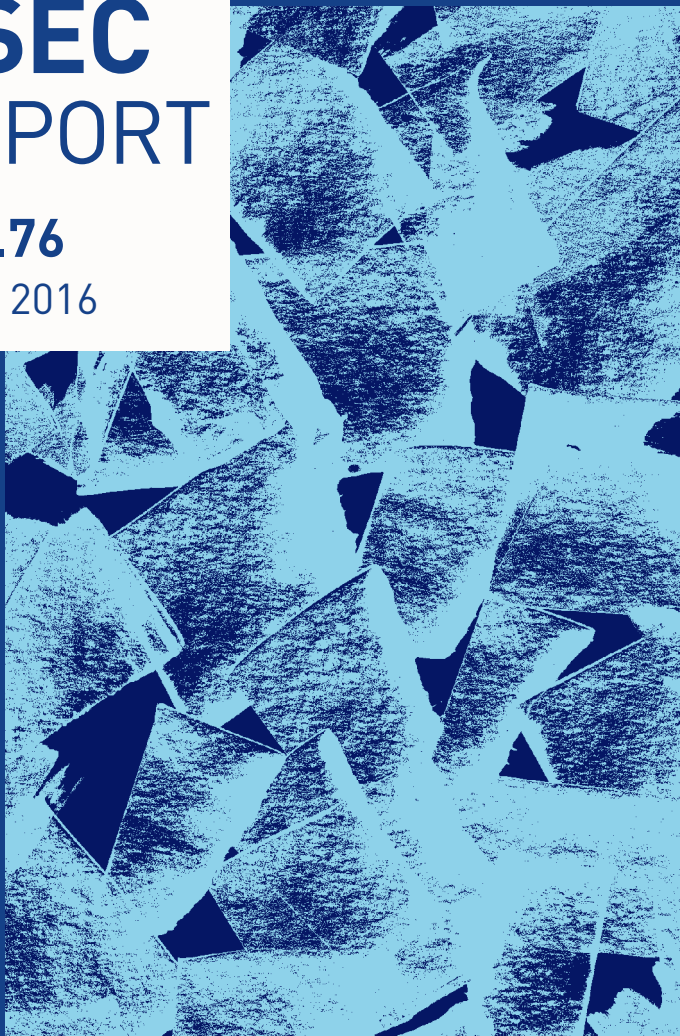


ASEC REPORT

VOL.76

April, 2016



AhnLab

ASEC REPORT

VOL.76 April, 2016

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

2016년 4월 보안 동향

Table of Contents

1 보안 통계 STATISTICS	01 악성코드 통계	4
	02 웹 통계	6
	03 모바일 통계	7
2 보안 이슈 SECURITY ISSUE	01 리눅스를 노리는 빌게이츠 봇넷(BillGates botnet) 주의	10
	02 영화 '쏘우(Saw)'를 모방한 직쏘(Jigsaw) 랜섬웨어 등장	12
3 악성코드 상세 분석 ANALYSIS IN-DEPTH	이동식 저장장치로 유포되는 VBE 스크립트 악성코드	16

