2018.05.03

Analysis Report

Detailed Analysis of Red Eyes Hacking Group

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com

Table of Contents

Abstract

Red Eyes attack group has also been tracked as Geumseong121, Group 123, ScarCruft, APT37, Reaper, and Ricochet Chollima. Based on the contents of malicious files used in the attacks, it appears that its main targets are organizations and individuals whose work involves North Korea. These include North Korean defectors, human rights activists for North Korea, North Korean researchers, and journalists. In some cases, it has even accessed South Korean military related documents.

Red Eyes group's main method is to send a document via email or mobile messenger to deliver the malware. Typically, executable files in formats such as .vbs or .exe are inserted in documents. The group also exploits the Encapsulated PostScript (EPS) vulnerability of the Hangul word-processing program, which is widely used throughout South Korea.

Microsoft Office documents have also been used in attacks. In October 2017, the group launched an attack that exploited Microsoft Word's Dynamic Data Exchange (DDE) feature. In February 2018, Red Eyes exploited the zero-day Adobe Flash Player vulnerability (CVE-2018-4878).[1] It was later revealed, however, that the first such attack had taken place in November 2017. Then, in March 2018, Red Eyes launched a targeted mobile malware attack.[2]

The activities of Red Eyes were first detected in the fall of 2016, not long after the disappearance of an earlier group of hackers that were active from 2015 to the spring of 2016. That earlier group carried out Operation ProgamsByMe in 2015 and is thought to be affiliated with Red Eyes. Red Eyes use a variety of methods and is known to include text strings within their code such as “First,” “Happy,” and “Work.”

In this report, we will take a closer look at the main activities of Red Eyes and another group that may be affiliated with it.

[1] http://blog.talosintelligence.com/2018/02/group-123-goes-wild.html

[2] https://byline.network/2018/03/1-1052/

Overview of the Activities of Red Eyes

Hacking attempts have targeted North Korean defectors and human rights activists for North Korea over the course of five years. In one case, a website operated by North Korean defectors was attacked. An investigation carried out by major domestic and overseas security vendors revealed that some of the attacks were the work of a group called Red Eyes.

Red Eyes attack group is also known as Geumseong121, Group 123, ScarCruft, APT37, Reaper, and Ricochet Chollima. Based on the contents of malicious files used in the attacks, it appears that its main targets are organizations and individuals whose work involves North Korea. These include North Korean defectors, human rights activists for North Korea, North Korean researchers, and journalists. In some cases, it has even accessed Korean military related documents.

The information about the group was first reported by Cisco Talos, a threat intelligence team, in 2017,[3] but Red Eyes received more attention at the end of January 2018, when it launched an attack that exploited the zero-day Adobe Flash Player vulnerability (CVE-2018-4878).[4] Soon after, cybersecurity companies released their findings: FireEye released its analysis of the group in February,[5] and in March, ESTsecurity announced its findings on mobile malware that had been distributed through a mobile messenger.

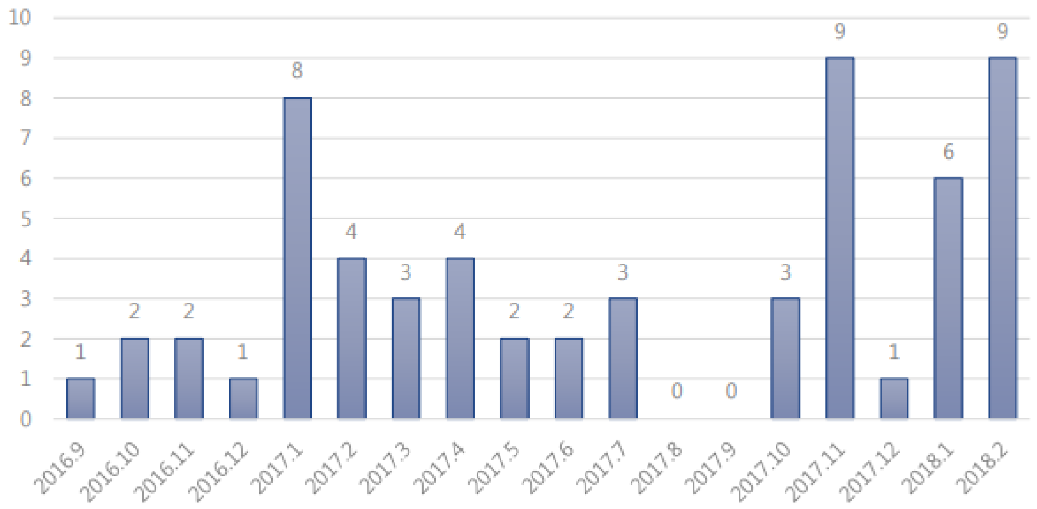
[3] http://blog.talosintelligence.com/2017/02/korean-maldoc.html

[4] http://blog.talosintelligence.com/2018/02/group-123-goes-wild.html

[5] https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html

1. Current Status and Characteristics

Malware with Red Eyes characteristics were discovered repeatedly beginning in the fall of 2016 through the end of 2017. The occurrence of the malware is shown in Figure 1. Most of the malware took the form of document files, droppers, or backdoors.



[Figure 1] Occurrence of Malware from Red Eyes Group (Sept. 2016-Feb. 2018)

One of the characteristics of malware from this group is that it uses a program database (PDB) text string. Table 1 shows the PDB text strings that were used to gain information about the malware, such as its version and type.

d:\HighSchool\version 13\2ndBD\T+M\T+M\Result\DocPrint.pdb

D:\HighSchool\version 13\First-Dragon(VS2015)\Sample\Release\DogCall.pdb

D:\HighSchool\version 13\VC2008(Version15)\T+M\T+M\TMProject\Release\ErasePartition.pdb

E:\Happy\Work\Source\version 12\First-Dragon\Sample\Release\DogCall.pdb

e:\Happy\Work\Source\version 12\T+M\Result\DocPrint.pdb

[Table 1] PDB Strings in Red Eyes Group Malware

2. Main Attacks and Methods

Red Eyes spreads malware mainly by sending malicious email attachments to their targets. In March 2018, it also used mobile messenger texts to send malware.

They mainly exploit the EPS vulnerability of the Hangul (.hwp) word-processing program, which is widely used in South Korea, or used the method of inserting executable files, such as .vbs or .exe. They also use Microsoft Office documents for attacks. In October 2017, the group launched an attack that exploited Microsoft Word's DDE feature. Then, in February 2018, it used a Microsoft Office file to exploit the zero-day Adobe Flash Player vulnerability (CVE-2018-4878). This method of attack was later identified to have first taken place in November 2017.

Red Eyes group has been active since 2016. Its main attacks are listed in [Table 2].

