

ASEC REPORT

VOL.74

February, 2016



AhnLab

ASEC REPORT

VOL.74 February, 2016

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 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.

2016년 2월 보안 동향

Table of Contents

1	01 악성코드 통계	4
보안 통계	02 웹 통계	6
STATISTICS	03 모바일 통계	7
2	01 PAC 설정을 악용한 파밍 악성코드	10
보안 이슈	02 HydraCrypt 랜섬웨어	13
SECURITY ISSUE		
3	Adwind 분석 보고서	16
악성코드 상세 분석		
ANALYSIS IN-DEPTH		

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

03 모바일 통계

보안 통계

01

악성코드 통계

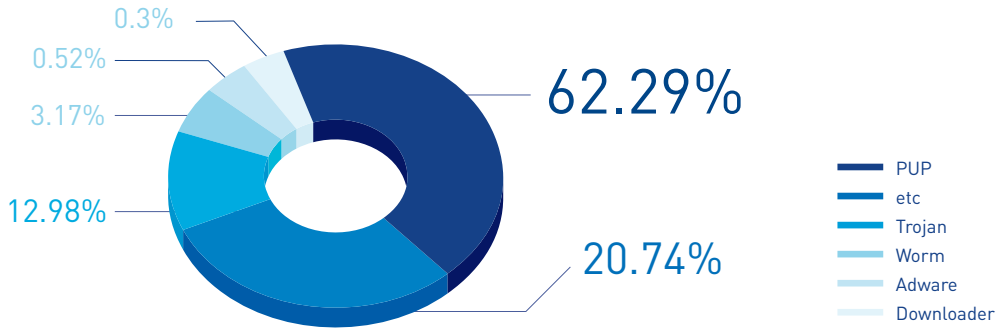
ASEC이 집계한 바에 따르면, 2016년 2월 한 달간 탐지된 악성코드 수는 1,183만 547건으로 나타났다. 이는 전월 1,506만 1,417건에 비해 323만 870건 감소한 수치다. 한편 2월에 수집된 악성코드 샘플 수는 349만 3,468건이다.



[그림 1-1] 악성코드 추이(2015년 12월 ~ 2016년 2월)

* '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.

[그림 1-2]는 2016년 2월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 62.29%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 12.98%, 웜(Worm)이 3.17%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 2월 주요 악성코드 유형

[표 1-1]은 2월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter이 총 22만 5,744건으로 가장 많이 탐지되었고, Malware/Win32.Generic 이 13만 8,659건으로 그 뒤를 이었다.

[표 1-1] 2016년 2월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	225,744
2	Malware/Win32.Generic	138,659
3	Trojan/Win32.Agent	100,579
4	Unwanted/Win32.HackTool	93,233
5	Trojan/Win32.Neshta	91,419
6	Trojan/Win32.Teslacrypt	78,411
7	HackTool/Win32.Crack	70,004
8	Trojan/Win32.Gen	69,434
9	Unwanted/Win32.Keygen	65,054
10	Trojan/Win32.Banki	60,172

보안 통계

02
웹 통계

2016년 2월에 악성코드 유포지로 악용된 도메인은 936개, URL은 7,900개로 집계됐다(그림 1-3). 또한 2월의 악성 도메인 및 URL 차단 건수는 총 635만 5,582건이다.



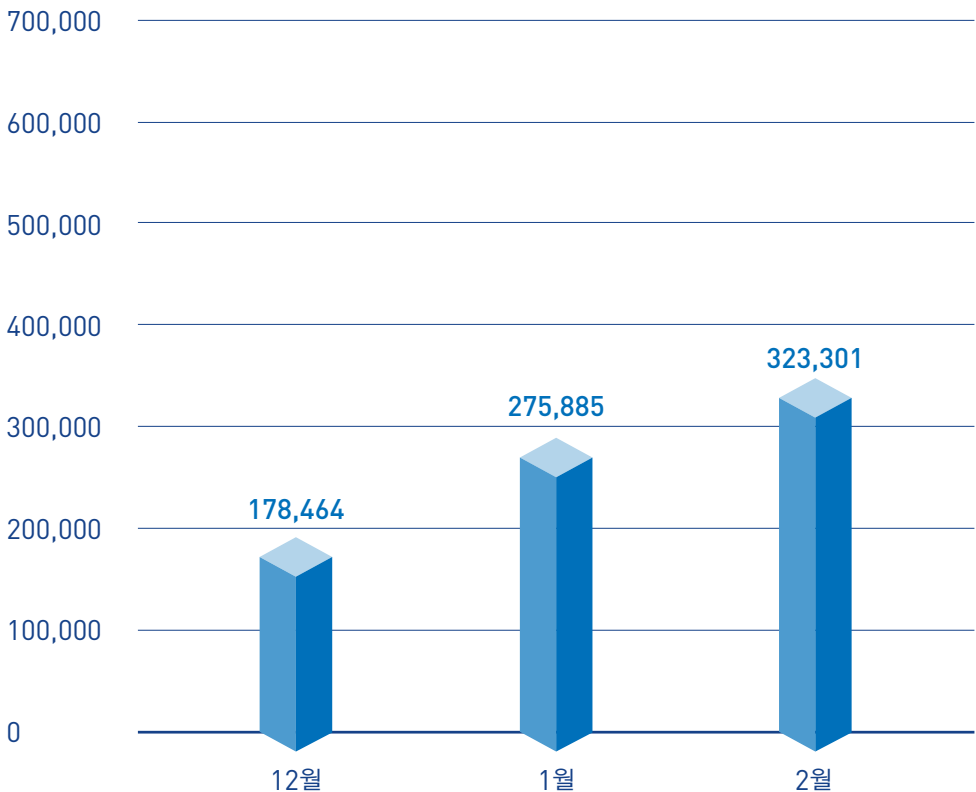
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 12월 ~ 2016년 2월)

* 악성 도메인 및 URL 차단 건수란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03

모바일 통계

2016년 2월 한 달간 탐지된 모바일 악성코드는 32만 3,301건으로 나타났다.