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

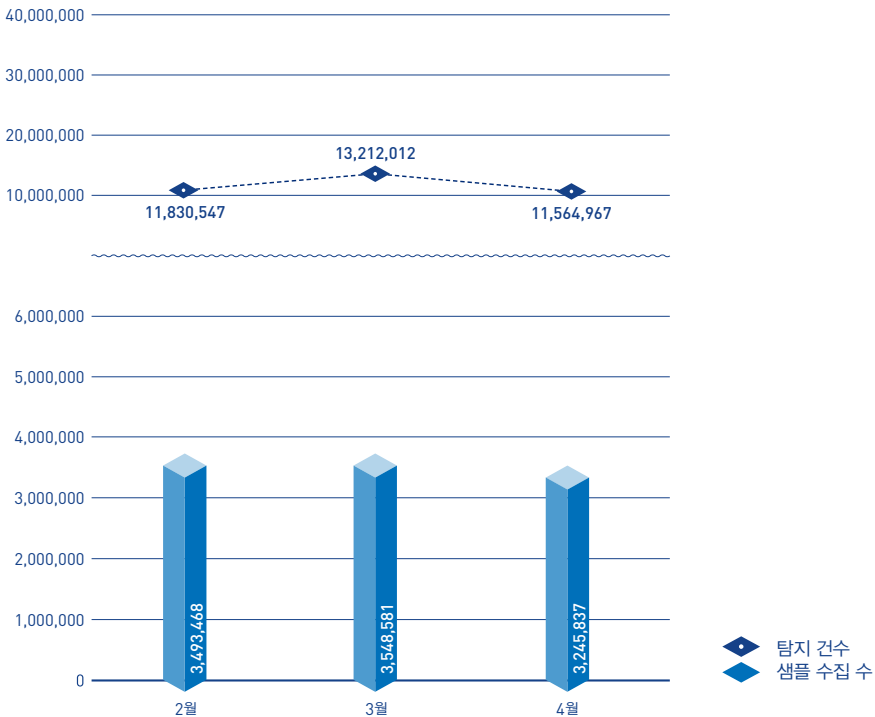
03 모바일 통계

보안 통계

01

악성코드 통계

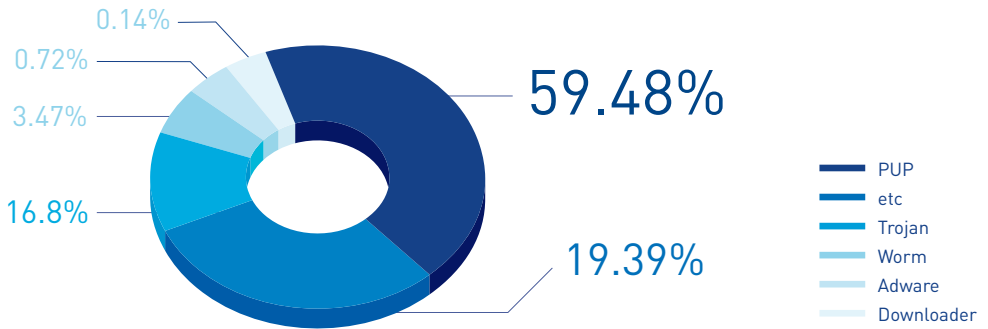
ASEC이 집계한 바에 따르면, 2016년 4월 한 달간 탐지된 악성코드 수는 1,156만 4,967건으로 나타났다. 이는 전월 1,321만 2,012건에 비해 1,64만 7,045건 감소한 수치다. 한편 4월에 수집된 악성코드 샘플 수는 324만 5,837건이다.



[그림 1-1] 악성코드 추이(2016년 2월 ~ 2016년 4월)

* '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.

[그림 1-2]는 2016년 4월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 59.48%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 16.8%, 웜(Worm)이 3.47%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 4월 주요 악성코드 유형

[표 1-1]은 4월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter 가 총 26만 913건으로 가장 많이 탐지되었고, Malware/Win32.Generic이 12만 9,941건으로 그 뒤를 이었다.

[표 1-1] 2016년 4월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	260,913
2	Malware/Win32.Generic	129,941
3	Trojan/Win32.Agent	126,658
4	ASD.Prevention	105,841
5	Unwanted/Win32.HackTool	97,057
6	Trojan/Win32.Neshta	88,807
7	Trojan/Win32.Banki	82,504
8	Unwanted/Win32.Keygen	66,734
9	HackTool/Win32.Crack	66,495
10	HackTool/Win32.AutoKMS	59,478

보안 통계

02
웹 통계

2016년 4월에 악성코드 유포지로 악용된 도메인은 648개, URL은 2,216개로 집계됐다(그림 1-3). 또한 4월의 악성 도메인 및 URL 차단 건수는 총 637만 3,536건이다.