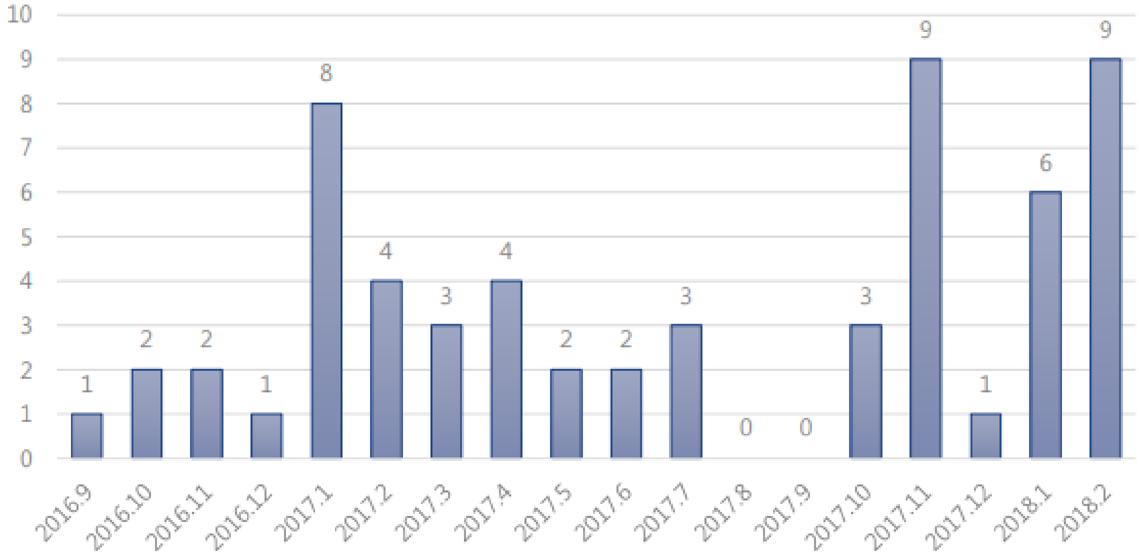
Date	Attack Method	Document Content
2016.09	Hangul EPS	Academic conference on North Korea
2016.09	Hangul EPS	News about North Korea and North Korean defectors
2017.01	Malware inserted in Hangul file	New year address of North Korea
2017.01	Hangul EPS	Announcement of support for public activities of private organization in 2017
2017.02	Hangul EPS	Résumés of Korean-Chinese migrants
2017.03	Hangul EPS	Political content (malware inserted in the document destroyed data on the hard disk)
2017.03	Hangul EPS	Military content
2017.03	Hangul EPS	Labor contracts
2017.05	Hangul EPS	News on a man who lived 555 days without a heart
2017.10	DDE	Confirmation of money transfers and content seemingly related to propaganda leaflets or balloons for North Korea
2017.10	Hangul EPS	Request for assistance for North Korean defectors
2017.11	Inserted .vbs file	Conference on the North Korean Human Rights Act
2017.11	Flash file attached to the Excel file	Cosmetics prices

[Table 2] Main Attacks by Red Eyes Group

The group first exploited the EPS vulnerability of the Hangul word program in the fall of 2016. The malicious documents concerned academic conferences and news about North Korea and matters relating to North Korean defectors.

In January 2017, a Hangul file containing the new year address of North Korea was used in an email attachment attack that used the file as loader for in-memory execution of another malware.

A variant of this malware was found in November 2016.



[Figure 2] Occurrence of Malware from Red Eyes Group (Sept. 2016-Feb. 2018)

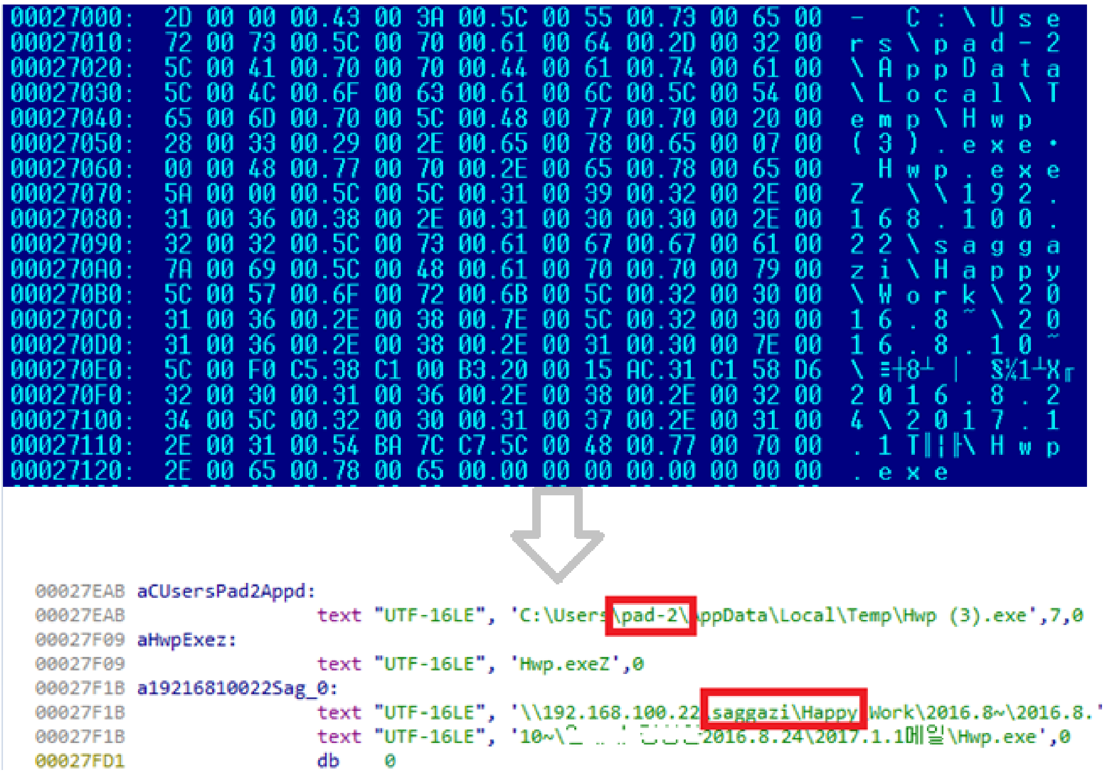
In February 2017, a DogCall backdoor was found in a Hangul file disguised as a résumé. The DDE-based attacks took place in late October and November 2017.

In November 2017, Red Eyes used an attack method where a .vbs file was linked in the body of a Hangul file concerning a civic organization for human rights in North Korea. (md5: 7ca1e08fc07166a440576d1af0a15bb1). If the user clicks on the text, an HncModuleUpdate.vbs file is executed to perform malicious tasks.

