

ASEC REPORT

VOL.74

February, 2016



AhnLab

ASEC REPORT

VOL.74 February, 2016

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF February 2016

Table of Contents

1

SECURITY STATISTICS

01 Malware Statistics	4
02 Web Security Statistics	6
03 Mobile Malware Statistics	7

2

SECURITY ISSUE

New HydraCrypt Ransomware Appears	10
-----------------------------------	----

3

IN-DEPTH ANALYSIS

A Java-Based Cross-Platform Malware: Adwind	13
---	----

1

SECURITY STATISTICS

01 Malware Statistics

02 Web Security Statistics

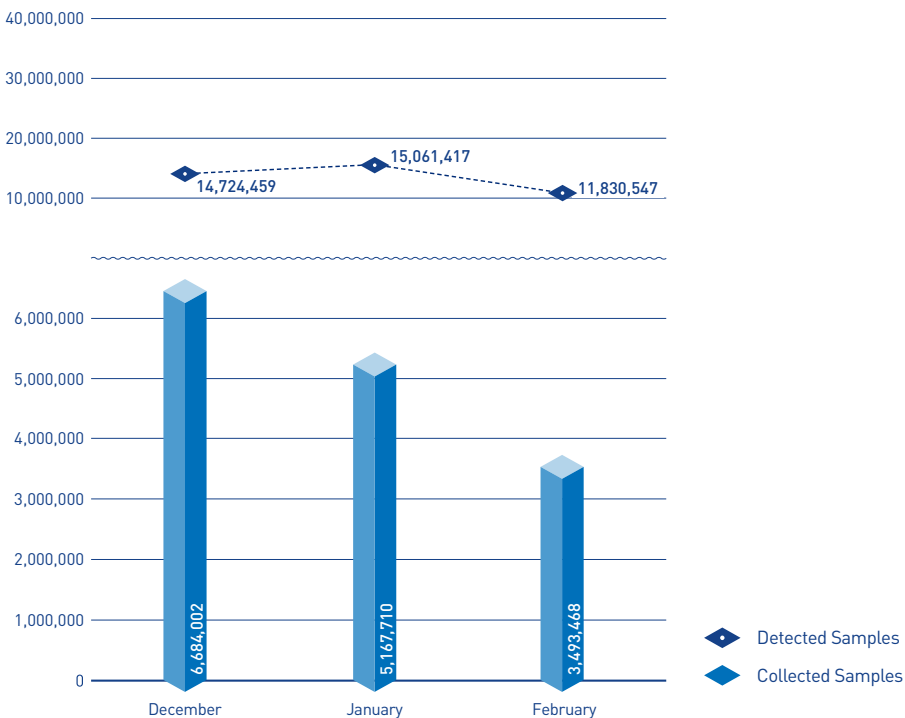
03 Mobile Malware Statistics

SECURITY STATISTICS

01

Malware Statistics

According to the ASEC (AhnLab Security Emergency Response Center), 11,830,547 malware were detected in February 2016. The number of detected malware decreased by 3,230,870 from 15,061,417 detected in the previous month as shown in Figure 1-1. A total of 3,493,468 malware samples were collected in February.

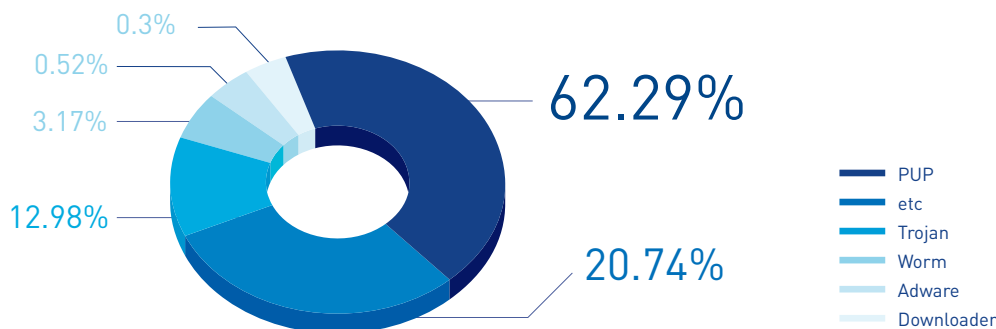


[Figure 1-1] Malware Trend

* "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers.

