JPCERT Coordination Center official Blog

blogs.jpcert.or.jp/en/2021/02/LODEINFO-3.html

喜野 孝太(Kota Kino)

February 18, 2021

Further Updates in LODEINFO Malware

LODEINFO

-
- Email

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.

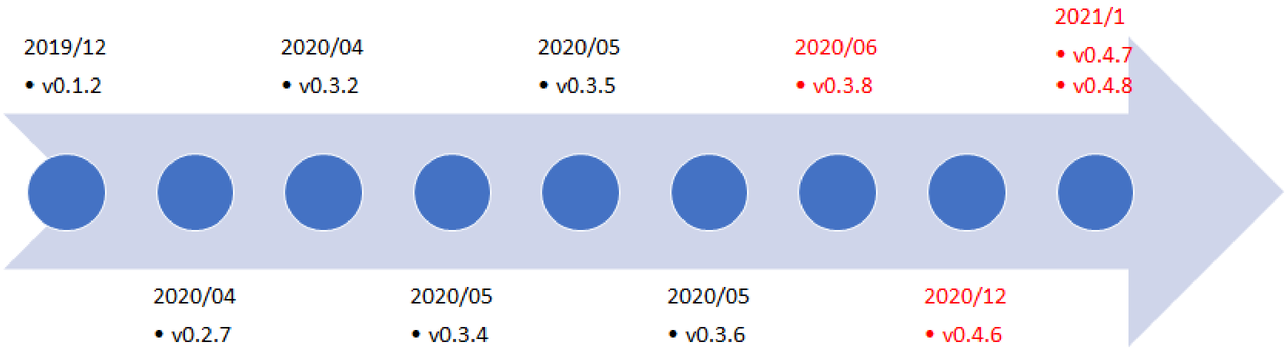
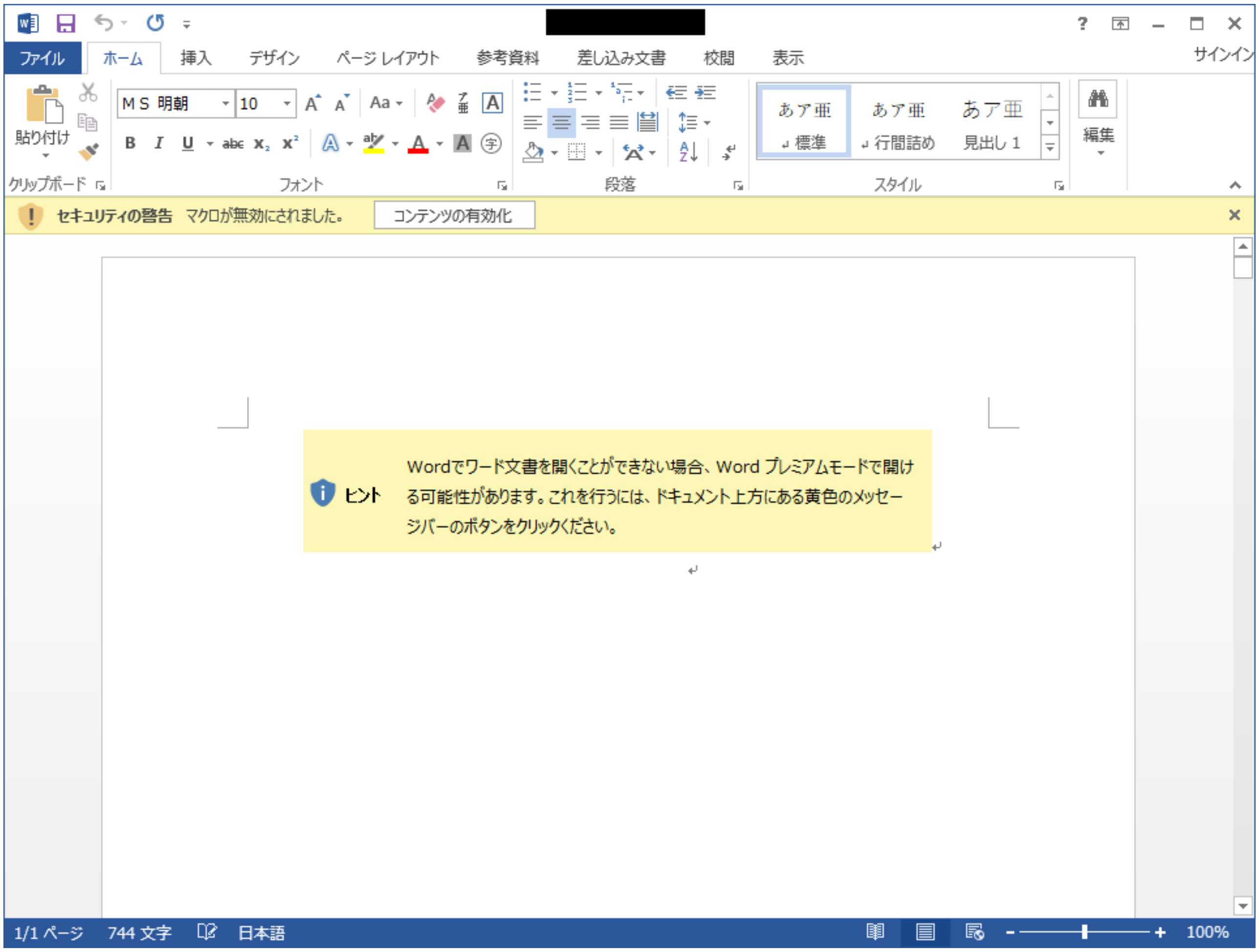