At the end of January 2018, the Korea National Computer Emergency Response Team (krCERT) within the Korea Internet & Security Agency (KISA) announced that it had discovered the Adobe Flash Player zero-day vulnerability. In fact, however, a similar attack had occurred in November 2017 using a document on cosmetics prices.

The malicious Hangul document (md5: 44bdeb6c0af7c36a08c64e31ceadc63c) discovered in January 2017, masquerading as the New Year address of North Korea, had an executable file inserted. Malware is executed if the user clicks on the file.

When an object is inserted in a Hangul file, it is possible to check the original file path as shown in Figure 3. This information can provide clues as to who may have developed the malware.



```
00027000:  2D 00 00 00.43 00 3A 00.5C 00 55 00.73 00 65 00  -   C : \ U s e
00027010:  72 00 73 00.5C 00 70 00.61 00 64 00.2D 00 32 00  r s \ p a d - 2
00027020:  5C 00 41 00.70 00 70 00.44 00 61 00.74 00 61 00  \ A p p D a t a
00027030:  5C 00 4C 00.6F 00 63 00.61 00 6C 00.5C 00 54 00  \ L o c a l \ T
00027040:  65 00 6D 00.70 00 5C 00.48 00 77 00.70 00 20 00  e m p \ H w p
00027050:  28 00 33 00.29 00 2E 00.65 00 78 00.65 00 07 00  ( 3 ) . e x e •
00027060:  00 00 48 00.77 00 70 00.2E 00 65 00.78 00 65 00    H w p . e x e
00027070:  5A 00 00 00.5C 00 5C 00.31 00 39 00.32 00 2E 00  Z   \ \ 1 9 2 .
00027080:  31 00 36 00.38 00 2E 00.31 00 30 00.30 00 2E 00  1 6 8 . 1 0 0 .
00027090:  32 00 32 00.5C 00 73 00.61 00 67 00.67 00 61 00  2 2 \ s a g g a
000270A0:  7A 00 69 00.5C 00 48 00.61 00 70 00.70 00 79 00  z i \ H a p p y
000270B0:  5C 00 57 00.6F 00 72 00.6B 00 5C 00.32 00 30 00  \ W o r k \ 2 0
000270C0:  31 00 36 00.2E 00 38 00.7E 00 5C 00.32 00 30 00  1 6 . 8 ~ \ 2 0
000270D0:  31 00 36 00.2E 00 38 00.2E 00 31 00.30 00 7E 00  1 6 . 8 . 1 0 ~
000270E0:  5C 00 F0 C5.38 C1 00 B3.20 00 15 AC.31 C1 58 D6  \ ≡┼8┴ │  $%1┴X╓
000270F0:  32 00 30 00.31 00 36 00.2E 00 38 00.2E 00 32 00  2 0 1 6 . 8 . 2
00027100:  34 00 5C 00.32 00 30 00.31 00 37 00.2E 00 31 00  4 \ 2 0 1 7 . 1
00027110:  2E 00 31 00.54 BA 7C C7.5C 00 48 00.77 00 70 00  . 1 T‖¦╟\ H w p
00027120:  2E 00 65 00.78 00 65 00.00 00 00 00.00 00 00 00  . e x e
```

```
00027EAB aCUsersPad2Appd:
00027EAB                 text "UTF-16LE", 'C:\Users\pad-2\AppData\Local\Temp\Hwp (3).exe',7,0
00027F09 aHwpExez:
00027F09                 text "UTF-16LE", 'Hwp.exeZ',0
00027F1B a19216810022Sag_0:
00027F1B                 text "UTF-16LE", '\\192.168.100.22\saggazi\Happy\Work\2016.8~\2016.8.'
00027F1B                 text "UTF-16LE", '10~\[illegible]2016.8.24\2017.1.1메일\Hwp.exe',0
00027FD1                 db    0
```

[Figure 3] Path of the Attachment Used in the Hangul Document

C:\Users\pad-2\AppData\Local\Temp\Hwp (3).exe

\\192.168.100.22\saggazi\Happy\Work\2016.8~\2016.8.10~\(University in Korea)\(Korean name)2016.8.24\2017.1.1mail\Hwp.exe

[Table 3] Path of an Inserted Document

As shown in Figure 3, the original file was attached from a path where the username of the system was “pad-2” and the mapped network folder was called "saggazi." The path also included the name of a university in South Korea and a name in Korean characters. Based on the presence of Korean characters and “saggazi,” a transliteration of a Korean word, it can be assumed that the malware creator is Korean or someone who is familiar with the language.

Detailed Analysis of Malware

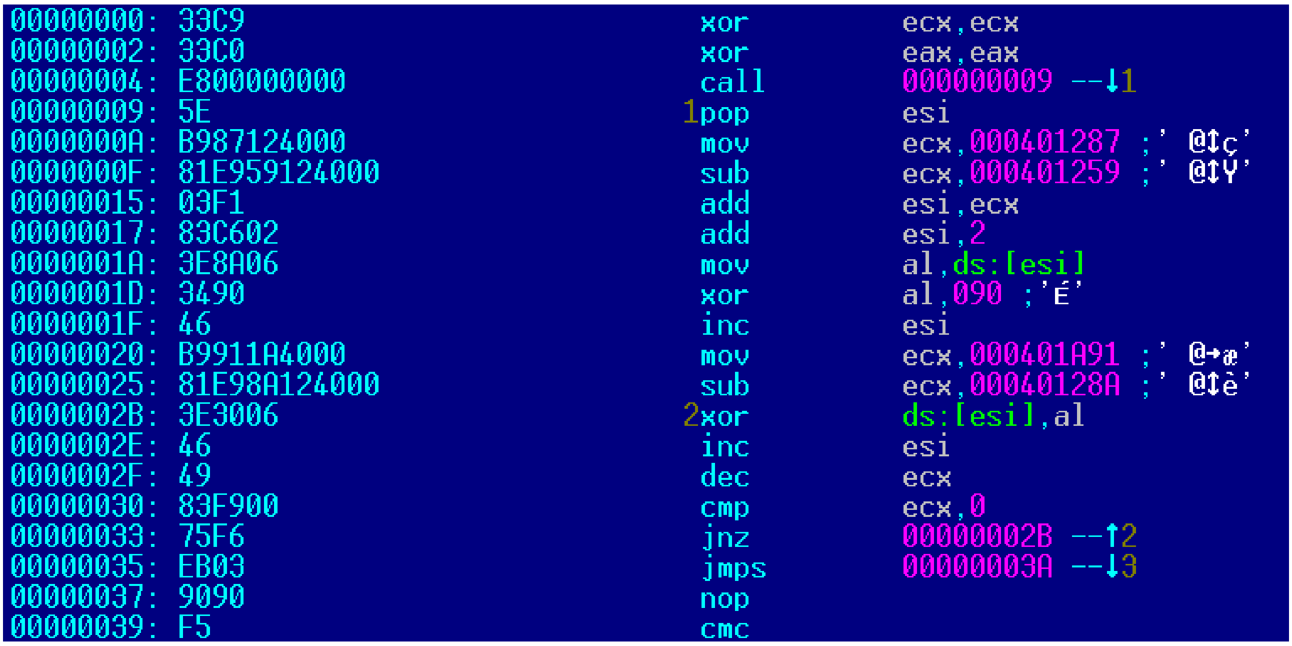
The malware distributed by Red Eyes group can be divided into four main types as shown in Table 4.