* "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in February 2016. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 62.29% of the total. It was followed by Trojan (12.98%) and Worm (3.17%).



[Figure 1-2] Proportion of Malware Type in February 2016

Table 1-1 shows the Top 10 malware threats in February categorized by alias. Trojan/Win32.Starter was the most frequently detected malware (225,744), followed by Malware/Win32.Generic (138,659).

[Table 1-1] Top 10 Malware Threats in February 2016 (by Alias)

Rank	Alias from AhnLab	No. of detections
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

SECURITY STATISTICS

02

Web Security Statistics

In February 2016, a total of 936 domains and 7,900 URLs were compromised and used to distribute malware. In addition, 6,355,582 malicious domains and URLs were blocked.



[Figure 1-3] Blocked Malicious Domains/URLs in February 2016

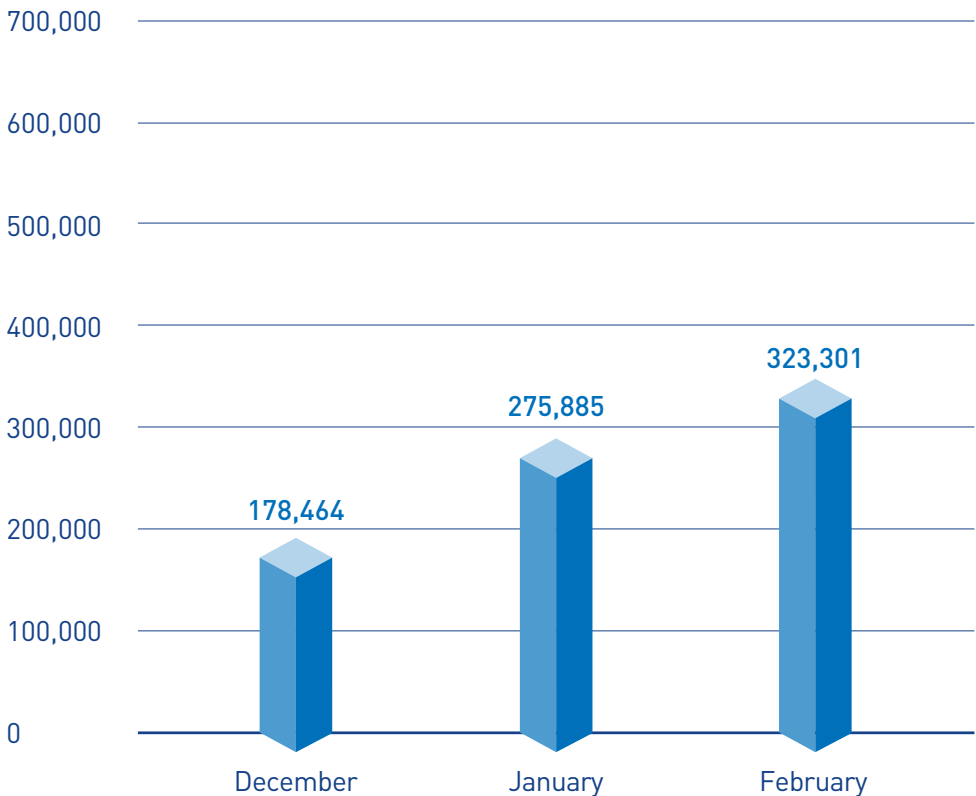
* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

03

Mobile Malware Statistics

In February 2016, 323,301 mobile malware were detected as shown in Figure 1-4.