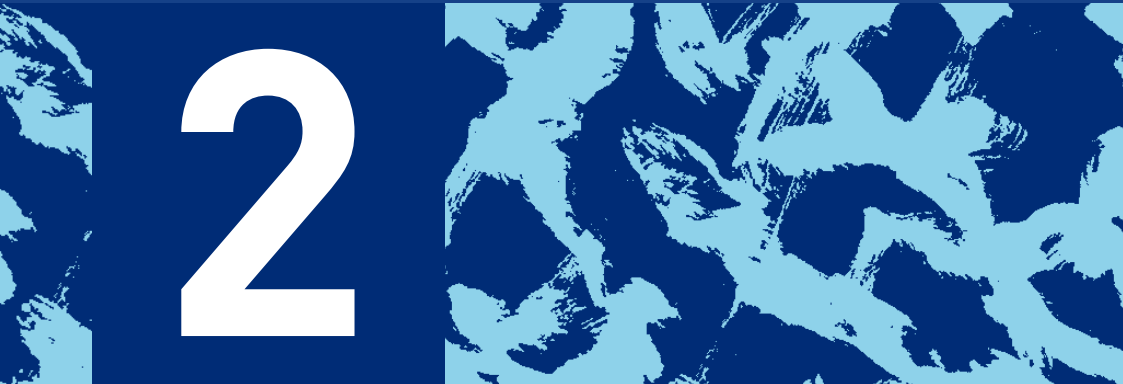


[그림 1-4] 모바일 악성코드 추이(2015년 12월 ~ 2016년 2월)

[표 1-2]는 2월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2016년 2월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	70,760
2	Android-PUP/SmsReg	36,360
3	Android-PUP/Noico	34,774
4	Android-Trojan/Moavt	17,481
5	Android-Trojan/FakeInst	15,076
6	Android-PUP/Dowgin	11,111
7	Android-Trojan/SmsSpy	9,003
8	Android-PUP/Skymobi	5,993
9	Android-PUP/Airpush	5,755
10	Android-Trojan/SmsSend	5,677



2

보안 이슈 SECURITY ISSUE

01 PAC 설정을 악용한 파밍 악성코드

02 HydraCrypt 랜섬웨어

01

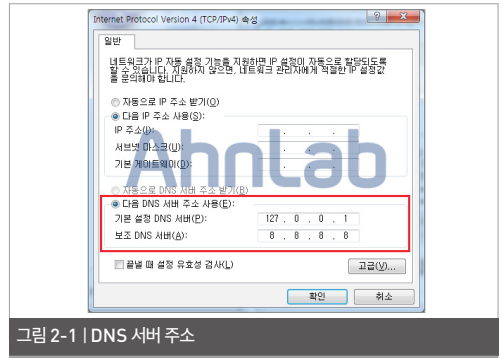
PAC 설정을 악용한 파밍 악성코드

파밍(Pharming)은 금융 기관 사이트로 위장한 웹 페이지로 접속을 유도하여, 사용자가 입력한 개인 정보 및 금융 정보를 탈취하는 공격 기법이다. 파밍은 이전부터 익히 알려진 공격 기법으로, 대부분의 사용자들이 한 번쯤은 경험해 보았을 것이다.

이와 같은 유형의 파밍 악성코드는 그 동안 사용자들에게 많이 노출되었기 때문에 더 이상 이전만큼 급전 피해가 속출하는 상황은 아니다. 하지만 스마트폰이나 PC를 이용한 비대면 금융 거래가 점점 증가하는 추세에 따라, 파밍 공격 기법 또한 지속적으로 발전하고 있다. 최근에는 그간 발견되지 않은 PAC 설정을 악용한 새로운 유형의 파밍 악성코드가 발견됐다. 다음 사례를 통해 살펴보자.

1. 프록시 자동 설정(Proxy Auto-Configuration, PAC) 스크립트 이용

기존의 파밍 악성코드는 DNS 서버 주소와 사용자 PC의 "C:\Windows\System32\drivers\etc" 경로 내에 있는 hosts 파일, hosts.ics 파일을 변조하여 사용자를 금융 기관 사이트로 위장한 웹 페이지로 유도했다.



한편 최근 새롭게 발견된 파밍 악성코드는 백신 제품의 탐지를 우회하고자 프록시 자동 설정(이하 PAC) 스크립트를 이용하고 있다. PAC 스크립트는 웹 캐시에 대한 정보를 브라우저에 설정하지 않고, 별도의 파일에 저장한다. 이렇게 생성된 별도 파일을 특정 서버에 업로드 한 다음, [그림 2-2]와 같이 PAC 스크립트의 경로를 지정하여 사용한다.