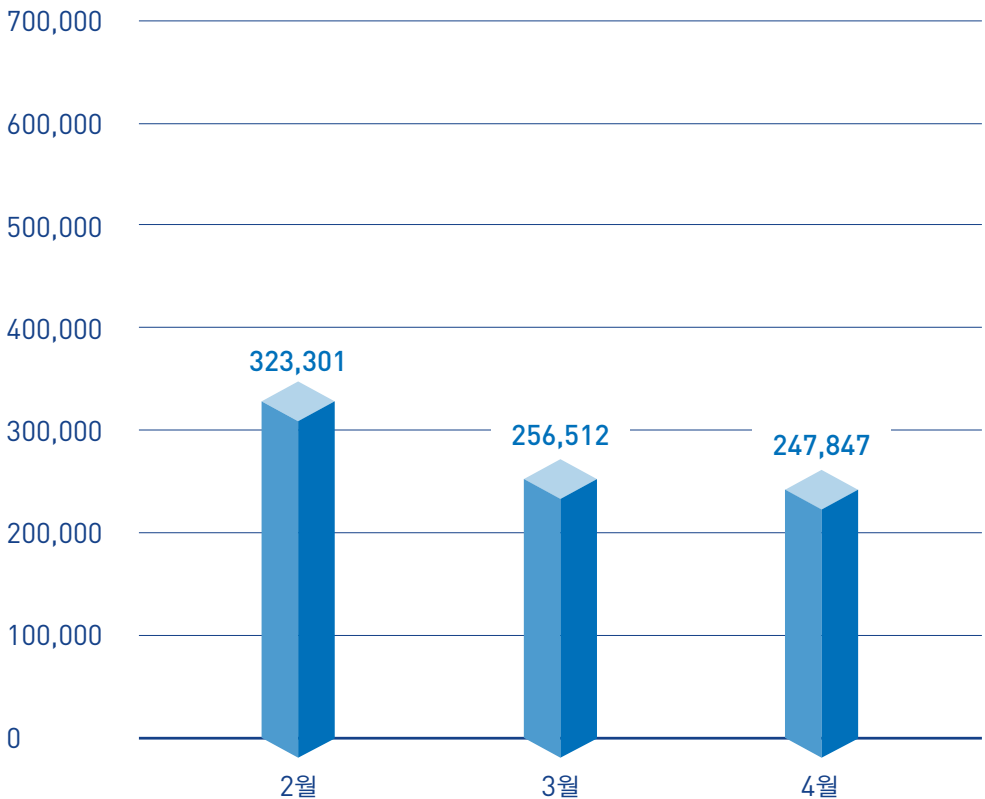
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2016년 2월 ~ 2016년 4월)

* 악성 도메인 및 URL 차단 건수란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03

모바일 통계

2016년 4월 한 달간 탐지된 모바일 악성코드는 24만 7,847건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이(2016년 2월 ~ 2016년 4월)

[표 1-2]는 4월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 4월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	63,488
2	Android-PUP/SmsReg	26,873
3	Android-PUP/Noico	20,396
4	Android-Trojan/SmsSpy	9,567
5	Android-PUP/Dowgin	9,315
6	Android-PUP/Zdpay	8,723
7	Android-Trojan/SmsSend	8,110
8	Android-Trojan/Moavt	6,637
9	Android-Trojan/FakeInst	5,783
10	Android-Trojan/Agent	5,035

2

보안 이슈

SECURITY ISSUE

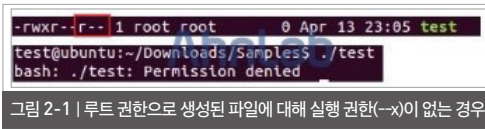
- 01 리눅스를 노리는 빌게이츠 봇넷(BillGates botnet) 주의
- 02 영화 ‘쏘우(Saw)’를 모방한 직쏘(Jigsaw) 랜섬웨어 등장

01

리눅스를 노리는 빌게이츠 봇넷 (BillGates botnet) 주의

최근 리눅스(Linux) 운영체제에서 감염 시스템의 정보 수집, 시스템 파일 교체, DDoS 공격 등을 수행하는 빌게이츠 봇넷(BillGates botnet)이 발견됐다. 해당 악성코드는 감염 시스템 내에서 속성이 변경되어 삭제 불가능해 리눅스 사용자들의 피해가 우려된다.

파일별 계정 권한 관리가 명확한 리눅스 운영체제는 파일의 읽기/쓰기/실행 권한이 [소유자/그룹/그 외 일반 사용자]로 각각 구분되어 있다. 따라서 [그림 2-1]과 같이 권한이 할당되지 않은 경우, 관리자 권한인 루트(root) 계정 사용자가 파일의 권한을 변경해주지 않으면 실행이 허용되지 않는다.



