RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

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

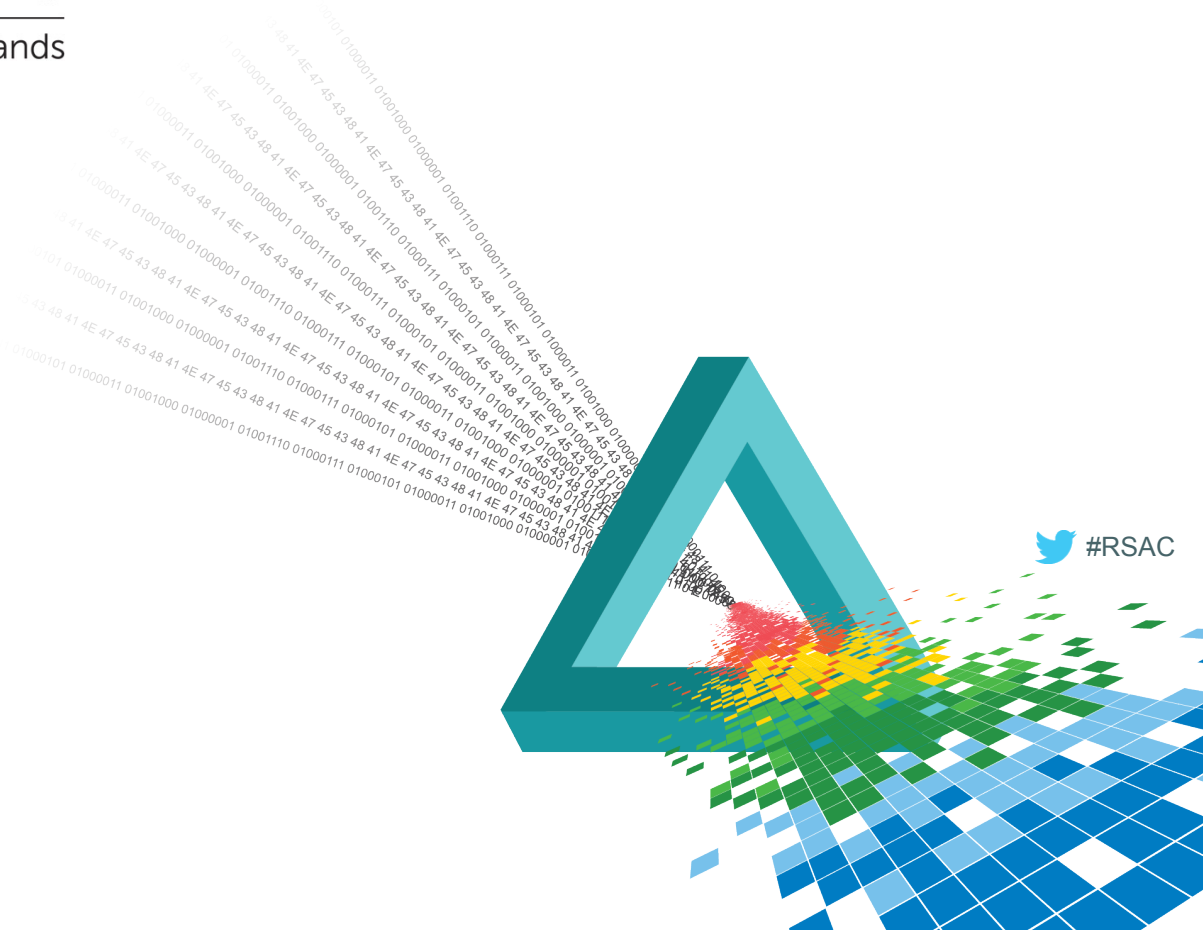
Sun Huang

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

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/IceIX/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

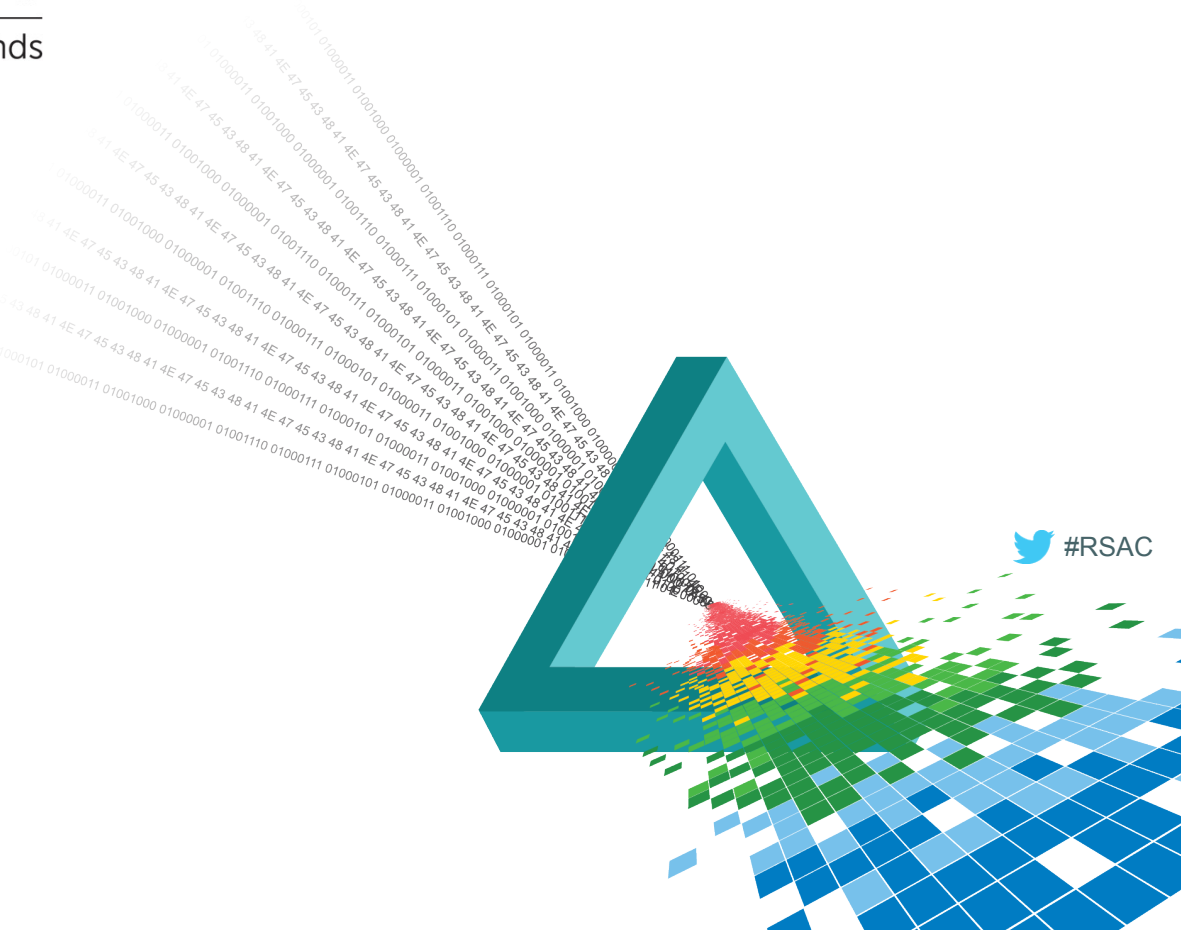
- Endpoint ownership, data extraction & exfiltration
  - Are NOT capable of developing own trojans
  - Use whatever off-the-shelf trojans they can get hold of
  - Most used trojan features:
    - Web inject – steals specific banking accounts
    - Wallet stealer – steals virtual currencies
- Also phish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



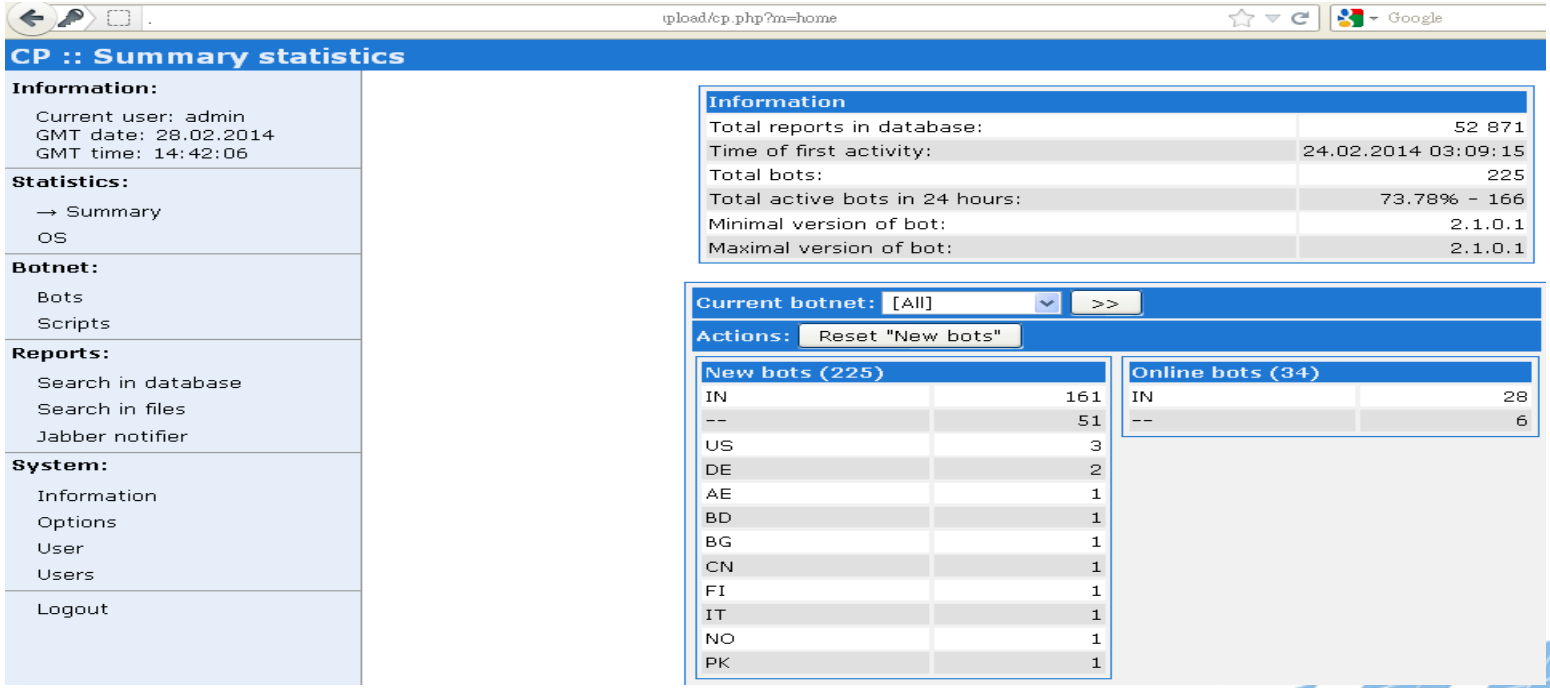
Crimeware usage

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.