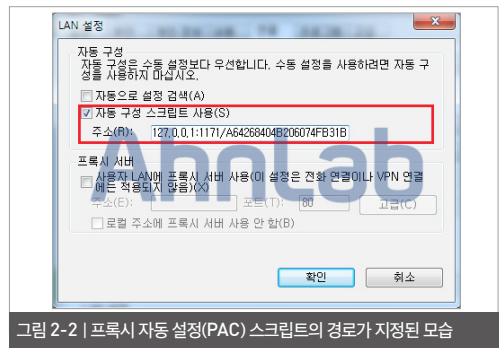


표 2-1 | PAC 파일 정보

```
var dowla = {
  "ea7921b63846854dd57dc9277e34528cce350fa9": 1,
  ...생략...
  "f314482664afb023f55e5d948774635262d56bdb4": 1
};
var po = "SOCKS 127.0.0.1:1157";
var ekl = 'DIRECT';
var hasOwnProperty = Object.hasOwnProperty;

function FindProxyForURL(wkql, woal) {
  if (hasOwnProperty.call(dowla, i11_lwo(woal))) {
    return po
  }
  return ekl
}
```

PAC 파일은 공격 대상이 아닌 사이트는 모두 직접(DIRECT) 연결되도록 작성되어 있다. 즉, [그림 2-3]과 같이 공격 대상 주소인 주요 포털 사이트 및 금융 사이트로의 연결 시도가 아닐 경우, 정상 웹 페이지를 출력한다.

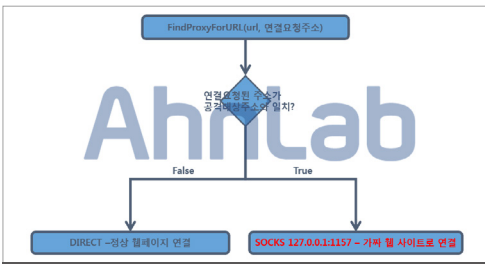


그림 2-3 | PAC 파일에 의한 네트워크 연결 구조



그림 2-4 | 변수 'dowla'에 선언된 공격 대상 사이트

표 2-2 | 공격 대상 사이트

[변수 dowla 정보]

www.**star.com	ea7921b63846854dd57dc9277e34528cce350fa9
www.**hyup.com	6c780b275734e4391562b3dff5a7756633ba7a8
www.k**co.kr	33859e317cf5b7d57ec77cbb82d8225e8080ae10
www.i**co.kr	463c43b8bf3d105bd8b90f87a762a61b35f78975
www.h***bank.com	4483a10b6e4689c5b6ffe01cd06af58ecb36e28
www.e***bank.go.kr	c9f5025cb48435b27b7bace6fa5abb55767206d
www.e***bank.co.kr	b1484496f37a2376f8fd2bb9b5c75c131032eb5
www.**han.com	2efb211fd18dcb380c357367fcb14c5088c2a7
www.k***co.kr	52bec35d1a5c0ecd0af7c769a8a603304b469814
www.w***bank.com	595dc993cbebcf89e65dc5ea3cf159fca3523254
www.n***.com	62c116033e335ca54eb19ec34ff8a7b0cc9130
www.d***.net	9e2d1f20d59ad10525b2bfa16133b631235a5bce
www.z**com	83f6975e027788645b4c00ef25b5146fed5565cc
www.c*.co.kr	943823bad8f9493912f1507b1102ddda8724c35e
www.b***bank.co.kr	93cd406ba7d35f7eda09a2400f31bacd740d2953
www.c***bank.co.kr	fc018a9fbaced3ec83d3509d97211c908d96bd8f
www.**bank.co.kr	eb3dfbb25f6dd9cfb0f8b3cae7fe9c964ab3ac
www.s***up.co.kr	8ca13f57362cabed97720663eeec034b5c08a563
www.**bank.com	b8363cd02ee0d3592f4872d801740064bfdf07c0
www.s*****d.co.kr	fdc93ff8035c20656262b4b061e9bbf320b46877
www.s*.co.kr	2edace762f11f327490aa8f54100140bd6d4b1ba
www.n***.com	8aaf0a929a9ad04e43c683d1c0a34d21975f2e41
www.h*****net	a4fc7941e5299e9343317114033db7920daa571d

공격 대상 사이트는 [그림 2-4]와 같이 PAC 파일 내에서 변수 'dowla'로 선언되어 있으며, [표 2-2]와 같은 형식으로 암호화되어 있음을 확인할 수 있다.

2. 확장자를 인증서(.crt) 파일로 위장

파밍 악성코드는 일반적으로 정상 프로세스에 악의적인 코드를 삽입하거나, 악성 DLL 파일을 인젝션하는 방법을 사용한다. 이번 사례는 후자의 경우로, 앞

서 발견된 악성 DLL 파일을 이용하는 파밍 악성코드의 유형과 같지만, [그림 2-5]와 같이 해당 악성 파일을 인증서 확장자인 .crt로 위장하여 은폐한다.

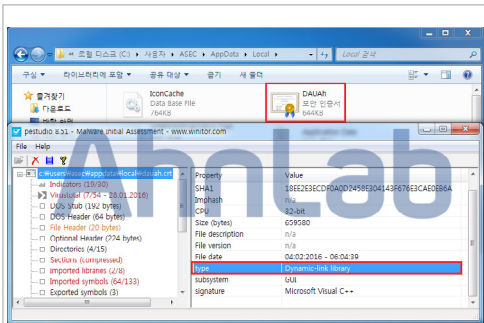


그림 2-5 | 보안 인증서로 위장한 악성 DLL 파일

해당 파일은 [그림 2-5]와 같이 겉보기에는 .crt 확장자를 가진 보안 인증서 파일처럼 보이지만, 사실은 실행 가능한 DLL 파일이다. 이러한 악성 DLL 파일은 정상 프로세스인 rundll32.exe에 인젝션되어 실행된다.