Category	Description
Reloader (DocPrint)	Loader that executes another malware in-memory
Reloaderx	Collects system information and downloads additional files
Redoor (DogCall)	Uses backdoor function
Wiper	Destroys data on the hard disk

[Table 4] Main Malware of Red Eyes Group

1. Reloader (DocPrint)

The Reloader (DocPrint) executes another malware in-memory using a wscript.exe file. The actual malware is encrypted and a similar decryption code is found in its variants.



```
00000000: 33C9                        xor      ecx,ecx
00000002: 33C0                        xor      eax,eax
00000004: E800000000                  call     000000009 --↓1
00000009: 5E                         1pop      esi
0000000A: B987124000                  mov      ecx,000401287 ;' @↕ç'
0000000F: 81E959124000                sub      ecx,000401259 ;' @↕Ÿ'
00000015: 03F1                        add      esi,ecx
00000017: 83C602                      add      esi,2
0000001A: 3E8A06                      mov      al,ds:[esi]
0000001D: 3490                        xor      al,090 ;'É'
0000001F: 46                          inc      esi
00000020: B9911A4000                  mov      ecx,000401A91 ;' @→æ'
00000025: 81E98A124000                sub      ecx,00040128A ;' @↕è'
0000002B: 3E3006                     2xor      ds:[esi],al
0000002E: 46                          inc      esi
0000002F: 49                          dec      ecx
00000030: 83F900                      cmp      ecx,0
00000033: 75F6                        jnz      00000002B --↑2
00000035: EB03                        jmps     00000003A --↓3
00000037: 9090                        nop
00000039: F5                          cmc
```

[Figure 4] Main Decryption Code

2. Reloaderx

Reloaderx (md5: 6Cec7de9d4797895775e2add9d6855ba) is executed in-memory by DocPrint (md5: 0ff0f3f0722dd122a0f5c3d4c7752675, fc0a9850f7b6a91f7757d64c86cfc141), which was inserted in the Hangul file disguised as the 2017 New Year address of North Korea.

Reloaderx collects the following system information and downloads additional malware:

Computer name

User name

Execution path

BIOS model

Variants of Reloaderx were also discovered in November 2016, and they shared the same C&C server addresses as follows:

MD5	C&C Server Address
9cd11aa7872f9cba98264113d3d72893	www.w****ush.co.kr/bbs/data/image/work/webproxy.php
9f1e60e0c794aa3f3bdf8a6645ccabdc	www.belasting-telefoon.nl/images/banners/temp/index.php

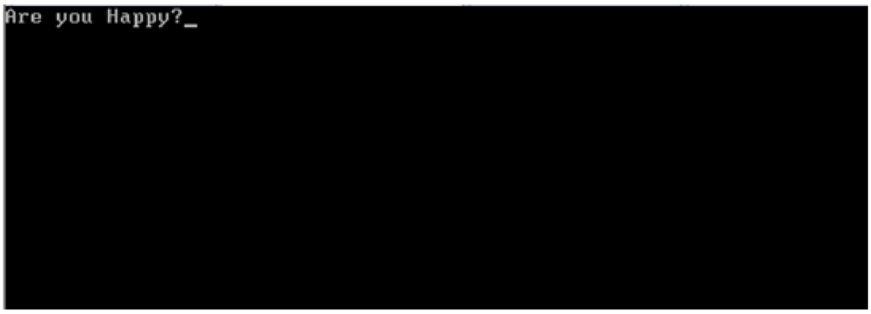
[Table 5] Reloaderx Malware and Its C&C Server Address

3. Redoor (DogCall)

Redoor, also known as DogCall or ROKRAT, was first discovered in February 2017. Redoor is the malware executed by Reloader that acts as a loader. Until January 2017, Reloader executed Reloaderx, but in February of that year it began executing Redoor. It is a commonly used backdoor, and was used as recently as March 2018.

4. Wiper

One kind of malware used by Red Eyes group destroys all data on the hard disk when executed. After destroying the data and rebooting the system, it would display the message “Are you Happy?” as shown in Figure 5.

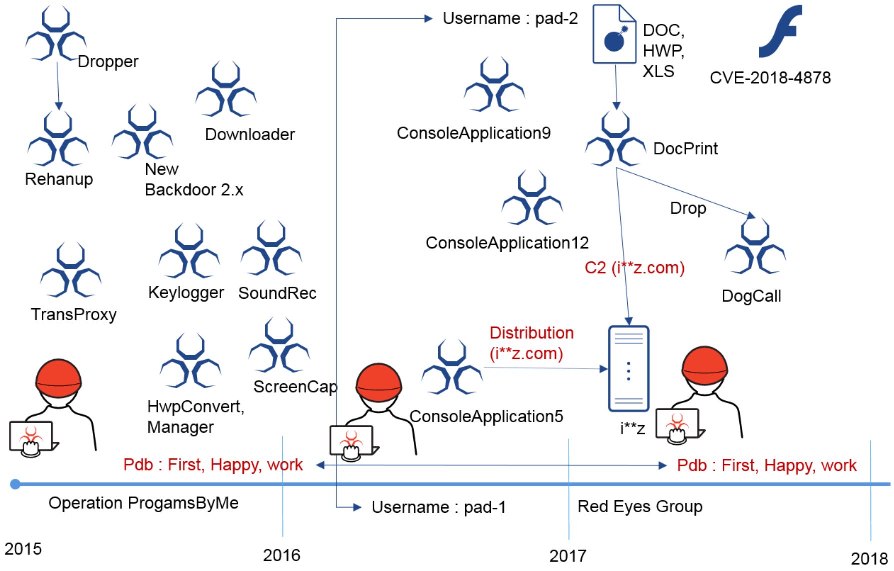


```
Are you Happy?_
```

[Figure 5] Message Displayed after Hard Disk Destruction

Possible Association with Other Attack Groups

In the aforementioned cases involving the Hangul document, we saw that the malware creator's system username was "pad-2" and that the file path included text strings such as "First," "Happy," and "Work." This suggests an association between the Hangul attacks and other attacks that have occurred since 2015.