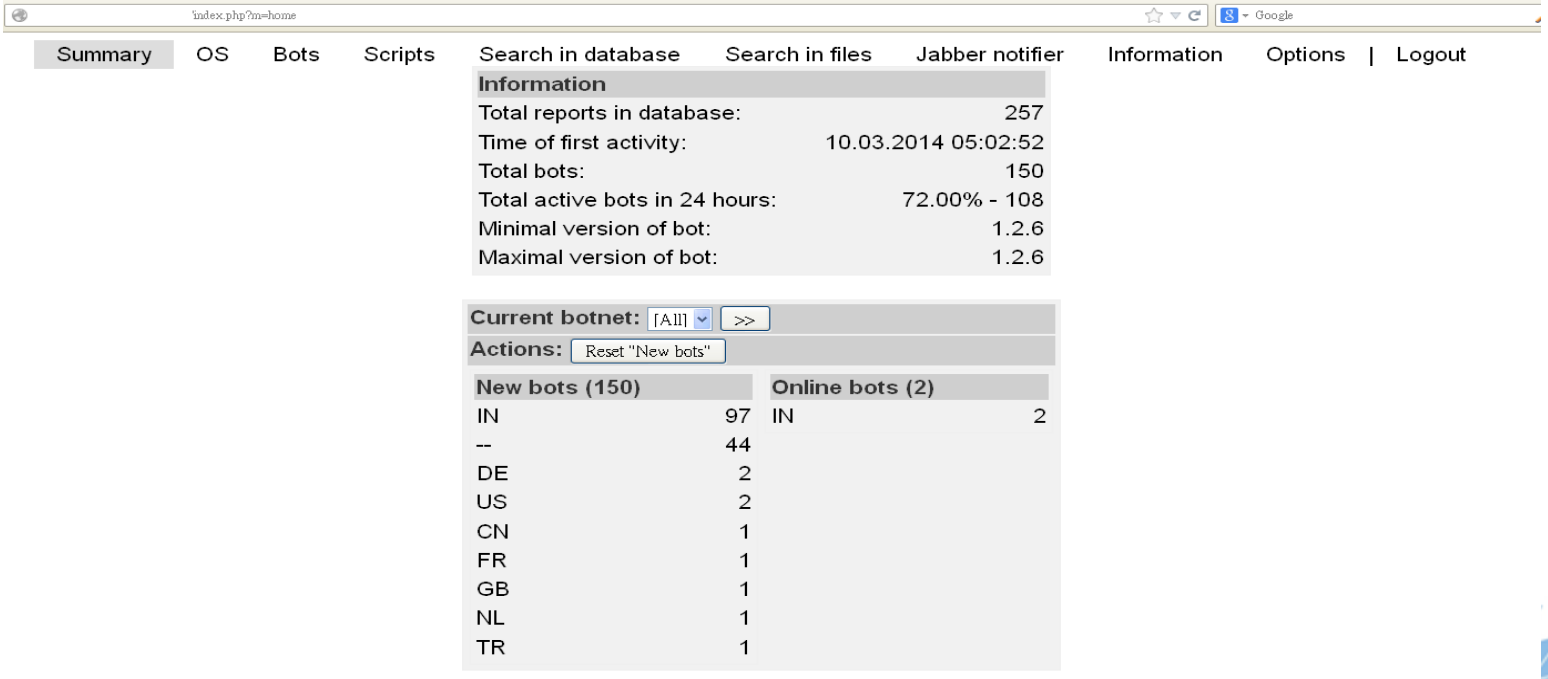
Banking trojan panels

- Zeus



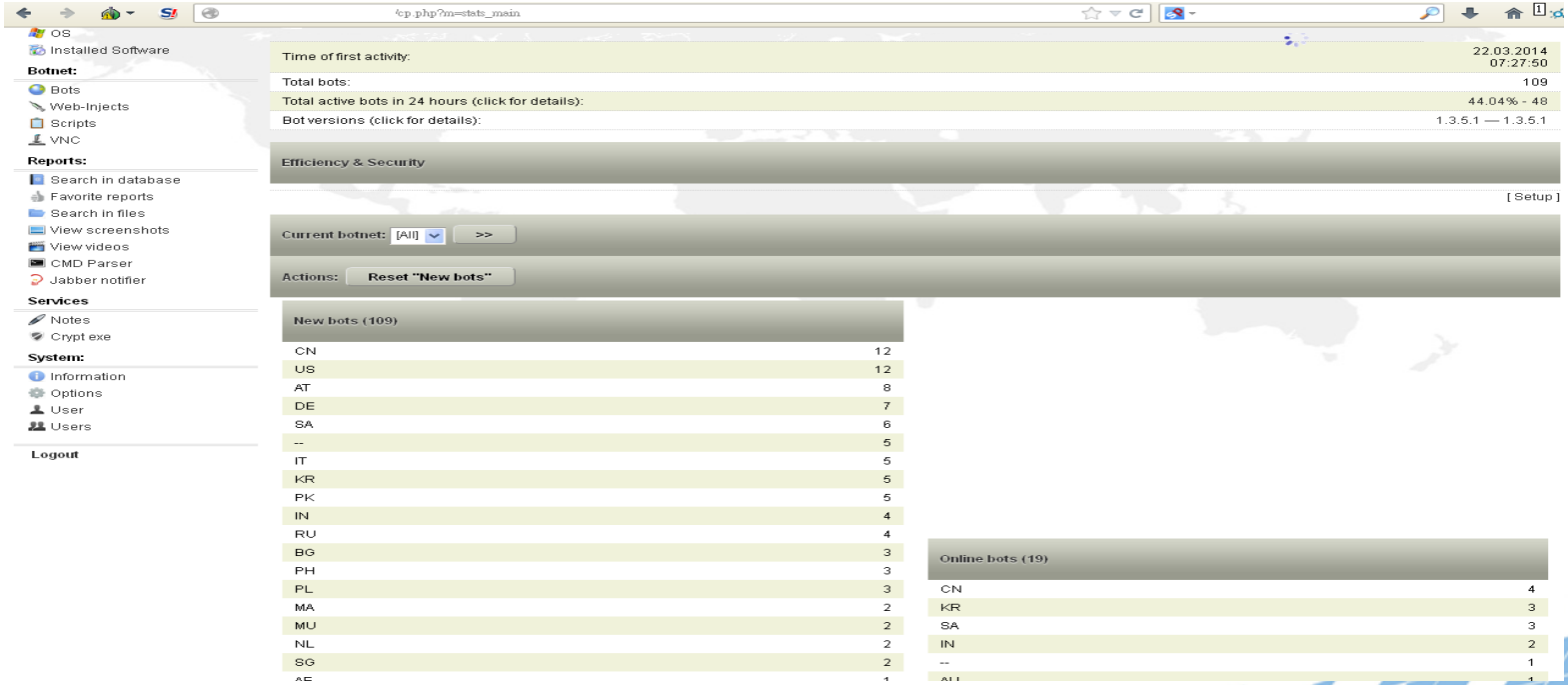
Banking trojan panels

- Zeus/ICEIX



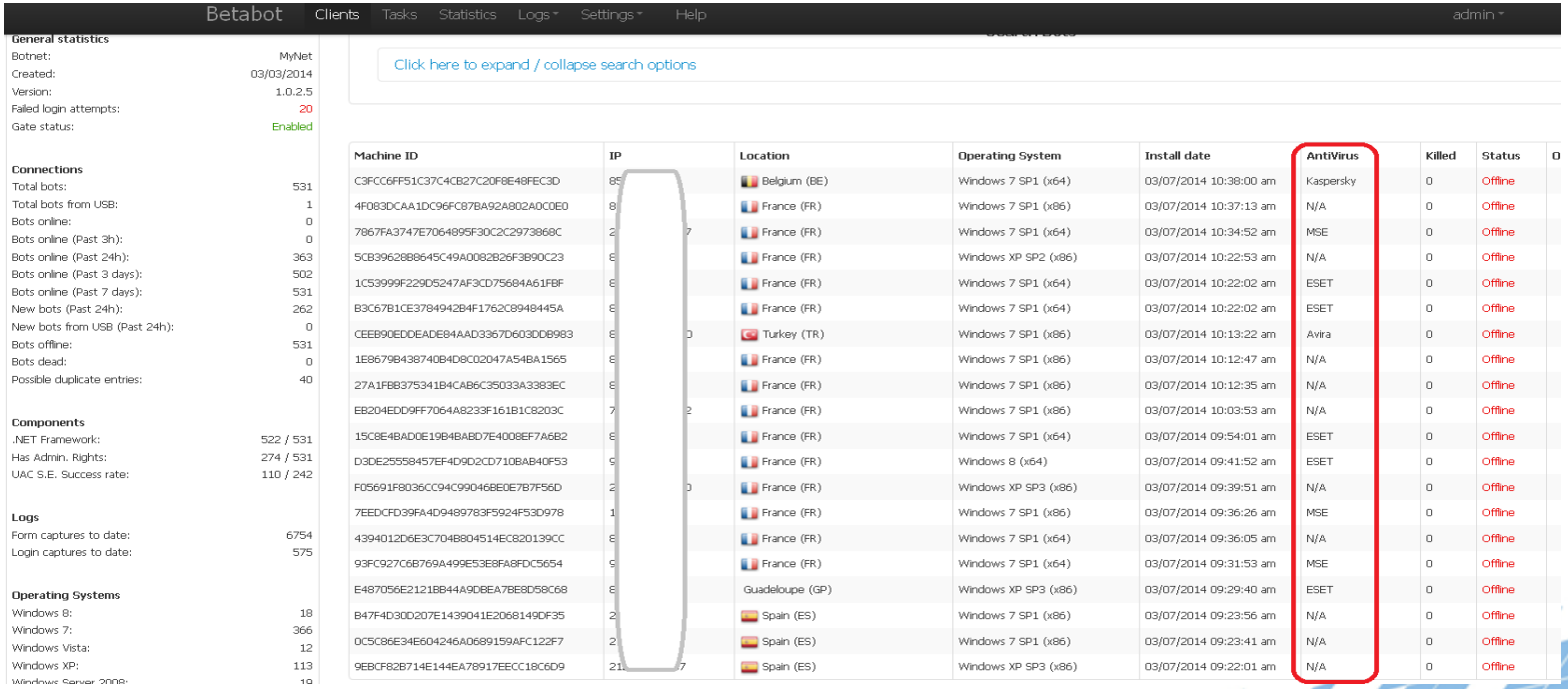
Banking trojan panels

- Zeus/ICEIX/Citadel



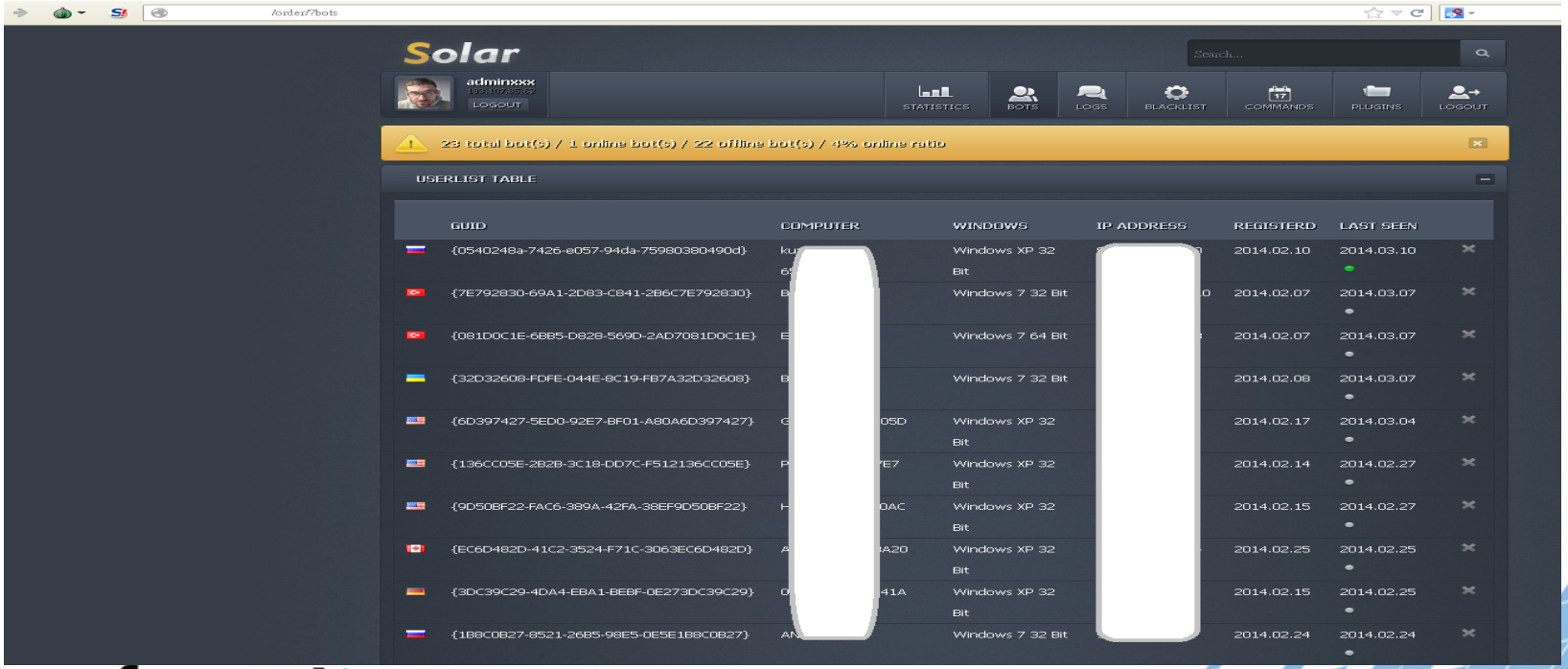
Banking trojan panels

- Zeus/ICEIX/Citadel/Betabot



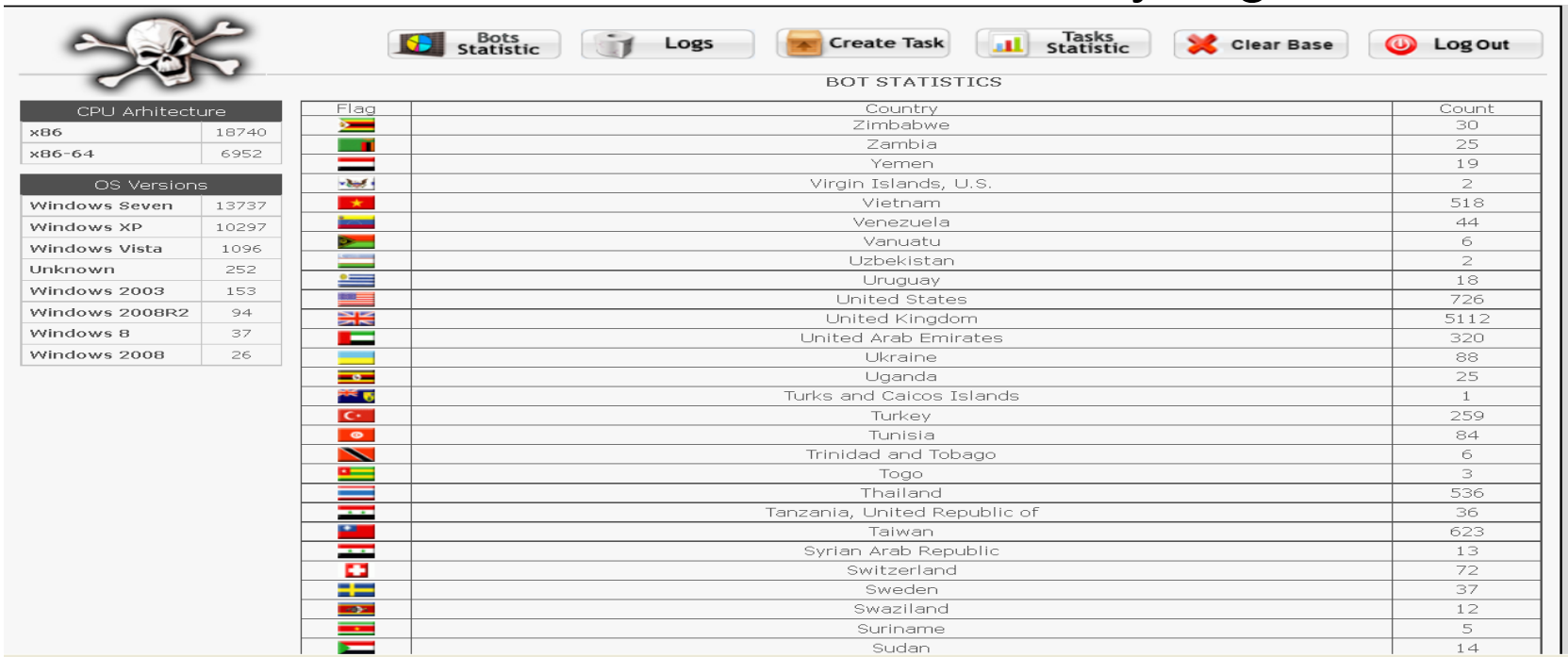
Banking trojan panels

