

# Since the Hacking of Sony Pictures

## Lazarus (Hidden Cobra) Group's Activities in South Korea

Cha Minseok (Jacky Cha, 車珉錫)

Senior Principal Malware Researcher

Virus Bulletin Conference (October 3, 2018)

AhnLab



# Contents

- [01](#) Sony Pictures Hack
- [02](#) Lazarus Group's Activities in South Korea
- [03](#) Operation Red Dot (2011-2015)
- [04](#) Operation Big Pond (2015-2017) & Operation Coin Rush (2017-2018)
- [05](#) Lazarus Connections
- [06](#) Who is behind it?
- [07](#) Conclusion

**AhnLab**

01

# Sony Pictures Hack

AhnLab

- Sony Pictures Hack
  - Erased Sony's computer infrastructure
  - Leaked confidential data, unreleased films, and more

## Sony Hacker Paralysis Rea – Update



by Mike Fleming Jr

November 25, 2014 8:19am



Gift of GOP for 4th day: Their Privacy

```

Their Privacy
Raw
1  by GOP
2
3  We are the GOP working all over the world.
4  We know nothing about the threatening email received by Sony staffers, but you should wisely judge by yours
5
6
7  Message to SONY
8
9      We have already given our clear demand to the management team of SONY, however, they have refused t
10     It seems that you think everything will be well, if you find out the attacker, while no reacting to
11     We are sending you our warning again.
12     Do carry out our demand if you want to escape us.
13     And, Stop immediately showing the movie of terrorism which can break the regional peace and cause t
14     You, SONY & FBI, cannot find us.
15     We are perfect as much.
16     The destiny of SONY is totally up to the wise reaction & measure of SONY.
17
18
19  Their Privacy
20
21     Amy Pascal(Co-Chairman SPE & Chairman MPG), Stephen Mosko(President, SPT)
22
23
24  Password: diespe123

```

\* Source : <https://deadline.com/2014/11/sony-computers-hacked-skull-message-1201295288> & <https://gist.github.com/anonymous/7b9a0a0ac94065ccfc5b>

- Similarities & Motivation?

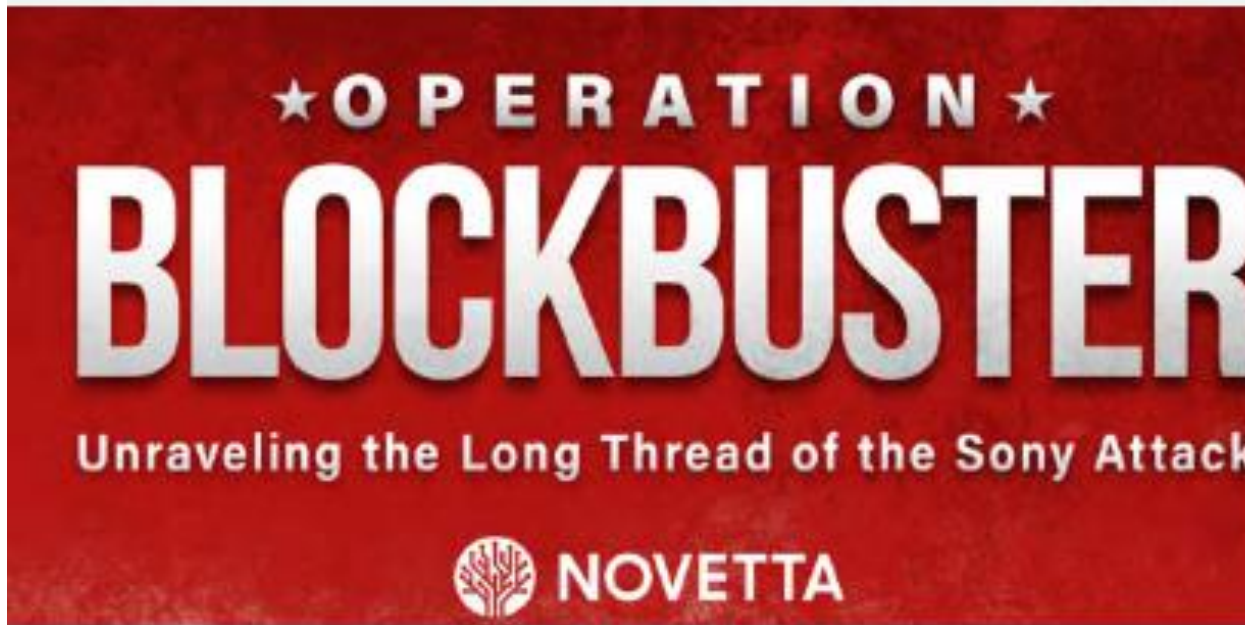
- Similar to South Korea incidents? Because of "The Interview"?



\* Source : <http://imgur.com/qXNgFVz> & <https://www.imdb.com/title/tt2788710/mediaviewer/rm2264792576>



- Related Reports (2016)
  - Operation Blockbuster, Blue Coat Report



FROM SEOUL TO SONY:

THE HISTORY OF THE DARKSEOUL GROUP  
AND THE SONY INTRUSION MALWARE  
DESTOVER

By Snorre Fagerland, Blue Coat Systems Inc.

February 2016

\* Source : <https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf> & <https://www.yumpu.com/en/document/view/55505308/the-history-of-the-darkseoul-group-and-the-sony-intrusion-malware-destover/72>

- Criminal complaint (2018)

AO 91 (Rev. 11/11) Criminal Complaint

## UNITED STATES DISTRICT COURT

COPY

for the

Central District of California

United States of America

v.

PARK JIN HYOK, also known as ("aka")  
"Jin Hyok Park," aka "Pak Jin Hek,"

Defendant.



Case No. MJ 18-1479

### CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los

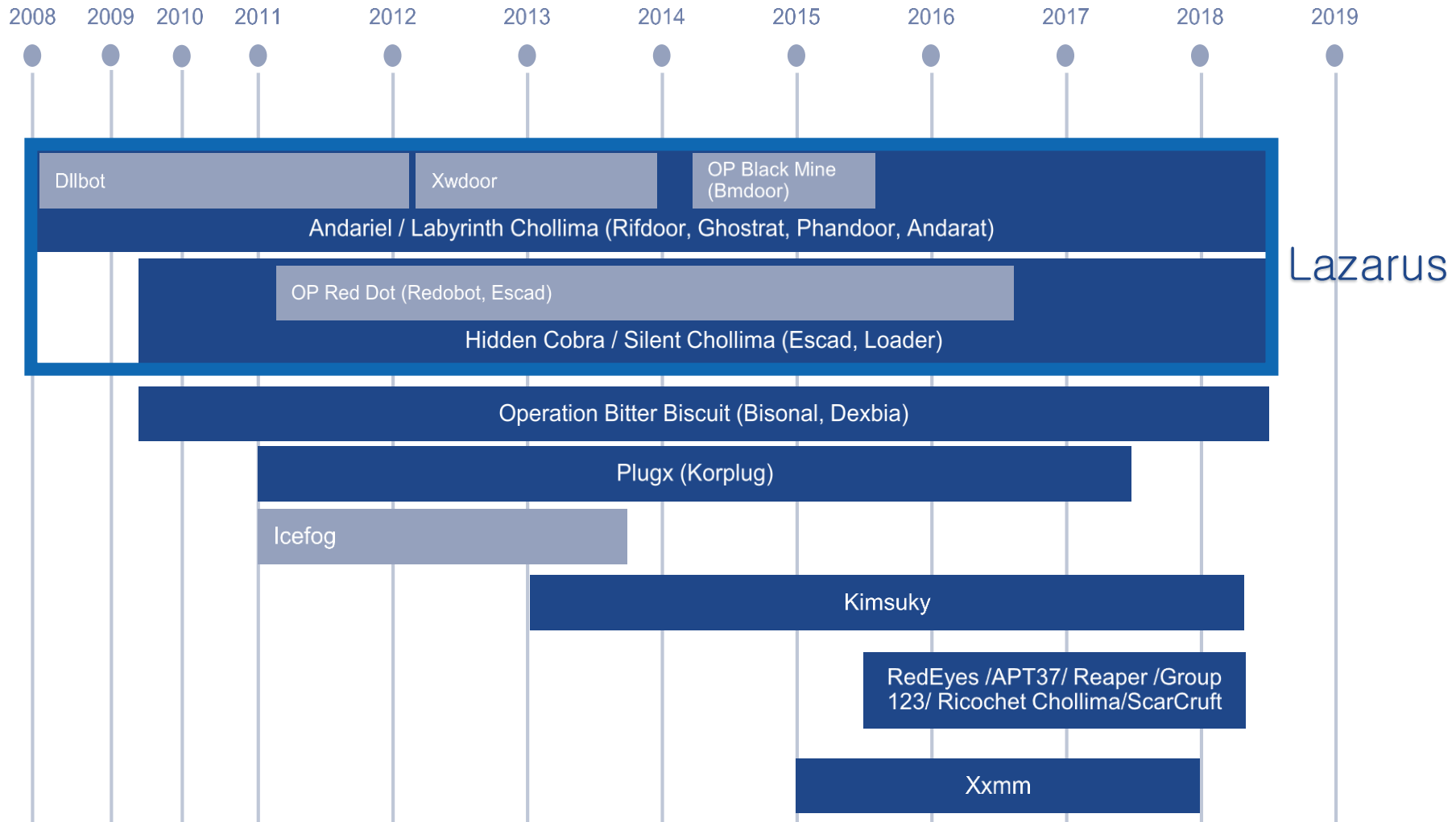
Angeles in the Central District of California, the defendant violated:

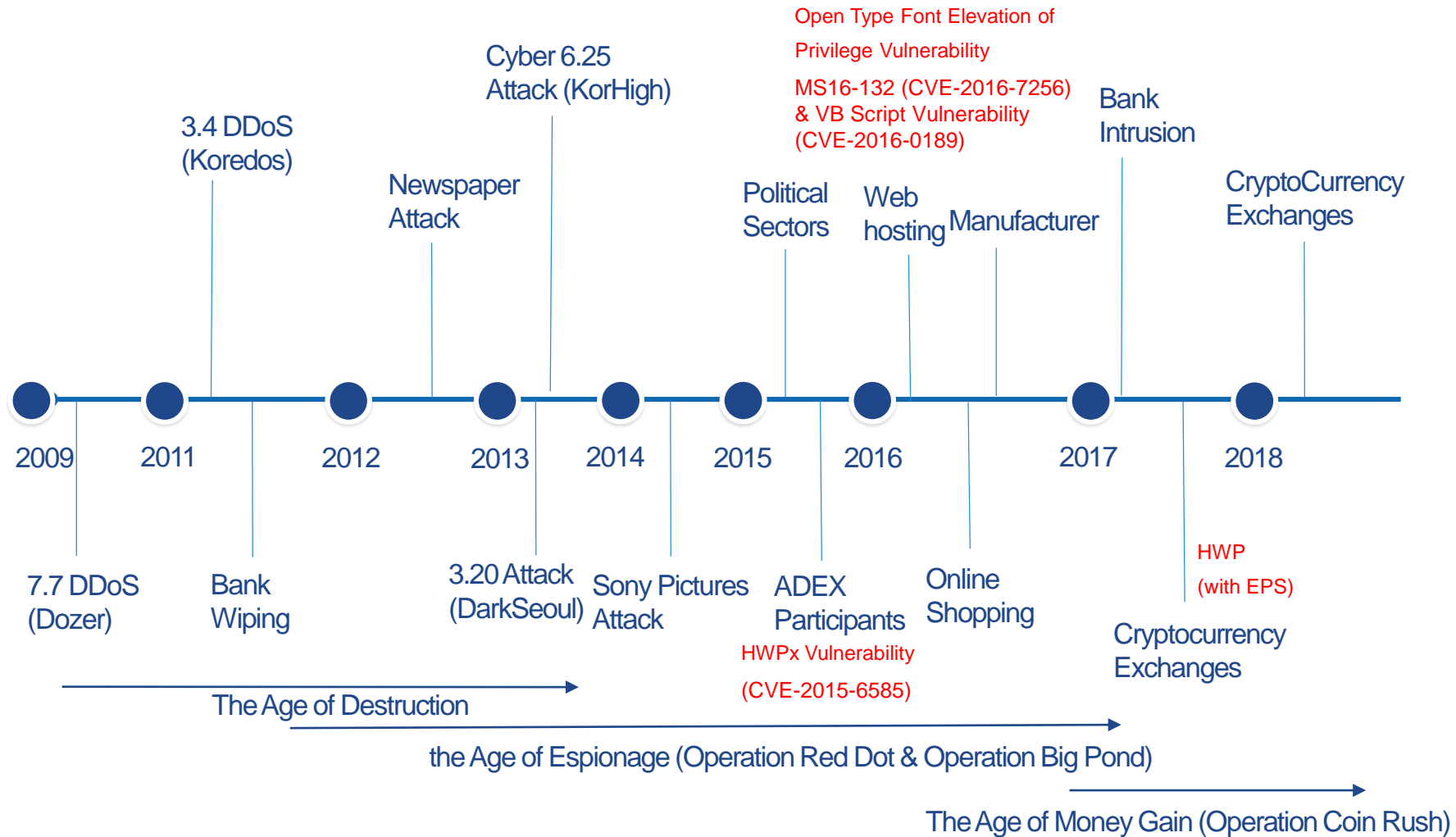
\* Source : <https://assets.documentcloud.org/documents/4834220/2018-09-06-PARK-COMPLAINT-UNSEALED.pdf>



02

# Lazarus Group's Activities in South Korea





- Newspaper Hacking (June 9, 2012)

- Website defacement and shutdown

- Additional attacks? (2012-xx-19 & 2012-xx-29) -> incidents



## 시스템 오류로 인한 안내드립니다.

안녕하세요. [redacted]입니다.  
6월 8일 오후부터 시스템 오류로 인한 오류가 발생하였습니다.  
이에 빠른 조치를 취하고 있으며 작업이 완료 되는대로  
다시 공지 사항을 통해 안내해드리겠습니다.

신문구독 관련 고객센터센터 서비스는  
오류 복구시까지 사용이 불가합니다.  
조속한 시간 내 이용이 가능하도록 조치하도록 하겠습니다.

감사합니다.

- Released internal data
  - IsOne claimed responsibility

The image shows a screenshot of a web browser displaying a forum post and a file explorer window. The forum post, from a site with the URL [http://www.seoprise.com/board/view.php?uid=63383&table=global\\_2](http://www.seoprise.com/board/view.php?uid=63383&table=global_2), contains the text "IsOne opening to the public information" and "o.kr hacked data". A link is provided: <http://www.sozuan.net/download/Hacking%20public.rar>. The file explorer window shows a directory named "Network Structure" containing various files such as "메인 스위치 pass.xls", "20120326\_IT 자산현황.xlsx", and "네트워크 구성도(관계사).ppt".

이름	수정한 날짜	유형	크기
100629 메인 스위치 pass.xls	2012-06-10 오후 6:...	XLS 파일	27KB
20120326_IT 자산현황.xlsx	2012-06-06 오전 9:...	XLSX 파일	1,765KB
iPhone_iPad 사용자 현황_20110216.xlsx	2012-06-06 오전 9:...	XLSX 파일	505KB
NAS 접속 방법	2012-06-06 오전 9:...	텍스트 문서	1KB
net view command	2012-06-06 오전 3:...	텍스트 문서	4KB
System 구성 종합_201205.xlsx	2012-06-06 오전 7:...	XLSX 파일	5,225KB
Tape 수동 방법	2012-06-06 오전 9:...	텍스트 문서	1KB
관리적노트북_20120125.xlsx	2012-06-06 오전 7:...	XLSX 파일	13KB
네트워크 구성도(관계사).ppt	2012-06-10 오후 5:...	PPT 파일	677KB
네트워크 구성도(본사_IP대역).ppt	2012-06-10 오후 6:...	PPT 파일	1,679KB
네트워크 구성도(전체).ppt	2012-06-10 오후 6:...	PPT 파일	1,115KB
노트PC 사용 현황_20120125.xlsx	2012-06-06 오전 7:...	XLSX 파일	68KB
시스템실 이전 계획_20110705 - 원본.pptx	2012-06-06 오전 6:...	PPTX 파일	761KB
시스템현황_20110805-R01.pptx	2012-06-10 오후 6:...	PPTX 파일	5,817KB
신규 전산실 책배치.vsd	2012-06-06 오전 6:...	VSD 파일	361KB
신규 전산실 서버RACK 구성.vsd	2012-06-06 오전 9:...	VSD 파일	6,494KB
조직별 PC현황	2012-06-06 오전 7:...	Office Open XML ...	19KB

\* Source : [http://www.seoprise.com/board/view.php?uid=63383&table=global\\_2](http://www.seoprise.com/board/view.php?uid=63383&table=global_2)

03

# Operation Red Dot (2011-2015)

- Dropper (2011)

- Creates lsacfg.dll, c\_1581.nls, msvcr70.dll

- Contains 'm'

```
.004031F0: 64 65 70 65 6E 64 20 6F 6E 20 69 74 20 77 69 6C depend on it wil
.00403200: 6C 20 66 61 69 6C 20 74 6F 20 73 74 61 72 74 2E l fail to start.
.00403210: 00 00 00 00 3A 4C 31 0D 0A 64 65 6C 20 22 25 73 :L1Model "%s"
.00403220: 22 0D 0A 69 66 20 65 78 69 73 74 20 22 25 73 22 "Model exist "%s"
.00403230: 20 67 6F 74 6F 20 4C 31 0D 0A 64 65 6C 20 22 25 goto L1Model "%
.00403240: 73 22 0D 0A 00 00 00 00 6D 73 76 63 72 74 2E 62 s"Model msvcr70.
.00403250: 61 74 00 00 46 2E 69 6C 2E 65 54 69 20 6D 65 54 at FileTimeT
.00403260: 20 6F 2E 53 79 73 2E 74 65 2E 6D 20 54 69 20 6D o.System Time
.00403270: 65 00 00 00 47 20 65 2E 74 56 6F 20 6C 75 2E 6D e GetVolume
.00403280: 65 49 6E 66 20 6F 72 6D 20 61 74 69 6F 6E 4E loc_40161A: ; CODE XREF: XorA7_40160E+1F↓j
.00403290: 47 2E 65 74 44 69 20 73 6B 46 2E 72 65 65 2E mov al, [ecx]
.004032A0: 70 2E 2E 61 63 65 2E 45 78 41 00 00 47 65 2E test al, al
.004032B0: 20 54 69 20 63 2E 6B 43 2E 20 6F 75 6E 74 00 jz short loc_401628
.004032C0: 53 69 7A 2E 65 6F 2E 66 52 2E 65 73 2E 6F 7E cmp al, 0A7h
.004032D0: 20 20 72 63 65 00 00 00 4C 6F 63 2E 2E 6B 53 jz short loc_401628
.004032E0: 2E 73 6F 2E 75 72 63 65 00 00 00 4C 2E 6E xor al, 0A7h ; xor AL,0xA7
mov [ecx], al
00401628 loc_401628: ; CODE XREF: XorA7_40160E+10↑j
; XorA7_40160E+14↑j
00401628 add byte ptr [ecx], 6Dh ; 'm'
00401628 inc ecx
00401628 dec edx
0040162C jnz short loc_40161A
0040162F
```

- xor 0xA7

- Interesting submission (!)

- Timeline

-

Discovery Data	Targets	Description
2011.7	Universities	National Defense-related colleges
2014.4	Medical institutions	One of the samples was linked to the Wannacry Ransomware. Keylogger software was also found



- Dropper - Redobot (2011-2014)

- Different xor key
- Check BMZA. What is "BM"?

```
int __stdcall WinMain(HINSTANCE
{
    int v4; // esi

    GetAPI_401617();
    GetAPI_401C7A();
    GetAPI_401E64();
    if ( !Dropper_40102C() )
    {
        service_4012F5();
        Service_40142F(v4);
    }
    DropBAT_40147D();
    return 0;
}
```

```
.00404010: 42 4D 5A 41 00 00 00 00 5C 00 00 00 25 73 25 73 BMZA \ %s%s
.00404020: 25 73 22 25 73 22 00 00 25 53 79 73 74 65 6D 52 %s"%s" %SystemR
.00404030: 6F 6F 74 25 00 00 00 00 5C 73 79 73 74 65 6D 33 oot% \system3
.00404040: 32 5C 00 00 73 76 63 68 6F 73 74 2E 65 78 65 20 2\ svchost.exe
.00404050: 2D 6B 20 00 53 4F 46 54 57 41 52 45 5C 4D 69 63 -k SOFTWARE\Mic
.00404060: 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 20 4E rosoft\Windows N
.00404070: 54 5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E T\CurrentVersion
.00404080: 5C 53 76 63 68 6F 73 74 00 00 00 00 53 65 72 76 \Svchost Serv
.00404090: 69 63 65 44 6C 6C 00 00 25 73 25 73 25 73 00 00 iceD11 %s%s%
```