[Figure 6] Overview of Similarities between Attacks, 2015–2018

Operation ProgamsByMe (2015)

Operation ProgamsByMe started in July 2015 and continued until April 2016. The characteristic of this malware is that it contained the text string "ProgamsByMe," which could reflect either a typographical error or an intentional misspelling of "Programs."

The attack group that carried out this attack sent email to the targets, either exploiting the vulnerabilities of Hangul or disguising the malware as an update for another popular program. In one case, malware was distributed via a specific Active-X installation file.

This group of hackers attempted to attack an ICT company in May 2015 by disguising malware as a security update (malware removal and patch update) for the Hancom Office suite, which includes Hangul (md5 : 89c3254aa577d3788f0f402fe6e5a855).

In January 2016, this group distributed malware (md5: 06ae5d62d56f21cd2676989743b9626c) purporting to discuss countermeasures to North Korea's nuclear weapons program, “Truth and countermeasures on North Korea's hydrogen bomb game.hwp”. In February 2016, it used malware (md5: d00e3196bc847e63fc4b255e8ab06d1c) disguised as a piracy investigation program of the Korean National Police Agency (md5: f793deeee9dc4235d228e68d27057dcc). In March 2016, the group attacked a media organization and additionally installed keyloggers.

Date	Attack Target	Key Points
2015.07	IT company	Attack method not confirmed
2016.01	Unknown	Disguised as a Hancom update file
2016.01	Unknown	Infection using the file, Truth and countermeasure on North Korea's hydrogen bomb game.hwp
2016.02	Unknown	Disguised as the software piracy investigation program of the Korean Police Agency
2016.04	Unknown	Disguised as the Chrome installer and a screen-capture tool
2016.03	Media organization	Unidentified infection method (but an added keylogger was discovered)

[Table 6] Main Attacks involving Operation ProgamsByMe

The malware used in the attacks listed in Table 6 all contain the PDB string “ProgamsByMe.” It also includes text strings such as “First,” “Happy,” and “Work,” and include the use of a tilde (~) for the date of creation.

The types of malware used by the group behind Operation ProgamsByMe are shown in Table 7.

PDB Contents	Function
Backdoor	Backdoor
CppUACSelfElevatrion	Dropper (drops additional malware and includes text strings, as shown in Figure 7)
FirstUrlMon	Downloader
HwpConvert	Malicious HWP production tool
Installer, InstallBD	Dropper
Manager, Manager_Them	Malware control
KeyLogger, OffSM	Keylogger
PrivilegeEscalation	Elevates privileges
ScreenCap	Screen capture
SoundRec	Recording

[Table 7] Main Malware from the Group behind Operation ProgamsByMe

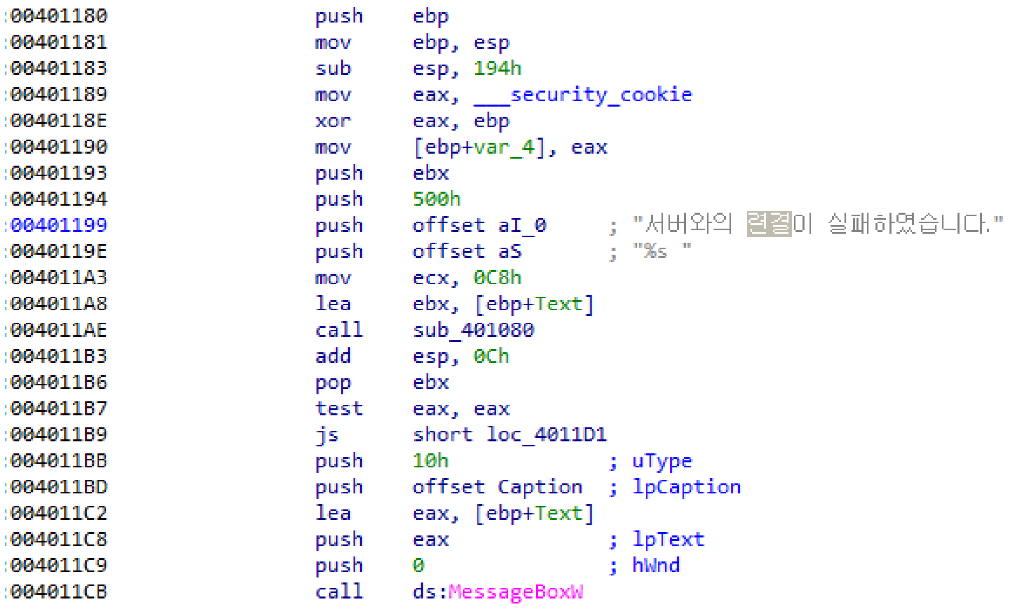
The group also used tools such as keylogging, recording, and screen capture tools in the attack to monitor attack targets.

In addition, the code had some interesting features.

■ Awkward Korean messages

The dropper that was created and widely distributed in August 2015 included CppUACSelfElevation.pdb in its PDB.

This dropper (md5: 9ac2ffd3f1cea2e01ed77c2e7b4a29e7) displays an error message which is closer to North Korean language usage, which sounds awkward to South Koreans.