이번에 발견된 빌게이츠 봇넷은 파일 권한 정책이 아닌 파일의 속성과 관련된 사례로, 서버가 감염되었을 때 공격자가 파일의 속성을 변경하여 악성코드를 삭제할 수 없도록 설정한 경우다. 이와 관련하여 리눅스의 감염 시스템에서 파일 속성이 변경된 경우라도 해

당 악성 파일을 삭제할 수 있도록 하는 조치 방법을 자세히 살펴보자.

먼저 공격자가 파일의 속성을 변경한 후, [그림 2-2]와 같이 삭제 시도를 하면 '실행이 허가되지 않았다 (Operation not permitted)'라는 메시지가 출력되며 해당 파일이 삭제되지 않는다.

```
test@ubuntu:~/Downloads/Samples$ rm -rf samples
rm: cannot remove 'samples': Operation not permitted
```

그림 2-2 | rm 명령어를 통한 삭제 시도

이때 파일이 삭제되지 않는 원인을 파일 권한 문제로 판단하고, 파일 시스템에 기록된 정보를 이용하여 루트 계정 및 inode를 제거하는 방법으로 다시 삭제 시도하면, 마찬가지로 동일한 메시지가 발생하며 파일이 삭제되지 않는다.

```
test@ubuntu:~/Downloads/Samples$ ls -li
443022 samples
test@ubuntu:~/Downloads/Samples$ rm -rf . 443022 -exec rm -rf {} \;
rm: cannot remove './samples': Operation not permitted
```

그림 2-3 | inode 제거를 통한 삭제 시도

[그림 2-2], [그림 2-3]의 경우처럼 파일의 삭제가 불가능한 경우, 'lsattr' 명령을 통해 해당 파일의 속성

을 조회하면 [그림 2-4]와 같이 ‘i’ 속성이 추가되어 있음을 확인할 수 있다.

```
test@ubuntu:~/Downloads/Samples$ ls -l
443022 samples
test@ubuntu:~/Downloads/Samples$ find . -min 443022 -exec rm -rf {} \;
rm: cannot remove './samples': Operation not permitted
```

그림 2-4 | 파일 속성 조회

이처럼 ‘i’ 속성이 추가되어 있는 경우에는 [그림 2-5]와 같이 루트 권한으로 ‘chattr’ 명령을 통해 해당 파일의 속성을 변경한 후, 다시 삭제를 시도하면 해당 파일이 정상적으로 삭제된다.

```
test@ubuntu:~/Downloads/Samples$ sudo chattr -R -i samples
[sudo] password for test:
test@ubuntu:~/Downloads/Samples$ lsattr samples
--S-----e-- samples
test@ubuntu:~/Downloads/Samples$ rm -rf samples
```

그림 2-5 | 파일 속성 변경 후 제거 시도

‘chattr’ 명령은 파일의 속성 추가 시에는 +[추가할 속성], 제거 시에는 -[제거할 속성]을 통하여 수행할 수 있으며, -R 옵션을 추가로 부여하는 경우에는 하위 디렉토리까지 모두 포함되어 적용된다. 이는 윈도우(Windows) 운영체제의 ‘attrib’ 명령과 유사하다.

표 2-1 | 리눅스 파일 속성 및 ‘chattr’ 명령어 예시

[명령어 예시 (i, S 속성 추가)]	
chattr +iS samples	
[파일 속성명 중 일부]	[설명]
a [CAP LINUX IMMUTABLE capability]	추가 작성만 가능, 삭제 불가
I [CAP LINUX IMMUTABLE capability]	삭제, 변경, 링크파일 생성 등
S	파일이 변경되면 디스크 동기화
u	파일 삭제 시 내용 백업

이번 리눅스 악성코드 사례와 같이 파일의 속성이 변경되어 삭제가 불가능한 경우가 있어 파일의 권한뿐만 아니라 속성에 대해서도 다시 한번 확인하는 것이 필요하다. 단, 중요 파일이나 로그 파일 등은 ‘i’나 ‘a’ 속성을 적용하는 정상적인 경우도 있다. 즉, 이러한 속성이 적용되어 있는 파일이라고 해서 모두 악성 파일은 아니므로, 정확히 악성으로 확인된 파일에 대해서만 삭제를 진행할 것을 권장한다.