Figure 1：LODEINFO versions

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.)



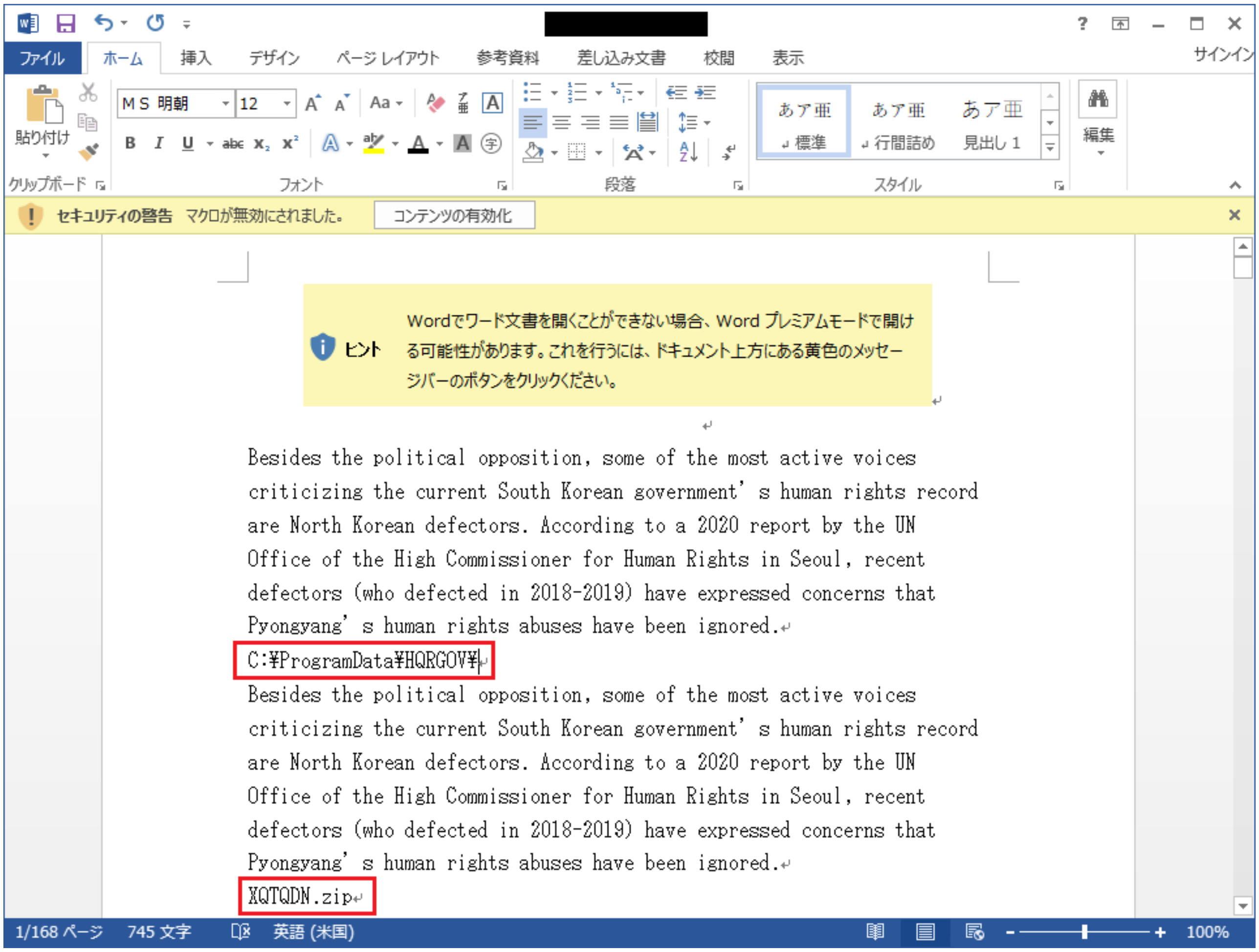
[redacted]

