GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

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

Fidelis Threat Advisory #1013

RAT in a jar: A phishing campaign using Unrecom

May 21, 2014

Document Status: 1.0
Last Revised: 2014-05-21

Executive Summary

In the past two weeks, we have observed an increase in attack activity against the U.S. state and local government, technology, advisory services, health, and financial sectors through phishing emails with what appears to be a remote access trojan (RAT) known as Unrecom. The attack has also been observed against the financial sector in Saudi Arabia and Russia.

As Unrecom[1] is a comprehensive multi-platform Java-based remote access tool, currently not detected by most AntiVirus products, it presents a risk to a large number of potential victims, regardless of operating system. The following is a screenshot of the Unrecom RAT v.2.0 (Version in Spanish):

Over time, various reports in the community have documented the evolution of this tool. This evolution is to be expected, but its low detection rate, recent use this month through phishing emails campaigns against multiple sectors in the U.S. and association with past campaigns involving a variety of RATs captured our attention. The evolution of Unrecom RAT dates from its beginnings as a tool known as Frutas RAT, subsequently branded as Adwind RAT, and now Unrecom RAT.

In 2013, it was reported that Frutas RAT was used in phishing email campaigns against high profile companies in Europe and Asia in sectors such as finance, mining, telecom, and government[2].

Unrecom RAT provides the attacker with full control over the compromised system, once infected. It has some of the following capabilities:

- Collection of System Information (e.g. IP, OS version, memory RAM information, Java version, Computer Name, User account compromised, etc.)
- Upload & Execute additional malware, typically exploiting vulnerabilities derived from collected system information
- 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

In the past, variants of the DarkComet and AcromRAT malware have also been observed beaconing to the same Command & Control (CnC) servers used by the Unrecom RAT in this campaign.

This document will provide information about the recent phishing campaigns observed with this RAT and some of the network indicators.

Threat Overview

The increased threat activity against the U.S. state and local government, technology, advisory services, and health sectors in the past two weeks is of great concern to us as it is being carried through phishing emails with what appears to be a tool known as Unrecom RAT.

The phishing emails try to trick the users into thinking the emails are legitimate by attaching the RAT with the some of the following names: Payment Invoice.jar, Payment details.jar, POR#94586.zip/POR#94586.jar, INV#94586.zip/INV#94586.jar, Invitation.jar, reports-pdf.jar, US$25k.jar, and DBC_BANK_IMG_23456_156.jar, and Iremit_Transfer_Error_Page.jar.

Some of the email message subjects observed during this campaign are:

Subject:	Thank you
Subject:	FW: URGENT CONFIRMATION P/I #94578
Subject:	Invitation
Subject:	Payment details
Subject:	Transfer Investigation report
Subject:	US$25,000 TT COPY ATTACHED
Subject:	Remittance Error 2089/234- Reported lost of data (Complete and email back)
Subject:	Transfer error, kindly reverse to us.

It appears that the latest version of this RAT is 3.2 and is being sold at “unrecom[.]net” for $500 (Enterprise Version) and $200 (Full Version).

We find it interesting that on their website, the authors of this software recommend Unrecom RAT buyers to not scan created servers (malware deployed to Victim systems) at Virustotal nor Metascan. This is

indicative of the adaptive, counter-intelligence techniques being adopted as threat actors become aware that many security researchers use these services to gather threat intelligence.

Significantly, malware objects seen in previous campaigns like DarkComet and ArcomRAT[8] have also been observed beaconing to the same CnC servers Unrecom RAT is currently using. DarkComet is known to be a popular RAT used in threat activity in the Middle East [6,7].

Risk Assessment

A remote access tool provides an attacker with full control over the victim system. Once a system has been compromised, the attacker may install one or more backdoors. These backdoors provide a persistent foothold, using a separate command and control channel; allowing future access less likely to be correlated to the original activity.

Through its modular plugin framework, this particular tool lets the attacker obtain System Information (e.g. IP, OS version, memory RAM information, Java version, Computer Name, User account compromised, etc.), Upload & Execute additional malware, Capture Webcam, Remote Desktop, File Manager, Browser Password Recovery, Capture Microphone, Keylogger, etc.