최근 리눅스 운영체제를 노리는 악성코드가 꾸준히 증가하고 있다. DDoS 공격이나 백도어 등 리눅스 악성코드의 기능도 다양해지고 있으며, 앞으로 더욱 고도화될 것으로 예상된다. 리눅스 시스템을 안전하게 이용하기 위해서는 반드시 암호를 설정해야 하며, 최신 보안 업데이트를 적용해야 한다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Linux/Backdoor.1223123.B

02

영화 ‘쏘우(Saw)’를 모방한 직쏘(Jigsaw) 랜섬웨어 등장

현재 가장 이슈가 되고 있는 보안 위협은 단연 랜섬웨어다. 근 2년간 수십여 종의 랜섬웨어가 발견되었으며, 지금도 새로운 변종과 다양한 공격 기법을 이용해 사용자들을 위협하고 있다. 최근에는 사회공학적 기법을 적용하여 사용자의 심리를 교묘하게 이용하는 신종 랜섬웨어가 등장했다. 영화 ‘쏘우(Saw)’를 모방한 직쏘(Jigsaw) 랜섬웨어를 자세히 살펴보자.

“게임을 시작하지(I want to play a game)”라는 메시지를 시작으로 살인을 시작한다. 이번에 발견된 직쏘 랜섬웨어 또한 [그림 2-7]과 같이 영화 속 직쏘의 대사를 모방한 메시지와 이미지를 통해 사용자에게 감염 사실을 알린다.



그림 2-6 | 영화 ‘쏘우(Saw)’를 모방한 직쏘(Jigsaw) 이미지

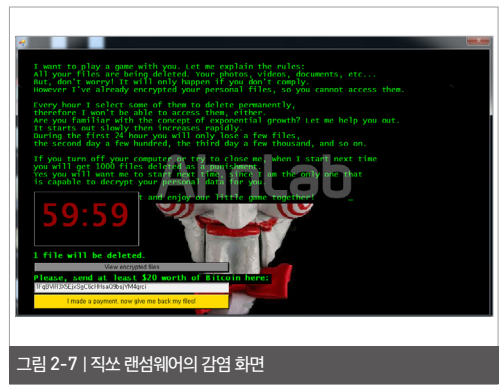
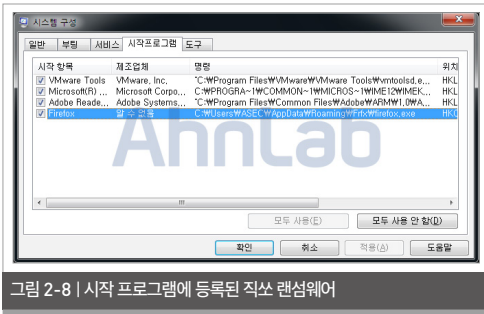


그림 2-7 | 직쏘 랜섬웨어의 감염 화면

[그림 2-7]의 감염 화면에는 “사용자의 문서, 사진, 비디오 등의 파일을 암호화했으며 비트코인을 지불하라”는 메시지가 나타난다. 이와 함께 매 시간마다 암호화된 파일을 삭제할 것이라고 경고해 사용자를 심리적으로 조급하게 만들어 지불을 유도한다는 점이 특징이다.

영화 속 직쏘 캐릭터는 꼭두각시 인형을 통해 전달한



또한 해당 랜섬웨어는 [그림 2-8]과 같이 시작 프로그램에 등록되어 부팅 시 자동으로 실행된다. 따라서 [그림 2-7]의 감염 화면과 함께 60분의 카운트다운을 지속적으로 노출시킴으로써 사용자의 심리적 부담을 증가시킨다.

직소 랜섬웨어에 감염되면 시스템 내에 특정 확장자를 갖는 파일들이 암호화되며, 암호화되는 파일 확장자는 [표 2-2]와 같다. 암호화 이후에는 해당 파일명 끝에 .fun이라는 확장자가 추가된다.