- Zeus/ICEIX/Citadel/Betabot/Solarbot



Banking trojan panels

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



Bots Statistic | Logs | Create Task | Tasks Statistic | Clear Base | Log Out

CPU Arhitecture	
x86	18740
x86-64	6952

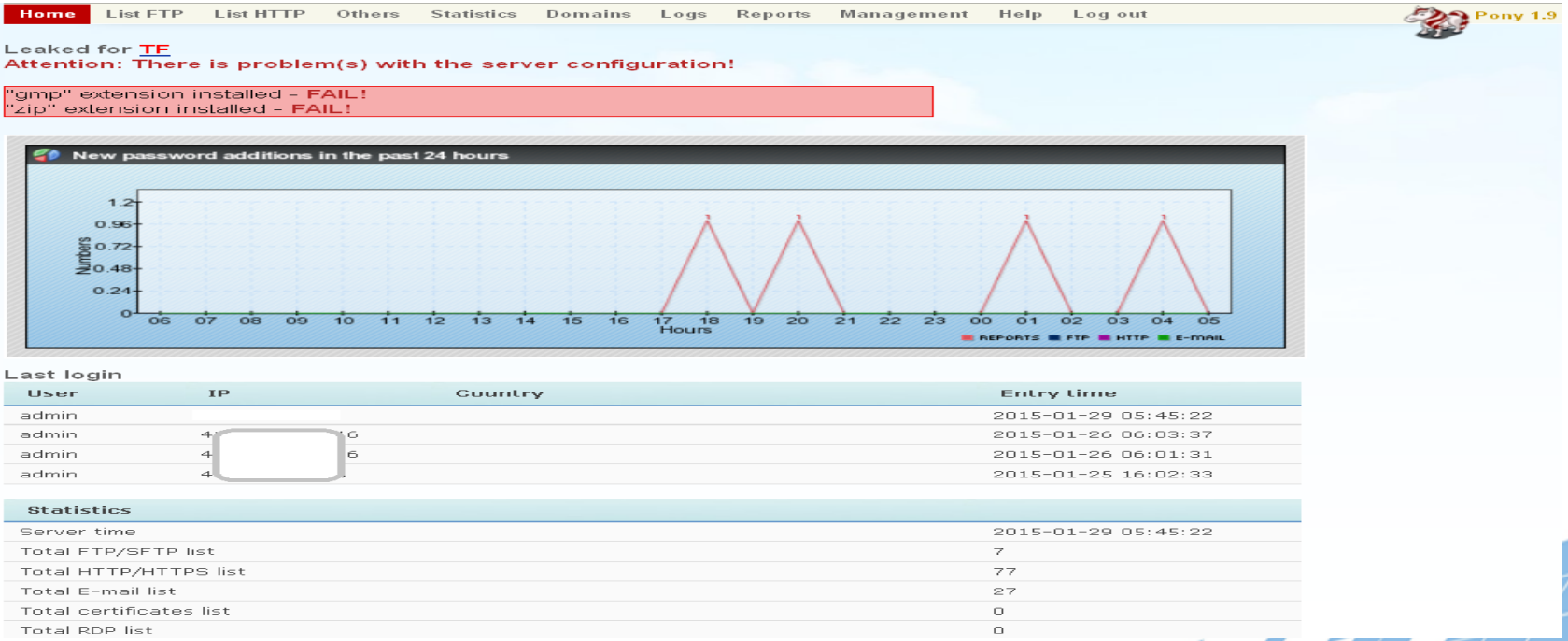
OS Versions	
Windows Seven	13737
Windows XP	10297
Windows Vista	1096
Unknown	252
Windows 2003	153
Windows 2008R2	94
Windows 8	37
Windows 2008	26