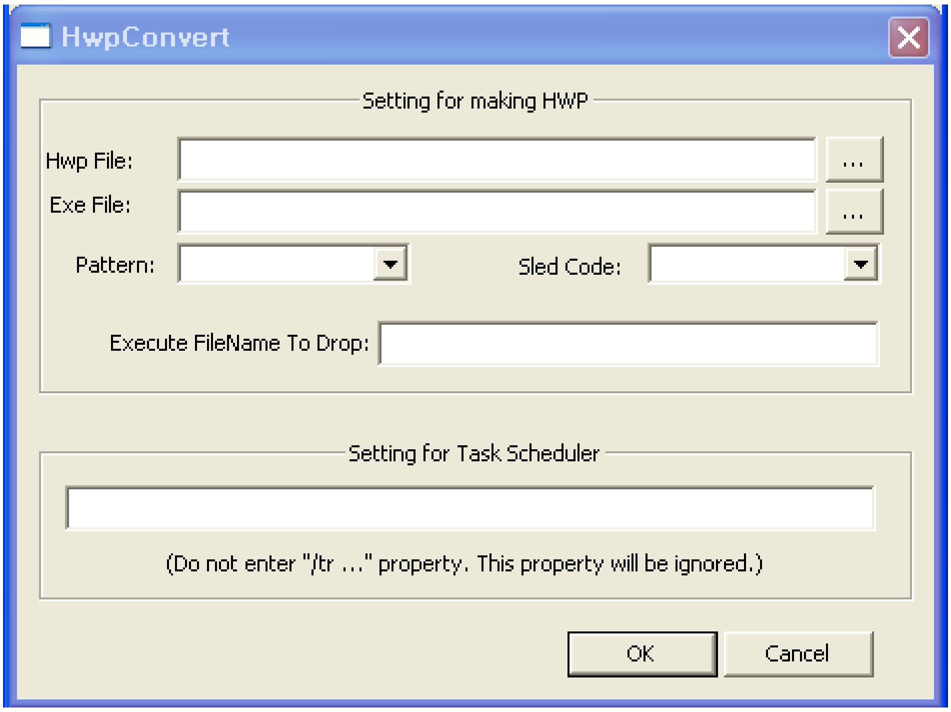


```
00401180                push    ebp
00401181                mov     ebp, esp
00401183                sub     esp, 194h
00401189                mov     eax, ___security_cookie
0040118E                xor     eax, ebp
00401190                mov     [ebp+var_4], eax
00401193                push    ebx
00401194                push    500h
00401199                push    offset aI_0     ; "서버와의 련결이 실패하였습니다."
0040119E                push    offset aS       ; "%s "
004011A3                mov     ecx, 0C8h
004011A8                lea     ebx, [ebp+Text]
004011AE                call    sub_401080
004011B3                add     esp, 0Ch
004011B6                pop     ebx
004011B7                test    eax, eax
004011B9                js      short loc_4011D1
004011BB                push    10h             ; uType
004011BD                push    offset Caption  ; lpCaption
004011C2                lea     eax, [ebp+Text]
004011C8                push    eax             ; lpText
004011C9                push    0               ; hWnd
004011CB                call    ds:MessageBoxW
```

[Figure 7] Awkward-Sounding Korean Message (in Gray)

■ Tools believed to have been used by the attacker

There are also programs that seem to be tools internally used by the attacker. The attacker used these tools to add malware to the Hangul file (md5: 2f0492f53d348bea993b7ae5983508a6).



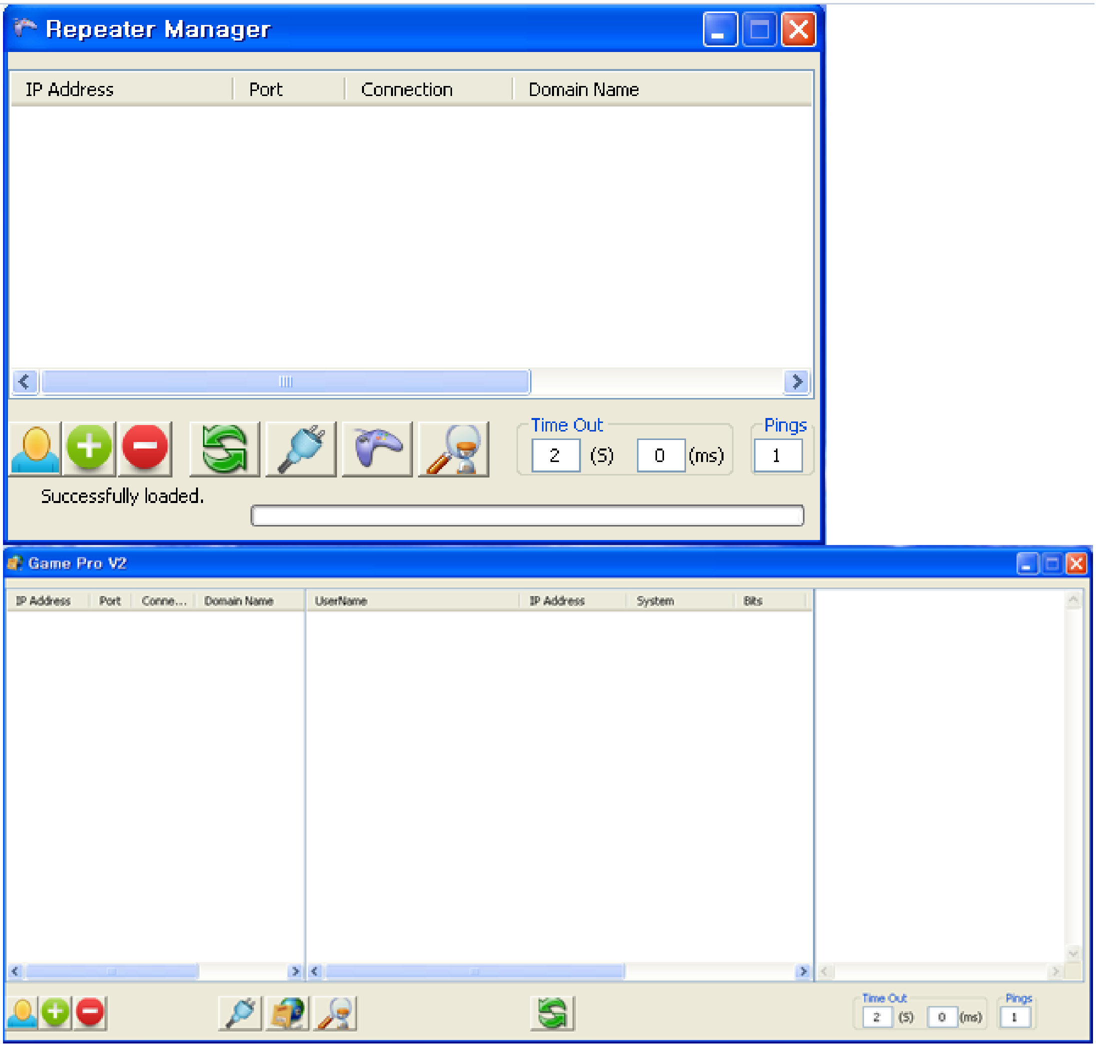
(Do not enter "/tr ..." property. This property will be ignored.)

[Figure 8] Malicious HWP File Generator

This tool included the following PDB.

D:\TASK\ProgamsByMe(2015.1~)\ShellCode\Debug\HwpConvert.pdb

The attacker also seems to have used a management program (md5: 5ef03b48b4ae68c572028c7257 2444d2).



Successfully loaded.