Indicators and Mitigation Strategies

The following will present detailed information about some of the phishing emails observed and the attached malware:

1. Invitation.jar

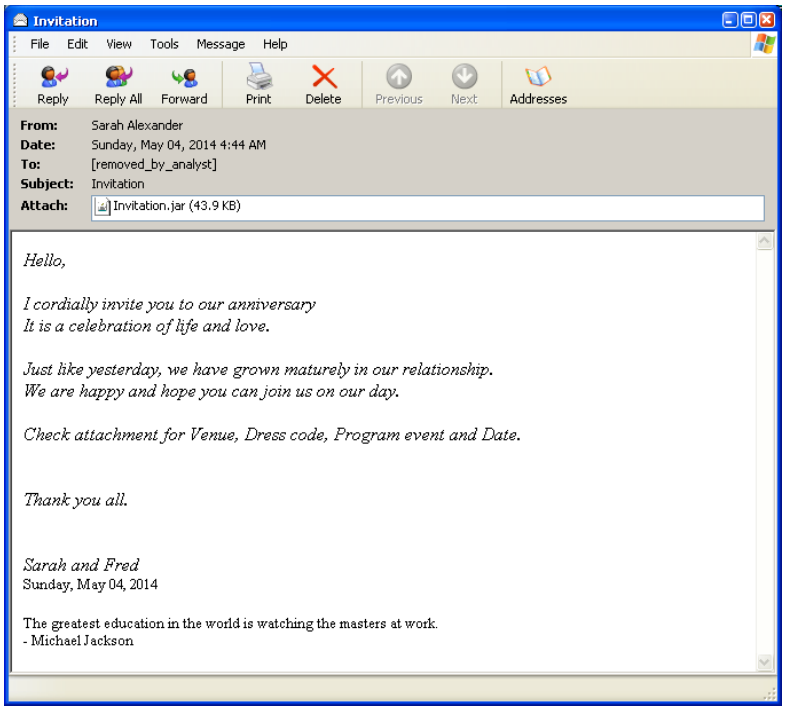
```
File Name:  Invitation.jar
File Size:  43866 bytes
MD5:        859c4c667dd0f44f80b60242d93c4b0f
SHA1:       40859bc18ea0ffa9bcf5af699336fbdbfd6be7f1
```

The “Invitation.jar” malware was sent in a phishing email that contained some of the following details:

From	Sarah Alexander <mthomas3@mybluelight[.]com>
Subject	Invitation
Date	Sun, 4 May 2014 08:44:53 GMT
Attachment	Invitation.jar
Reply-To	marvinflames@gmail.com
X-Originating-Ip	87.117.232[.]203
Message body	*Hello,* *I cordially invite you to our anniversary* *It is a celebration of life and love.* *Just like yesterday, we have grown maturely in our relationship.* *We are happy and hope you can join us on our day.* *Check attachment for Venue, Dress code, Program event and Date.* *Thank you all.*

	Sarah and Fred Sunday, May 04, 2014 The greatest education in the world is watching the masters at work. - Michael Jackson

The following is a screenshot of the email:



The “Invitation.jar” malware beaconed to “**magnumbiz.no-ip[.]biz**” over port “**1505**”.

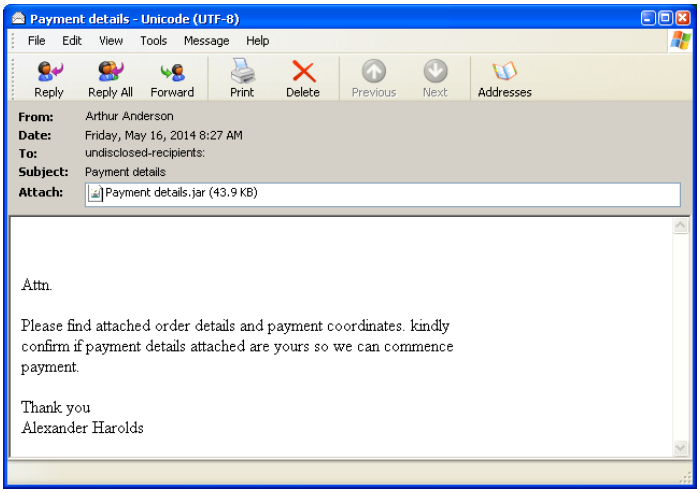
2. Payment details.jar

```
File Name:  Payment details.jar
File Size:  43887 bytes
MD5:        bd0aba05d8263fb1a9a3adcae01fc3b7
SHA1:       c60551e65cbe54899d1cd1f637b572455dc33b1b
```