セキュリティの警告　マクロが無効にされました。　コンテンツの有効化

ヒント　Wordでワード文書を開くことができない場合、Word プレミアムモードで開ける可能性があります。これを行うには、ドキュメント上方にある黄色のメッセージバーのボタンをクリックください。

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.



ヒント　Wordでワード文書を開くことができない場合、Word プレミアムモードで開ける可能性があります。これを行うには、ドキュメント上方にある黄色のメッセージバーのボタンをクリックください。

Besides the political opposition, some of the most active voices criticizing the current South Korean government' s human rights record are North Korean defectors. According to a 2020 report by the UN Office of the High Commissioner for Human Rights in Seoul, recent defectors (who defected in 2018-2019) have expressed concerns that Pyongyang' s human rights abuses have been ignored.

C:¥ProgramData¥HQRGOV¥

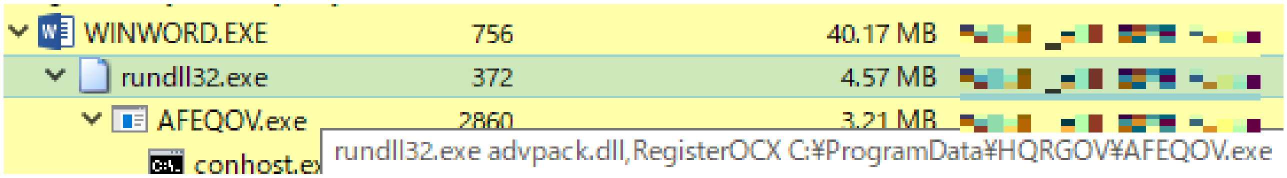
Besides the political opposition, some of the most active voices criticizing the current South Korean government' s human rights record are North Korean defectors. According to a 2020 report by the UN Office of the High Commissioner for Human Rights in Seoul, recent defectors (who defected in 2018-2019) have expressed concerns that Pyongyang' s human rights abuses have been ignored.