Time Out 2 (S) 0 (ms)

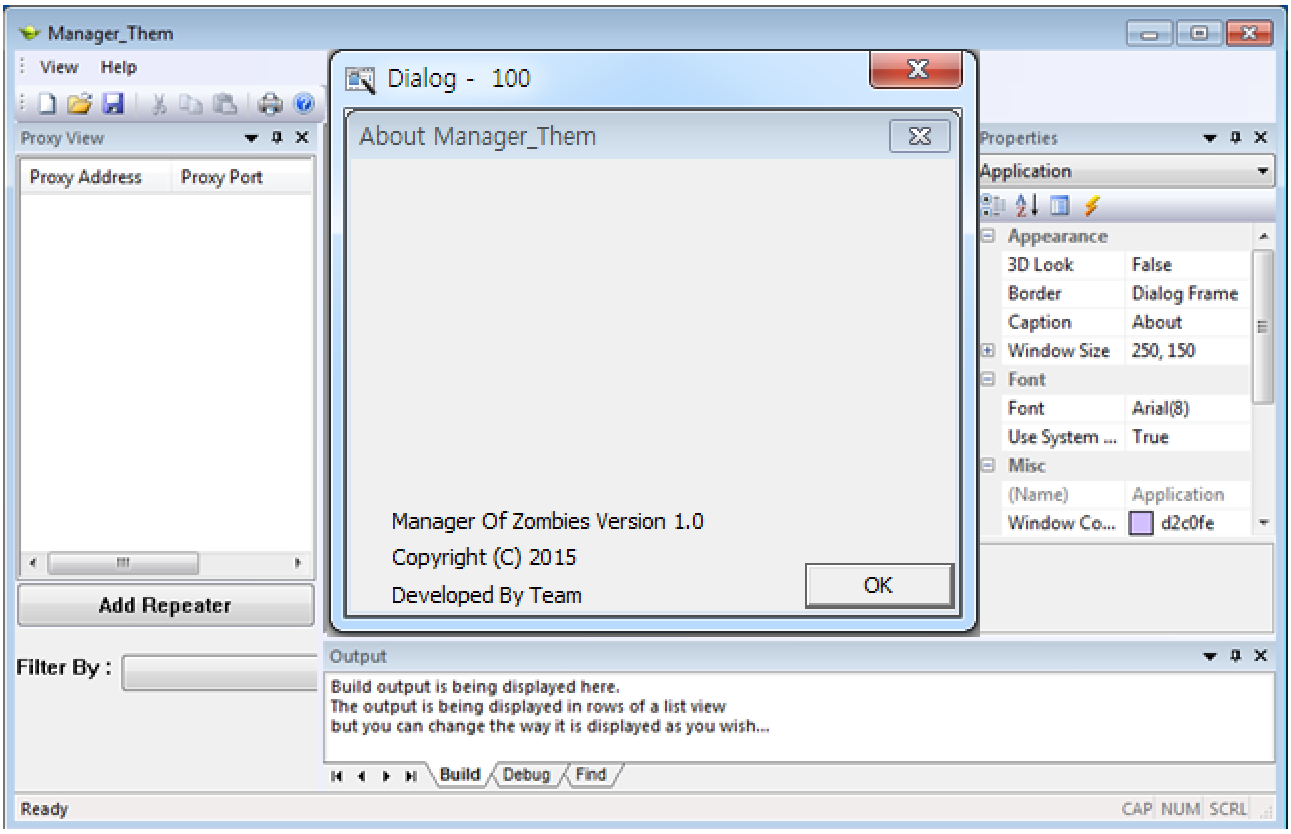
Pings 1

[Figure 9] The Management Program Used by the Attacker

The program contains the following PDB:

E:\task\ProgamsByMe(2015.1~)\EXE_AND_SERVICE\EXE_AND_SERVICE\Release\Manager.pdb

Another management program used by the attacker (md5: 49d30adaab769fbea2ef69e09c6598c5) is called Manager of Zombies Version 1.0. In the program information, the malware creators refer to themselves as the "Team," as shown in Figure 10.



Manager Of Zombies Version 1.0
Copyright (C) 2015
Developed By Team

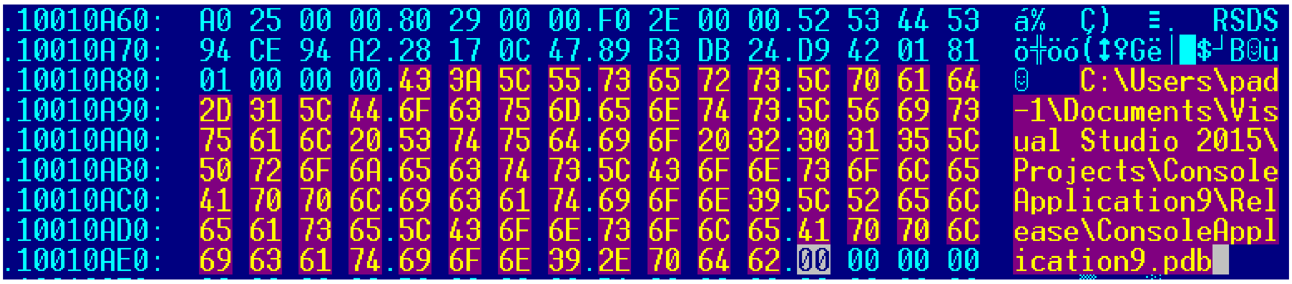
Build output is being displayed here.
The output is being displayed in rows of a list view
but you can change the way it is displayed as you wish...

Appearance
3D Look False
Border Dialog Frame
Caption About
Window Size 250, 150
Font
Font Arial(8)
Use System ... True
Misc
(Name) Application
Window Co... d2c0fe

[Figure 10] The Management Program Used by the Attacker

Malware Created by the User "Pad-1" (2016)

As mentioned before, the document distributed in 2017 disguised as the New Year address of North Korea (md5: 44bdeb6c0af7c36a08c64e31ceadc63c) came from a person whose system username was "pad-2." However, malware designed from the system where the username was "pad-1" was discovered from December 2016 to January 2017. This malware included the following PDB: C:\Users\pad-1\Documents\Visual Studio 2015\Projects\ConsoleApplication9\Release\ConsoleApplication9.pdb.



```
.10010A60:  A0 25 00 00.80 29 00 00.F0 2E 00 00.52 53 44 53  á%  Ç)  ≡.  RSDS
.10010A70:  94 CE 94 A2.28 17 0C 47.89 B3 DB 24.D9 42 01 81  ö╫öó(↕♀Gë│█$┘B☺ü
.10010A80:  01 00 00 00.43 3A 5C 55.73 65 72 73.5C 70 61 64  ☺   C:\Users\pad
.10010A90:  2D 31 5C 44.6F 63 75 6D.65 6E 74 73.5C 56 69 73  -1\Documents\Vis
.10010AA0:  75 61 6C 20.53 74 75 64.69 6F 20 32.30 31 35 5C  ual Studio 2015\
.10010AB0:  50 72 6F 6A.65 63 74 73.5C 43 6F 6E.73 6F 6C 65  Projects\Console
.10010AC0:  41 70 70 6C.69 63 61 74.69 6F 6E 39.5C 52 65 6C  Application9\Rel
.10010AD0:  65 61 73 65.5C 43 6F 6E.73 6F 6C 65.41 70 70 6C  ease\ConsoleAppl
.10010AE0:  69 63 61 74.69 6F 6E 39.2E 70 64 62.00 00 00 00  ication9.pdb
```

[Figure 11] Malware Created in a System with Username pad-1

Malwares created on a system with username “pad-1” can be classified into four types as shown in Table 8.