The “Payment details.jar” malware was sent in a phishing email that contained some of the following details:

From	Arthur Anderson <alexanderharolds@arthurandersen[.]com>
Subject	Payment details
Date	Fri, 16 May 2014 12:27:27 +0000
Attachment	Payment details.jar
Reply-To	<alexanderharolds@arthurandersen[.]com>
Return-Path	alexanderharolds@arthurandersen[.]com
User-Agent	Internet Messaging Program (IMP) H5 (6.1.4)
Message body	Attn. Please find attached order details and payment coordinates. kindly confirm if payment details attached are yours so we can commence payment. Thank you Alexander Harolds

The following is a screenshot of the email:



The “Payment details.jar” malware beaconed to “**morechedder.no-ip[.]org**” over port “**100**”.

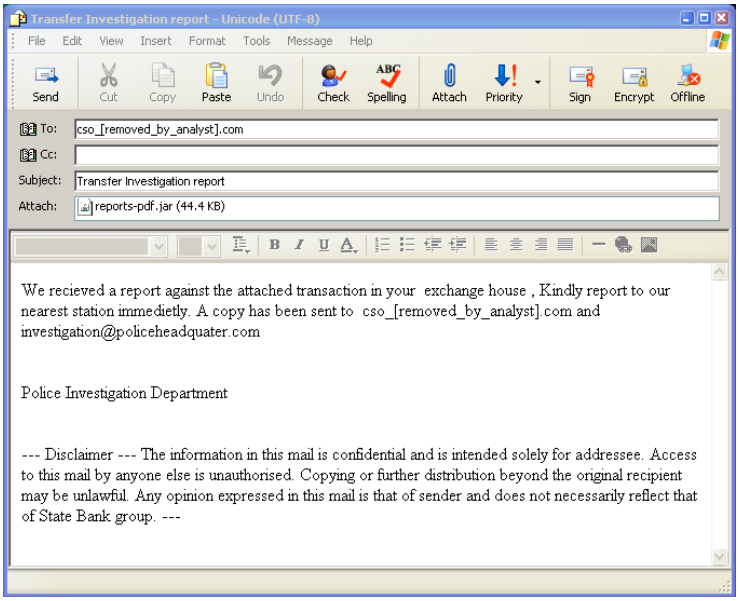
3. reports-pdf.jar

```
File Name:  reports-pdf.jar
File Size:  44237 bytes
MD5:        39ad2cab9829ff6a1107b97f1496b499
SHA1:       1e9ab96ace86a45a33c4ff88a97186efb55e51fb
```

The “reports-pdf.jar” malware was sent in a phishing email that contained some of the following details:

From	"Police Department" <cmmds@sbt.co[.]in>
Subject	Transfer Investigation report
Date	Mon, 05 May 2014 07:34:35 -0700
Attachment	reports-pdf.jar
Message body	We recieved a report against the attached transaction in your exchange house , Kindly report to our nearest station immedietly. A copy has been sent to cso_*[removed_by_analyst]*.com and investigation@policeheadquater[.]com Police Investigation Department --- Disclaimer --- The information in this mail is confidential and is intended solely for addressee. Access to this mail by anyone else is unauthorised. Copying or further distribution beyond the original recipient may be unlawful. Any opinion expressed in this mail is that of sender and does not necessarily reflect that of State Bank group. ---

The following is a screenshot of the email:



The “reports-pdf.jar” malware beaconed to “**184.22.201[.]27**” over port “**3030**”.