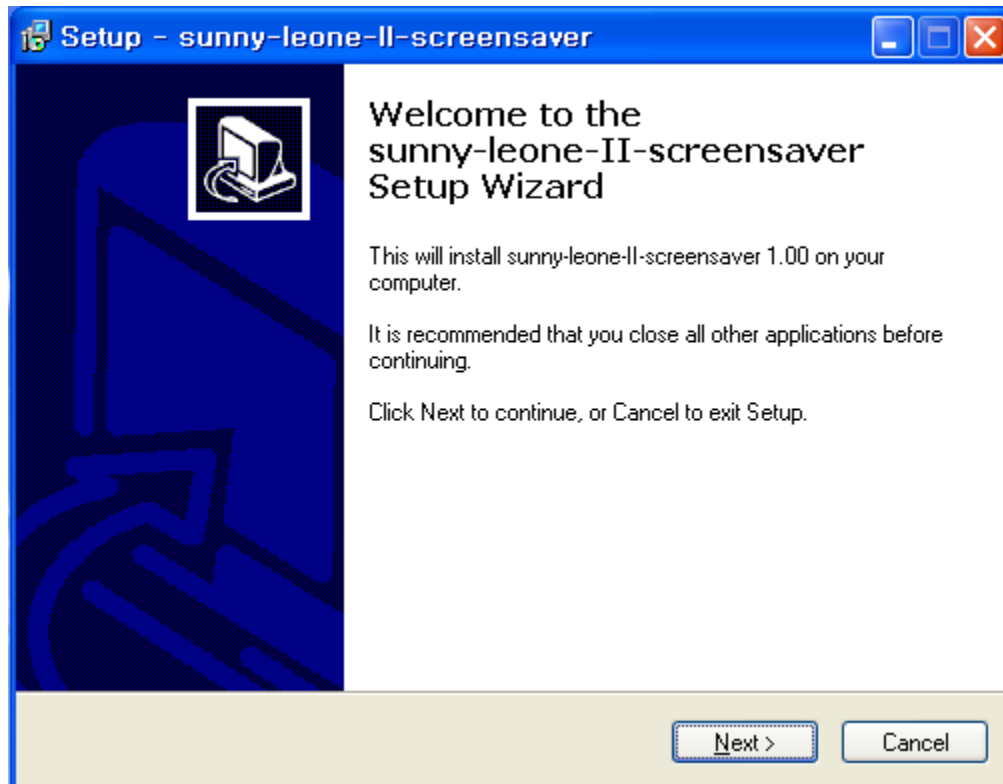
- Backdoor - Redobot (2011-2014)

- DLL files (30 - 40 KB)

- Filename: wines.dll, winsec.dll, rdmgr.dll, tcpsys.dll, svcmgr.dll, rnamsvc.dll, httpcmgr.dll, icmpsec.dll, netmag.dll

```
.10005790: 54 69 2E 6D 65 00 00 00 47 2E 65 74 41 64 2E 61 Ti.me GetAd.a
.100057A0: 70 74 65 2E 72 73 49 2E 2E 6E 66 6F 00 00 00 00 pte.rsI..nfo
.100057B0: 55 20 2E 52 4C 20 2E 44 6F 2E 77 6E 6C 20 6F 2E U .RL .Do.wnl o.
.100057C0: 61 64 20 54 2E 6F 46 2E 69 6C 20 2E 65 41 00 00 ad T.of.il .eA
.100057D0: 44 65 6C 20 2E 65 74 20 65 55 72 6C 2E 43 2E 61 Del .et eUrl.C.a
.100057E0: 63 20 68 65 2E 45 6E 74 2E 72 79 41 00 00 00 00 c he.Ent.ryA
.100057F0: 57 61 6B 65 6E 20 75 70 2E 00 00 00 52 65 73 74 Waken up. Rest
.10005800: 61 72 74 2E 00 00 00 00 55 53 42 20 66 6F 75 6E art. USB foun
.10005810: 64 2E 00 00 47 65 20 2E 74 50 72 20 6F 2E 78 79 d. Ge .tPr o.xy
.10005820: 53 2E 65 73 20 75 20 2E 65 72 00 00 54 45 4D 50 S.er v er TEMP
.10005660: 55 20 2E 52 4C 20 2E 44 6F 3C 2E 77 6E 6C 3E 20 U .RL .Do<.wnl>
.10005670: 6F 2E 61 20 64 20 2D 54 2E 6F 46 2E 69 6C 20 2E o.a d -T.of.il .
.10005680: 65 41 00 00 44 65 2D 20 6C 20 2E 65 74 20 65 55 eA De- l .et eU
.10005690: 72 20 6C 2E 43 2E 61 63 20 2D 20 68 65 2E 45 6E r l.C.ac - he.Ent
.100056A0: 74 2E 72 79 41 00 00 00 57 41 4B 45 00 00 00 00 .10005010: 78 00 00 00 47 3C 65 2E 74 56 6F 3C 6C 75 2E 6D x G<.tVo<lu.m
.100056B0: 52 45 53 45 54 00 00 00 55 53 42 00 47 65 20 2E .10005020: 65 49 20 6E 66 3C 6F 72 6D 3C 61 20 74 69 6F 6E eI nf<orm<a tion
.100056C0: 74 50 72 20 6F 2E 78 79 53 2E 65 72 20 76 20 20 .10005030: 41 00 00 00 47 2E 65 74 44 69 3C 73 6B 46 20 2E A G.etDi<skF .
.100056D0: 65 72 00 00 54 45 4D 50 00 00 00 25 73 64 2E .10005040: 72 65 65 2E 53 70 2E 2E 61 63 65 2E 45 78 41 00 ree.Sp .ace.ExA
.100056E0: 65 25 73 63 20 25 73 20 32 3E 25 73 00 00 00 00 .10005050: 47 2E 3E 65 74 44 3C 72 69 2E 2E 76 65 20 54 79 G.>etD<ri..ve Ty
.100056F0: 25 73 64 2E 65 25 73 63 20 25 73 20 3E 25 73 20 .10005060: 2E 70 65 41 00 00 00 00 47 65 2E 74 4C 2E 6F 67 .peA Ge.tL.og
.10005700: 32 3E 26 31 00 00 00 00 63 6D 00 00 78 65 20 2F .10005070: 69 20 2E 63 61 3C 6C 44 72 2E 2E 69 76 65 73 00 i .ca<lDr..ives
.10005710: 00 00 00 00 43 61 6E 6E 6F 74 20 63 72 65 61 74 .10005080: 47 65 2E 2E 74 20 43 6F 6D 2E 70 75 2E 2E 74 65 Ge..t Com.pu..te
.10005720: 65 20 72 65 6D 6F 74 65 20 66 69 6C 65 2E 00 00 .10005090: 72 2E 4E 61 2E 6D 65 41 00 00 00 00 47 2E 3E 65 r.Na.meA G.>e
.10005730: 43 61 6E 6E 6F 74 20 6F 70 65 6E 20 72 65 6D 6F .100050A0: 74 2E 53 79 2E 73 74 3C 3C 65 6D 44 69 2E 72 65 t.Sy.st<<emDire
.10005740: 74 65 20 66 69 6C 65 2E 00 00 00 00 52 65 6D 6F .100050B0: 20 63 2E 3C 74 6F 72 79 41 00 00 00 47 65 2E 74 c.<toryA Ge.t
.10005750: 74 65 20 66 69 6C 65 20 6E 6F 74 20 66 6F 75 6E .100050C0: 4C 2E 6F 63 61 6C 2E 2E 54 69 20 2E 6D 65 00 00 L.local..Ti.me
.10005760: 64 2E 00 00 4E 6F 20 64 72 69 76 65 2E 00 00 00 .100050D0: 2E 46 69 6E 2E 2E 3C 64 2E 43 2E 6C 6F 20 73 65 .Fin..<d.C.lo se
.100050E0: 00 00 00 00 46 2E 2E 69 6E 64 2E 4E 20 2E 65 78 F..ind.N.ex
.100050F0: 2E 74 46 2E 2E 69 6C 65 41 00 00 00 46 69 2E 6E .tF..ileA Fin
```

- Dropper - Fake installer (2014)
  - Fake Sunny Leone screensaver
  - tmsn.exe -> drop netmonsvc.dll, tmscompg.msi, BAT



\* Source : [https://en.wikipedia.org/wiki/Sunny\\_Leone](https://en.wikipedia.org/wiki/Sunny_Leone)

## Sunny Leone

From Wikipedia, the free encyclopedia

**Karenjit Kaur Vohra**<sup>[6]</sup> (born May 13, 1981),<sup>[1]</sup> known by her **stage name Sunny Leone** (/liˈoʊni/), is a Canadian-born Indian-American actress and **model**, currently active in Indian film industry.<sup>[7]</sup> She is a former **pornstar**.<sup>[8][9]</sup> She has an American citizenship. She has also used the stage name **Karen Malhotra**.<sup>[10][11]</sup> She was named *Penthouse* Pet of the Year in 2003, was a contract performer for *Vivid Entertainment*, and was named by *Maxim* as one of the 12 top **porn stars** in 2010.

She has played roles in independent mainstream events, films and television



- Uninstaller: un.exe

- Stops services & deletes related files

```
00408020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00408030: 5C 00 00 00 74 00 6D 00 73 00 63 00 6F 00 6D 00 \ t m s c o m
00408040: 70 00 67 00 2E 00 6D 00 73 00 69 00 00 00 00 00 p g . m s i
00408050: 6E 00 65 00 74 00 6D 00 6F 00 6E 00 73 00 76 00 n e t m o n s v
00408060: 63 00 2E 00 64 00 6C 00 6C 00 00 00 70 00 6D 00 c . d l l p m
00408070: 73 00 6C 00 6F 00 67 00 2E 00 6D 00 73 00 69 00 s l o g . m s i
00408080: 00 00 00 00 70 00 6D 00 73 00 63 00 6F 00 6E 00 p m s c o n
00408090: 66 00 69 00 67 00 2E 00 6D 00 73 00 69 00 00 00 f i g . m s i
004080A0: 4E 00 65 00 74 00 4D 00 6F 00 6E 00 53 00 76 00 N e t M o n S v
004080B0: 63 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 open :L1)
004080C0: 0A 64 64 64 64 64 64 64 64 64 64 64 64 64 64 64 "%s" if ex
004080D0: 69 73 73 73 73 73 73 73 73 73 73 73 73 73 73 73 "%s" goto L1
004080E0: 0D 0A 64 64 64 64 64 64 64 64 64 64 64 64 64 64 l "%s"
004080F0: 77 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 001pdm.bat
00408100: 38 22 40 40 40 40 40 40 40 40 40 40 40 40 40 40 @ 'q@ Pq@
00408110: 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8
00408120: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 u L
```

```
v2 = OpenServiceW(v0, L"NetMonSvc", 0xF01FFu);
if ( v2 )
{
do
ControlService(v2, 1u, &ServiceStatus);
while ( ServiceStatus.dwCurrentState != 1 );
DeleteService(v2);
}
}
else
{
v2 = v4;
}
CloseHandle(v2);
CloseHandle(v1);
delete_401000(aPmsconfigMsi); // pmsconfig.msi
delete_401000(aPmslogMsi); // pmslog.msi
delete_401000(aNetmonsvcDll); // netmonsvc.dll
delete_401000(aTmscompMsi); // tmscomp.msi
```

- Operation Red Dot (2014-2015)