XQTQDN.zip

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
```

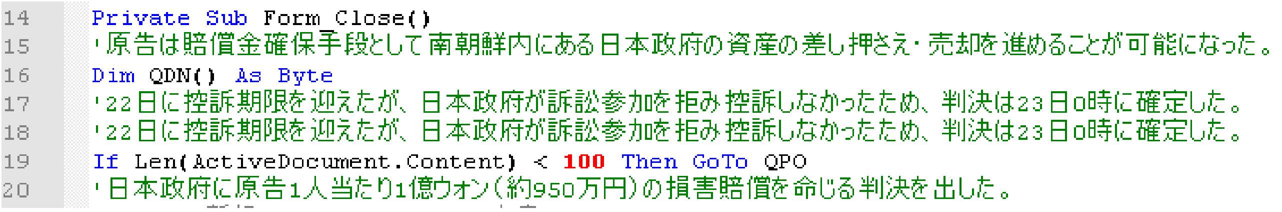


WINWORD.EXE	756	40.17 MB	[redacted]
rundll32.exe	372	4.57 MB	[redacted]
AFEQOV.exe	2860	3.21 MB	[redacted]
conhost.ex			

```
rundll32.exe advpack.dll,RegisterOCX C:¥ProgramData¥HQRGOV¥AFEQOV.exe
```

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

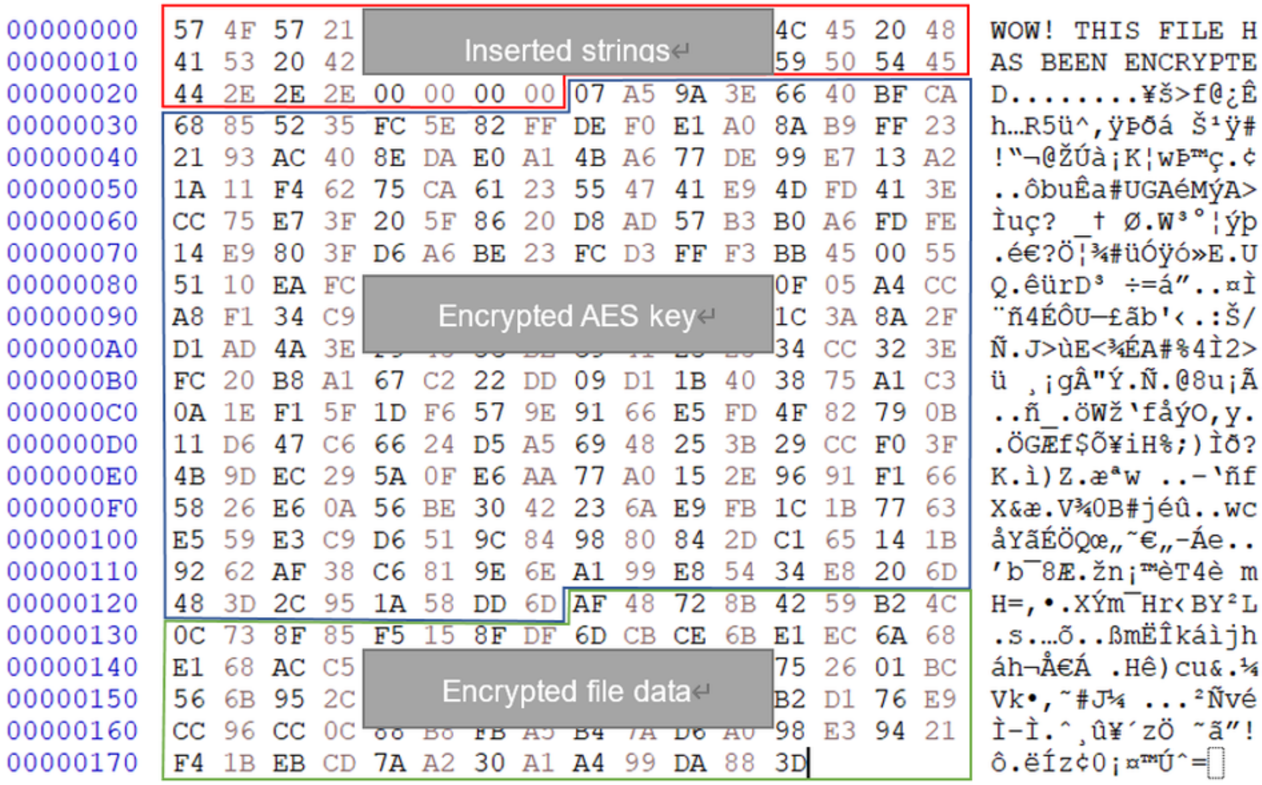
The latest LODEINFO v0.4.8 has the following additional commands compared to v.0.3.6. (See Appendix A for details.)

- 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

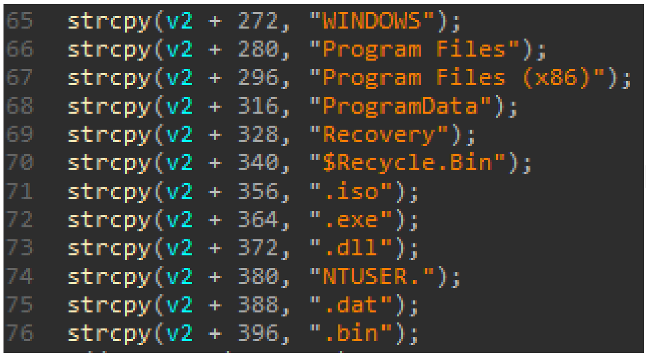
“ransom” command has been implemented in v.0.3.8 and after. The encryption algorithm is a combination of AES and RSA. The files are first encrypted with an AES key generated for each fille. The key is then encrypted with the RSA public key embedded in the malware. After that, the message `“WOW! THIS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