4. US$25k.jar

```
File Name:  US$25k.jar
File Size:  43853 bytes
MD5:        ccfbc03a5beb1adb66f058b1f5a84d98
SHA1:       cfd0a4d6535f6323e4423bbd07027d294887ea25
```

The “US$25k.jar” malware was sent in a phishing email that contained some of the following details:

From	"Milker Trading Ltd" <rbecerra@pauluhn.com[.]mx>
Subject	US$25,000 TT COPY ATTACHED
Date	Wed, 14 May 2014 03:28:43 -0500
Attachment	US$25k.jar
X-Get-Message-Sender-Via\ authenticated_id	rbecerra@pauluhn.com[.]mx
X-AntiAbuse	Sender Address Domain - pauluhn.com[.]mx
User-Agent	SquirrelMail/1.4.22
Message body	Hello, We have not received any email from you again regarding the previous Inquiry. Please see attached the TT Copy of the USD25,000 as directed by our sales Manager. Kindly check and confirm to me the date of dispatch of our last order. Regards Milker Trading Ltd Auggenthal 1 94140 Ering Mexico.

The “US$25k.jar” malware beaconed to “**toba.no-ip[.]biz**” over port “**1505**”.

5. Payment Invoice.jar

```
File Name:  Payment Invoice.jar
File Size:  44237 bytes
MD5:        44f011702ff80b337124d4879607f6b1
SHA1:       b2474bffcbeaabdd111f3909075fc7f556901c62
```

The “Payment Invoice.jar” malware was sent in a phishing email that contained some of the following details:

From	Johnson Kelly <johnsonkelly52@live[.]com>
Subject	Thank you
Date	Sat, 10 May 2014 10:45:55 -0700
Attachment	Payment Invoice.jar
Return-Path	johnsonkelly52@live[.]com
Message	Here is the invoice

The “Payment Invoice.jar” malware beaconed to “**greengreen1.no-ip[.]biz**” over port “**100**”.

6. INV#94586.jar

```
File Name:  INV#94586.jar
File Size:  43885 bytes
MD5:        06c2760060d41533b36572ae3c1ba2df
SHA1:       0350f53a821933e05bf82508b1e458c83d37b7c8
```

The “INV#94586.jar” malware was sent in a phishing email that contained some of the following details:

From	Diosdado <kdiosdado@lilbello[.]com>
Subject	FW: URGENT CONFIRMATION P/I #94578
Date	11 May 2014 19:10:47 -0700
Attachment	INV#94586.zip
Disposition-Notification-To	sales@ttc-qroup[.]com
Message body	Good Day, *Please find the attached document.* Regards, Diosdado Procurement Officer Mobile: +966 54 073 5573 Tel.: +966 13 341 9915, Ext. 283 Fax: +966 13 340 4869 Email: *diosdado@lilbello[.]com* P.O Box 11976, Jubail - 31961. SA

The “INV#94586.jar” malware beaconed to “**192.95.21[.]44**” over port “**1511**”.

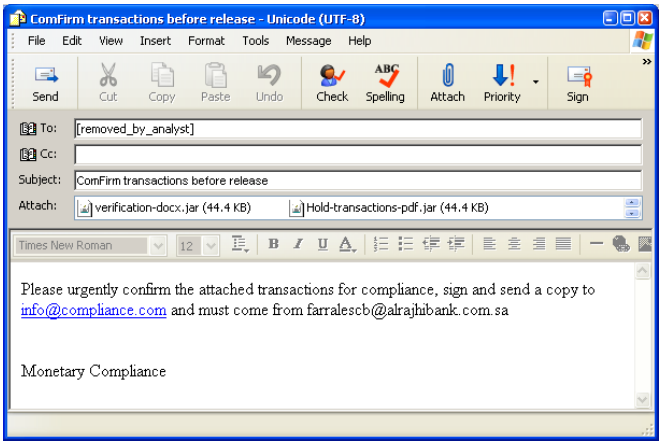
- Hold-transactions-pdf.jar, and verification-docx.jar

```
File Name:  Hold-transactions-pdf.jar, and verification-docx.jar
File Size:  44292 bytes
MD5:        bc84b115d98988c5489d6acf96046b78
SHA1:       33731d6a7360719566391a7c4395abb090d02d0f
```

The “Hold-transactions-pdf.jar/verification-docx.jar” malware was sent in a phishing email that contained some of the following details:

From	"Compliance Verification" <abdul.razzak@uaeexchange[.]com>
Subject	ComFirm transactions before release
Date	Sun, 18 May 2014 16:31:12 -0700
Attachment	Hold-transactions-pdf.jar, and verification-docx.jar
Message body	Please urgently confirm the attached transactions for compliance, sign and send a copy to info@compliance.com and must come from farralescb@alrajhibank.com.sa Monetary Compliance

The following is a screenshot of the email:



The “Hold-transactions-pdf.jar/verification-docx.jar” malware beaconed to “**184.22.201[.]27**” over port “**3030**”.