[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in February 2016. Android-PUP/SmsPay was the most distributed malware with 70,760 of the total.

[Table 1-2] Top 10 Mobile Malware Threats in February 2016 (by alias)

Rank	Alias from AhnLab	No. of detections
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

SECURITY ISSUE

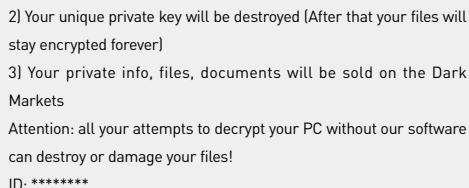
New HydraCrypt Ransomware Appears

SECURITY ISSUE

New HydraCrypt Ransomware Appears

With new or variants of ransomware sprouting up all over the world in increasing numbers, a new HydraCrypt ransomware has been discovered being distributed via the Angler exploit kit.

HydraCrypt ransomware generates files, writes to registry, deletes the system recovery point, and creates a connection to a C&C server. In addition, a README~.txt file is created in the folder that is targeted by HydraCrypt for encryption, as shown in Figure 2-1.

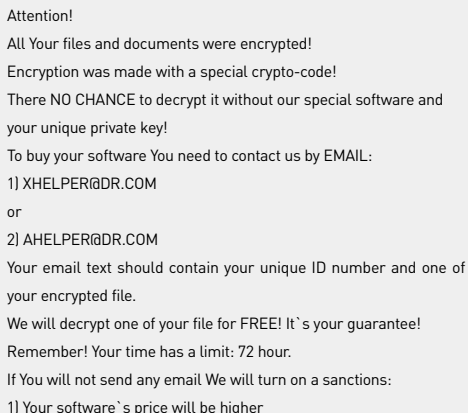


2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
3) Your private info, files, documents will be sold on the Dark Markets
Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!
ID: *****

Figure 2-1 | README_DECRYPT_HYDRA_ID_~.txt

As shown in Figure 2-1, HydraCrypt makes a threat also seen in previously-spotted ransomware “Offline” and “Chimera”, setting a deadline of 72 hours to send an email before victim’s files are exposed. A unique ID value is displayed in the popup window that signals the system has been infected, and, like other types of ransomware, transmits the infected PC’s information to the C&C server.

Ransomware creators have continued to profit from designing and distributing ransomware that encrypts key files and restoring them in return for a ransom payment. Such malware are expected to continue to evolve and mutate in 2016,



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

and spread even more widely and fiercely. Files encrypted by a ransomware are generally impossible to restore, requiring extra care by users.

In order to prevent being damaged from ransomware, security updates for applications in use should always be applied and programs kept at their latest versions, and email from suspicious

senders should not be opened. Users should also avoid visiting certain ad sites or unwittingly downloading and installing unknown programs.

The relevant alias identified by V3 products, AhnLab's anti-virus program, is as below:

<Alias identified by V3 products>

Win-Trojan/Malpacked3.Gen



3

IN-DEPTH ANALYSIS

A Java-Based Cross-Platform Malware: Adwind

IN-DEPTH ANALYSIS

A Java-Based Cross-Platform Malware: Adwind

Adwind is a Java-based cross-platform malware that has infected over 400,000 systems across the globe recently. Variants of Adwind include Unrecom, JSocket and Alienspy. The Adwind family of malware are written in Java and appeared to have been created by the same attacker or at least a single group of conspirators, due to the similarities in interface and options they share.

Adwind was first discovered in 2013, but it had not largely been spared in South Korea until now. However, Adwind malware have been increasingly spotted in South Korea since October of 2015. Adwind currently makes up the lion's share of all Java malware currently being distributed in Korea, followed by Exploit and Agent.

This report reviews the major characteristics of Adwind malware by examining actual cases of Adwind infections.

1. Key features of Adwind malware

Adwind is a cross-platform malware that operates under Android, Mac, Linux and Windows operating systems. Adwind usually infects a system when a user executes a file attached to an email or a document, or via an exploit kit. The following illustrates a case of an Adwind infection.