위의 두 가지 사례에서 소개한 파밍 악성코드는 공격 형태만 다를 뿐, 이전에 유포된 파밍 악성코드와 마찬가지로 사용자의 금융 정보 탈취가 목적인다는 점은 동일하다. 이렇듯 파밍 공격 기법은 점점 더 고도화되고 있다. 파밍으로 인한 피해를 방지하기 위해서는 보안 업데이트를 설치하여 드라이브-바이 다운로드(Drive-by-download) 공격을 예방하고, 프로그램 설치 시 함께 설치되는 제휴 프로그램이 꼭 필요한 프로그램인지 주의하여 설치해야 하며, 백신 제품의 엔진을 최신으로 유지하는 사용자의 올바른 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Agent (2016.01.28.07)

Trojan/Win32.Banki (2016.01.31.05)

02

HydraCrypt 랜섬웨어

랜섬웨어는 PC에 저장된 문서, 그림 파일 등을 암호화한 다음, 비트 코인과 같은 일종의 몸값을 지불해야만 다시 접근할 수 있도록 하여 사용자에게 치명적인 피해를 입히는 악성코드다. 이와 같은 랜섬웨어가 다양한 유형으로 등장하여 점점 고도화되는 가운데, 이번에는 Angler Exploit kit을 통해 유포되고 있는 HydraCrypt 랜섬웨어가 새롭게 등장했다.

먼저 HydraCrypt 랜섬웨어의 실행 후 행위부터 자세히 살펴보자. HydraCrypt 랜섬웨어는 다음 [표 2-3]에서 확인할 수 있는 것처럼 파일 생성, 레지스트리 등록, 시스템 복원 지점 삭제, C&C 접속과 같은 일련의 행위를 수행한다.

표 2-3 | 랜섬웨어 실행 후 행위

[파일 생성]

```
%AppData%\ChromeSettings3264\[랜덤문자열].exe
[암호화 파일 폴더]\README_DECRYPT_HYDRA_ID_[감염PC별 생성된 ID값].txt
```

[레지스트리 등록]

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
ChromeSettingsStart3264 - "%AppData%\ChromeSetings3264\[랜덤문자열].exe"
Microsoft Internet Explorer Update - "랜섬웨어 처음 실행된 경로"
(OS_Win7 이상)
```

[볼륨 웨도우 복사본 삭제(시스템 복원 지점 삭제) (Windows 7 이상)]

```
cmd /c net stop vss
cmd /c vssadmin Delete Shadows /All
cmd /c wmic shadowcopy delete
```

[C&C 접속]