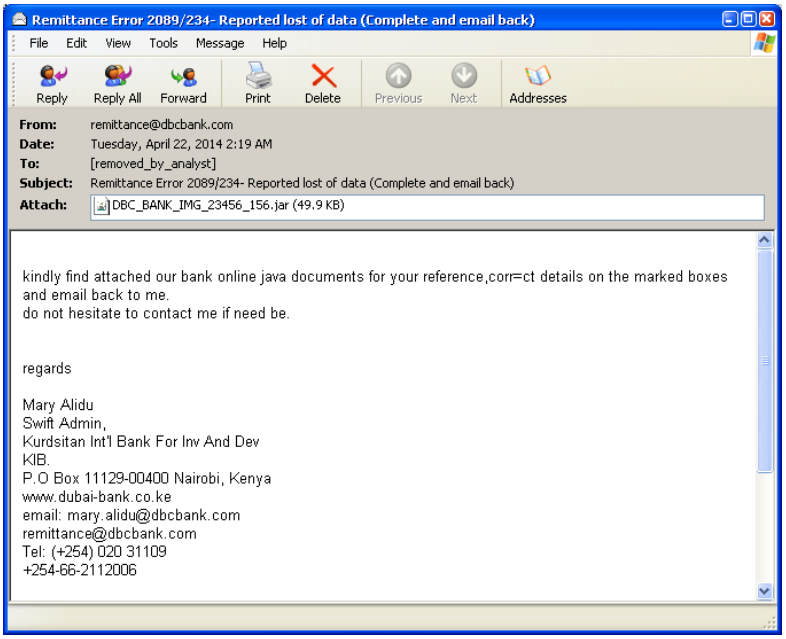
7. DBC_BANK_IMG_23456_156.jar

```
File Name:  DBC_BANK_IMG_23456_156.jar
File Size:  50508 bytes
MD5:        fca329c46f50e031597babe07fee46a8
SHA1:       5c1a2351749c864a38473aafe1146de4eb4de40d
```

The “DBC_BANK_IMG_23456_156.jar” malware is a corrupted file, but it was sent in a phishing email that contained some of the following details:

From	"remittance@dbcbank[.]com" <remittance_dbcbank1@aol[.]com>
Subject	Remittance Error 2089/234- Reported lost of data (Complete and email back)
Date	Tue, 22 Apr 2014 02:19:27 -0400 (EDT)
Attachment	DBC_BANK_IMG_23456_156.jar
X-MB-Message-Source	WebUI
X-mailer	SCM
X-Originating-IP	41.138.184[.]85
Message body	kindly find attached our bank online java documents for your reference,corr=ct details on the marked boxes and email back to me. do not hesitate to contact me if need be. regards Mary Alidu Swift Admin, Kurdsitan Int'l Bank For Inv And Dev KIB. P.O Box 11129-00400 Nairobi, Kenya www.dubai-bank.co.ke email: mary.alidu@dbcbank.com remittance@dbcbank.com Tel: (+254) 020 31109 +254-66-2112006 IMPORTANT: This e-mail (including all attachments) is intended solely for<B= the use of individual or entity to whom it is addressed and may contain confidential and privileged information. If you have received it in error,<=r> please contact us immediately by return e-mail and delete it from your system. Please note that the sender shall not be liable for the improper<BR= this communication , nor for any delay in its receipt or damage to your system.