BOT STATISTICS

Flag	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

Banking trojan panels

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

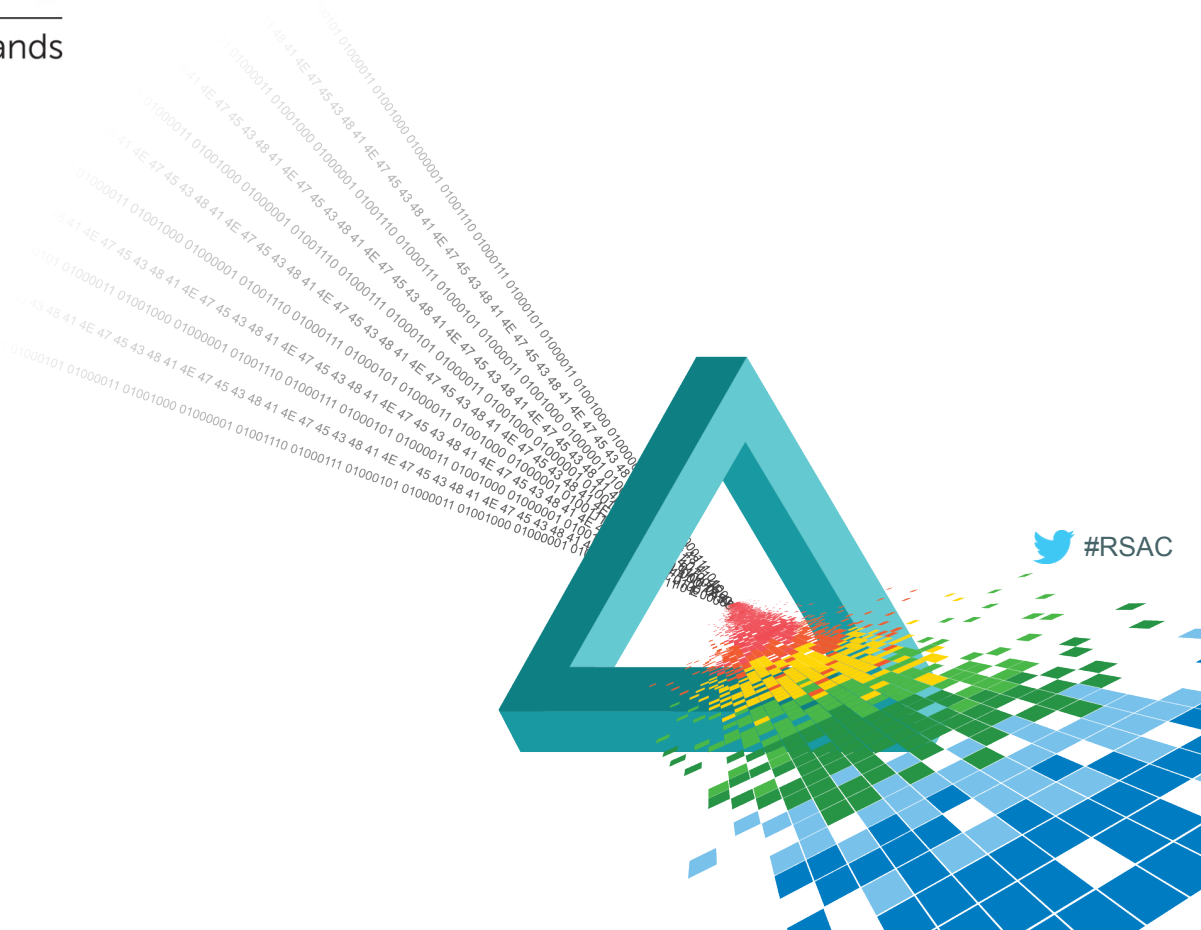


Banking trojan features

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

RSAConference2015

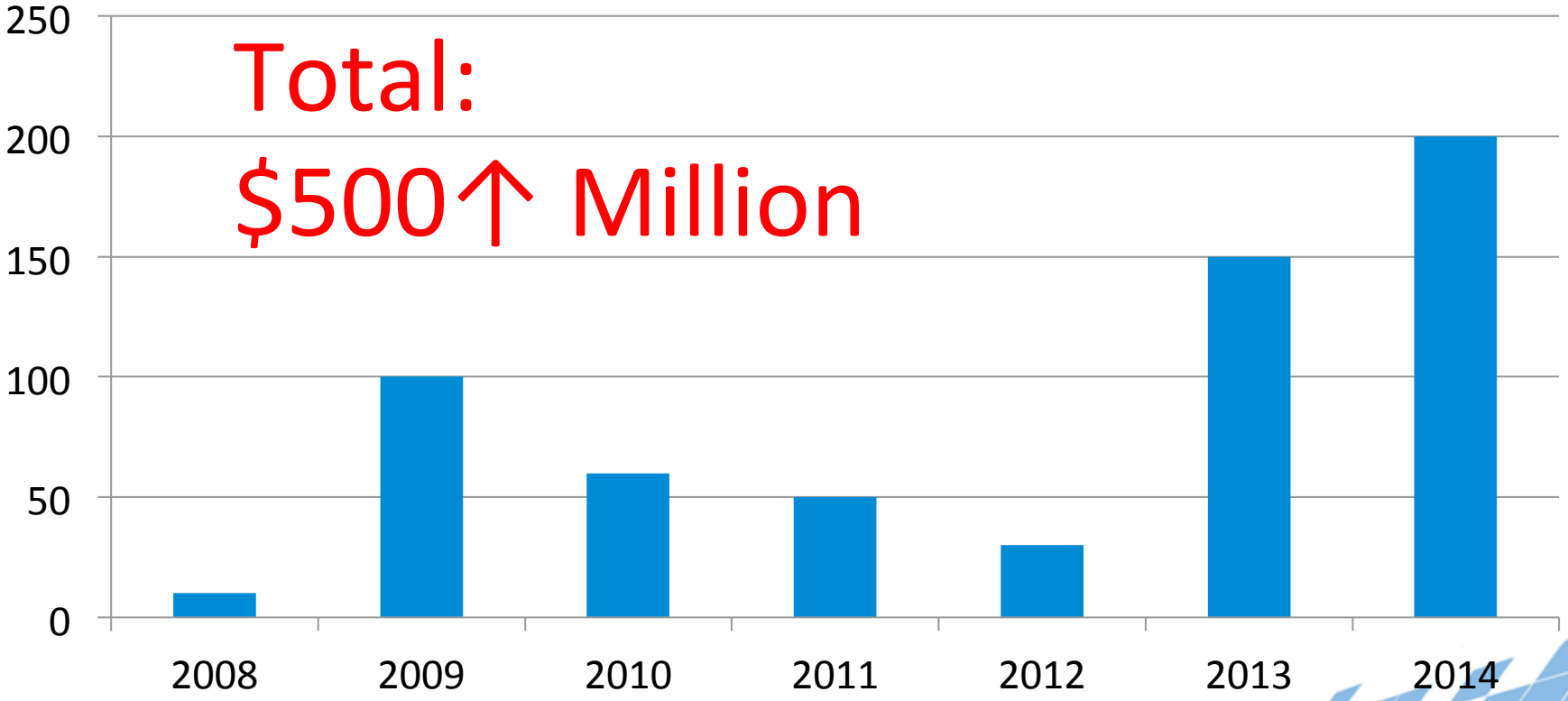
Singapore | 22-24 July | Marina Bay Sands



Monetization

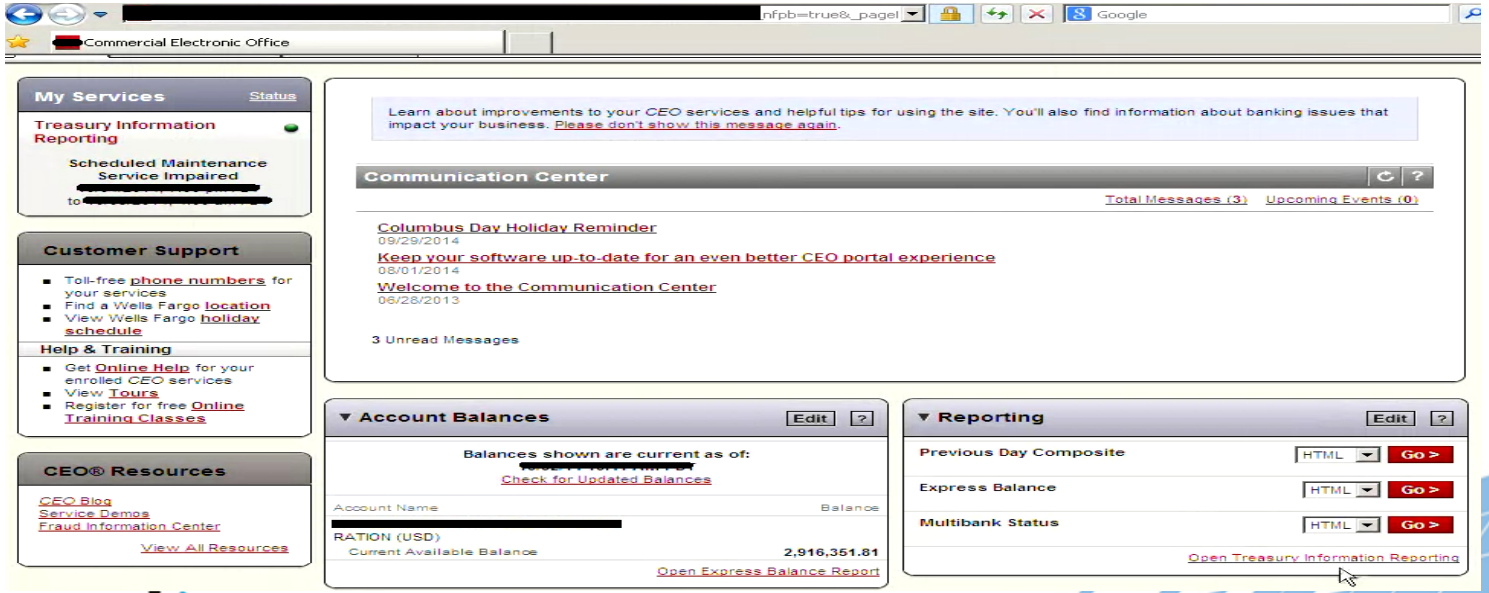
proofpoint

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.



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	$5332	5	
Members	Sales	New Update	Online

History Order

Different price by industry

Email	Type	Total	Payment	Date Added	Status
gururaj###@###	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!

1/23/2014 12:02 AM

Admin Tools-no1 Update

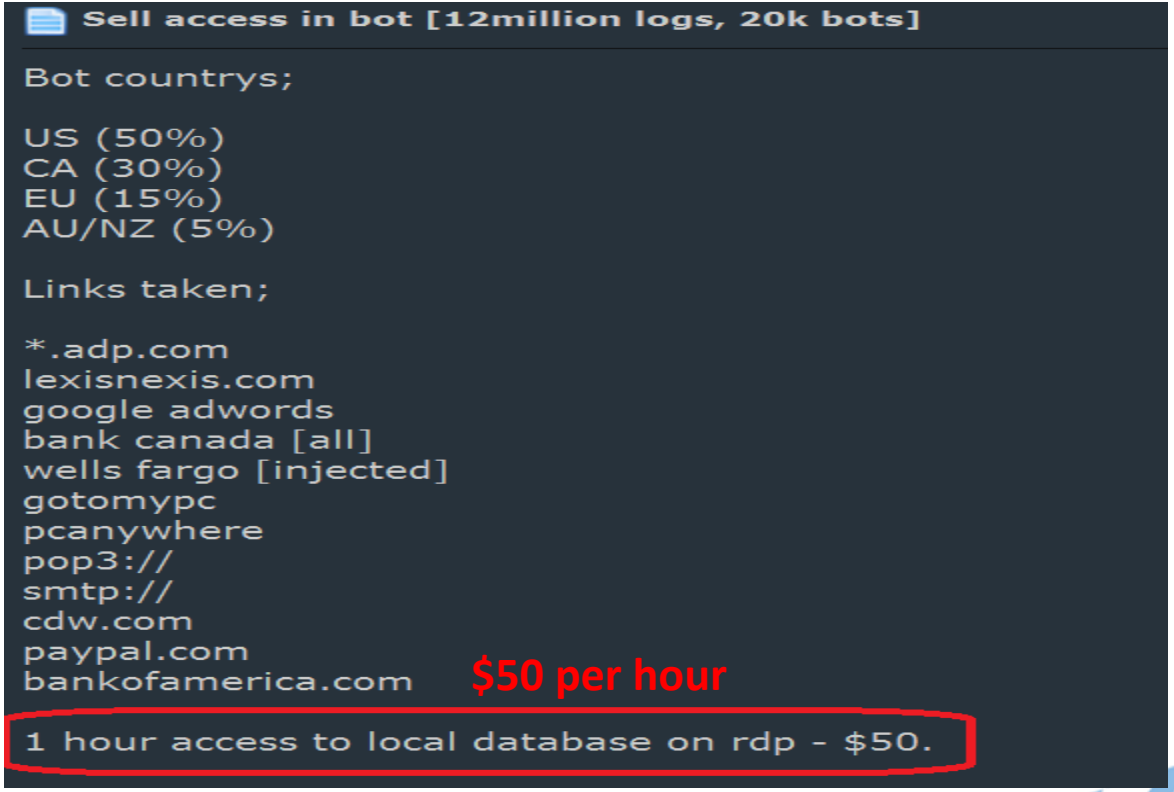
Add function attachment 2MB support any file type image and .zip , word, pdf, txt **Update**

MAILER PRO

Thank You!

11/11/2013 7:02 AM

Anything useful to you?



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',
        '.php', '.asp', '.aspx', '.exe', '.pl', '.cgi',
         '.cmd', '.bat', '.phtml', '.htaccess');
73      $fd_hash  = 0;
74      $fd_size  = strlen($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/

```
72    $bad_exts = array('.php3', '.php4', '.php5',
      '.php', '.asp', '.aspx', '.exe', '.pl', '.cgi',
       '.cmd', '.bat', '.phtml', '.htaccess');
73    $fd_hash  = 0;
74    $fd_size  = strlen($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 расширении, и указываем маску файла.
91      if(($ext = strrchr($last_name, '.')) === false
        || in_array(strtolower($ext), $bad_exts) !==
        false)$file_path .= '.dat';
92      $ext_pos = strrpos($file_path, '.');
93
94      //FIXME: Если имя слишком большое.
95      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/

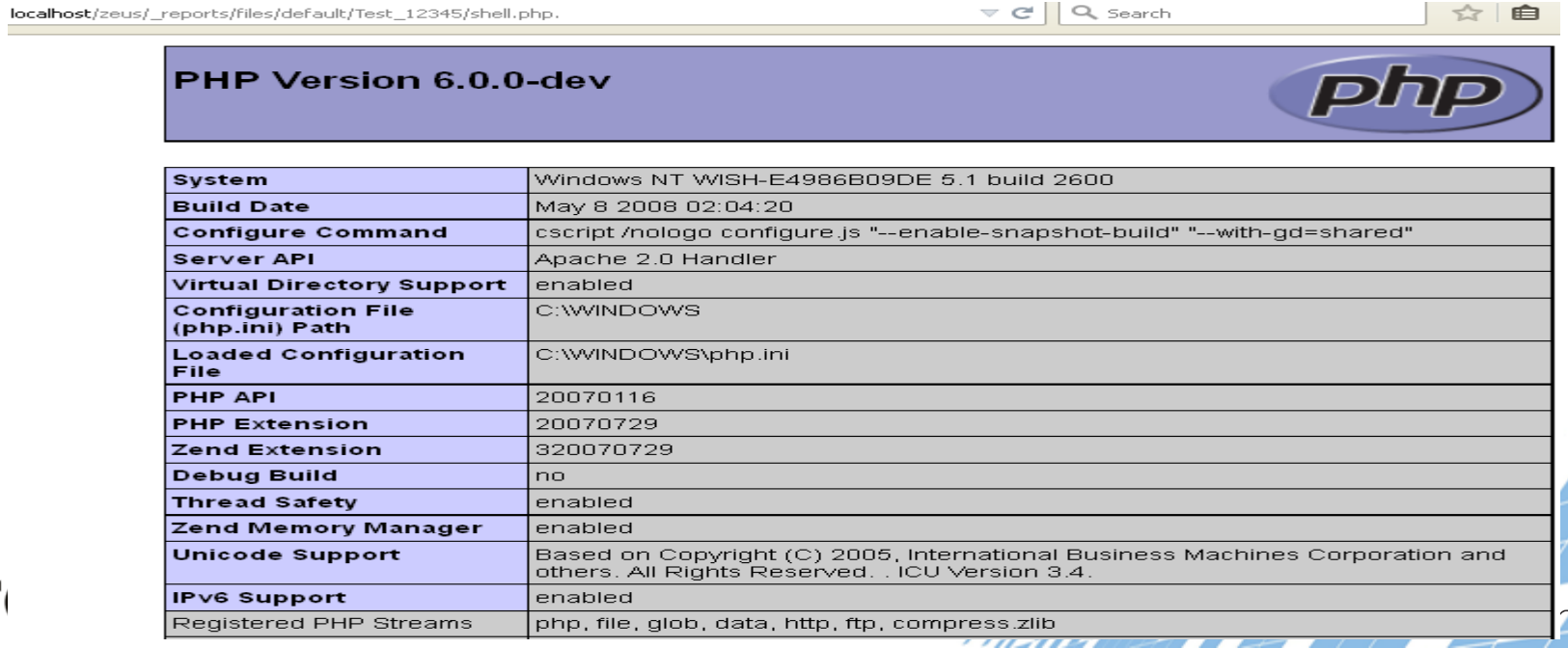
```
90      //Проверяем расширении, и указываем маску файла.
91      if(($ext = strrchr($last_name, '.')) === false
        || in_array(strtolower($ext), $bad_exts) !==
        false)$file_path .= '.dat';
92      $ext_pos = strrpos($file_path, '.');
93
94      //FIXME: Если имя слишком большое.
95  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