A JAR (Java Archive) file is attached to a Microsoft Word document file, and an icon embedded in the main body as shown in Figure 3-1 entices the user to click on it. When the user opens the file, a malicious JAR file is executed if Java is installed on the system, infecting the PC.

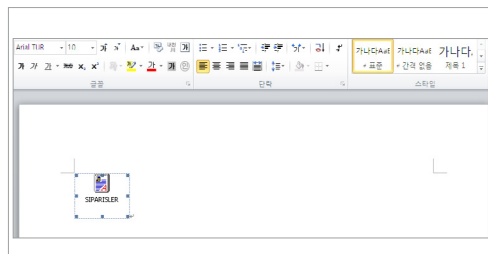


Figure 3-1 | JAR (Java Archive) file in a Word document

In the case of Android OS, a server is created as APK (Android Application Package), and JAR (Java Archive) for Mac, Linux and Windows OS. The server includes the basic functions plus plugins, if any are present. The infected PC or device attempts to establish a connection to the C&C IP, and the builder lying in wait at the C&C server can remotely issue commands to the infected PC.

The basic functions carried out by this particular malware under Windows OS environment are as follows.

- Displays a message popup on the infected PC
- Opens a designated URL (accessed via the infected PC's Web browser)
- Downloads and executes file from remote source
- Detects IP information of infected PC
- Attempts to run a RAT on the infected PC (rerun, update, log out, delete)

The malware can also carry out additional tasks via plugins. Features of the malware can be expanded via the use of different types of plugins, with the most common types as follows.

- Transmit Webcam images
- Keylogging
- Theft of email or FileZilla data (login information)
- Hijack browser information (Web site IDs and passwords stored on the browser)
- Run console

2. Adwind builder analysis

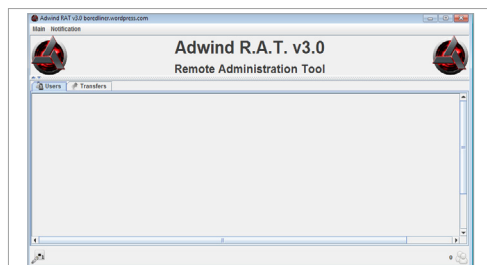


Figure 3-2 | Adwind 3.0 client screen

Adwind 3.0, reviewed by this report, includes a function for logging in with a user ID and password registered with the malware's original designer. A successful login will display an interface screen as shown in Figure 3-2.

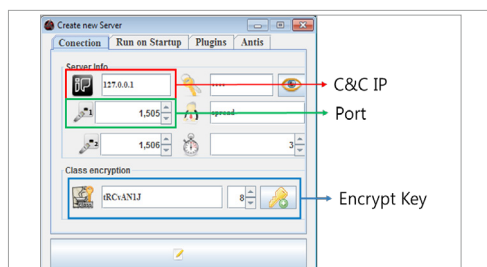
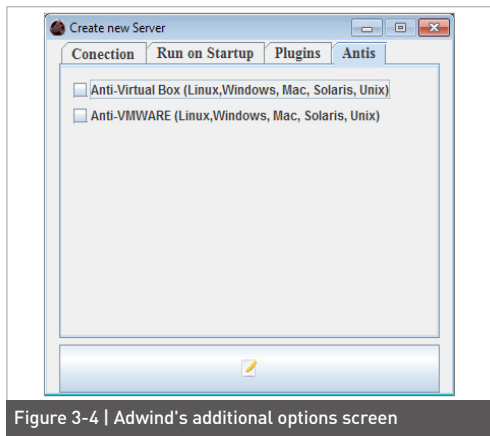