.wmv, .vob, .m3u8, .dat, .csv, .efx, .sdf, .vcf, .xml, .ses, .Qbw, .QBB, .QBM, .QBI, .QBR, .Cnt, .Des, .v30, .Qbo, .Ini, .Lgb, .Qwc, .Qbp, .Aif, .Qba, .Tlg, .Qbx, .Qby, .1pa, .Qpd, .Txt, .Set, .Iif, .Nd, .Rtp, .Tlg, .Wav, .Qsm, .Qss, .Qst, .Fx0, .Fx1, .Mx0, .FPx, .Fxr, .Fim, .ptb, .Ai, .Pfb, .Cgn, .Vsd, .Cdr, .Cmx, .Cpt, .Csl, .Cur, .Des, .Dsf, .Ds4, ., .Drw, .Dwg, .Eps, .Ps, .Prn, .Gif, .Pcd, .Pct, .Pcx, .Plt, .Rif, .Svg, .Swf, .Tga, .Tiff, .Psp, .Ttf, .Wpd, .Wpg, .Wi, .Raw, .Wmf, .Txt, .Cal, .Cpx, .Shw, .Clk, .Cdx, .Cdt, .Fpx, .Fmv, .Img, .Gem, .Xcf, .Pic, .Mac, .Met, .PP4, .Pp5, .Ppf, .Xls, .Xlsx, .Xlsm, .Ppt, .Nap, .Pat, .Ps, .Prn, .Sct, .Vsd, .wk3, .wk4, .XPM, .zip, .rar

감염된 파일의 목록은 C:\Users\[사용자명]\AppData\Roaming\System32Work\경로에 EncryptedFileList.txt에 저장되며, 감염된 파일과 삭제된 파일 목록은 [그림 2-9]와 같은 UI 형식으로 보여준다.

표 2-2 | 암호화 대상 파일 확장자

.jpg, .jpeg, .raw, .tif, .gif, .png, .bmp, .3dm, .max, .accdb, .db, .dbf, .mdb, .pdb, .sql, .dwg, .dxf, .c, .cpp, .cs, .h, .php, .asp, .rb, .java, .jar, .class, .py, .js, .aaf, .aep, .aepx, .plb, .prel, .prproj, .aet, .ppj, .psd, .indd, .indl, .indt, .indb, .inx, .idml, .pmd, .xqx, .xqx, .ai, .eps, .ps, .svg, .swf, .fla, .as3, .as, .txt, .doc, .dot, .docx, .docm, .dotx, .dotm, .docb, .rtf, .wpd, .wps, .msg, .pdf, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xltw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .wav, .mp3, .aif, .iff, .m3u, .m4u, .mid, .mpa, .wma, .ra, .avi, .mov, .mp4, .3gp, .mpeg, .3g2, .asf, .asx, .flv, .mpg,



그림 2-9 | 삭제된 파일 목록

.net framework로 개발된 직쏘 랜섬웨어는 꾸준히 변종이 발견되고 있다. 안랩에서 수집한 직쏘 랜섬웨어의 변종을 확인한 결과, 암호화·복호화 코드와 파일의 속성을 파이어폭스(firefox)로 위장하는 등의 유사점이 많은 것으로 보아 동일한 제작자가 지속적인

으로 변종을 유포하고 있는 것으로 추정된다.

위협할 전망이다.

```
private static void EncryptFile(SymmetricAlgorithm alg, string inputFile, string outputFile)
{
    byte[] array = new byte[4096];
    using (FileStream fileStream = new FileStream(inputFile, FileMode.Open))
    {
        using (FileStream fileStream2 = new FileStream(outputFile, FileMode.Create))
        {
            using (CryptoStream cryptoStream = new CryptoStream(fileStream2, alg.CreateEncryptor(), CryptoStreamMode.Write))
            {
                int num;
                do
                {
                    num = fileStream.Read(array, 0, array.Length);
                    if (num != 0)
                    {
                        cryptoStream.Write(array, 0, num);
                    }
                } while (num != 0);
            }
        }
    }
}

private static void DecryptFile(SymmetricAlgorithm alg, string inputFile, string outputFile)
{
    byte[] array = new byte[4096];
    using (FileStream fileStream = new FileStream(inputFile, FileMode.Open))
    {
        using (FileStream fileStream2 = new FileStream(outputFile, FileMode.Create))
        {
            using (CryptoStream cryptoStream = new CryptoStream(fileStream2, alg.CreateDecryptor(), CryptoStreamMode.Write))
            {
                int num;
                do
                {
                    num = fileStream.Read(array, 0, array.Length);
                    if (num != 0)
                    {
                        cryptoStream.Write(array, 0, num);
                    }
                } while (num != 0);
            }
        }
    }
}
}
```