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          }
105     $bad_exts = array('.php', '.asp', '.exe', '.pl'
        , '.cgi', '.cmd', '.bat', '.cfm', '.jsp', '.sh'
        , '.phtm');
122     if(($ext = strrchr($last_name, '.')) === false
        || strstr_array(strtolower($last_name),
        $bad_exts))$file_path .= '.txt';
123     $ext_pos = strrpos($file_path, '.');
```

File upload vulnerability has been fixed

- Fixed in Zeus Robot

File upload vulnerability has been fixed

- Fixed in Zeus Robot

File upload vulnerability has been fixed

- Fixed in Zeus Robot

C2 remote command execution

- 0day
- Affected: All Zeus / IceIX / 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 | fsarc.php

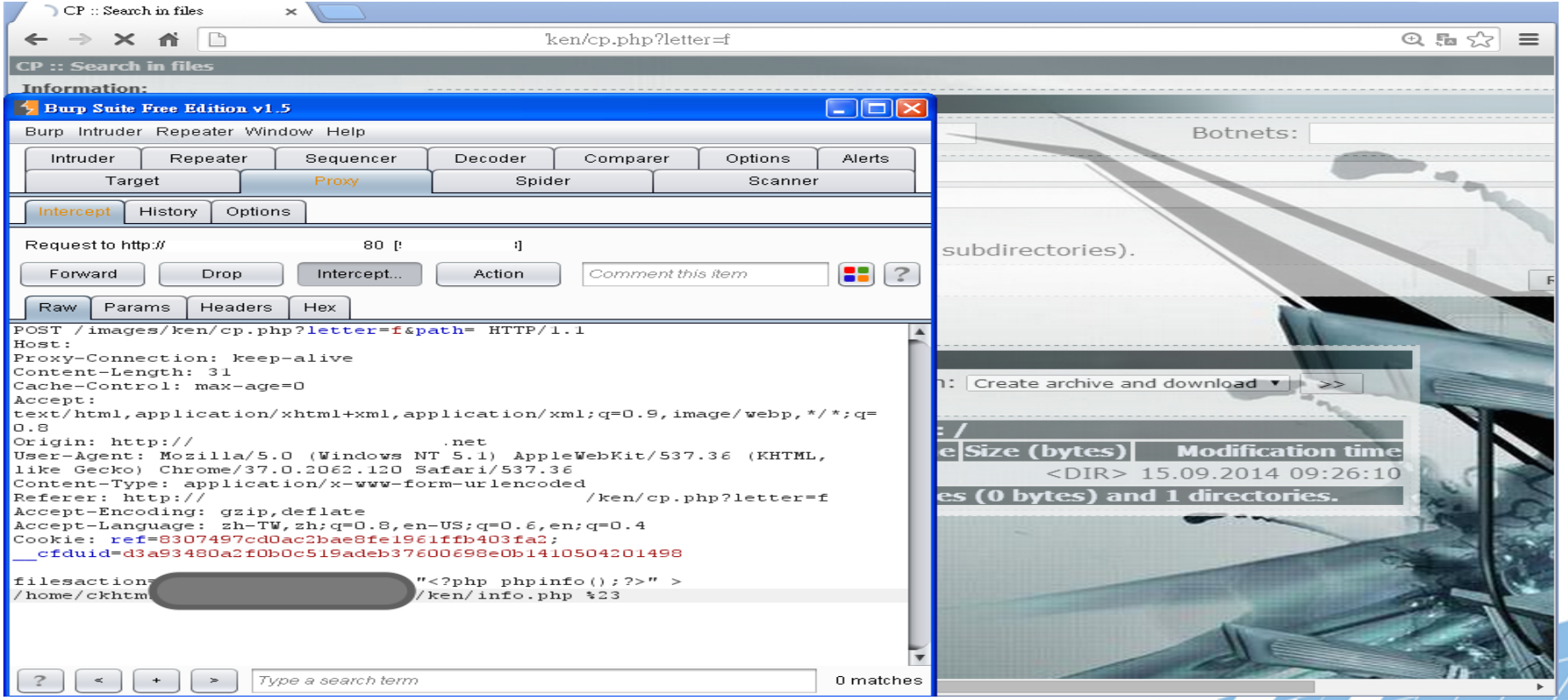
```
13
14    IN $archive - string, полный путь по которому должен быть созда
15    IN $files   - array, список файлов для добавления в архив.
16
17    Return      - mixed, имя архива - в случаи успешного создания а
18  */
19  function fsarcCreate($archive, $files)
20  {
21    error_reporting(E_ALL);
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

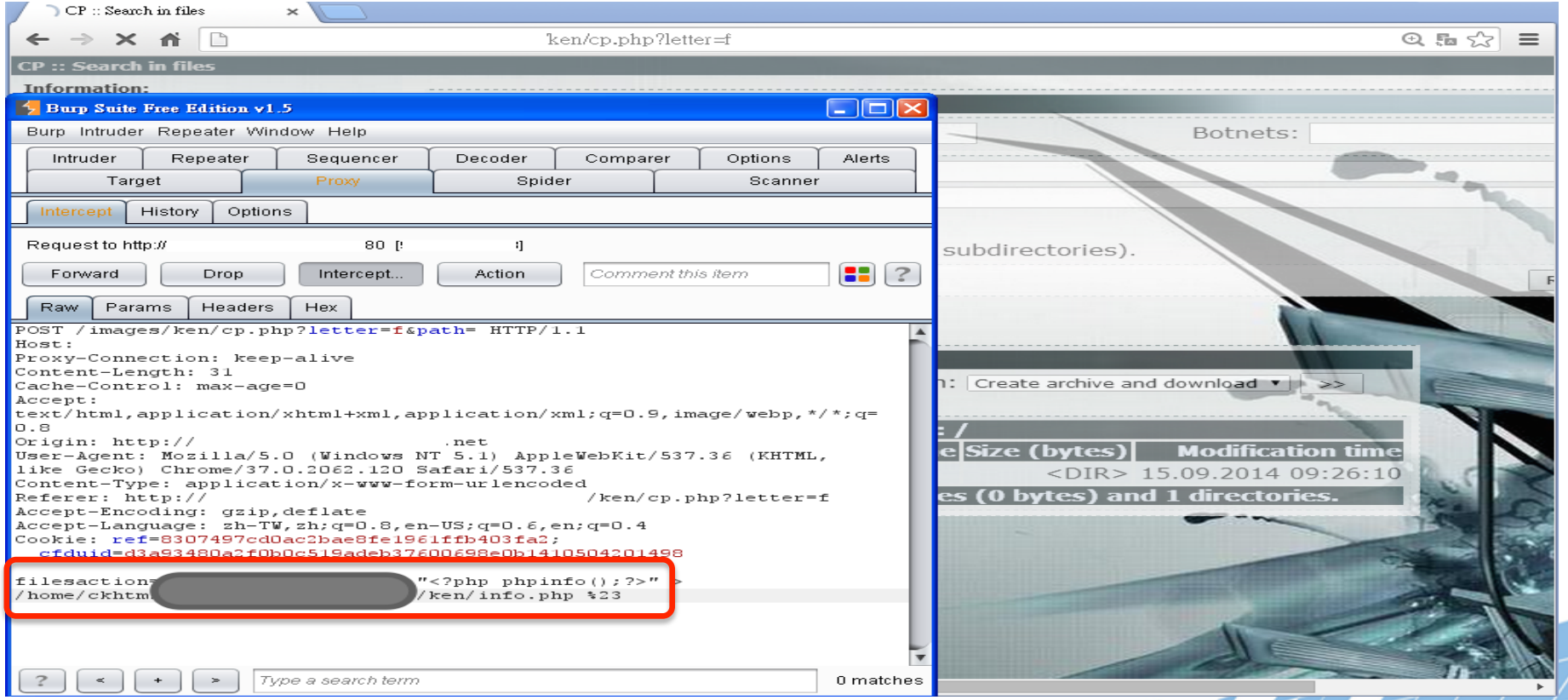
reports_files.php

```
58    if($_POST['filesaction'] ==  ) && $_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') || ($arcfile = fsarcCreat
74
75      httpDownloadHeaders(baseNameEx($arcfile), @filesize($arcfile
76      echo @file_get_contents($arcfile);
77      @unlink($arcfile);
78      die();
79    }
80  }
```

