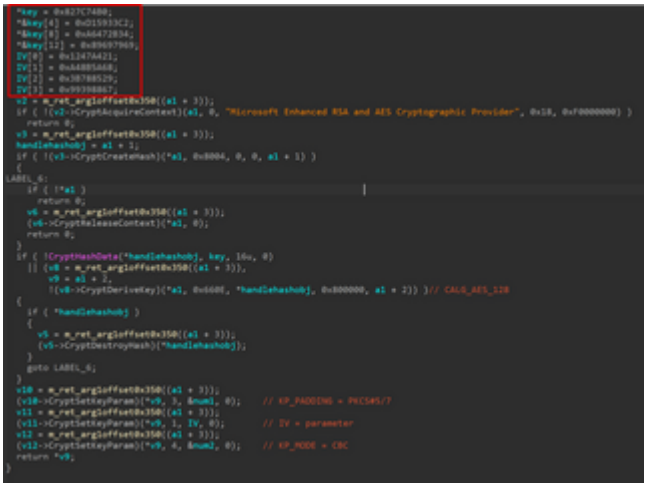
Appendix C C&C servers

- www.evonzae.com
- 45.76.216.40
- 103.140.45.71
- 139.180.192.19
- 167.179.84.162
- 167.179.65.11

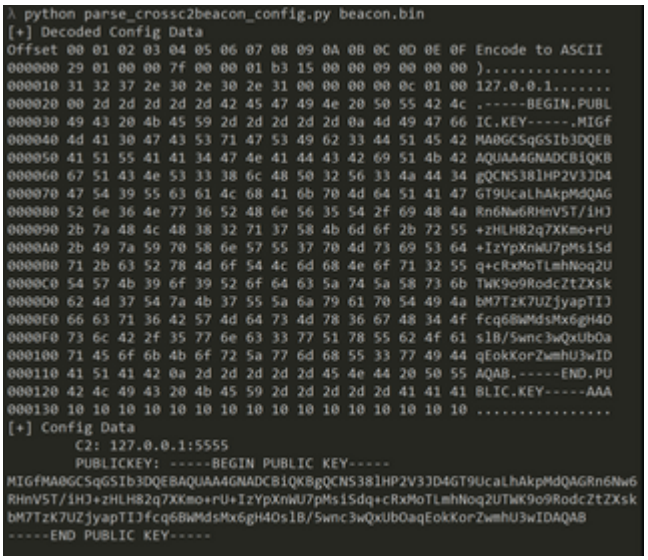
喜野 孝太(Kota Kino)

Kota Kino is Malware/Forensic Analyst at Incident Response Group, JPCERT/CC since August 2019.

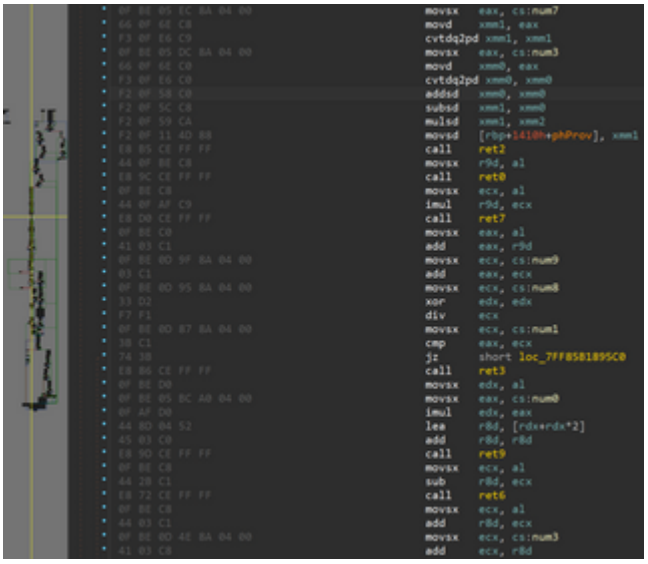
Related articles

- 

  [Update on Attacks by Threat Group APT-C-60]

- 

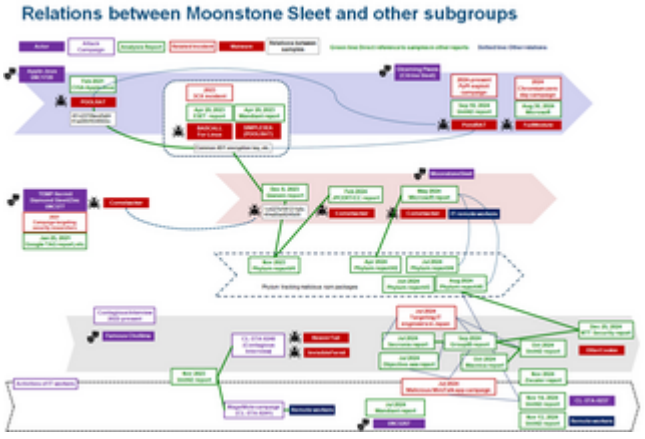
  [CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks]

- 

  [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/2021/02/LODEINFO-3.html