```
drivers-*****.eu
```

HydraCrypt 랜섬웨어의 암호화 대상 파일이 위치한 폴더에는 README~.txt 파일이 생성되는데, 그 내용은 [표 2-4]와 같다.

표 2-4 | README_DECRYPT_HYDRA_ID_~.txt

[README~.txt 정보]

Attention!

All Your files and documents were encrypted!

Encryption was made with a special crypto-code!

There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:

1) XHELPER@DR.COM

or

2) AHELPER@DR.COM

Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It's your guarantee!

Remember! Your time has a limit: 72 hour.

If You will not send any email We will turn on a sanctions:

1) Your software's price will be higher

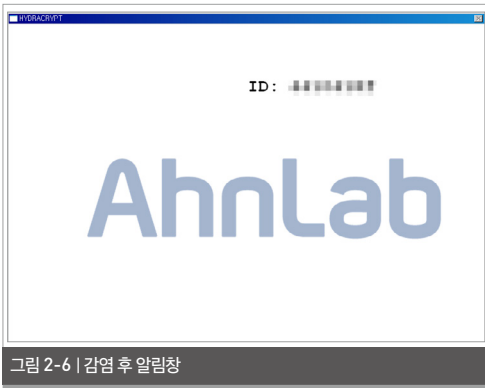
2) Your unique private key will be destroyed (After that your files will stay encrypted forever)

3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

ID: *****

위 메시지에서 72시간 내에 메일을 보내지 않으면(Offline 랜섬웨어) 파일을 유포할 것(Chimera 랜섬웨어) 등 기존에 유포된 Offline 랜섬웨어 및 Chimera 랜섬웨어와 유사한 형태의 협박 내용이 있음을 확인할 수 있다. 또한, 감염 후 발생하는 알림창에서는 [그림 2-6]과 같이 고유 ID 값이 노출되며, 일반적인 랜섬웨어와 마찬가지로 감염 PC의 정보를 C&C로 전송하는 과정을 거친다.



악성코드 제작자들이 랜섬웨어를 유포하여 사용자의

중요 파일을 암호화하고 이를 복호화 시켜주는 조건으로 꾸준히 수익을 올리고 있는 만큼, 2016년에도 랜섬웨어는 다수의 변종을 생성하며 지속될 것으로 보인다. 복호화 방법이 없는 랜섬웨어에 감염된 경우에는 암호화된 파일들을 돌킬 수 없기 때문에 그 무엇보다 사용자들의 보안 의식이 중요하다.

사용 중인 응용 프로그램의 보안 업데이트는 반드시 진행하여 항상 최신 버전으로 유지해야 하며, 확인되지 않은 메일의 첨부 파일은 실행하지 않는 것이 좋다. 또한, 특정 광고성 사이트를 방문하거나 프로그램을 설치하지 않도록 인터넷 사용 시 각별한 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Win-Trojan/Malpacked3.Gen

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

Adwind 분석 보고서

Adwind 분석 보고서

1. 개요

Adwind 악성코드는 최근 400,000건 이상의 감염을 일으키고 있는 Cross Platform 기반의 JAVA 악성코드이다.

Adwind 계열 악성코드는 Unrecom, JSocket, Alienspy 등이 존재하며 비슷한 인터페이스 및 옵션을 가지고 있는 것으로 보아, 동일 제작자가 제작했거나 최초 제작자와 연관된 사람들이 제작한 것으로 추정된다.

이 글을 시작하기 전에 Server와 Client에 대해 다음과 같이 정의한다.

Server : 감염자 PC에 설치되는 악성코드

Client : 공격자 PC에 설치되는 관리 프로그램

2. 국내 현황

전체 JAVA 샘플 중 Adwind의 비중이 압도적이며, 그 다음으로 Exploit, Agent 순으로 많이 접수됐다.

Adwind의 경우 2013년부터 만들어졌으나 국내의 경우 크게 이슈가 되지 않은 샘플이었다. 고객으로부터의 접수 또한 많지 않았으나, 2015년 10월을 기점으로 꾸준히 접수되고 있다.