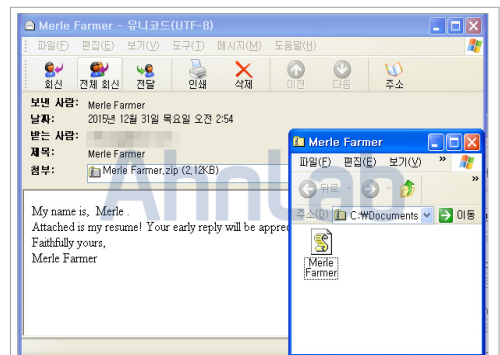
Figure 3-3 | Creating a new Adwind server file

As Adwind creates a server (a malicious JAR file installed on the infected PC), the C&C (client IP) and two ports (default and optional) are inputted. A randomizer key labeled "Class encryption" is used to encrypt Adwind Class, a class file that carries out malicious functions if decoded and run.

In addition, Adwind features anti-VM and anti-Virtual Box options, as show in Figure 3-4.



When a PC is infected by Adwind, a connection is made to the client (builder) as shown in Figure 3-6. IP information, system name, operating system, RAM information, JRE version and port number are displayed, and the attacker can issue commands to control the infected PC.



Adwind Builder not only includes the JAR files that acts as the basic RAT, but a downloader that accesses and downloads a file from a designated address, and a feature that creates a JAR file that acts as a binder, malware that remains on the infected system and allows remote access.

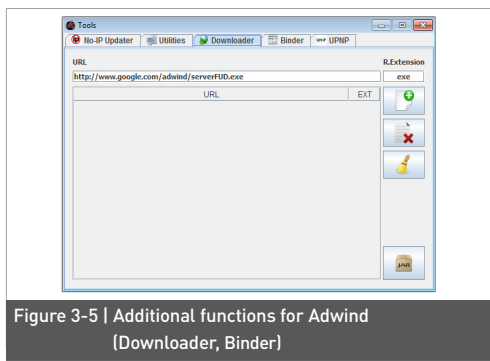


Figure 3-6 | Screen showing an infected PC

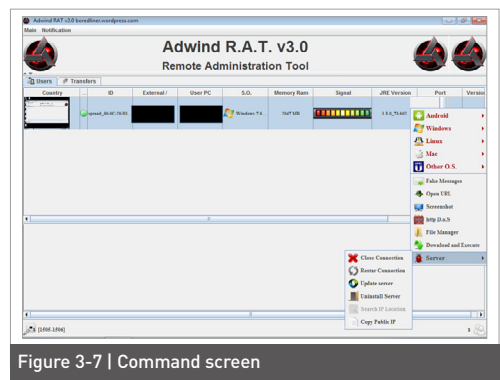


Figure 3-7 | Command screen

3. Adwind structure

Adwind's structure and the role of each component are as follows.

An analysis of the extracted code from Principal.Class shown in Figure 3-12 indicates the presence of processes for verifying and loading plugins, and checking anti-VM and anti-Virtual Box.

```

Constants.attrs = {
    Constants.attrs.put("urlpath", server.getServerPath());
}
catch (Exception ex) {}

public Principal() throws Exception
{
    try {
        @Manager.getLookedFile(@Manager.getLookedFile(Constants.class));
        @Manager.put("AuditorsClass", @Manager.get("AuditorsClass", @AuditorsClass));
        catch (ClassNotFoundException ex) {} catch (InstantiationException ex) {} catch (IllegalAccessException ex) {}

    public void init()
    {
        try {
            loadPlugins();
            boolean success = @Boolean.parseBoolean(Constants.getProperty("success"));
            boolean idok = @Boolean.parseBoolean(Constants.getProperty("idok"));
            if (idok) {
                @Boolean.parseBoolean(Constants.getProperty("idok"));
                System.exit(-1);
            }
            if (success) {
                @Boolean.parseBoolean(Constants.getProperty("success"));
                System.exit(-1);
            }
            Constants.attrs.put("urlpath", Constants.getProperty("urlpath"));
            String url = Constants.getProperty("url");
            String password = Constants.getProperty("password");
            int port1 = Integer.parseInt(Constants.getProperty("port1"));
            int port2 = Integer.parseInt(Constants.getProperty("port2"));
            int delay = Integer.parseInt(Constants.getProperty("delay")) * 1000;
            boolean installer = @Boolean.parseBoolean(Constants.getProperty("install"));
            String name = "...";
            if (installer) {
                @Boolean.parseBoolean(Constants.getProperty("install"));
                String name = Constants.getProperty("name");
            }
        }
    }
}