PDB Contents	Function
ConsoleApplication5	External file loader
ConsoleApplication9	Loader with malware
ConsoleApplication12	Listen on a specific port
None	System information collection and screen capture (no information on PDB, but created from the same shellcode)

[Table 8] Malware Created by User "pad-1"

A variant (md5: f0a5385d0d9f7c546b25a7448ca5b1c9) of ConsoleApplication5.pdb was downloaded in December 2016 from the address http://www.i***.com/admin/data/bbs/review2/im/jquery_min_1.5.1.js. This web address (i ***.com) is identical to the address used in Red Eyes attacks that took place in January and March 2017.

The attacker distributed malware to manufacturing companies using the filenames jquery_min_1.5.1.js and jquery_min_2.2.2.js.

Sample MD5	Distribution address
f0a5385d0d9f7c546b25a7448ca5b1c9	http://www.i**z.com/admin/data/bbs/review2/im/jquery_min_1.5.1.js
8b55d52b12cf319d9785ad8eeeade5ea	http://dr-*****s.com/admin/data/banner/jquery_min_1.5.1.js
2fdbb9a500143a2dd3d226a1cc3e45b5	http://dr-*****s.com/admin/data/banner/jquery_min_2.2.2.js

[Table 9] Information on ConsoleApplication5.pdb Variants

Malware that includes the ConsoleApplication9.pdb downloads a file from the address below.

Sample MD5	Distribution address
2fdbb9a500143a2dd3d226a1cc3e45b5	http://dr-v****s.com/admin/data/banner/jquery_min_2.2.2.js

[Table 10] Information on ConsoleApplication9.pdb Malware

No PDB information exists, but malware (md5: f613c9276d0deb19d0959aa2fbfc737c) from the same decryption code as the one that contained the pad-1 string included a screen capture function and a way of collecting system information. By the fall of 2017, nine variants of this malware had been found.

AhnLab's Response

AhnLab's anti-malware software, V3, detects and remediates malware of the Red Eyes group under the following aliases:

- Trojan/Win32.Agent (2017.02.07.00)

- Trojan/Win32.Backdoor (2015.08.01.00)

- Trojan/Win32.Reloaderx (2016.11.06.00)

Conclusion

The Red Eyes group appeared in the fall of 2016 and is now drawing significant attention. The group uses a variety of methods but can be identified by a code that includes text strings such as "First," "Happy," and "Work." Red Eyes may very well be behind Operation ProgamsByMe, which took place in 2015; it is likely that they are at least associated with it either directly or indirectly. Red Eyes appeared right after the disappearance of a group that was active in 2015 through to the spring of 2016.

This suggests that the activities of Red Eyes in South Korea date back to 2015, and possibly even earlier. Because the hackers seem to have used the same source code but different compilation paths for the malware, we can conclude that there is more than one attacker involved.

Currently, the Red Eyes group is targeting other countries in addition to South Korea. There is a clear need to continue monitoring its movements.

Appendix

The PDB information for the malware used in Operation ProgamsByMe from 2015 to 2016 is as follows:

C:\Users\Naughty Develop\Desktop\New Backdoor2.5-with-cmd-resource\New Backdoor2.3\Release\Backdoor.pdb
D:\FirstBackDoor(2015_1_10)\FirstBackDoor(2015_1_10)\Release\FirstUrlMon.pdb
D:\TASK\ProgamsByMe(2015.1~)\2010Main\EXE_AND_SERVICE\Release\Manager.pdb
D:\TASK\ProgamsByMe(2015.1~)\FirstBackDoor(2015_7_24)\Release\office.pdb
D:\TASK\ProgamsByMe(2015.1~)\FirstBackdoor(2015_7_24)\Release\PrivilegeEscalation.pdb
D:\TASK\ProgamsByMe(2015.1~)\Happy\2010PHV2\EXE_AND_SERVICE\Release\KeyLogger.pdb
D:\TASK\ProgamsByMe(2015.1~)\Happy\2010PHV2\EXE_AND_SERVICE\Release\ScreenCap.pdb
D:\TASK\ProgamsByMe(2015.1~)\HncUpdateUAC\C++\Release\CppUACSelfElevation.pdb
D:\TASK\ProgamsByMe(2015.1~)\HncUpdateUAC\C++\Release\Installer.pdb
D:\TASK\ProgamsByMe(2015.1~)\HncUpdateUAC\C++\Release\Manager_Them.pdb
D:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative
Backdoor\KeyLogger_ScreenCap_Manager\Release\SoundRec.pdb
D:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative Backdoor\KeyLogger_ScreenCap_Manager\Release\Manger.pdb
D:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative
Backdoor\KeyLogger_ScreenCap_Manager\Release\ScreenCap.pdb
D:\TASK\ProgamsByMe(2015.1~)\ShellCode\Debug\HwpConvert.pdb
D:\TASK\ProgamsByMe(2015.1~)\ShellCode\Release\UACTest.pdb
E:\Task\ProgamsByMe(2015.1~)\EXE_AND_SERVICE\EXE_AND_SERVICE\Debug\Manager.pdb
E:\task\ProgamsByMe(2015.1~)\EXE_AND_SERVICE\EXE_AND_SERVICE\Release\TransProxy.pdb
N:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative Backdoor\Installer\Release\Installer.pdb
N:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative Backdoor\New Backdoor2.4\Release\InstallBD.pdb
P:\PH2015_2.2\New Backdoor2.2\New Backdoor2.2\Release\CppUACSelfElevation.pdb
P:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative Backdoor\New Backdoor2.3\Release\InstallBD.pdb
T:\TASK\ProgamsByMe(2015.1~)\MyWork\Relative Backdoor\New Backdoor2.3-with-cmd-resource\New
Backdoor2.3\Release\Backdoor.pdb
z:\work\4th\plugin\OffSM\Release\OffSM.pdb
Z:\work\4th\plugin\SM\Release\SM.pdb
Z:\work\n1st\Agent\Release\HncUp.pdb
Z:\work\n1st\Agent\Release\PotPlayerUpdate.pdb