3. Adwind 계열 악성코드의 특징

Cross Platform 악성코드인 Adwind는 Android, Mac, Linux, Windows OS에서 동작한다. 주로 메일에 첨부된 파일이나 문서에 첨부된 파일 실행 시 감염되거나, Exploit Kit에 의해 감염되기도 한다.

다음은 실제 고객으로부터 접수된 사례이다.

MS 워드 파일에 JAR(Java Archive) 파일이 첨부되었으며, [그림 3-1]과 같이 본문에 아이콘이 존재하여 사용자의 더블클릭을 유도함을 확인할 수 있다.

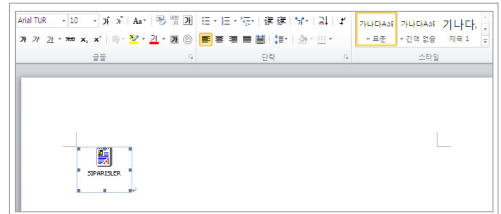


그림 3-1 | MS 워드 파일에 첨부된 JAR(Java Archive) 파일

해당 파일을 더블클릭하면 JAVA가 설치된 경우 악성 JAR이 실행되어 사용자 PC가 감염된다.

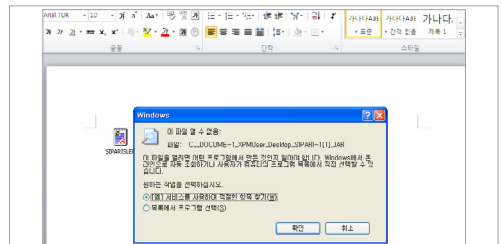


그림 3-2 | JAR 파일 실행(더블클릭 후)

Android OS 계열의 경우, APK(Android application package)로 Server를 생성하며 Mac, Linux, Window OS 계열의 경우에는 JAR(Java Archive)로 Server를 생성한다.

Server는 기본 기능 + Plugin 형태로 작성된다. 감염된 PC나 기기는 C&C IP로 접속을 시도하며, 해당 C&C에 Builder가 대기하여 감염자 PC에 원격으로 명령을 내릴 수 있다.

Windows OS에서는 다음과 같은 기본 기능을 제공한다.

- 감염자 PC에 메시지 박스를 띄워 메시지 보내기
- 특정 URL 열기 (감염자 PC 브라우저 실행을 통해 접속)
- 원격지 파일 다운로드 이후 실행
- 감염자 PC의 IP 정보 조회
- 감염자 PC RAT (재실행, 업데이트, 접속 종료, 삭제)

추가적인 기능은 Plugin을 이용하여 실행이 가능하다. Plugin 종류에 따라 기능을 확장할 수 있으며 대표적인 Plugin은 다음과 같다.

- 웹캠 전송
- 키로깅
- 메일, 파일질라 데이터 얻기(로그인 정보 얻기)
- 브라우저 정보 탈취(브라우저에 자동으로 저장된 웹사이트 ID, 비밀번호 탈취)
- 콘솔 실행

4. Adwind Builder 분석

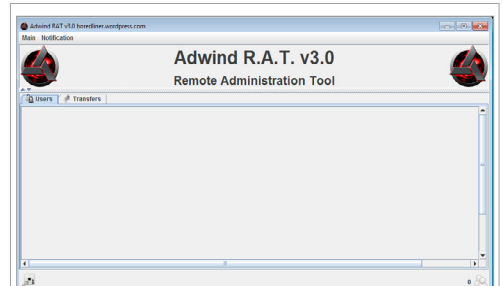


그림 3-3 | Adwind 3.0 악성코드 Client 화면

이 글에서 언급되는 Adwind 3.0의 경우, 악성코드 제작자에 등록된 사용자 ID와 Password 인증 절차를 거친다. 로그인에 성공하면 [그림 3-3]과 같은 인터페이스 화면이 생성된다.

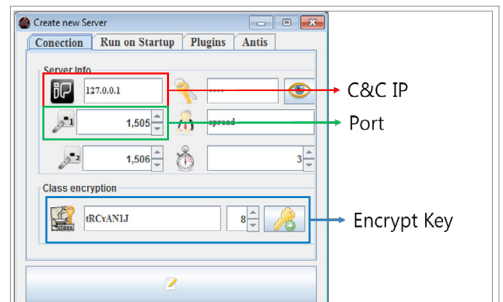
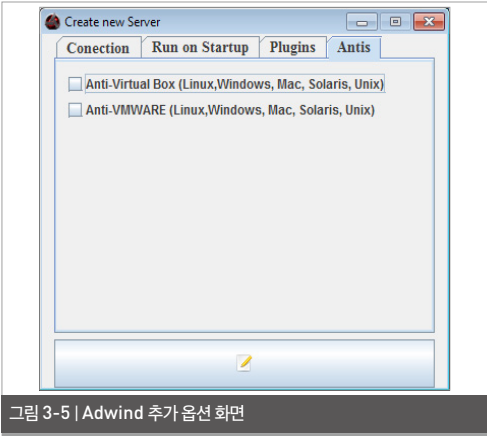
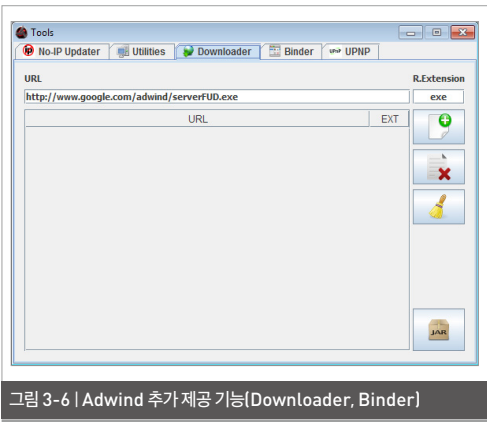


그림 3-4 | Adwind Server File 생성 시 화면

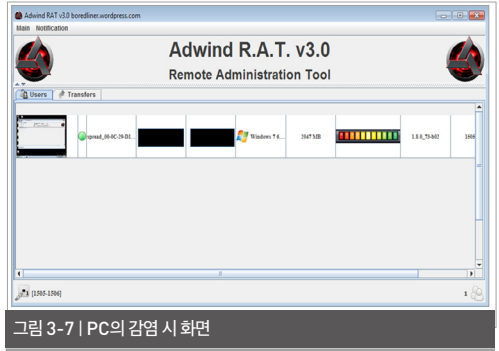
Adwind는 [그림 3-4]와 같이 Server(감염자 PC에 설치된 악성 JAR 파일) 생성 시 감염자 PC에서 접속할 C&C(Client IP)와 포트 2개(기본 포트, 옵션 포트)를 입력받는다. 그리고 추가적으로 Class encryption이라는 랜덤 키를 이용하여 Adwind Class(실행 시 디코딩 후 악의적인 행동을 하는 Class 파일)를 암호화한다. Adwind의 구조는 이후 설명에서 언급하도록 한다.



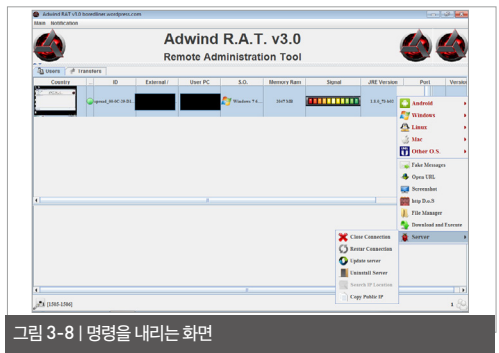
Adwind는 [그림 3-5]와 같이 추가적으로 Anti-VMWARE, Anti-Virtual Box 옵션 기능을 가진다.



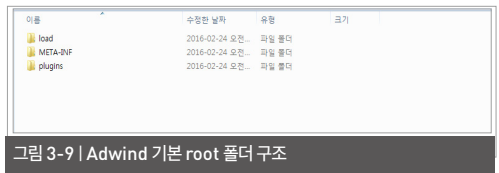
Adwind Builder는 기본적인 RAT 기능을 하는 JAR 파일 뿐만 아니라 특정 주소의 파일을 다운로드 받아 실행하는 Downloader와 공격자가 원격에서 접속할 수 있도록 감염 PC에 상주하는 악성코드인 Binder 기능을 하는 JAR 파일을 생성하는 부가 기능을 가진다.