The following is a screenshot of the email:



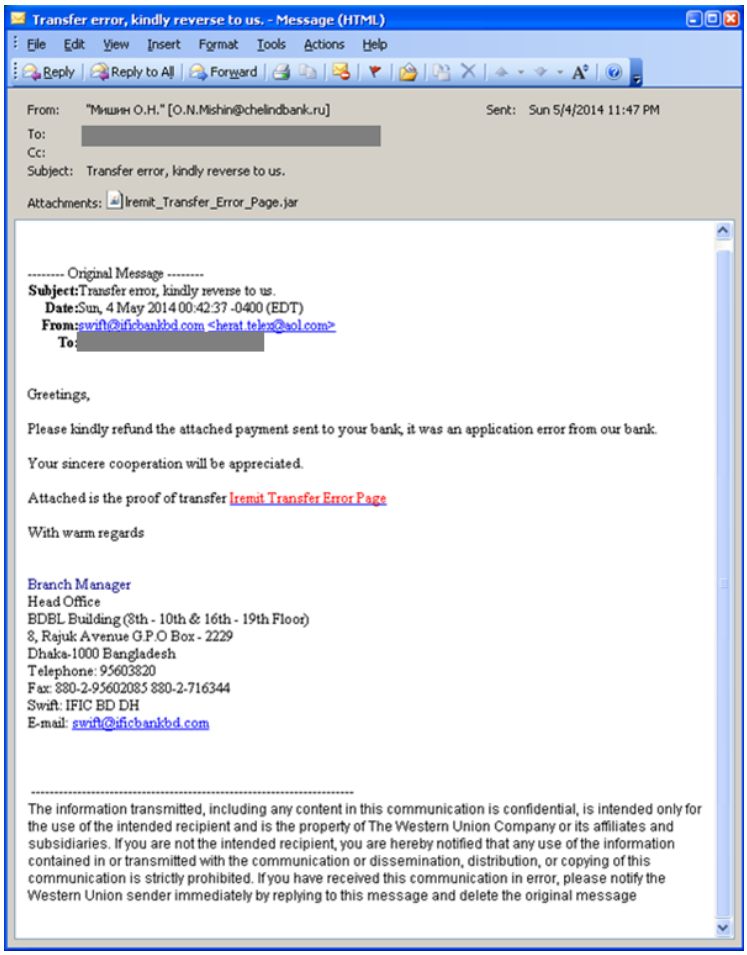
8. Iremit_Transfer_Error_Page.jar

```
File Name:  lremit_Transfer_Error_Page.jar
File Size:  43861 bytes
MD5:        8811a91e0ef5b181b1f0433d913faaaf
SHA1:       ca771a56a8e63565b0638e84bac0db0e6c0fadf8
```

The “Iremit_Transfer_Error_Page.jar” malware was sent in a phishing email that contained some of the following details:

From	"Мишин О.Н." [O.N.Mishin@chelindbank[.]ru]
Subject	Transfer error, kindly reverse to us.
Date	Mon, 5 May 2014 09:47:22 +0600
Attachment	Iremit_Transfer_Error_Page.jar
Return-Path	<O.N.Mishin@chelindbank[.]ru>
Message body	-------- Original Message -------- Subject: Transfer error, kindly reverse to us. Date: Sun, 4 May 2014 00:42:37 -0400 (EDT) From: swift@ificbankbd.com <herat.telex@aol.com> To: [removed_by_analyst] Greetings, Please kindly refund the attached payment sent to your bank, it was an application error from our bank. Your sincere cooperation will be appreciated. Attached is the proof of transfer Iremit Transfer Error Page With warm regards Branch Manager Head Office BDBL Building (8th - 10th & 16th - 19th Floor) 8, Rajuk Avenue G.P.O Box – 2229 Dhaka-1000 Bangladesh Telephone: 95603820 Fax: 880-2-95602085 880-2-716344 Swift: IFIC BD DH E-mail: swift@ificbankbd.com --- The information transmitted, including any content in this communication is confidential, is intended only for the use of the intended recipient and is the property of The Western Union Company or its affiliates and subsidiaries. If you are not the intended recipient, you are hereby notified that any use of the information contained in or transmitted with the communication or dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the Western Union sender immediately by replying to this message and delete the original message

The following is a screenshot of the email:



"**Iremit Transfer Error Page**", in the above email, has a link pointing to "http://radaxis[.]by/images/sola/httpsiremit.com.aui-remit-to-the-philippines-cheapest-remittance-service-for-pinoy-in-australi.zip"

The "Iremit_Transfer_Error_Page.jar" malware beaconed to "**resultpage92.no-ip[.]biz**" over port "**5353**".