```

Figure 3-12 | Extracted Principal.Class

5. Unrecom builder analysis

Unrecom is an Adwind-family malware that, like Adwind, is operated using an ID and password that is verified by the malware's original creator after payment.

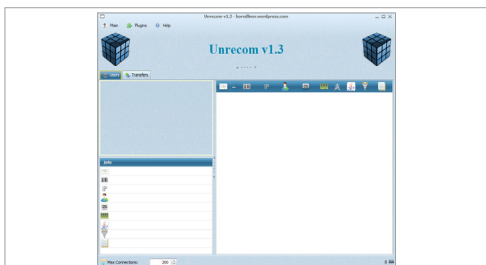


Figure 3-13 | Unrecom client command screen

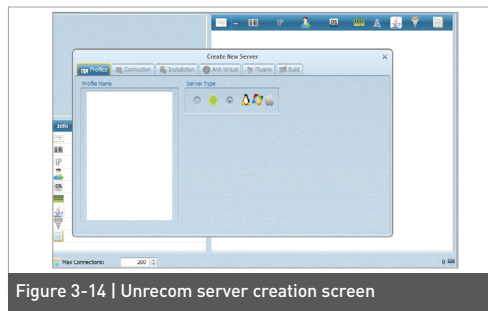


Figure 3-14 | Unrecom server creation screen

Like Adwind, Unrecom is a Java cross-platform malware that creates servers on Windows, Linux, Mac and Android environments.

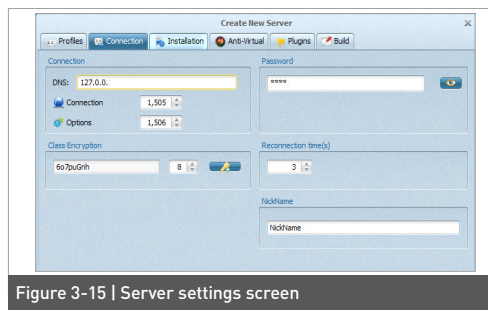


Figure 3-15 | Server settings screen

As is the case with Adwind, Unrecom also allows the controller to set a class password string and connection IP (C&C), and features anti-VM and anti-Virtual Box functions. The interface is simpler than Adwind. The primary difference between the two malware is the ability to store config settings in the build tab, allowing previously-used settings to be loaded. Downloader and binder functions, however, are not offered.

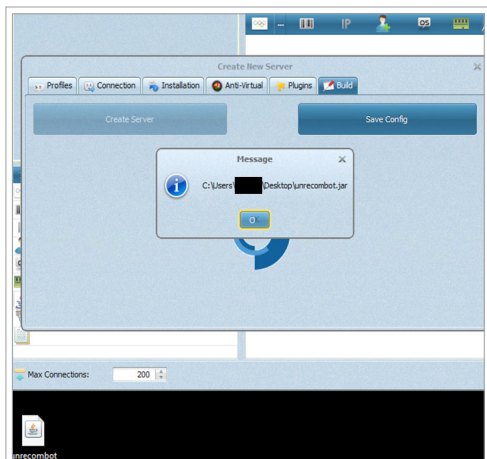


Figure 3-16 | Popup message indicating a successful JAR file creation

When a server file based on Windows, Linux or MAC OS environments is generated, a JAR (Java Archive) file is generated. An APK file is created on an Android system.