PC가 감염된 경우 [그림 3-7]과 같이 Client(Build er)에 접속된다. 접속 시에는 IP 정보, 컴퓨터 이름, 운영체제, RAM 정보, JRE 버전, 접속 포트 등이 표시되며, 공격자는 명령을 내려 감염자 PC를 조작할 수 있다.



공격자는 [그림 3-8]과 같이 명령을 내릴 감염자 PC의 행에서 마우스 오른쪽 버튼을 클릭하여 악의적인 명령을 전송할 수 있다.



- load 폴더: Class 암호 파일 및 Class Loader, 암호가 해제된 이후 실행될 Data가 존재(암호화되어 있음)

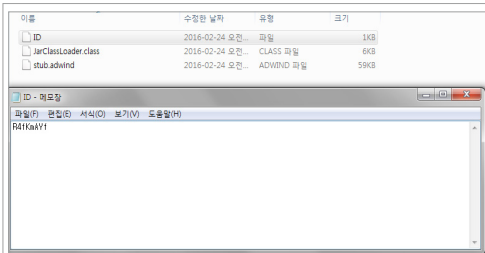


그림 3-10 | load 폴더 및 ID 파일의 내부 문자열(암호화 키)

- ID: 8Byte 데이터 파일(디코딩 키)
- JarClassLoader.class: main Class(MANIFEST.MF에 명시됨)
- stub.adwind: 암호화 형태로 ID 파일을 통해 복호화 후 실행됨.

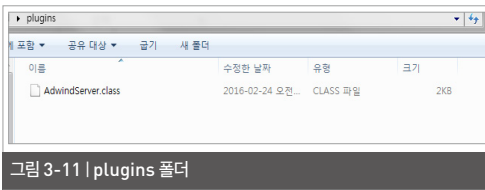


그림 3-11 | plugins 폴더

- plugins 폴더: Adwind에서 실행하는 Plugin에 대한 폴더. Adwind는 기본 명령 외 추가 명령들을 실행하기 위해 이러한 Plugin을 필요로 함.

분석 당시, Adwind 사이트에서 Plugin 다운로드를 시도하면 사이트가 정상적으로 동작하지 않아 Plugin들이 다운로드되지 않았다.

5. Adwind Server 분석

Adwind는 기본적으로 Builder부터 Server까지 JAVA 난독화 툴을 이용하여 내부 코드들을 보호하고 있다.

다음 분석 정보는 Adwind 3.0으로부터 생성된 Server를 디컴파일하고 일부 코드를 수정하여 디버깅하면서 확인된 내용이다. 디컴파일을 통해 확인된 Main Class 및 Package 환경에 맞춰 코드를 수정하면서 디버깅을 진행한다.

Adwind 계열의 악성코드는 내부 코드를 보호하기 위해 상용 난독화 툴을 사용한다. 해당 난독화 툴을 직접 디버깅하여 확인한 결과 Config 및 Class 파일을 메모리에 적재하고 동적으로 실행하는 것을 확인했으며, 적재되는 Config 및 Main Class(Principal.Class) 파일은 다음과 같다.



그림 3-12 | Config 내용



그림 3-13 | 추출된 Principal.Class

[그림 3-13]의 추출된 Principal.Class의 코드를 분석한 결과, Plugin 설정 여부 확인 및 로드, Anti-VMWARE, Anti-Virtual Box를 확인하는 과정들이 존재한다.(Config 설정에 따른 초기화 여부 확인 및 초기화)

6. Unrecom Builder 분석

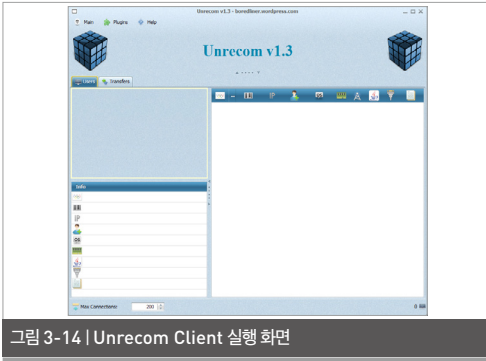


그림 3-14 | Unrecom Client 실행 화면

Unrecom은 Adwind 계열의 악성코드로, Adwind와 동일하게 악성코드 제작자에게 비용을 지불하고 사용자 ID와 Password를 인증한 다음 사용하는 형식으로 제작되었다.

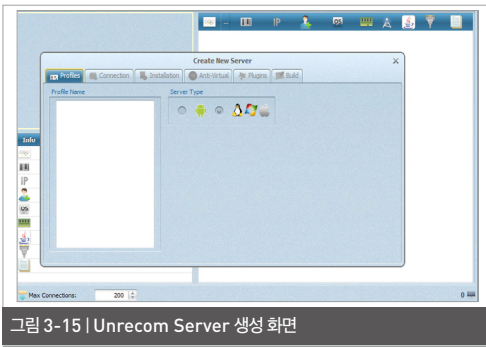


그림 3-15 | Unrecom Server 생성 화면

또한 Unrecom은 Adwind와 마찬가지로 JAVA Cross Platform 악성코드이며, 기본적으로

Windows, Linux, Mac, Android OS를 타깃으로 Server를 생성한다.

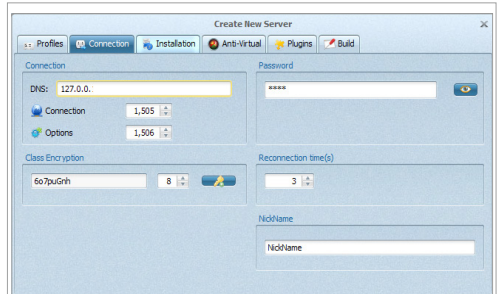


그림 3-16 | Server 설정화면