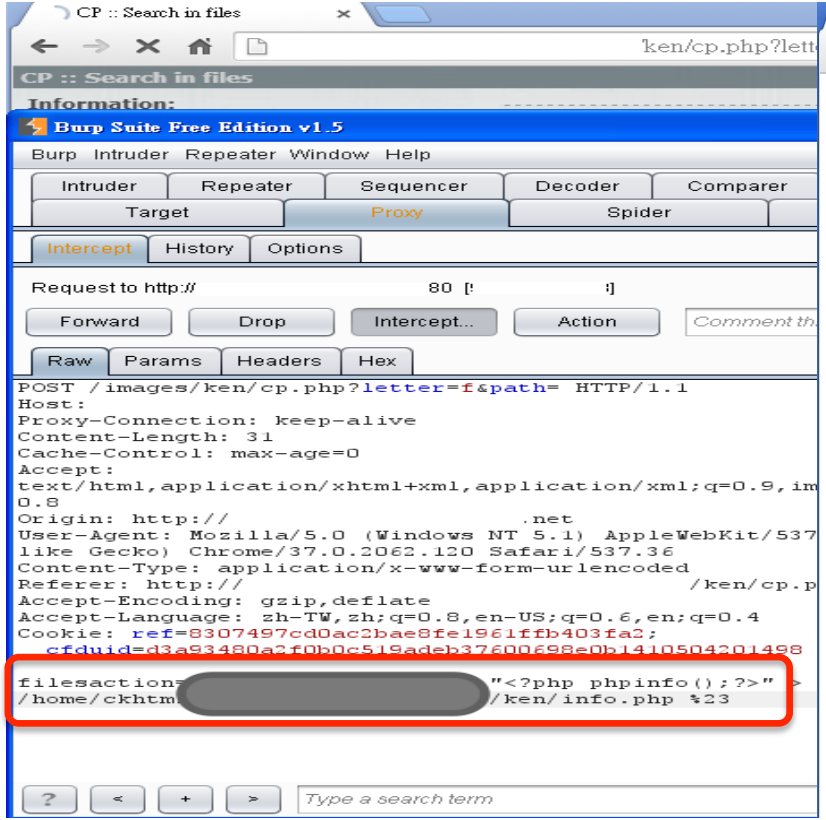
C2 remote command execution



C2 remote command execution



C2 remote command execution



Reflected cross site scripting

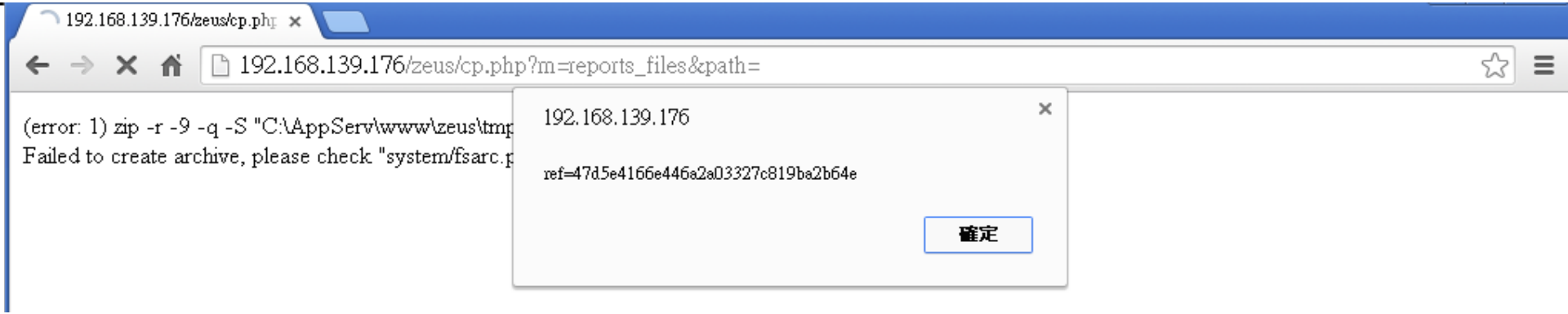
- 0day
- Affected: All Zeus / IceIX / Citadel
- Source: reports_files.php (database search)
- Sink: fsarc.php (file archiving)
- Affected parameter: files
- Cookie stealing or client side exploitation

Reflected cross site scripting

reports_files.php | fsarc.php

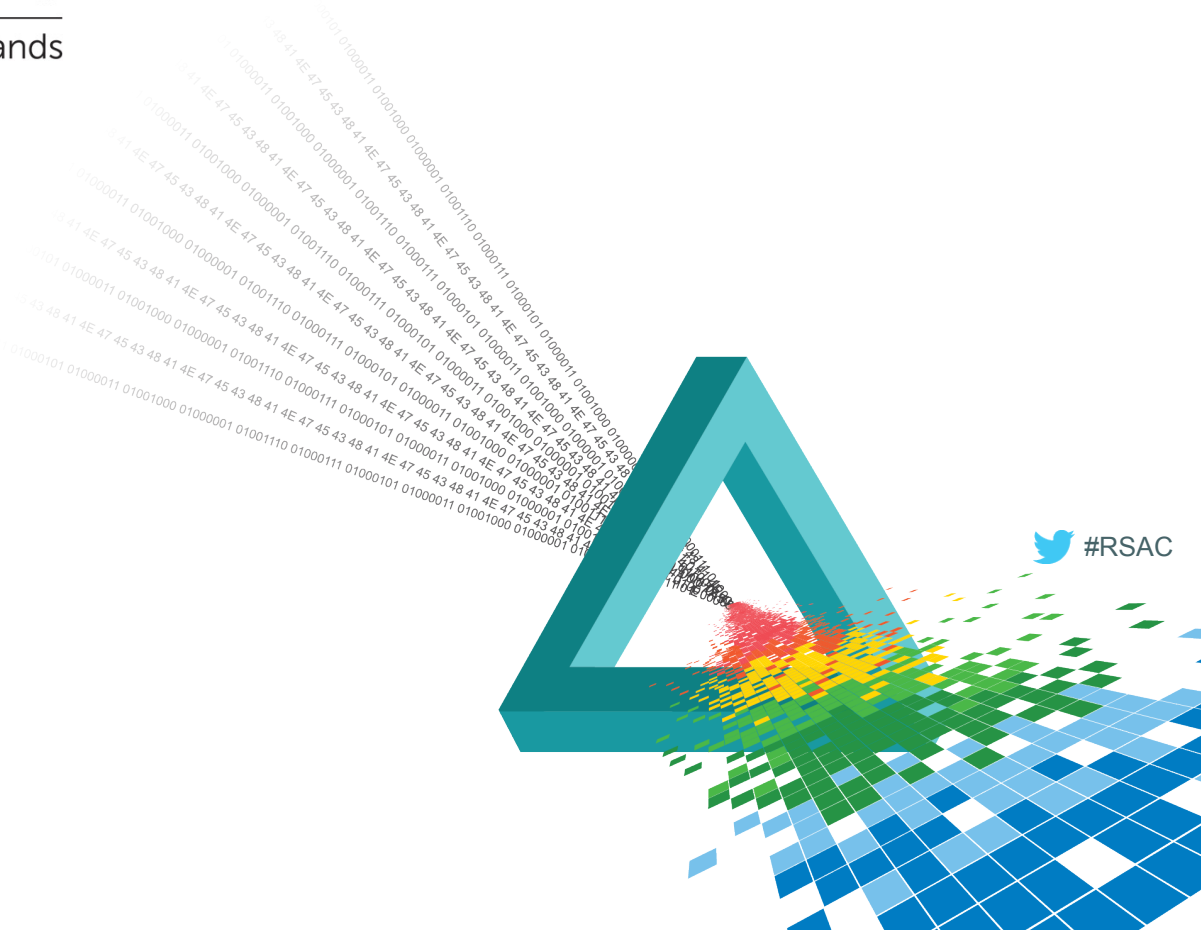
```
13
14    IN $archive - string, полный путь по которому должен быть созда
15    IN $files   - array, список файлов для добавления в архив.
16
17    Return      - mixed, имя архива - в случаи успешного создания а
18  */
19  function fsarcCreate($archive, $files)
20  {
21    error_reporting(E_ALL);
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  ?>
```

Reflected cross site scripting



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

Actor attribution methodology

proofpoint

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	a		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

- HTTP_REFERER : http://[redacted]/sitemap/30/cp.php?letter=home
- HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.104 Safari/537.36
- REMOTE_ADDR : 41.79.219.202, 41.79.219.202, 41.79.219.202

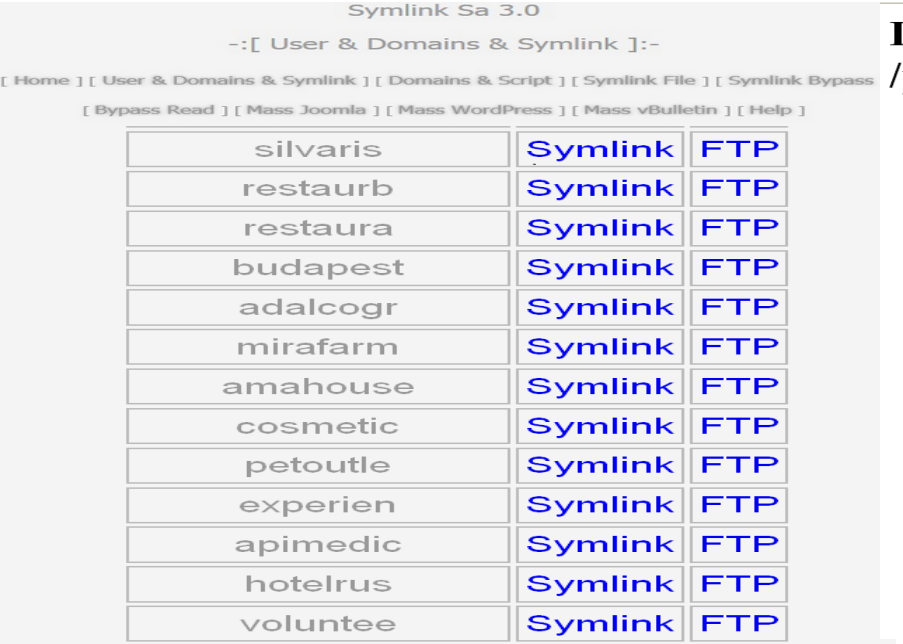
2015-01-28
17:02:13

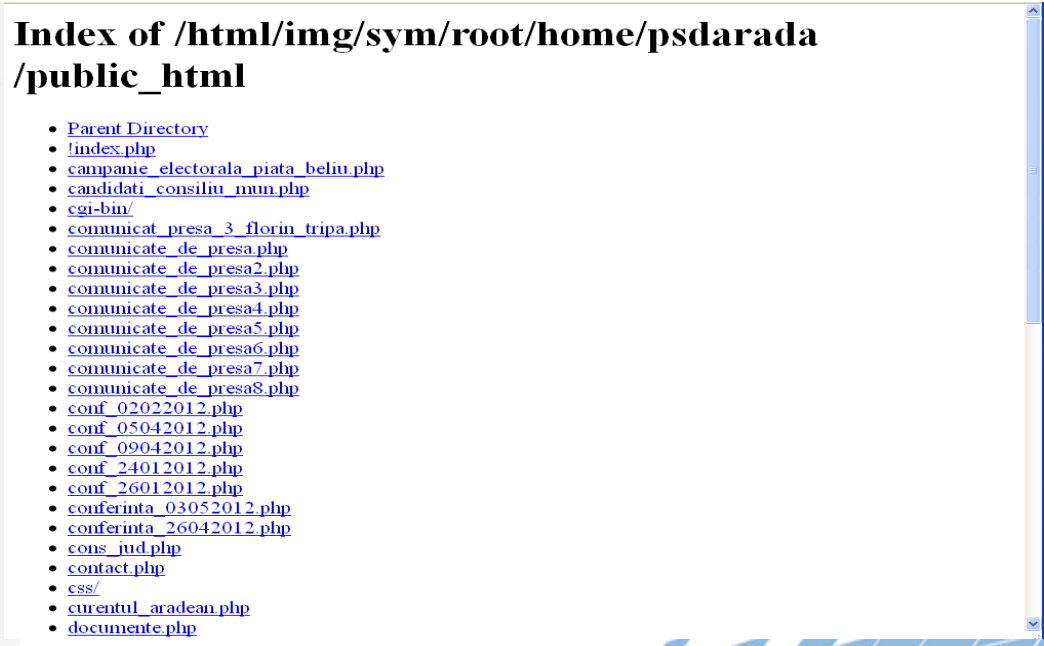
- domain : [redacted]
- screen : 1366x768
- browser_name : Chrome
- browser_version : 38.0.2125.104
- language : en-US
- Osystem : Windows 7
- flash_version : 15.0 r0

- HTTP_REFERER : http://[redacted]/sitemap/30/cp.php?rm=0&letter=e&date1=150128&date2=150128&members=&memberships=&ips=&countries=&q=&blt=0
- HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.104 Safari/537.36
- REMOTE_ADDR : 41.79.219.202, 41.79.219.202, 41.79.219.202