```
00000000  57 4F 57 21                         4C 45 20 48  WOW! THIS FILE H
00000010  41 53 20 42                         59 50 54 45  AS BEEN ENCRYPTE
00000020  44 2E 2E 2E 00 00 00 00 07 A5 9A 3E 66 40 BF CA  D........¥š>f@¿Ê
00000030  68 85 52 35 FC 5E 82 FF DE F0 E1 A0 8A B9 FF 23  h…R5ü^‚ÿÞðá Š¹ÿ#
00000040  21 93 AC 40 8E DA E0 A1 4B A6 77 DE 99 E7 13 A2  !“¬@ŽÚà¡K¦wÞ™ç.¢
00000050  1A 11 F4 62 75 CA 61 23 55 47 41 E9 4D FD 41 3E  ..ôbuÊa#UGAéMýA>
00000060  CC 75 E7 3F 20 5F 86 20 D8 AD 57 B3 B0 A6 FD FE  Ìuç? _† Ø.W³°¦ýþ
00000070  14 E9 80 3F D6 A6 BE 23 FC D3 FF F3 BB 45 00 55  .é€?Ö¦¾#üÓÿó»E.U
00000080  51 10 EA FC                         0F 05 A4 CC  Q.êürD³ ÷=á”..¤Ì
00000090  A8 F1 34 C9                         1C 3A 8A 2F  ¨ñ4ÉÔU—£ãb'‹.:Š/
000000A0  D1 AD 4A 3E                         34 CC 32 3E  Ñ.J>ùE<¾ÉA#%4Ì2>
000000B0  FC 20 B8 A1 67 C2 22 DD 09 D1 1B 40 38 75 A1 C3  ü ¸¡gÂ"Ý.Ñ.@8u¡Ã
000000C0  0A 1E F1 5F 1D F6 57 9E 91 66 E5 FD 4F 82 79 0B  ..ñ_.öWž‘fåýO‚y.
000000D0  11 D6 47 C6 66 24 D5 A5 69 48 25 3B 29 CC F0 3F  .ÖGÆf$Õ¥iH%;)Ìð?
000000E0  4B 9D EC 29 5A 0F E6 AA 77 A0 15 2E 96 91 F1 66  K.ì)Z.æªw ..–‘ñf
000000F0  58 26 E6 0A 56 BE 30 42 23 6A E9 FB 1C 1B 77 63  X&æ.V¾0B#jéû..wc
00000100  E5 59 E3 C9 D6 51 9C 84 98 80 84 2D C1 65 14 1B  åYãÉÖQœ„˜€„-Áe..
00000110  92 62 AF 38 C6 81 9E 6E A1 99 E8 54 34 E8 20 6D  ’b¯8Æ.žn¡™èT4è m
00000120  48 3D 2C 95 1A 58 DD 6D AF 48 72 8B 42 59 B2 4C  H=,•.XÝm¯Hr‹BY²L
00000130  0C 73 8F 85 F5 15 8F DF 6D CB CE 6B E1 EC 6A 68  .s.…õ..ßmËÎkáìjh
00000140  E1 68 AC C5                         75 26 01 BC  áh¬Å€Á .Hê)cu&.¼
00000150  56 6B 95 2C                         B2 D1 76 E9  Vk•,˜#J¼ ...²Ñvé
00000160  CC 96 CC 0C                         98 E3 94 21  Ì–Ì.ˆ¸û¥´zÖ ˜ã”!
00000170  F4 1B EB CD 7A A2 30 A1 A4 99 DA 88 3D           ô.ëÍz¢0¡¤™Úˆ=
```

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.



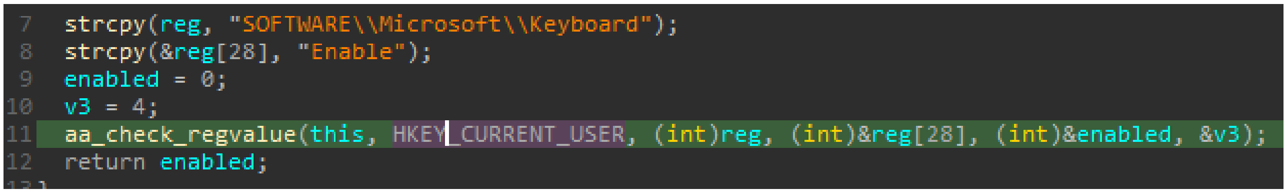
```
strcpy(v2 + 272, "WINDOWS");
strcpy(v2 + 280, "Program Files");
strcpy(v2 + 296, "Program Files (x86)");
strcpy(v2 + 316, "ProgramData");
strcpy(v2 + 328, "Recovery");
strcpy(v2 + 340, "$Recycle.Bin");
strcpy(v2 + 356, ".iso");
strcpy(v2 + 364, ".exe");
strcpy(v2 + 372, ".dll");
strcpy(v2 + 380, "NTUSER.");
strcpy(v2 + 388, ".dat");
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.