그림 2-10 | 직소 랜섬웨어의 소스코드 일부

이번 사례와 같이 최근 발견되고 있는 사회공학적 기법을 적용한 랜섬웨어는 사용자의 심리적 불안감을 극대화하여 금전적 이익을 취하고 있다. 또한 기술적 측면에서도 더욱 교묘하고 고도화된 방법을 모색하고 있다. 지난 2015년을 기점으로 화두가 되고 있는 랜섬웨어는 앞으로도 다변화된 방법으로 사용자를

랜섬웨어는 암호화 알고리즘을 이용하여 파일을 암호화하기 때문에 감염된 이후에는 사실상 복구가 어렵다. 따라서 랜섬웨어에 의한 피해를 최소화하기 위해서는 출처를 알 수 없거나 의심스러운 이메일은 가급적 즉시 삭제하고, 평소 중요한 데이터를 백업해두는 등 사용자의 각별한 노력이 필요하다.

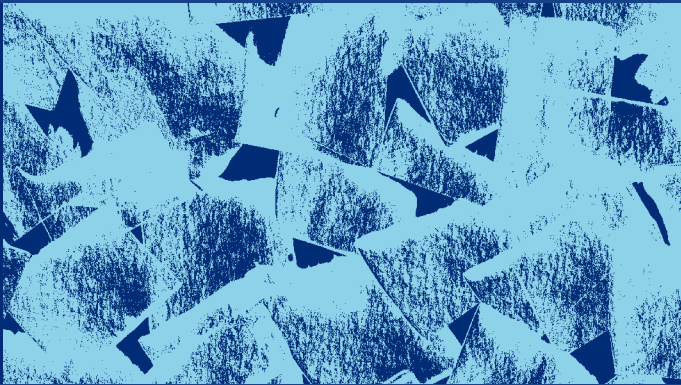
V3 제품에서는 직소 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Filecoder (2016.04.14.05)
 Trojan/Win32.Filecoder (2016.04.14.05)
 Trojan/Win32.Ransom (2016.04.13.09)
 Trojan/Win32.Agent (2016.04.14.04)
 Trojan/Win32.Agent (2016.04.14.04)
 Trojan/Win32.Jigsaw (2016.04.12.03)



3



악성코드 상세 분석 ANALYSIS-IN-DEPTH

이동식 저장장치로 유포되는 VBE 스크립트 악성코드

악성코드 상세 분석

이동식 저장장치로 유포되는 VBE 스크립트 악성코드

최근 이동식 저장장치의 사용이 늘어나면서, 이를 노리는 악성코드가 지속적으로 등장하고 있다. 해당 악성코드는 장치 내 파일들의 속성을 숨김으로 변경하고 파일의 바로가기를 생성하고 있어, 사용자들의 각별한 주의가 필요하다.

이번에 발견된 VBE 스크립트 악성코드 또한 이동식 저장장치를 통해 유포되는 악성코드의 일종으로, [그림 3-1]과 같이 스크립트 파일 형태를 띄고 있다.

[그림 3-2]의 더미 데이터에서 “FF D8 FF E0 xx xx 4A 46 49 46” 값은 JPEG 파일 구조에서 확인할 수 있는 헤더 값으로, 실제 해당 악성 스크립트는 [그림 3-3]과 같은 jpg 파일을 내부에 가지고 있음을 확인했다.

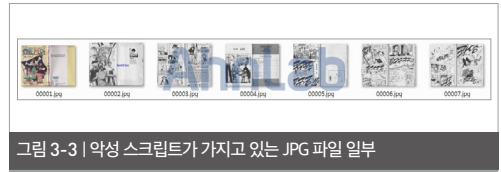


그림 3-3 | 악성 스크립트가 가지고 있는 JPG 파일 일부

이와 같은 의미 없는 더미 데이터들을 삭제한 후 실제 악성 행위를 수행하는 스크립트만을 확인하면 [그림 3-4]와 같이 파일 크기가 272KB로 줄어든다.