Summary of Indicators:

Email Subject	Filename	MD5 File Hash	CnC	Port
Invitation	Invitation.jar	859c4c667dd0f44f80b60242d93c4b0f	magnumbiz.no-ip[.]biz	1505
Payment details	Payment details.jar	bd0aba05d8263fb1a9a3adcae01fc3b7	morechedder.no-ip[.]org	100
Transfer Investigation report	reports-pdf.jar	39ad2cab9829ff6a1107b97f1496b499	184.22.201[.]27	3030
US$25,000 TT COPY ATTACHED	US$25k.jar	ccfbc03a5beb1adb66f058b1f5a84d98	toba.no-ip[.]biz	1505
Thank you	Payment Invoice.jar	44f011702ff80b337124d4879607f6b1	greengreen1.no-ip[.]biz	100
INV#94586.jar	FW: URGENT CONFIRMATION P/I #94578	06c2760060d41533b36572ae3c1ba2df	192.95.21[.]44	1511
ComFirm transactions before release	Hold-transactions-pdf.jar verification-docx.jar	bc84b115d98988c5489d6acf96046b78	184.22.201[.]27	3030
Remittance Error 2089/234-Reported lost of data (Complete and email back)	DBC_BANK_IMG_23456_156.jar	fca329c46f50e031597babe07fee46a8	N/A	N/A
Transfer error, kindly reverse to us.	Iremit_Transfer_Error_Page.jar	8811a91e0ef5b181b1f0433d913faaaf	resultpage92.no-ip[.]biz	5353
Remittance Error 2089/234-Reported lost of data (Complete and email back)	DBC_BANK_IMG_23456_156.jar	8842ce373c910c012a0aa58e37b3d080	magawalton.no-ip[.]biz	1505

Further Analysis And Correlation

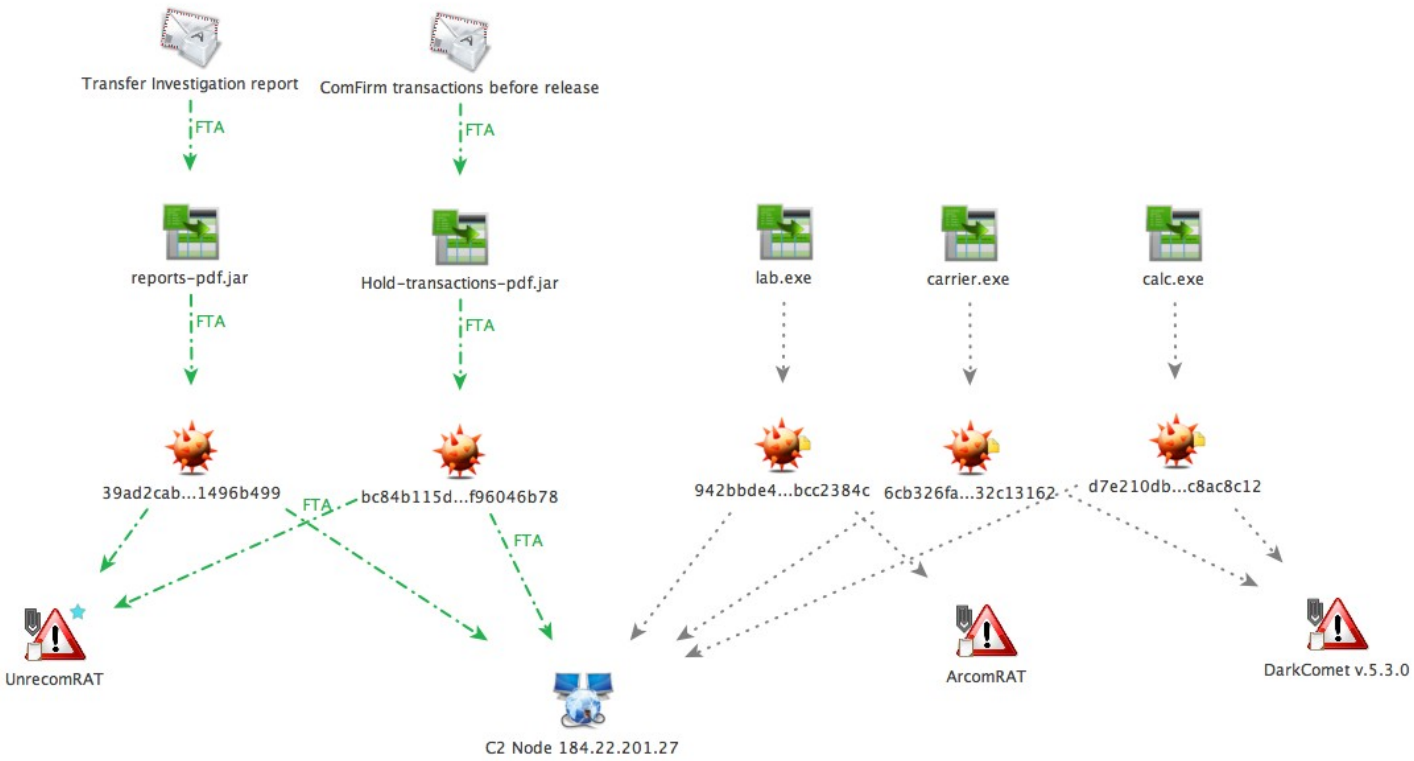
One simple example of how the emails in this phishing campaign are related is that the Command and Control node (184.22.201[.]27) that the malware communicates with is shared by two separate phishing emails in this campaign, as shown in the diagram below.