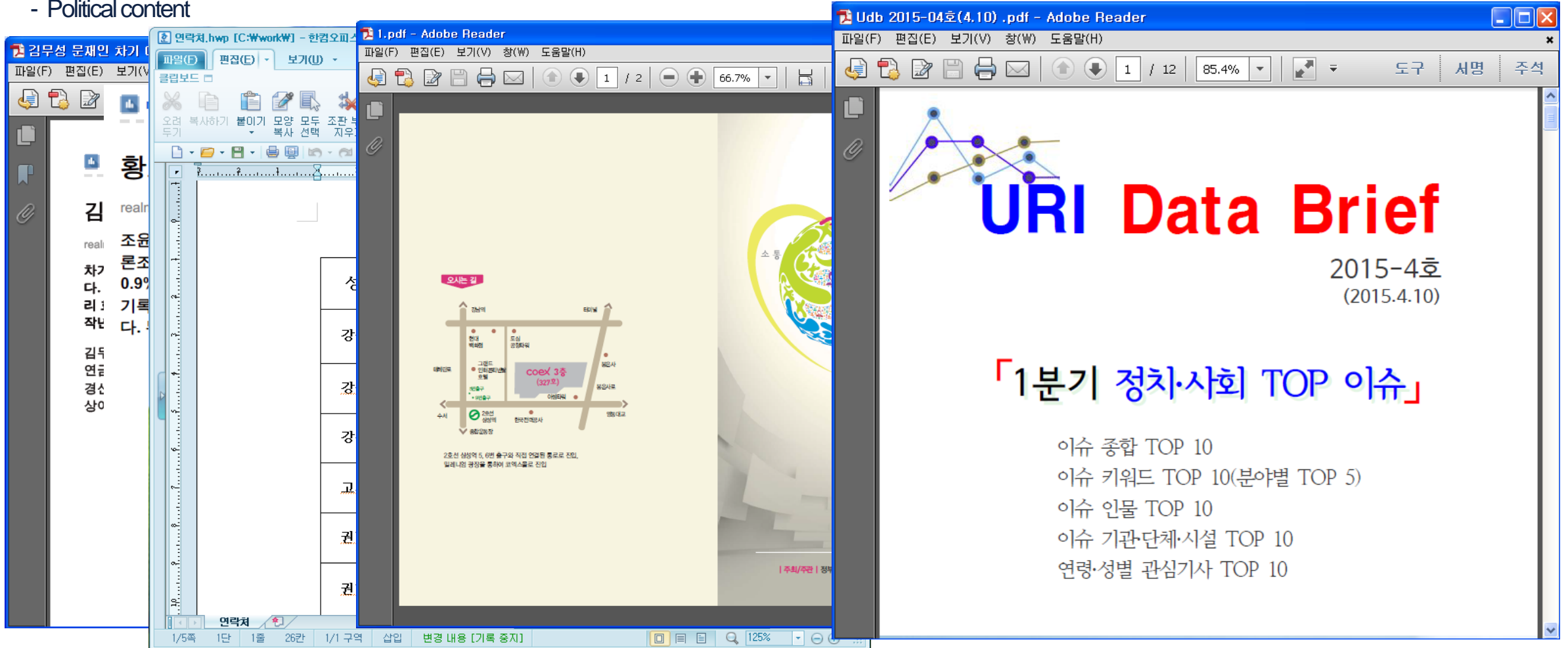
- Main targets: North Korea Research institutes, Political Organization, Defense Industry
- Infection Vectors: Disguised as documents (e.g., HWP, PDF), Fake Installer, HWP exploit
- Malware: Escad, Duuzer
- Filenames: AdobeArm.exe, msnconf.exe

```
.004177B0: 00 00 00 00.56 69 72 20.74 75 61 6C.41 2E 2E 6C      Vir tualA..l
.004177C0: 6C 6F 63 00.56 69 72 20.2E 20 74 75.61 6C 20 46      loc Vir . tual F
.004177D0: 72 65 65 45.78 00 00 00.57 72 69 74.2E 20 65 50      reeEx Writ. eP
.004177E0: 72 6F 63 65.20 2E 20 73.73 4D 65 6D.2E 6F 72 79      roce . ssMem.ory
.004177F0: 00 00 00 00.56 69 72 74.75 20 61 6C.41 6C 2E 6C      Virtu alA.l
.00417800: 6F 63 45 78.00 00 0.00410710: 61 6C 46 72.2E 20 65 65.00 00 00 00.56 69 72 20      alFr. ee Vir
.00417810: 69 2E 20 2E.76 65 5.00410720: 74 75 61 6C.41 2E 2E 6C.6C 6F 63 00.56 69 72 20      tualA..lloc Vir
.00417820: 2E 2E 47 65.74 2E 2.00410730: 2E 20 74 75.61 6C 20 46.72 65 65 45.78 00 00 00      . tual FreeEx
.00417830: 61 6C 44 20.20 2E 7.00410740: 57 72 69 74.2E 20 65 50.72 6F 63 65.20 2E 20 73      Writ. eProce . s
.00417840: 54 2E 65 20.6D 70 4.00410750: 73 4D 65 6D.2E 6F 72 79.00 00 00 00.56 69 72 74      sMem.ory Virt
.00417850: 2E 20 6D 65.57 00 0.00410760: 75 20 61 6C.41 6C 2E 6C.6F 63 45 78.00 00 00 00      u alA.llocEx
.00417860: 2E 6D 70 50.61 2E 7.00410770: 47 2E 20 65.74 44 72 20.69 2E 20 2E.76 65 54 79      G. etDr i. .veTy
.00417870: 43 6F 20 2E.6D 70 7.00410780: 2E 2E 70 65.57 20 00 00.2E 2E 47 65.74 2E 20 20      ..peW . .Get.
.00417880: 6D 65 57 00.47 65 2.00410790: 4C 6F 67 69.2E 2E 2E 63.61 6C 44 20.20 2E 72 69      Logi...calD .ri
.00417890: 6D 44 69 2E.72 65 6.004107A0: 76 65 73 00.47 65 20 74.54 2E 65 20.6D 70 46 69      ves Ge tT.e mpFi
.004178A0: 47 65 20 74.53 79 7.004107B0: 2E 20 6C 2E.65 4E 61 20.2E 20 6D 65.57 00 00 00      . l.eNa . meW
.004107C0: 47 65 2E 20.74 54 65 2E.2E 6D 70 50.61 2E 74 20      Ge. tTe..mpPa.t
.004107D0: 68 57 00 00.47 65 20 74.43 6F 20 2E.6D 70 75 74      hW Ge tCo .mput
.004107E0: 65 2E 20 72.4E 61 2E 2E.6D 65 57 00.47 65 20 74      e. rNa..meW Ge t
.004107F0: 53 79 20 73.74 2E 2E 65.6D 44 69 2E.72 65 63 74      Sy st..emDi.rect
```

Date	Attack Target	Infection Vector	Description
2014.11	Sony Pictures	?	Sample for the Sony Pictures hack. This sample was first uploaded to Virustotal in August 2014 but had been discovered in July 2014 in Korea.
2015.3	Political organizations	Fake Security Installer	
2015.4	Defense Industry	Disguised as a document file	Disguised as a deposit slip. First report of Duuzer.
2015.4	Defense Industry	Disguised as a document file	Masqueraded as a web invitation to a Korean Association conference. Similar to an attack code sample for the Sony Pictures Hack.
2015.5	Political organizations	Disguised as a document file	Document file related to a presidential election
2015.7	Conglomerates	?	Variant of Duuzer
2015.8	Governments	?	Variant of Duuzer
2015.9	Defense Industry	HWP Exploit	Loader
2015.9		Masqueraded as a security program	Korean Security program module that used normal certificates
2015.10	?	HWPx Exploit (CVE-2015-6585)	Resume of a person with military experience
2015.10 - 11	Defense Industry (ADE X Participants)	HWPx Exploit (CVE-2015-	Masqueraded as promotional document for a defense seminar

- Decoy documents

- Political content



- National Assembly Hacked (2015)

- NIS: Three lawmakers and 11 assistant PCs were hacked by North Korea and some of their documents were leaked.
- Targets: Blue House (Presidential Office), Ministry of National Defense, Ministry of Unification, The National Assembly of the Republic of Korea

## 국정원 "北, 국회의원 PC 3대·보좌진 PC 11대 해킹"

NSI : Three lawmakers and 11 assistant PCs were hacked by North Korea

[뉴스시스] 입력 2015.10.20 19:57

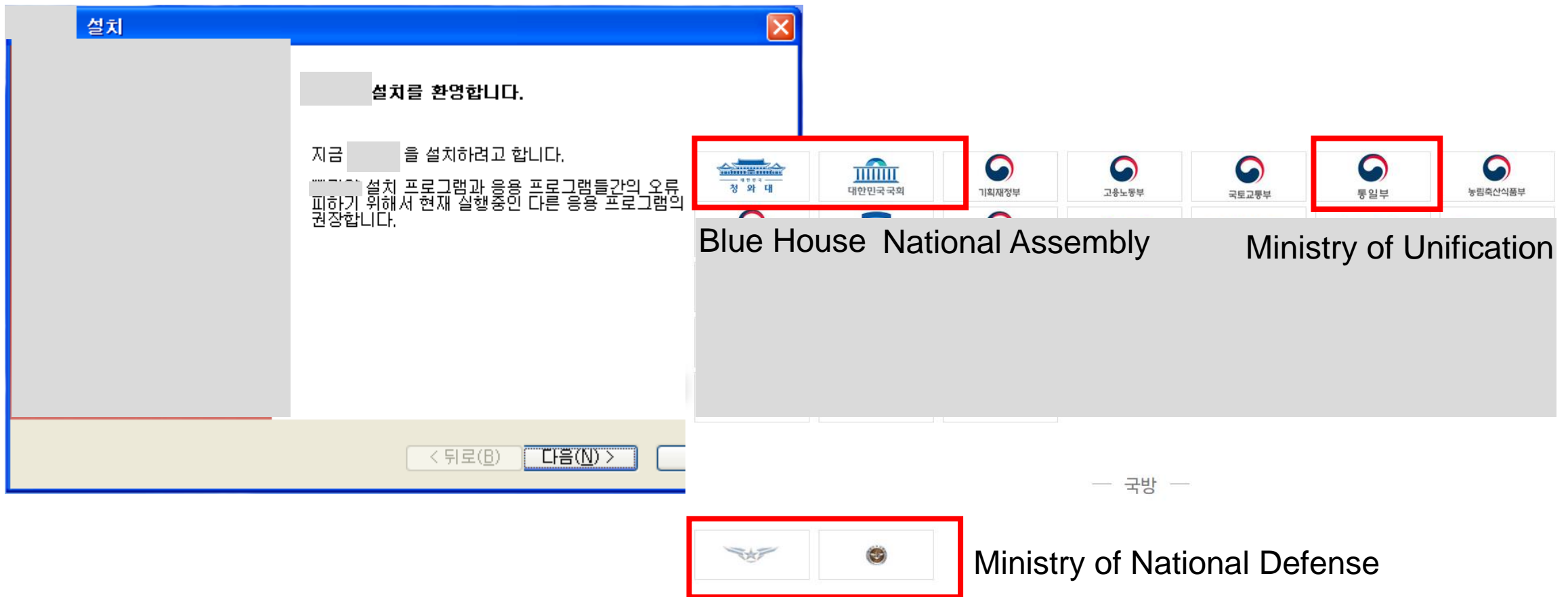


\* Source : <https://news.joins.com/article/18899410> & [http://www.ohmynews.com/NWS\\_Web/View/at\\_pg.aspx?CNTN\\_CD=A0002154495](http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002154495)



- Fake Security program Installer

- Modified Security Installer -> attack on a Political Organization



## •Seoul ADEX 2015 Attendees

- “There is a possibility that this hacking group could be connected with the Sony Pictures hacking group”

### 방산업체 타깃 북한 추정 해킹 공격...소니 악성코드와 유사



‘서울 ADEX 2015’ 운영본부 사칭한 북한 추정 스피어피싱 공격 포착  
자료수집 및 원격제어 악성코드 추가 전송...소니픽처스 악성코드와 유사

[보안뉴스 김경애] 북한 추정 해커조직이 지난 10월 20일부터 25일까지 경기도 성남 서울 공항에서 개최된 ‘서울 ADEX(Aerospace & Defense Exhibition) 2015’ 전시회 참가업체들을 대상으로 한글 취약점을 악용한 스피어피싱 공격을 감행한 정황이 포착됐다.