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

Figure 8： Keylog checks if it is enabled

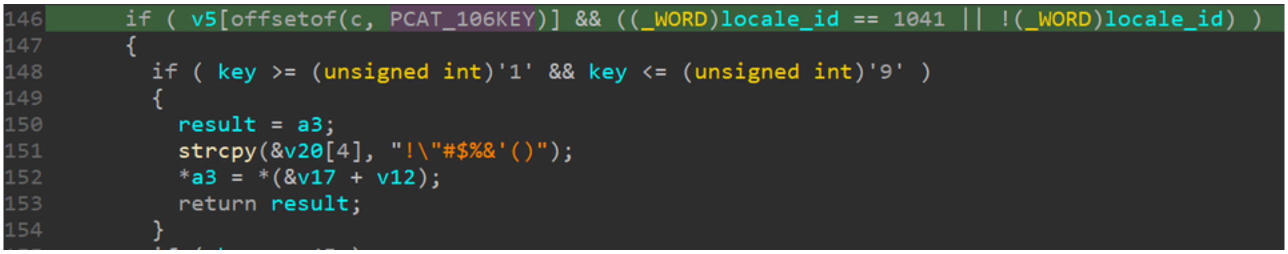
If it is enabled, a file named `“<NetBIOS name>.tmp”` is created in %TEMP% folder, and stolen key strings are encoded and stored there. An XOR key is used for encoding, which contains the first 1 byte of the SHA512 value of the device’s NetBIOS name. The following is an example of code to decode the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



```
    if ( v5[offsetof(c, PCAT_106KEY)] && ((_WORD)locale_id == 1041 || !(_WORD)locale_id) )
    {
      if ( key >= (unsigned int)'1' && key <= (unsigned int)'9' )
      {
        result = a3;
        strcpy(&v20[4], "!\"#$%&'()");
        *a3 = *(&v17 + v12);
        return result;
      }
```

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
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

-
- Email

Author

喜野 孝太(Kota Kino)

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

Was this page helpful?