Actors' tool for cPanel remote privilege escalation

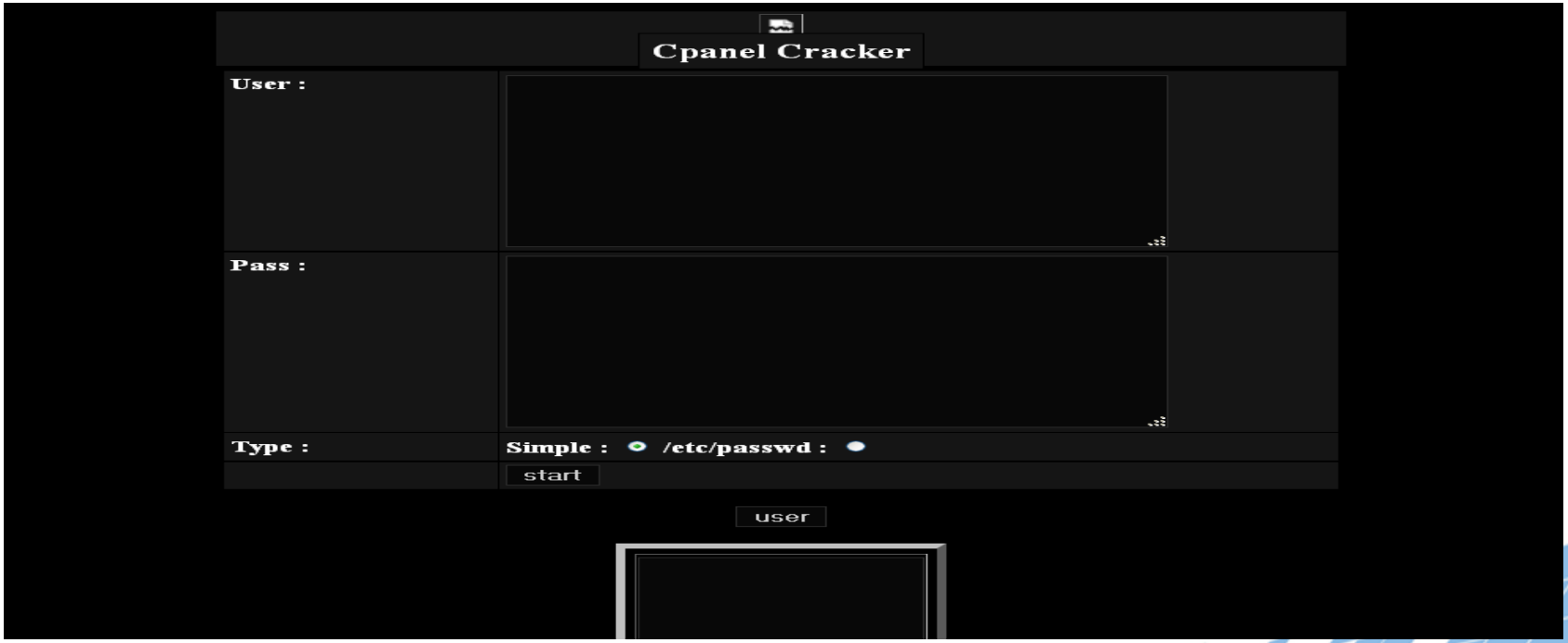
- cPanel apache Symlink Race Condition Vulnerability





Actors' tool for cPanel password bruteforcing

- cPanel password bruteforcing

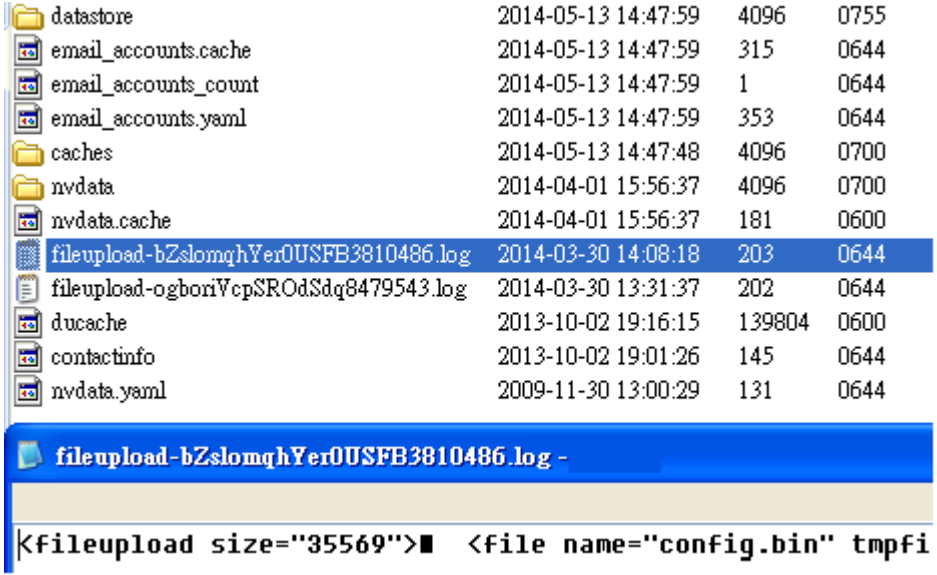


Actors' tool for cPanel password bruteforcing

- cPanel password bruteforcing

Upload & install C2 mostly via cPanel

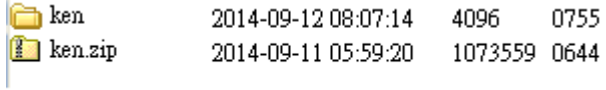
- Upload C2 panel, dropper and config files via cPanel



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-bZslomqhYer0USFB3810486.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

fileupload-bZslomqhYer0USFB3810486.log -

<fileupload size="35569"> <file name="config.bin" tmpfi

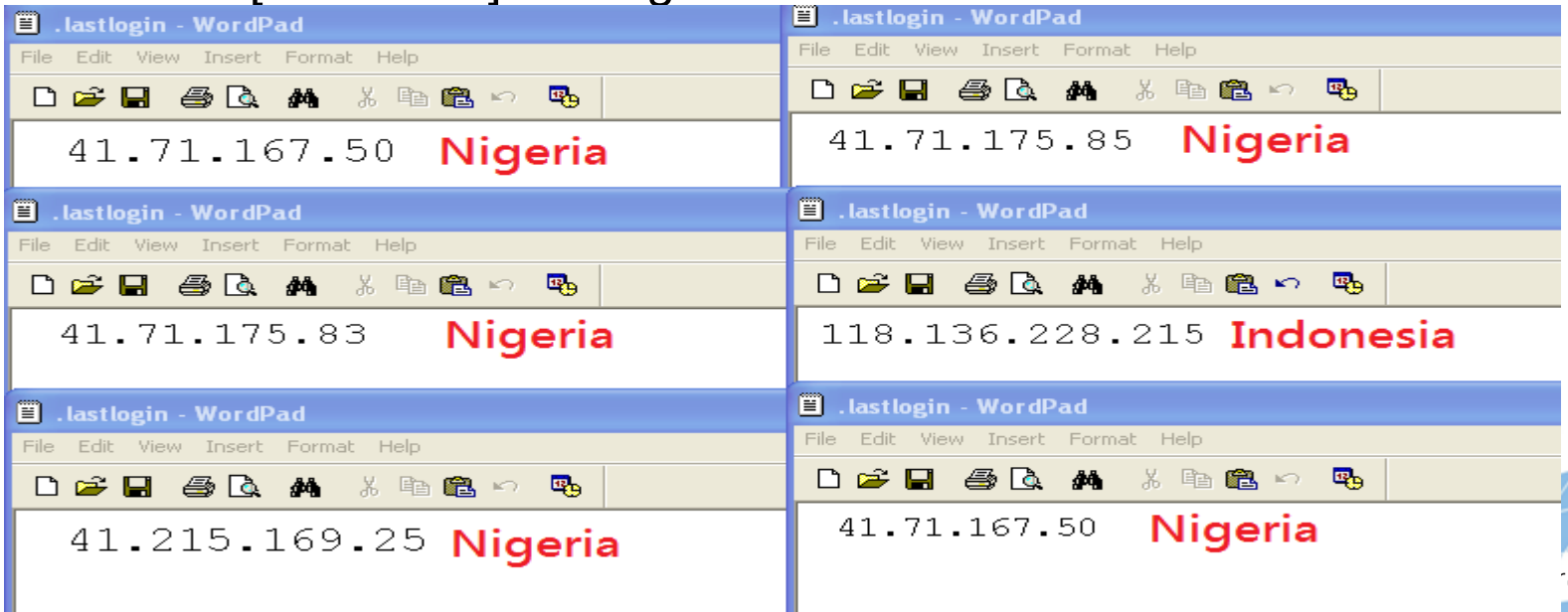


ken	2014-09-12 08:07:14	4096	0755
ken.zip	2014-09-11 05:59:20	1073559	0644

Citadel.1.3.5.1-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
Citadel.1.3.5.1-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

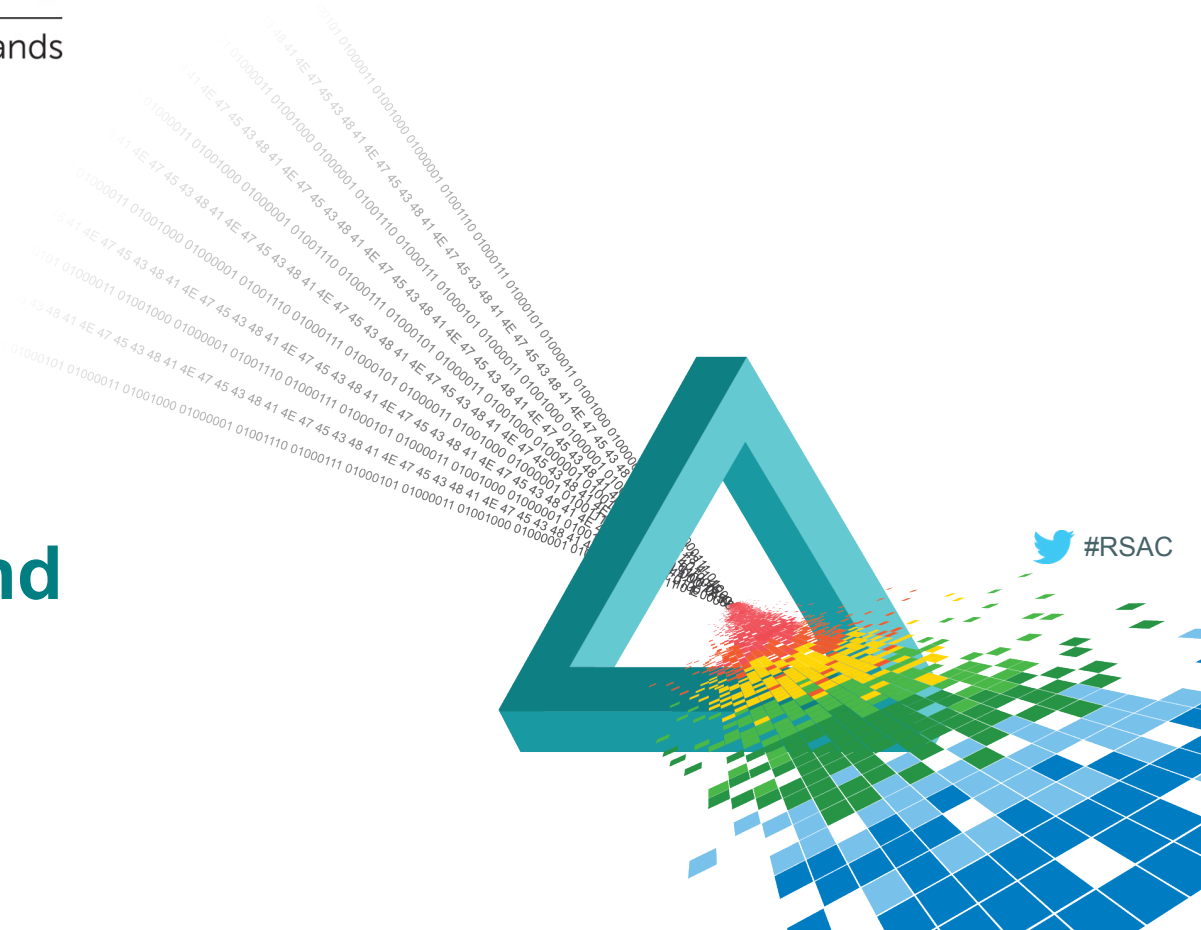
#	Hits		KBytes		URL
1	76759	12.70%	4797	0.35%	/phpmyadmin/theme/js/tinymce/jscripts/lager3/gate.php
2	33828	5.60%	861245	61.96%	/phpmyadmin/theme/js/tinymce/jscripts/lager3/file.php
3	22974	3.80%	1435	0.10%	/phpmyadmin/theme/video/colorbox/example5/eku2/gate.php
4	14039	2.32%	876	0.06%	/phpmyadmin/theme/video/colorbox/example5/exq/gate.php
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