### 소니픽처스 해킹 조직, 국내서 활동 포착

[AD] 새것보다 전시품 50% 반값할인



<최근 국내서 소니픽처스 해킹에 사용된 것과 같은 구조 악성코드가 발견됐다. 사진은 해킹된 소니픽처스 PC에 나타난 문구.>

지난해 미국 소니픽처스 주요 기밀자료를 빼돌린 해킹조직 활동이 국내에서 포착됐다. KTX·서울메트로 한국 수력원자력 등 주요 기반시설이 줄줄이 해킹당한 사실이 공개된 가운데 대형 사이버 공격 전초조건이 될 수 있어 주의가 요구된다.

\* Source : <http://www.boannews.com/media/view.asp?idx=48598&kind=0> & <http://www.etnews.com/20151007000172>

- ADEX 2015 Attendees (1)
  - HWP Vulnerability (CVE-2015-6585)

보낸 사람: [redacted]@daum.net  
보낸 날짜: 2015-10-15 (목) 오전 8:35  
받는 사람: [redacted]  
참조:  
제목: 2015 항공우주 무기체계 발전 세미나 초청장입니다 ([redacted])  
초청장.hwp (9 MB)

안녕하십니까. [redacted]입니다.  
대한민국 공군과 국방과학연구소는 항공우주 기술협력 증진을 목적으로 2015년도 항공우주 많은 참여 부탁드립니다.

- 기간/장소 : 2015. 10. 21(수)/ 서울공항(AD)  
- 주제 : 창조국방을 선도하는 항공우주 무  
- 주최 : 대한민국공군/ 국방과학연구소  
\* 자세한 내용은 초청장을 참고하시기 바랍  
연락처; [redacted]@daum.net

2015  
항공우주 무기체계  
발전세미나  
미래 전장을 고려한  
유·무인 항공기  
개발 방향  
창조국방을 선도하는  
항공우주무기체계 발전 방향  
일자 2015년 10월 21일(수)  
장소 ADEX 행사장 내 세미나실(서울공항)

대한민국공군  
국방과학연구소  
Agency for Defense Development

- Malware Sample Comparison

- Sony Pictures hack vs. attack in South Korea

```

v4 = &word_413B88;
do
{
    wcsncpy(v4, a0_0_0_0);
    v4 += 20;
}
while ( (signed int)v4 < (signed int)&unk_413D18 );
wcsncpy(&word_413B88, a203_131_222_10);
*(_DWORD *)dword_413E18 = 443;
wcsncpy(&word_413C50, a208_105_226_23);
dword_413E2C = 443;
dword_413E50 = 60;
dword_413E58 = 0;
dword_413E54 = 0;
dword_413E48 = 0;
dword_413E4C = 0;
dword_413E5C = 5;
v5 = time(0);
v6 = GetTickCount();
sub_4068EF(v6 ^ v5);
qword_413E40 = rand();
Movefile_403FF0();
sub_401350(v7, 0);
sub_4068BE((int)aEnd, v9);
return 0;

```

```

v4 = &word_41AF68;
do
{
    wcsncpy(v4, a0_0_0_0);
    v4 += 20;
}
while ( (signed int)v4 < (signed int)&unk_41B0F8 );
wcsncpy(&word_41AF68, a1_186_114_229);
dword_41B1F8 = 443;
wcsncpy(&word_41AFB8, a1_34_78_122);
dword_41B200 = 443;
wcsncpy(&word_41B008, a103_10_60_70);
dword_41B208 = 443;
wcsncpy(&word_41B058, a111_11_86_230);
dword_41B210 = 443;
wcsncpy(&word_41B0A8, a115_115_68_51);
dword_41B218 = 443;
dword_41B230 = 60;
dword_41B238 = 0;
dword_41B234 = 0;
dword_41B228 = 0;
dword_41B22C = 0;
dword_41B23C = 5;
v5 = time(0);
v6 = GetTickCount();
sub_40B43F(v6 ^ v5);
qword_41B220 = rand();
Move_404300();
sub_401390(v7, 0);
sub_40B40E((int)aEnd, v9);
return 0;

```

# 04

Operation Big Pond (2015-2017) & Operation Coin Rush (2017-2018)

AhnLab

- Operation Big Pond (2015.11 – 2017.2)

- Targets: Defense Contractors, Large Korean companies, Web hosting companies, Shopping malls

- Vulnerabilities: CVE-2016-0189 (Microsoft Internet Explorer 11 – VBScript Memory Corruption), CVE-2016-7256 (Open Type Font Elevation of Privilege

Vulnerability)

- Techniques: Big Size (> 50 MB), Loader -> Attempt to bypass the behavior-based security program

- Backdoor remained almost the same

- CVE-2016-7256 (MS16-132)

- AhnLab & KrCERT reported this vulnerability.

MS16-132	Open Type Font Elevation of Privilege Vulnerability	CVE-2016-7256	Kijong Son of KrCERT/CC in Korean Internet & Security Agency (KISA)
----------	---	---------------	---

CVE-ID	
<b>CVE-2016-7256</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
atmfd.dll in the Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Open Type Font Remote Code Execution Vulnerability."	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>• MS:MS16-132</li><li>• <a href="http://technet.microsoft.com/security/bulletin/MS16-132">URL:http://technet.microsoft.com/security/bulletin/MS16-132</a></li><li>• BID:94156</li><li>• <a href="http://www.securityfocus.com/bid/94156">URL:http://www.securityfocus.com/bid/94156</a></li></ul>	
Date Entry Created	
<b>20160909</b>	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20160909)	

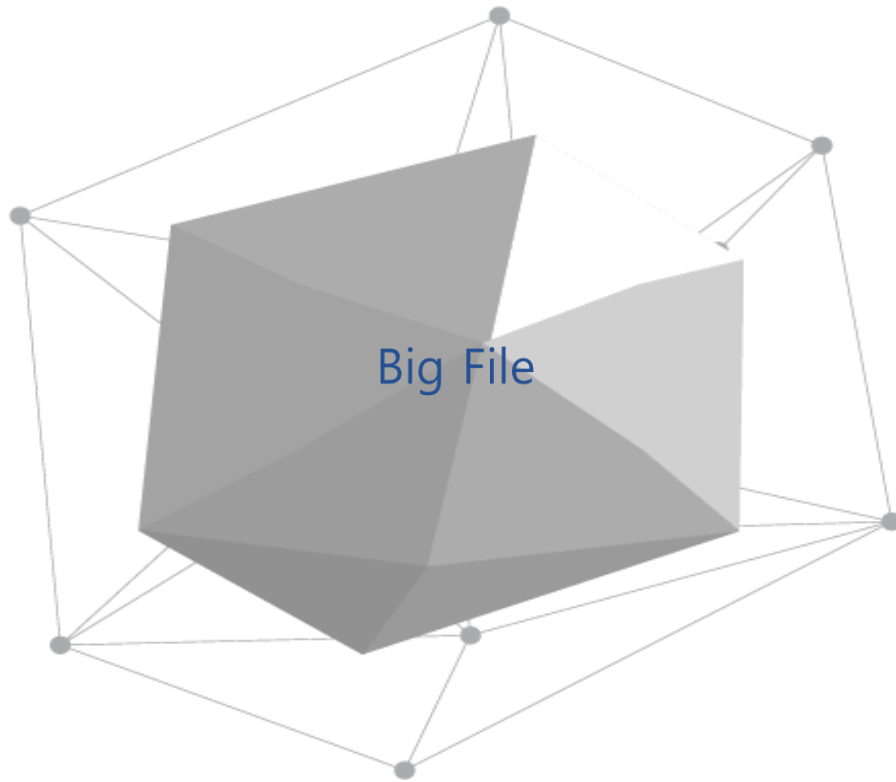
\* Source : <https://technet.microsoft.com/ko-kr/library/security/mt674627.aspx>, <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7256>

- Exploit (2015-2016)

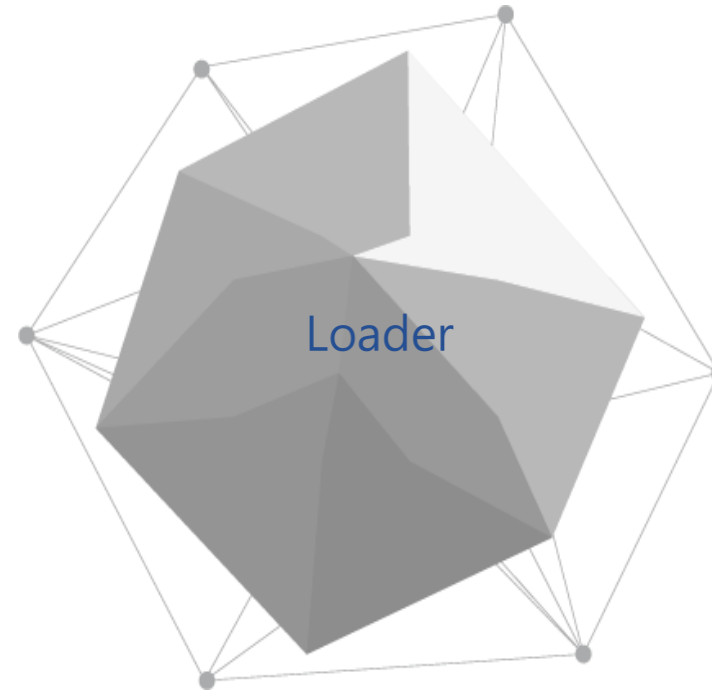
- The attacker had been using it since 2015.

```
00000000: 4F 54 54 4F 00 0C 00 80 00 03 00 40 43 46 46 20  OTTO ♀ C ♡ @CFF 4E 53 00 03 56 53 00  iFOP VK ♥NS ♥VS
00000010: 63 6C 83 3C 00 00 0B C8 00 00 03 56 47 53 55 42  ♀L ♣TGSUR ♣2 30 00 00 00 00 00 00  i°♥  ]3└0
00000020: 2C 53 2F 40  if ( !CreatePipe(&hReadPipe, &hWritePipe, 0, 0x1064u) ) /M ⚡P
00000030: 65 4D C1 2E  { printf("%s\n", "Could not Create a pipe!"); + ⚡P
00000040: 00 B4 00 10  return 0; - ⚡P
00000050: 04 1E 9F 3E  } f? |
00000060: 05 BE 02 2E  if ( !WriteFile(hWritePipe, v11, 0x1064u, &v26, 0) ) ⚡+ ⚡P
00000070: 07 2B 01 B  { printf("%s\n", "Could not write a pipe!"); ⚡P
00000080: 00 03 50 00  return 0; ⚡P
00000090: FD 68 52 3E  } ⚡P
000000A0: FF 86 00 3E  if ( dword_71126F90(66, v12, 0x400000, &v26) < 0 ) ⚡P
000000B0: 06 9E 02 6  { v17 = fopen(&FileName, "r+b"); ⚡P
00415A20: 73 00 00 00 6E 00 6F 00 74 00 65 00 70 00 61 00  s n o t e p a v18 = v17; ⚡P
00415A30: 64 00 2E 00 65 00 78 00 65 00 00 00 50 00 4D 00  d . e x e P M if ( !v17 ) ⚡P
00415A40: 00 00 00 00 78 00 65 00 20 00 2F 00 00 00 00 00  x e / ⚡P
00415A50: 6D 00 64 00 00 00 00 00 63 00 25 00 73 00 2E 00  m d c % s . { printf("%s\n", "There is no font files!"); ⚡P
00415A60: 65 00 25 00 73 00 63 00 20 00 22 00 25 00 73 00  e % s c " % s return 0; ⚡P
00415A70: 20 00 3E 00 20 00 25 00 73 00 20 00 32 00 3E 00  > % s 2 > } ⚡P
00415A80: 26 00 31 00 22 00 00 00 44 00 45 00 4D 00 00 00  & 1 " D E M fseek(v17, 3327, 0); ⚡P
00415A90: 5C 00 00 00 65 00 78 00 70 00 6C 00 6F 00 72 00  \ e x p l o r fwrite(&dword_71126F78, 4u, 1u, v18); ⚡P
00415AA0: 65 00 72 00 2E 00 65 00 78 00 65 00 00 00 00 00  e r . e x e fseek(v18, 3016, 0); ⚡P
00415AB0: 25 00 73 00 5C 00 2A 00 00 00 00 00 2E 00 00 00  % s \ * v19 = 0; ⚡P
00415AC0: 2E 00 2E 00 00 00 00 00 25 00 73 00 5C 00 25 00  . . % s \ % v20 = (char *)malloc(0x354u); ⚡P
00415AD0: 73 00 00 00 3A 00 3A 00 5C 00 00 00 25 00 73 00  s : : \ % s
00415AE0: 5C 00 00 00 67 77 64 66 2E 62 61 74 00 00 00 00  \ g w d f . b a t
```