Beginning at the top of the diagram and working down, on the left side of the diagram are two phishing emails, the details of which are referenced in the pages above as item numbers 2 & 3. Of note, these phishing emails were sent to users at two separate and unrelated organizations. As you can see, when compared to each other, these messages appear completely unrelated, other than the fact they both contain jar files that are sophomorically "obfuscated" as pdf.jar files.

Note that both the subjects, "Transfer investigation report" and "Confirm transactions before release" are comparatively unique as are the senders , "Police Department" cmmds@sbt.co[.]in and Arthur Anderson alexanderharolds@arthurandersen[.]com. In addition to the fact that the emails share no attributes, the malicious attachments are also unrelated.

Finally, and of most interest in this diagram, the central node at the bottom of the diagram, represents the Command and Control node (184.22.201[.]27) used by these two examples. While this shared resource is noteworthy, of particular interest is that it has also been used in other campaigns.

On the right side of the diagram are files used in two other campaigns using the ArcomRAT[8] and DarkComet[6,7], The fact that they share the same command-and-control infrastructure as the UnrecomRat campaign make this central node all the more interesting.



The Fidelis Take

This paper seeks to highlight this campaign targeting significant enterprises worldwide, utilizing a Java-based RAT malware that is currently detected by a small set of security tools. We are publishing these indicators so that others in the security research community can monitor for this activity and potentially correlate against other campaigns and tools that are being investigated.

Fidelis XPS™, the Advanced Threat Defense solution from General Dynamics Fidelis Cybersecurity Solutions detects all of the activity documented in this paper. The Fidelis Threat Research Team 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. Adwind RAT Rebranding, Nov 2013: http://www.crowdstrike.com/blog/adwind-rat-rebranding/index.html
2. Targeted Attacks Delivering Fruit, Aug 2013: http://www.symantec.com/connect/blogs/targeted-attacks-delivering-fruit
3. Remote Access Tool Takes Aim with Android APK Binder, Jul 2013: http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder
4. Old Java RAT Updates, Includes Litecoin Plugin, Apr 2014: http://blog.trendmicro.com/trendlabs-security-intelligence/old-java-rat-updates-includes-litecoin-plugin/
5. Cross-Platform Frutas RAT Builder and Back Door, Feb 2013: http://www.symantec.com/connect/blogs/cross-platform-frutas-rat-builder-and-back-door
6. DarkComet Analysis – Understanding the Trojan used in Syrian Uprising, Mar 2012: http://resources.infosecinstitute.com/darkcomet-analysis-syria/
7. DarkComet RAT - It is the END!, Jul 2012: http://www.symantec.com/connect/blogs/darkcomet-rat-it-end
8. Tsunami Warning Leads to Arcom RAT, Nov 2012 http://blog.trendmicro.com/trendlabs-security-intelligence/tsunami-warning-leads-to-arcom-rat/