그림 3-4 | 악성 스크립트

일반적인 악성 스크립트 파일은 KB 단위의 파일인 반면, 해당 악성 VBE 스크립트 파일의 크기는 약 70MB인 것으로 미루어 볼 때, 악성 행위와 관련이 없는 더미 데이터(dummy data)로 파일 크기를 늘린 것을 확인할 수 있다.

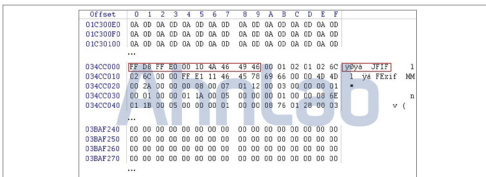


그림 3-2 | 악성 스크립트의 더미 데이터(dummy data)

또한 해당 악성 스크립트는 암호화되어 있으며, 복호화를 진행하면 [그림 3-6]과 같이 악성 행위를 수행하는 스크립트를 확인할 수 있다. 이는 앞서 확인된 바와 같이 더미 데이터를 이용하여 파일 크기를 증가시키고, 스크립트를 암호화함으로써 분석을 더욱 어렵게 하기 위한 것으로 보인다.



그림 3-5 | 암호화된 스크립트

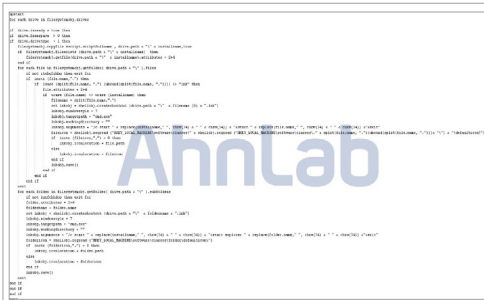


그림 3-6 | 악성 스크립트 일부

악성 스크립트가 실행되면 드라이브 종류가 이동식 (Removable)인 경우, [그림 3-7]과 같이 해당 스크립트가 실행된 장치 내의 파일 및 폴더들의 속성을 숨김으로 변경하고 바로가기 파일을 생성한다.

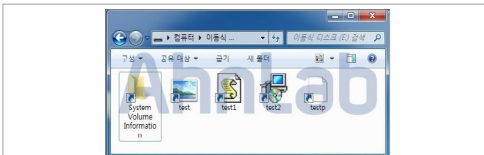


그림 3-7 | 바로가기로 변경된 파일 및 폴더

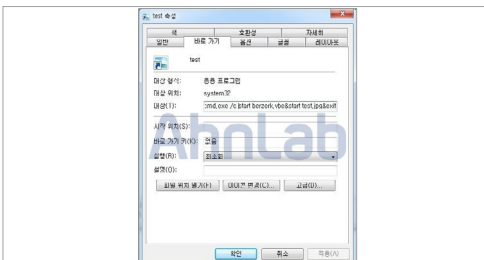


그림 3-8 | 바로가기 속성

또한 지속적인 감염 상태를 유지하기 위해, [그림 3-9]와 같이 레지스트리 및 시작 프로그램에 등록하여 Windows 시작 시 악성 스크립트가 실행될 수 있도록 한다.



그림 3-9 | 시작 프로그램 등록

휴대가 편리하여 세미나 발표 자료, 중요 문서 백업 등에 많이 활용되는 이동식 저장장치의 사용이 증가하면서 이를 노린 악성코드 또한 고도화되고 있다. 장치를 연결하는 것만으로도 PC를 쉽게 감염시킬 수 있어 학교나 도서관 등 공공장소에서의 2차 피해가 예상되므로 사용자들의 더욱 각별한 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

VBS/Encode (2016.04.19.00)

AhnLab

ASEC REPORT VOL.76

April, 2016

집필

안랩 시큐리티대응센터 (ASEC)

편집

안랩 콘텐츠기획팀

디자인

안랩 디자인팀

발행처

주식회사 안랩

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.