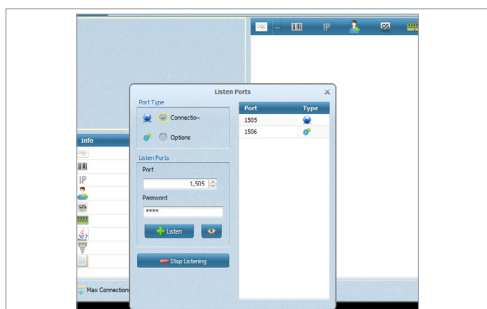


Figure 3-17 | Port Open

Like Adwind, Unrecom also uses two ports (default and optional). When the server is created, the default ports are set at 1505 and 1506. Similar basic

functions, features and default values between Adwind and Unrecom appear to point to the same designer.

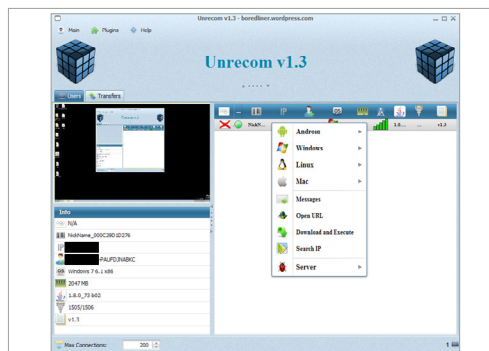


Figure 3-18 | Infection, and menu enabled after infection

Unrecom sends a similar set of information to its client as Adwind, and displays a similar menu. These are additional indications that Unrecom, Adwind, JSocket and Alienspy are either one and the same or are connected in some fashion.

6. Unrecom server analysis

The server generated by Unrecom's builder as a root folder as shown in Figure 3-19.

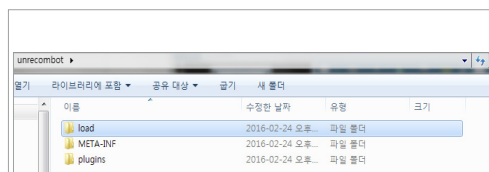


Figure 3-19 | Root folder structure of the server created by Unrecom

The basic structure is the same as that of Adwind. However, the use of plugins may alter the folder.

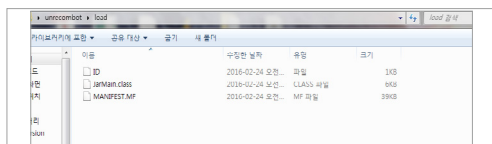


Figure 3-20 | Load folder

The load folder includes the same ID, JarLoad(Main Class) and a single encoded file as Adwind. The JAR file structure from the builder is essentially the same, differing only in the interface. The plugins folder is identical to that of Adwind, as well.

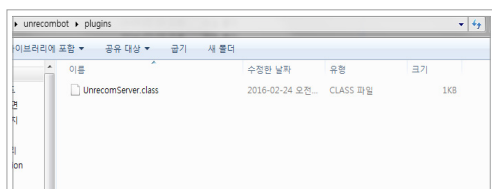


Figure 3-21 | plugins folder

Traditional malware written in Java were relatively simple and generally designed to exploit vulnerabilities, downloading and executing secondary malware. However, the recent types of Java-based malware such as Adwind and Unrecom have become more complex with larger modules that use remote access and obfuscation. In addition, the appearance of Adwind has led to a slew of similar malware such as Unrecom, designed to be able to execute a variety of functions with the addition of plugins.

Since being first discovered in 2013, the Adwind family of malware is potentially capable of proliferating widely due to its ability to attack across different platforms. Effective countermeasures must therefore be developed against Java-based malware.

AhnLab

ASEC REPORT

VOL.74
February, 2016

Contributors	ASEC Researchers
Editor	Content Creatives Team
Design	Design Team

Publisher	AhnLab, Inc.
Website	www.ahnlab.com
Email	global.info@ahnlab.com

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

©AhnLab, Inc. All rights reserved.