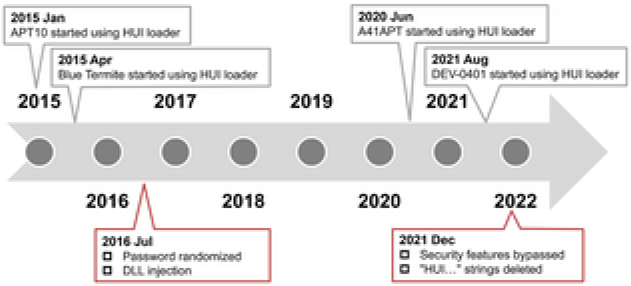
0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

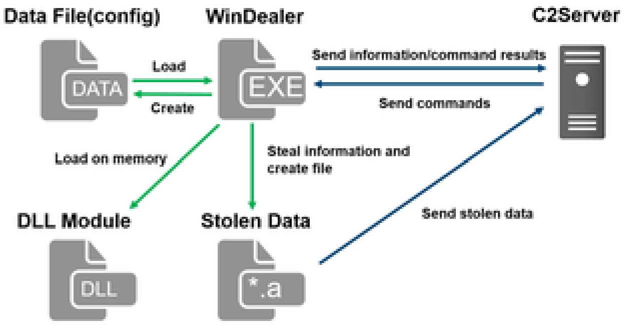
This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

please change the setting of your browser to set JavaScript valid. Thank you!

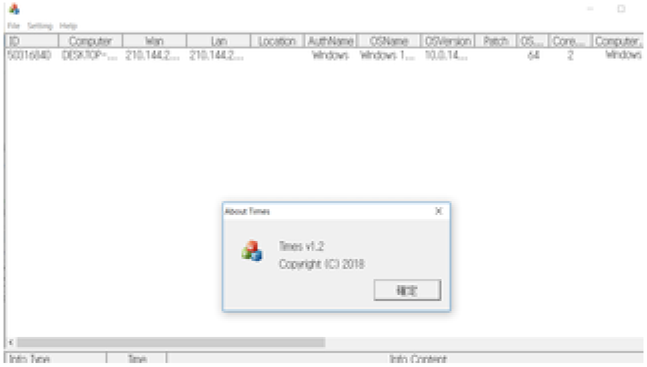
Related articles

- 
2015 Jan
APT10 started using HUI loader
2015 Apr
Blue Termite started using HUI loader
2020 Jun
A41APT started using HUI loader
2021 Aug
DEV-0401 started using HUI loader
2015
2017
2019
2021
2016
2018
2020
2022
2016 Jul
□ Password randomized
□ DLL injection
2021 Dec
□ Security features bypassed
□ "HUI..." strings deleted
  Analysis of HUI Loader
-

  Anti-UPX Unpacking Technique
-
  XXX-XXXX-XXXX
  SMS
  お客さま宛にお荷物のお届けにあがりましたが、不在のため持ち帰りました。下記よりご確認ください。
  http://xxx...
  12:00
  FAQ: Malware that Targets Mobile Devices and How to Protect Them

- 

  [Malware WinDealer used by LuoYu Attack Group]

- 

ID	Computer	Wan	Lan	Location	AuthName	OSName	OSVersion	Patch	OS...	Core...	Computer...
50016840	DESKTOP-...	210.144.2...	210.144.2...		Windows	Windows 1...	10.0.14...		64	2	Windows

  About Times

  Times v1.2
  Copyright (C) 2018

Info Type	Time	Info Content

  [Malware Gh0stTimes Used by BlackTech]

[Back]
[Top]
[Next]