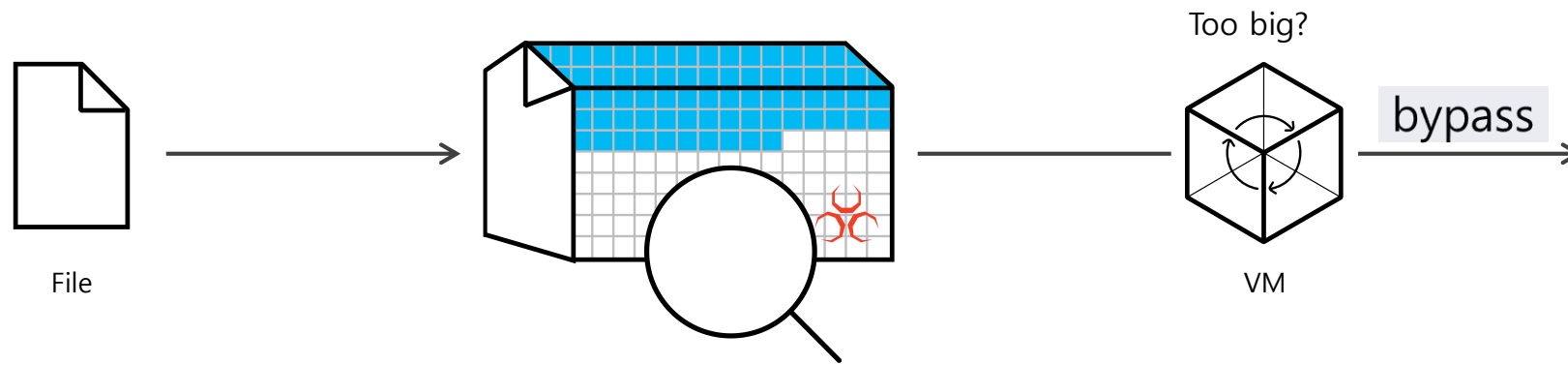


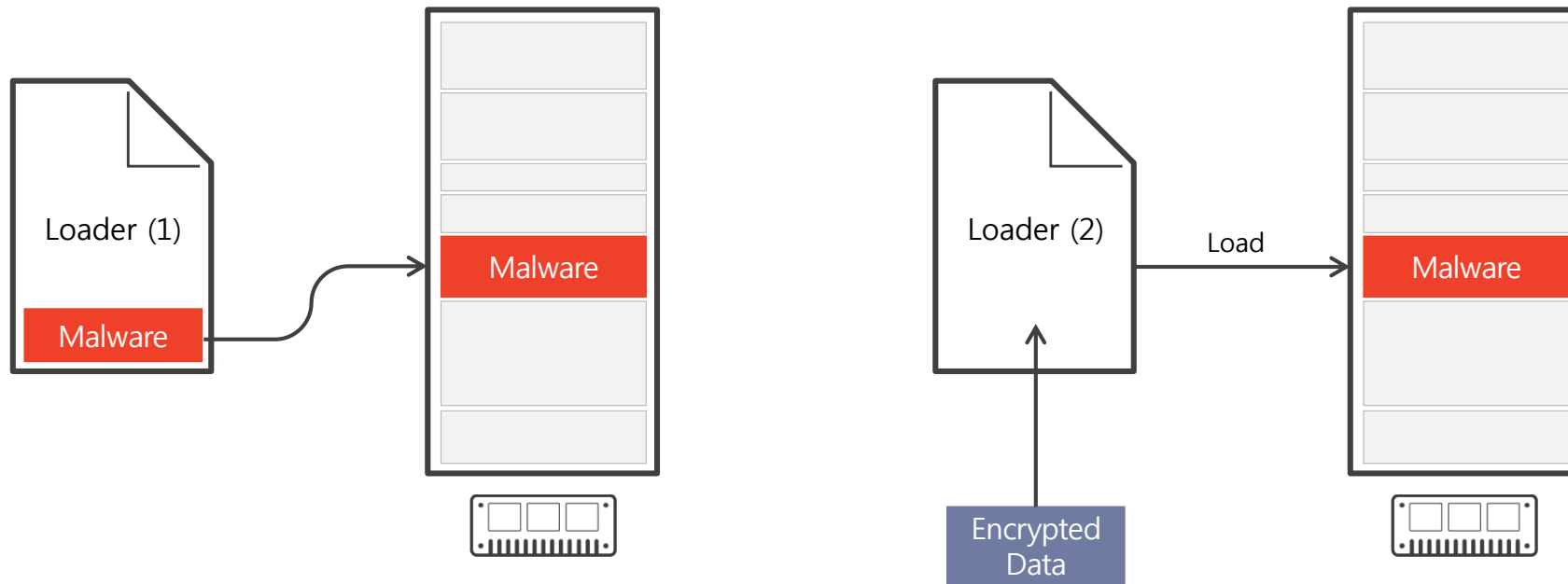


- Create Big size file (> 50 MB)
- Attempt to bypass behavior detection



- Actual malicious code exists in Loader or external file
- Don't drop additional file(s)





- Cryptocurrency Exchange Attacks in South Korea

CYBER RISK DECEMBER 16, 2017 / 11:34 AM / 9 MONTHS AGO

Economy

## Cryptocurrency firm Youbit to shut down North Korean hacker after hack

### South Korean cryptocurrency exchange hack sees \$40m in altcoin stolen

South Korean cryptocurrency exchange Coinrail has suffered a hack and lost some 30 percent of its coins worth



## Bithumb Hacked Second Time in a Year. Hackers Steal \$31 Million

By [Catalin Cimpanu](#)

June 20, 2018 04:00 AM 0

\* Source : <https://www.reuters.com/article/us-northkorea-southkorea-cryptocurrency/north-korean-hackers-behind-attacks-on-cryptocurrency-exchanges-south-korean-newspaper-reports-idUSKBN1EA02F> & [https://www.washingtonpost.com/business/economy/cryptocurrency-firm-youbit-to-shut-down-after-hack/2017/12/19/aa54d586-e4d1-11e7-a65d-1ac0fd7f097e\\_story.html](https://www.washingtonpost.com/business/economy/cryptocurrency-firm-youbit-to-shut-down-after-hack/2017/12/19/aa54d586-e4d1-11e7-a65d-1ac0fd7f097e_story.html) & <https://www.zdnet.com/article/south-korean-cryptocurrency-exchange-hack-sees-40m-in-altcoin-stolen/> & <https://www.bleepingcomputer.com/news/security/bithumb-hacked-second-time-in-a-year-hackers-steal-31-million/>

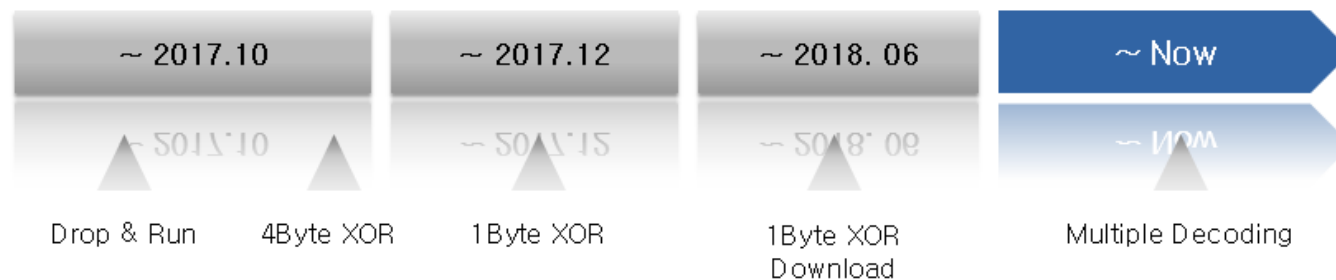


- EPS Shellcode in HWPs

-

## EPS Shellcode

- EPS TYPE A. Drop & Run
- EPS TYPE B. 4Byte XOR
- EPS TYPE C. 1Byte XOR
- EPS TYPE D. 1Byte XOR and Download
- EPS TYPE E. Multiple Decoding and Download