[그림 3-16]과 같이 Unrecom은 Adwind와 유사하게 접속 IP(C&C) 및 Class Password String을 설정할 수 있으며, Anti-VMWARE, Anti-Virtual Box 기능을 제공한다. 또한 Adwind보다 간결한 인터페이스를 제공하고 있다. Adwind와의 차이점은 Build Tab에 Config 설정을 저장하는 기능이 있어, 기존에 사용한 설정을 불러올 수 있다는 점이다. Downloader 및 Binder 기능은 제공하지 않는다.

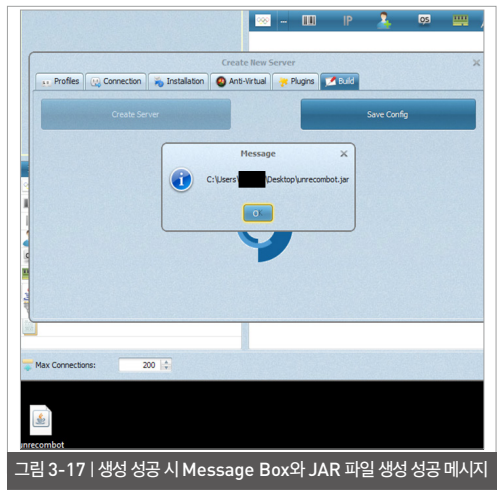


그림 3-17 | 생성 성공 시 Message Box와 JAR 파일 생성 성공 메시지

Windows, Linux, Mac OS 기반의 Server 파일을 생성할 경우, JAR(Java Archive) 파일을 생성한다. Android 기반의 Server 파일을 생성할 경우에는 APK(Android application package) 파일을 생성한다.

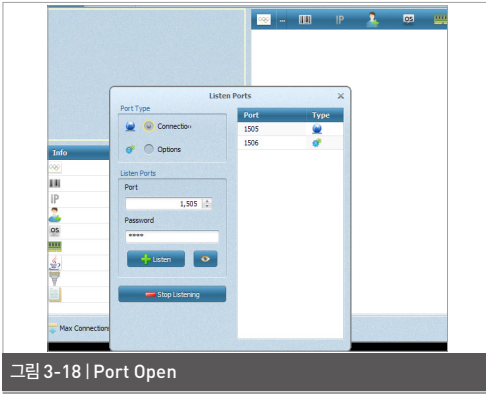


그림 3-18 | Port Open

포트 역시 Adwind와 같이 2개의 포트(기본 포트, 옵션 포트)를 사용한다. Server 생성 시, 기본 포트는 1505, 1506으로 설정되어 있다. 이처럼 Unrecom의 기본 기능 및 요소, Default 설정 값이 Adwind와 대부분 같이 제작자가 동일한 것으로 추정된다.

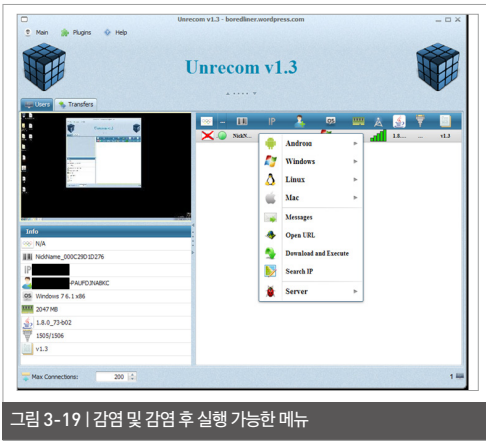


그림 3-19 | 감염 및 감염 후 실행 가능한 메뉴

Unrecom은 Adwind와 유사한 정보들을 Client로 제공하며, 마우스 오른쪽 버튼 클릭 시 사용할 수 있는 메뉴도 Adwind와 거의 동일하다. 이러한 특징을 통해 Unrecom, Adwind, Jsocket, Alienspy의 제작자가 동일하거나 서로 연관이 있을 것이라고 추정할 수 있다.

7. Unrecom Server 분석

Unrecom Builder에 의해 생성된 Server는 다음 [그림 3-20]과 같은 Root 폴더 구조를 가진다.

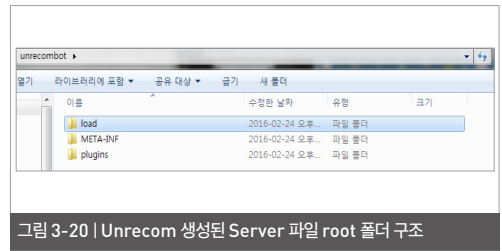


그림 3-20 | Unrecom 생성된 Server 파일 root 폴더 구조

Root 폴더 구조는 Adwind와 별다른 차이 없이 동일한 구조를 가진다. 단, Plugin 사용 시에는 달라질 수 있다.

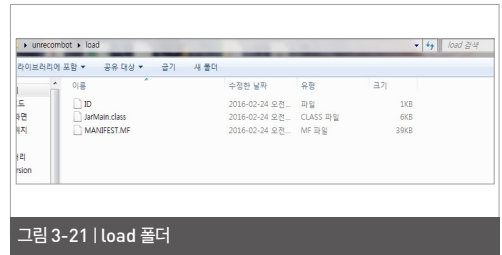
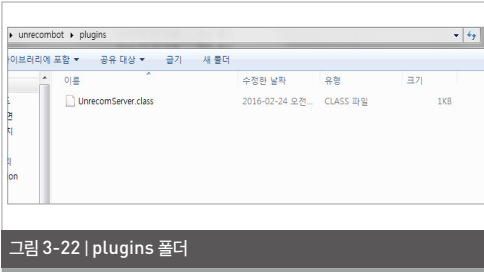


그림 3-21 | load 폴더

load 폴더는 Adwind와 동일하게 ID, JarMain.class, 인코딩된 파일 1개를 가진다. 인터페이스만 다를 뿐 Build되어 나오는 JAR 파일 구조는 거의 동일하다.



근에는 Adwind, Unrecom과 같이 원격제어 기능 및 난독화 기법을 사용하는 보다 복잡하고 큰 모듈 형태로 발전하고 있다. 또한, Adwind를 시작으로 Unrecom처럼 유사한 기능의 악성코드가 점점 증가하고 있으며, Plugin 형태로 제공되는 파일에 의해 다양한 기능이 쉽게 추가될 수 있는 구조이다.

plugins 폴더 역시 Adwind와 동일한 폴더 구조이다.

8. 결론

과거 JAVA로 제작된 악성코드는 대부분 취약점을 이용한 형태로, 또 다른 2차 악성코드를 다운로드하고 이를 실행하는 비교적 단순한 형태였다. 하지만 최

2013년부터 발견된 Adwind 계열 악성코드는 Cross Platform이라는 특성때문에 앞으로도 매우 급격하게 증가할 가능성이 존재한다. Adwind 계열 악성코드의 이러한 특성과 급격한 증가 속도로 보아, JAVA 기반 악성코드에 대한 대비가 충분히 이루어져야 할 것이다.

AhnLab

ASEC REPORT VOL.74 February, 2016

집필 **안랩 시큐리티대응센터 (ASEC)**
편집 **안랩 콘텐츠기획팀**
디자인 **안랩 디자인팀**

발행처 **주식회사 안랩**
 경기도 성남시 분당구 판교역로 220
 T. 031-722-8000
 F. 031-722-8901

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.