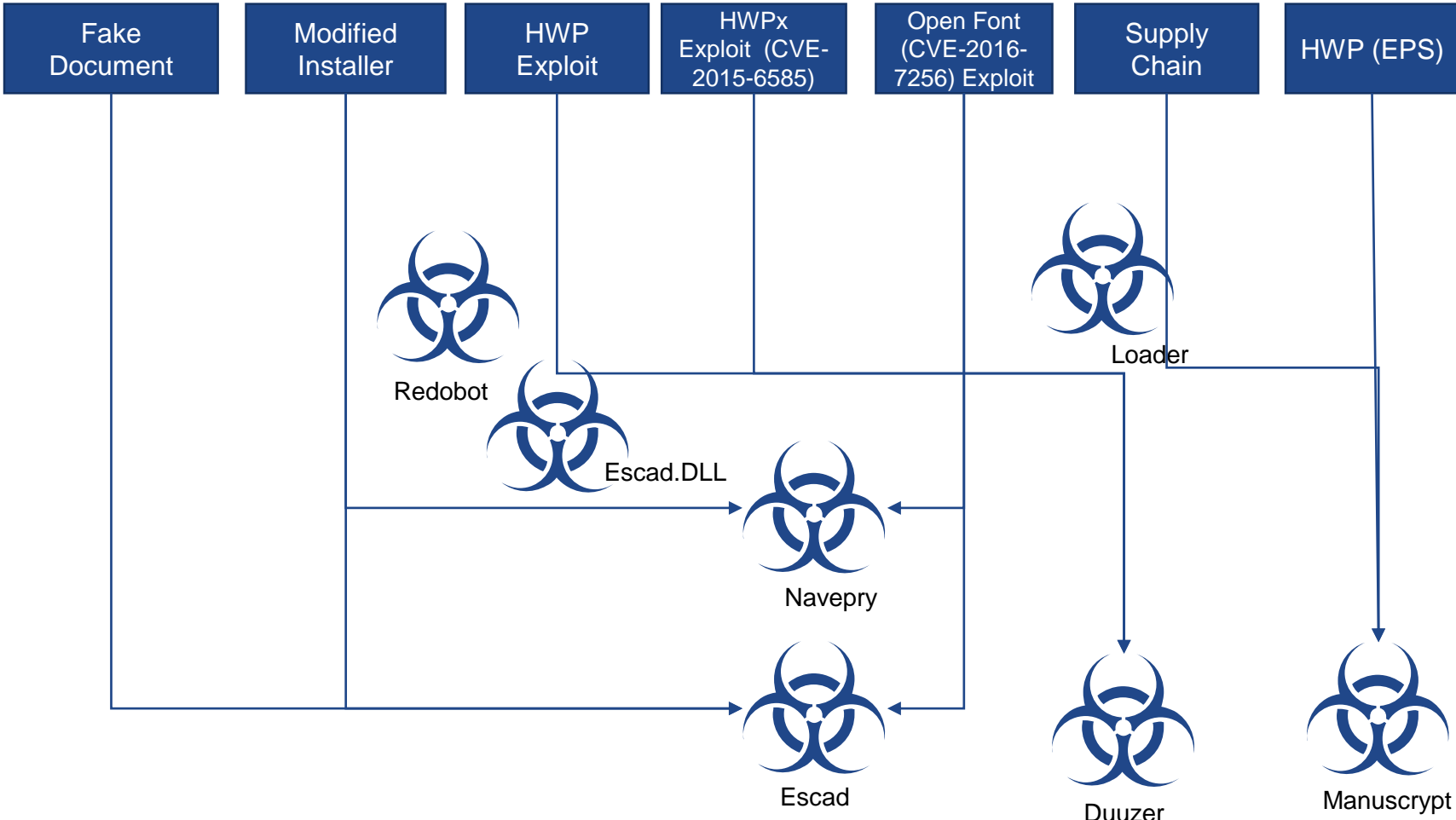


\* Source : Deep dive analysis of HWP malware targeting cryptocurrency exchange @ Seculinside

05

# Lazarus Connections

AhnLab





- Unique execute command

```

FF1564C0D360    call    GetTempFileNameA
8D542468       lea    edx,[esp][068]
8D84247C080000 lea    eax,[esp][00000087C]
52            push   edx
50            push   eax
686CE1D360    push   060D3E16C ; 'xe ' --↓2
6868E1D360    push   060D3E168 --↓3
8D8C248C0C0000 lea    ecx,[esp][000000C8C]
6854E1D360    push   060D3E154 ; '%sd.e%/c "%s > %s"' --↓4
51            push   ecx
FF15C8C1D360    call    wsprintfA
    
```

```

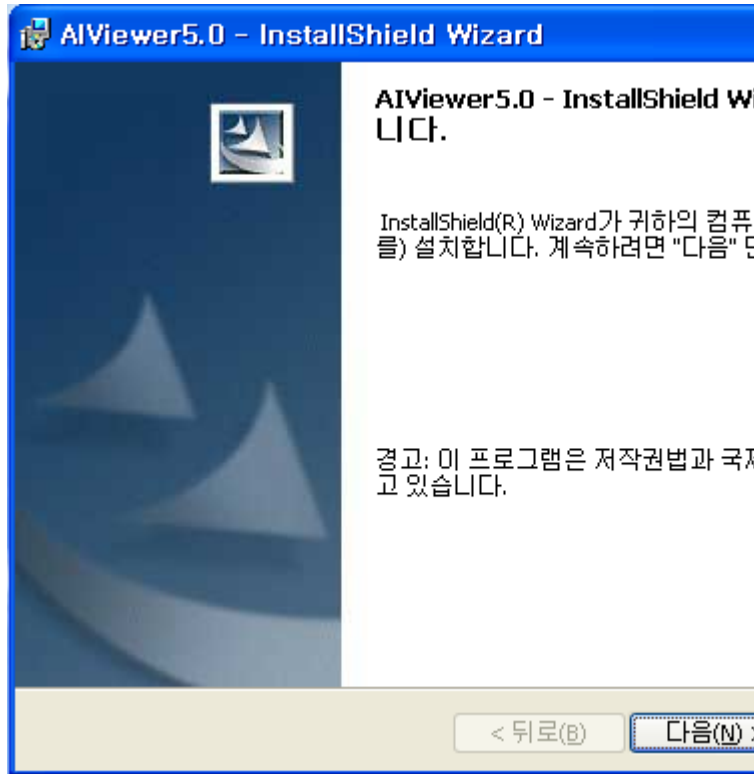
.10002F46: FF1594500010    call    GetTempFileNameA
.10002F4C: 8D4C2474       lea    ecx,[esp][074]
.10002F50: 8D94247C020000 lea    edx,[esp][00000027C]
.10002F57: 8BB42478440000 mov     esi,[esp][0000004478]
.10002F5E: 51            push   ecx
.10002F5F: 56            push   esi
.10002F60: 68D8610010    push   00401472: FF1524A04000    call    GetTempFileNameA
.10002F65: 68D4610010    push   00401478: 8B9424C4080000    mov     edx,[esp][0000008C4]
.10002F6A: 68BC610010    push   0040147F: 8D4C2474       lea    ecx,[esp][074]
.10002F6F: 52            push   00401483: 51            push   ecx
.10002F70: FF1540510010    call    00401484: 52            push   edx
    
```

```

00401472: FF1524A04000    call    GetTempFileNameA
00401478: 8B9424C4080000    mov     edx,[esp][0000008C4]
0040147F: 8D4C2474       lea    ecx,[esp][074]
00401483: 51            push   ecx
00401484: 52            push   edx
00401485: 6850B04000    push   00040B050 ; 'xe /' --↓2
0040148A: 684CB04000    push   00040B04C --↓3
0040148F: 8D8424D8060000 lea    eax,[esp][0000006D8]
00401496: 6838B04000    push   00040B038 ; '%sd.e%sc "%s > %s"' --↓4
0040149B: 50            push   eax
0040149C: E83F1D0000    call    0004031E0 --↓5
    
```

- Fake Installer (2013-2014)

- Fake Installers use different malware



AIViewer5.0 - InstallShield Wizard

AIViewer5.0 - InstallShield Wizard입니다.

InstallShield(R) Wizard가 귀하의 컴퓨터에 프로그램을 설치합니다. 계속하려면 "다음" 단추를 클릭하십시오.

경고: 이 프로그램은 저작권법과 국외 유통을 금지하고 있습니다.

< 뒤로(B)    다음(N) >

```
00431040: 61 70 70 73 2E 73 6B 79 70 65 61 73 73 65 74 73 apps.skypeassets
00431050: 2E 63 6F 6D 00 00 00 00 61 63 63 6F 75 6E 74 73 .com accounts
00431060: 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 00 31 2E 32 2E .google.com 1.2.
00431070: 37 2E 66 2D 68 61 6E 62 61 2D 77 69 6E 36 34 2D 7.f-hanba-win64-
00431080: 76 31 00 00 5A 38 30 32 30 35 36 5C 00 00 00 00 v1 Z802056\
00431090: 3A 3A 00 00 0A 5B 44 72 69 76 65 72 3A 25 73 5D :: [Driver:%s]
004310A0: 09 09 5B 56 6F 6C 75 6D 65 4E 61 6D 65 3A 25 73 °°[VolumeName:%s
004310B0: 5D 09 09 5B 53 4E 3A 25 58 5D 0A 00 25 73 5C 25 ]°°[SN:%X] %s\%
004310C0: 73 2E 74 6D 70 00 00 00 25 58 00 00 25 73 25 58 s.tmp %X %s%X
004310D0: 00 00 00 00 25 30 34 64 2D 25 30 32 64 2D 25 30 %04d-%02d-%0
004310E0: 32 64 20 25 30 32 64 3A 25 30 32 64 3A 25 30 32 2d %02d:%02d:%02
004310F0: 64 09 25 64 09 25 73 0A 00 00 00 0A 25 73 0A d°d°s° °s°

0041B0F0: 72 6D 76 67 5F 61 77 77 69 00 00 00 79 72 6D 77 rmvg_awwi yrmw
0041B100: 00 00 00 00 5F 5F 57 53 41 46 44 49 68 53 76 67 _WSAFDIhSvg
0041B110: 00 00 00 00 68 76 6D 77 00 00 00 00 68 76 6F 76 hvmw hvov
0041B120: 78 67 00 00 73 67 6C 6D 68 00 00 00 68 6C 78 70 xg sglmh hlxp
0041B130: 76 67 00 00 78 6F 6C 68 76 68 6C 78 70 76 67 00 vg xolhvhlxpvg
0041B140: 78 6C 6D 6D 76 78 67 00 61 78 78 76 6B 67 00 00 xlmvvg axxvkg
0041B150: 74 76 67 73 6C 68 67 79 62 6D 61 6E 76 00 00 00 tvgslhgybmanv
0041B160: 68 73 66 67 77 6C 64 6D 00 00 00 00 6F 72 68 67 hsfgwldm orhg
0041B170: 76 6D 00 00 57 53 41 53 67 61 69 67 66 6B 00 00 vm WSASgaigfk
0041B180: 68 76 67 68 6C 78 70 6C 6B 67 00 00 69 76 78 65 hvghlxplkg ivxe
0041B190: 00 00 00 00 57 53 41 43 6F 76 61 6D 66 6B 00 00 WSACovamfk
0041B1A0: 77 73 6F 63 6B 33 32 2E 64 6C 6C 00 77 73 32 5F wsock32.dll ws2_
0041B1B0: 33 32 2E 64 6C 6C 00 00 57 54 53 47 76 67 41 78 32.dll WTSGvgAx
```

- BM?

-Andariel's Dllbot (2009) vs. Redobot Dropper (2011) vs. Cyber 6.25 (2013) vs. Andariel's Bmdoor (2014)

```
00000000: 42 4D 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 BM
00000010: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040: 00404010: 42 4D 5A 41 00 00 00 00 5C 00 00 00 25 73 25 73 BMZA \ %s%s
00000050: 00404020: 25 73 22 25 73 22 00 00 25 53 79 73 74 65 6D 52 %s"%s" %SystemR
00000060: 00404030: 6F 6F 74 25 00 00 00 00 5C 73 79 73 74 65 6D 33 oot% \system3
00000070: 00404040: 32 5C 00 00 73 76 63 68 6F 73 74 2F 65 78 65 20 2\ suchost.exe
00000080: 00404050: 20 100101B0: 55 29 28 41 3B 4F 49 43 49 3B 47 52 3B 3B 3B 42 U)(A;OICI;GR;;;B
00000090: 00404060: 72 100101C0: 41 29 00 00 47 6C 6F 62 61 6C 5C 4D 69 63 72 6F A) Global\Micro
00000100: 00404070: 54 100101D0: 73 6F 66 74 55 70 67 72 61 64 65 4F 62 6A 65 63 softUpgradeObjec
00000110: 00404080: 5C 100101E0: 74 39 2E 36 2E 34 00 00 42 4D 36 57 00 00 00 00 t9.6.4 BM6W
00000120: 00404090: 69 100101F0: 72 62 00 00 7E 4D 52 00 9A 99 99 99 99 99 D9 BF rb ~MR üööööö
00010200: 9A 0045DFC0: 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 INGXXPADDINGPADD
00010210: 6F 0045DFD0: 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 INGXXPADDINGPADD
00010220: 5C 0045DFE0: 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 INGXXPADDINGPADD
00010230: 68 0045DFF0: 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 INGXXPADDINGPADD
00057800: 42 4D 7C 88 03 00 00 00 00 00 00 00 36 00 00 00 28 00 BMê 6 (
00057810: 00 00 86 01 00 00 9A 02 00 00 01 00 00 00 05 00 ä ü
00057820: 00 00 46 88 03 00 BA 05 00 00 BA 05 00 00 00 00 Fê
00057830: 00 00 00 00 00 00 DE D3 46 25 53 1D B0 50 D6 C0 |LF%S+P L
00057840: 7F F8 DD ED 72 F2 B8 43 FC F3 17 42 EB A5 CD 02 °| φr>7C^n<↑BδÑ=0
00057850: 47 F9 D3 25 7D BE 90 0A BC 73 57 43 A0 59 32 4A G•L%}↓É sWCáY2J
00057860: 0E CD DE 6F 5F D5 16 15 C0 F9 15 1E D8 54 56 A4 ß=|o_f_sL•S+TVñ
00057870: AC EA 9E EA C0 3C 3C 92 7F 1A 8F 10 DD B9 CA 5E %ΩRΩ<<ÆΔ→Ä|↑^
00057880: 3B 05 F4 F1 8B 38 33 ED B4 AC 49 95 38 ED 5F 05 ;|±i83φ+¼Iò8φ
```

06

Who is behind it?

AhnLab

- North Korea?

-



**PARK JIN HYOK**

**Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud  
(Computer Intrusion)**



\* Source : <https://www.fbi.gov/wanted/cyber/park-jin-hyok/download.pdf>

- Similar Code

- Attackers can mimic well-known characteristics.
- The drill samples in Korea are similar to this group's malwares.

Recorded Future decided to not attribute this attack to any actor; however, they **claimed** that they found similarities to BlueNoroff/Lazarus LimaCharlie malware loaders that are widely be

We can't dispute that part of the code really does resemble the Laz (MD5: 3c0d740347b0362331c882c2dee96dbf) and Bluenoroff (MD code to wipe files.

```
Buffer = 0;
memset(&v1, 0, 0xFFCu);
v10 = 0;
v19 = 0;
v1 = CreateFile(lpFileName, 0x4000000u, 0, 0, 3u, 0x80u, 0);
v2 = v1;
if (v2 == (HANDLE)-1)
    return GetLastError();
SetFilePointer(v1, -1, 0, 2u);
WriteFile(v2, &Buffer, 1u, &NumberOfBytesWritten, 0);
FlushFileBuffers(v2);
FileSize.QuadPart = 0x164;
GetFileSizeEx(v2, &FileSize);
SetFilePointer(v2, 0, 0, 0);
v4 = FileSize.HighPart;
v8 = FileSize.LowPart;
v9 = 0;
v7 = 0;
if ( FileSize.HighPart >= 0 && (FileSize.HighPart > 0 || FileSize.LowPart > 0) )
{
    while ( 1 )
    {
        v8 = _ORAND_( _PAIR_( v4, v5 ), _PAIR_( v7, v6 ));
        v11 = v5 - v6;
        v9 = ( _PAIR_( v4, v5 ) - _PAIR_( (unsigned int)v7, v6 ) ) >> 32;
        v10 = v5 - v8;
        if ( v9 < 0 || (unsigned __int8)((v9 < 0) ^ v9) | (v9 == 0) && v11 <= 0x1000 )
        {
            v15 = v9;
        }
        else
        {
            v10 = 0x1000;
            v15 = 0;
        }
        if ( !WriteFile(v2, &Buffer, v10, &NumberOfBytesWritten, 0) || !NumberOfBytesWritten )
            break;
        v4 = FileSize.HighPart;
        v12 = NumberOfBytesWritten + v8;
    }
}
```

Fig.12 Comparison of wiping module (left: Bluenoroff tool; right: OlympicDestroyer)

## OnionDog is not a Targeted Attack–It’s a Cyber Drill

Posted on: August 9, 2017 at 5:00 am    Posted in: Malware  
Author: Trend Micro Forward-Looking Threat Research Team



by Feike Hacquebord, Stephen Hilt and Fernando Mercês

Alleged attacks from North Korean actors are a hot security research topic. The infamous **Sony Pictures hack in 2014**, for instance, was reported by some to be the work of North Korean threat actors. There is a lot of interest in Lazarus too, which is purportedly a **North Korea-linked group** responsible for a couple of global bank heists that attempted to steal staggering amounts of money.



\* Source : <https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295> & <https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/>

- IP Address

- Reuses C&C Server
- Found North Korean IPs in C&C Servers
- Malware analysis training material included a North Korean IP




## 北, '눈엣가시' 데일리NK 지속적으로 해킹

한국인터넷진흥원 "공격자 IP에 '북한' 확인...서버공격·악성코드 심화"

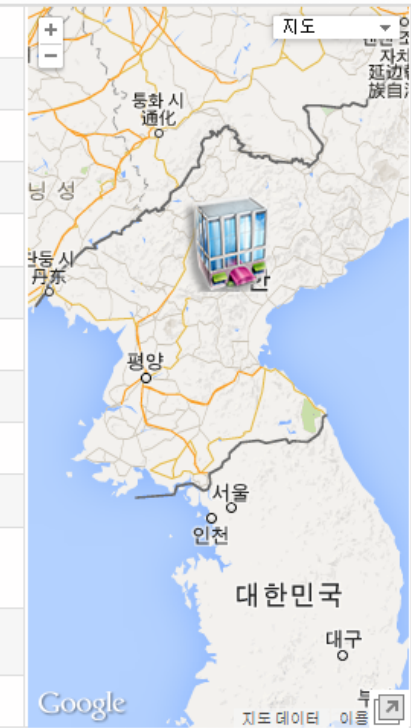
이상용 기자 | 2015-05-14 10:20

북한 해킹 조직이 데일리NK 사이트와 서버에 대한 해킹을 지속적으로 진행하고 있는 것으로 알려졌다. 김정운을 비롯한 북한 내 악의를 품고 이를 약화시키기 위한 해킹이라는 지적이 나온다.

한국인터넷진흥원(KISA)가 11일 본지에 발송한 분석결과에 따르면 홈페이지 해킹 관련, 공격자 IP(Internet Protocol) 중 '북한'이 있는 서버에서 웹shell이 발견됐고 해당 웹shell에 접근한 공격자 IP 중 상당수였던 것.

Current IP Range:	175.45.178.0 - 175.45.178.255
IP Range Location:	 North Korea
IP Owner:	 Star Joint Venture Co Ltd
Owner Full IP Range:	175.45.176.0 - 175.45.179.255
Owner Address:	Ryugyong-Dong Potong-Gang District
Owner Country:	 North Korea
Owner Phone:	+66 81 208 7602, +850 2 381 2321
Owner Website:	<a href="http://www.loxley.co.th">www.loxley.co.th</a>
All Owner IP Ranges:	<a href="#">175.45.176.0 - 175.45.179.255</a>
All Owner CIDR:	<a href="#">175.45.176.0/22</a>
All Owner IP Reverse DNS (Host)s:	<a href="#">naenara.com.kp</a>
Whois Record Updated:	02 Dec 2014

[Show Whois Additional Information from whois://whois.apnic.net](#)



\* Source : <http://www.dailynk.com/korean/read.php?catald=nk00100&num=106135> & <http://www.dailynk.com/korean/read.php?catald=nk00100&num=106135>

- Awkward Korean

- Nonsul (논술) in South Korean vs. Ronsul (론술) in North Korean, both have the meaning of “logical writing”
- Is this a mistake? If not, why are they so sloppy?



07

# Conclusion

AhnLab

- Takeaways

- Lazarus Group (including the Andariel Group): Motivation for attack seems to have changed (Confidential Information → Monetary benefit)
- They know Korean very well and understand Korea's culture and environment
- They used many Zeroday vulnerabilities
- They attack vulnerabilities in Korean software and disguised as famous Korean software
- Don't be fooled by Korean cyber drill
- They're active outside of South Korea

- Cooperation

- Attribution hell
- It's important to disclose and share information
- We must cooperate to fight them
- AhnLab will share relevant information with the members of industry



email : [minseok.cha@ahnlab.com](mailto:minseok.cha@ahnlab.com) / [mstoned7@gmail.com](mailto:mstoned7@gmail.com)

 [@mstoned7](https://twitter.com/mstoned7)

<https://www.facebook.com/xcoolcat7>



- Novetta, Operation BlockBuster (<https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf>)
- Snorre Fagerland, 'From Seoul to Sony : The History of the Darkseoul Group and the Sony intrusion malware Destrover' (<https://www.yumpu.com/en/document/view/55505308/the-history-of-the-darkseoul-group-and-the-sony-intrusion-malware-destrover/72>)
- KrCERT, 사이버 침해사고 정보공유 세미나 자료집 2016년 4분기(Analysis of recent APT attack and infringement cases 4Q 2016) ([https://www.boho.or.kr/data/reportView.do?bulletin\\_writing\\_sequence=25246](https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=25246))
- Seongsoo Park, Anatomy of attacks aimed at financial sector by the Lazarus group, (<https://www.slideshare.net/SeongsuPark8/area41-anatomy-of-attacks-aimed-at-financial-sector-by-the-lazarus-group-104315358/1>)
- JO Hyoje & LEE Hee-Joo, Deep dive analysis of hwp malware targeting cryptocurrency exchange
- Campaign DOKKAEBI : Documents of Korean and Evil Binary (<http://www.fsec.or.kr/user/bbs/fsec/21/13/bbsDataView/1063.do>)

More security, More freedom



AhnLab