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



#RSAC

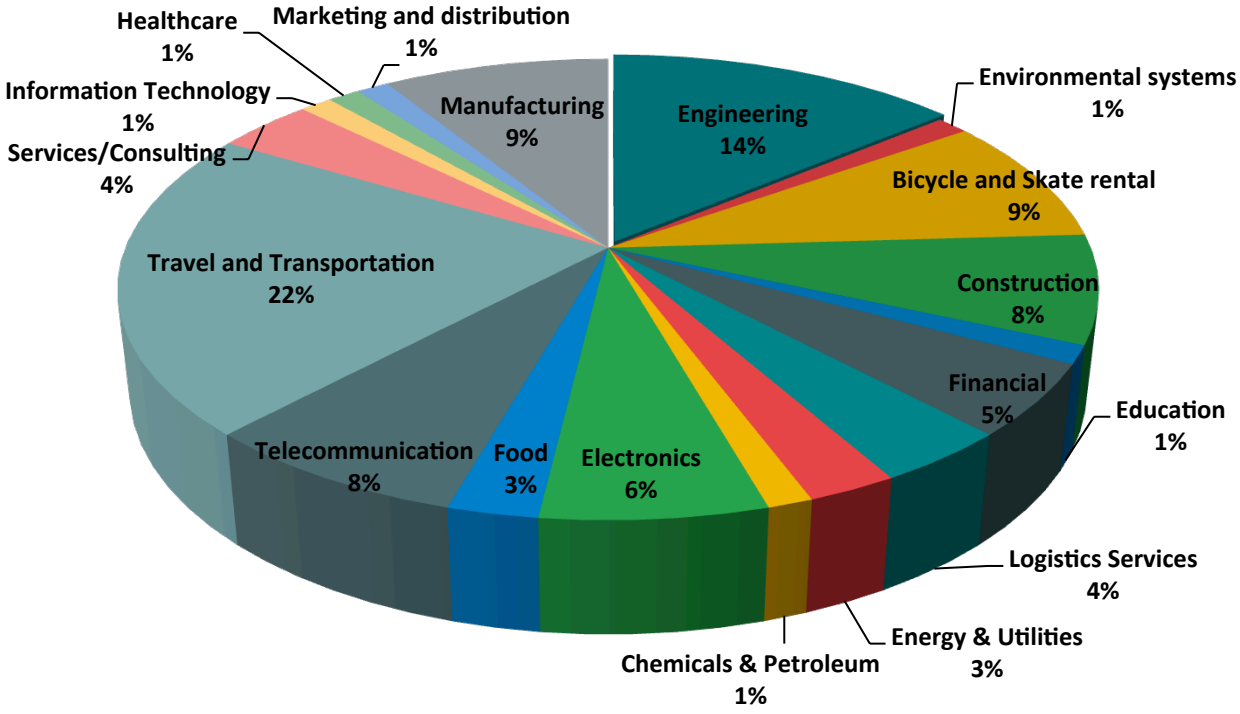
Those targeted and compromised

proofpoint

Overview of the nine actors

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

Singaporean victims by industry



- Logistics industry

******cs.com.sg

******ing.com.sg

- Oil / Energy industry

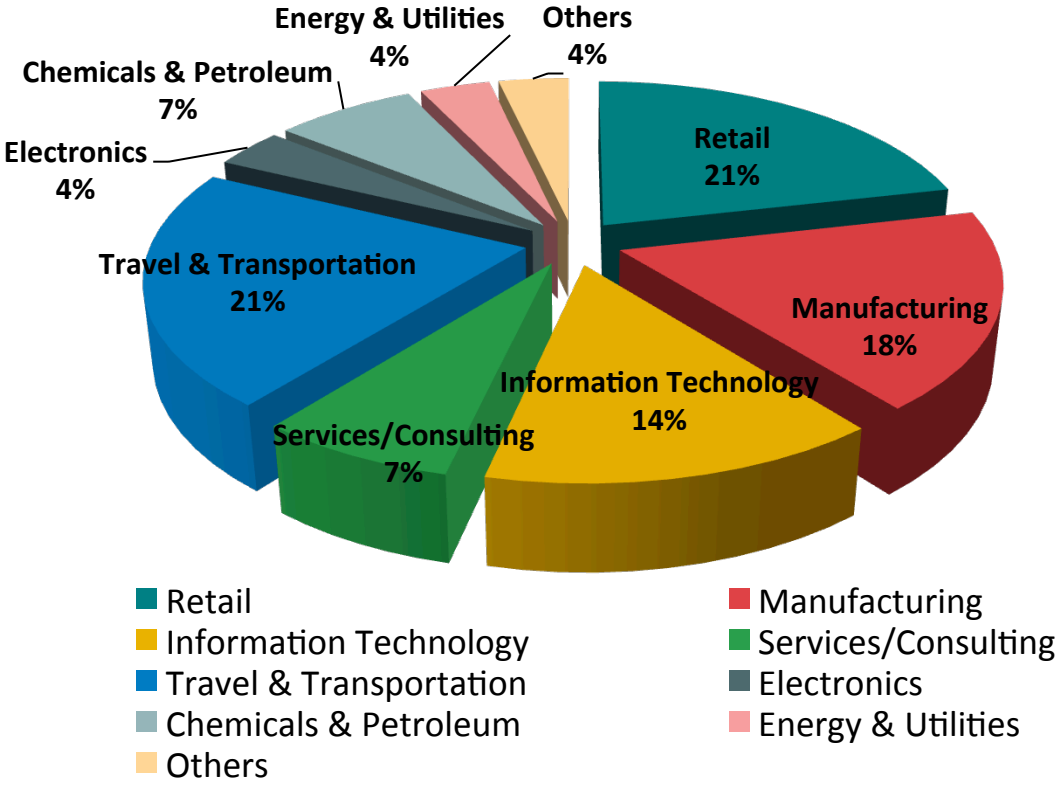
******ring.com.s

******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

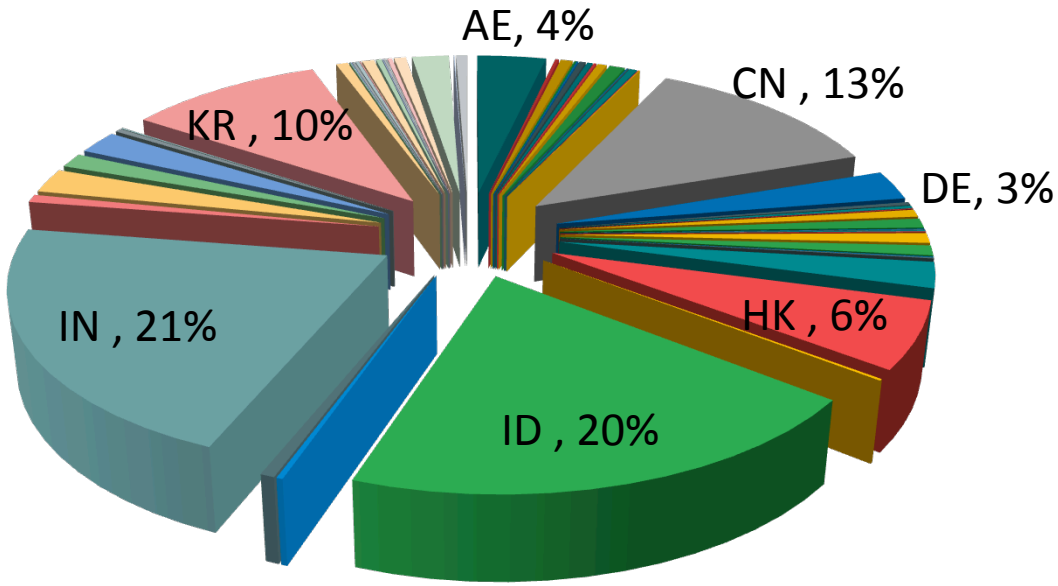
Group NG03 – Victims by industry



- 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

proofpoint

Group NG03 – Victims by country

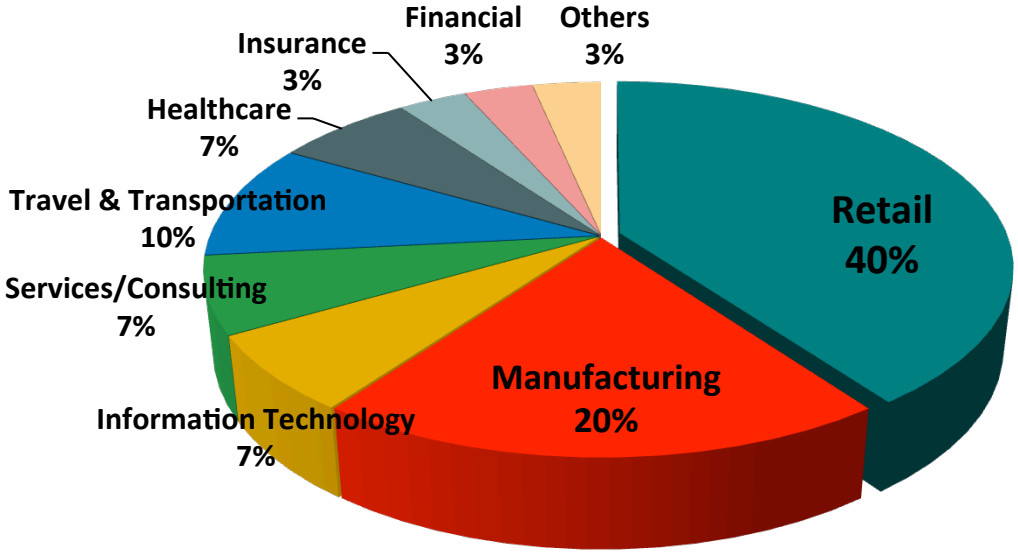


AE AR AT AU BA BD BE BF BG BH BT BY CA CH CI
CN DE DK DZ EC EG ES ET EU FI FJ FR GB GE GH
GR HK HU ID IE IL IN IR IT JO JP KE KH KR KW
KZ LB LK LT LU LV MA MD ME MO MU MX MY MZ NG

Group IN01

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

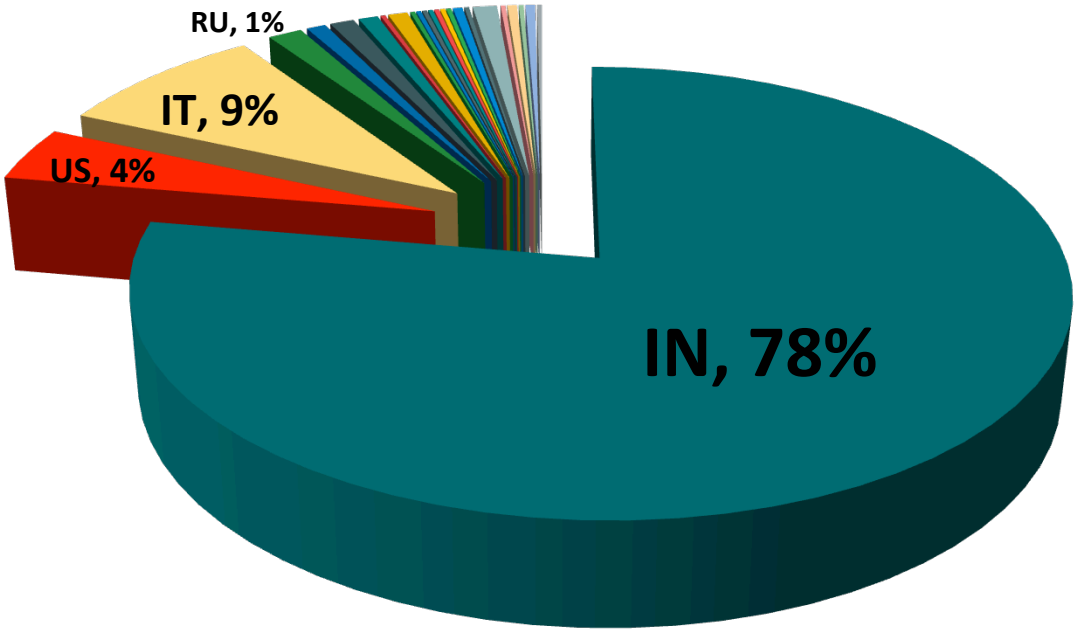
Group IN01 – Victims by industry



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

proofpoint

Group IN01 – Victims by country

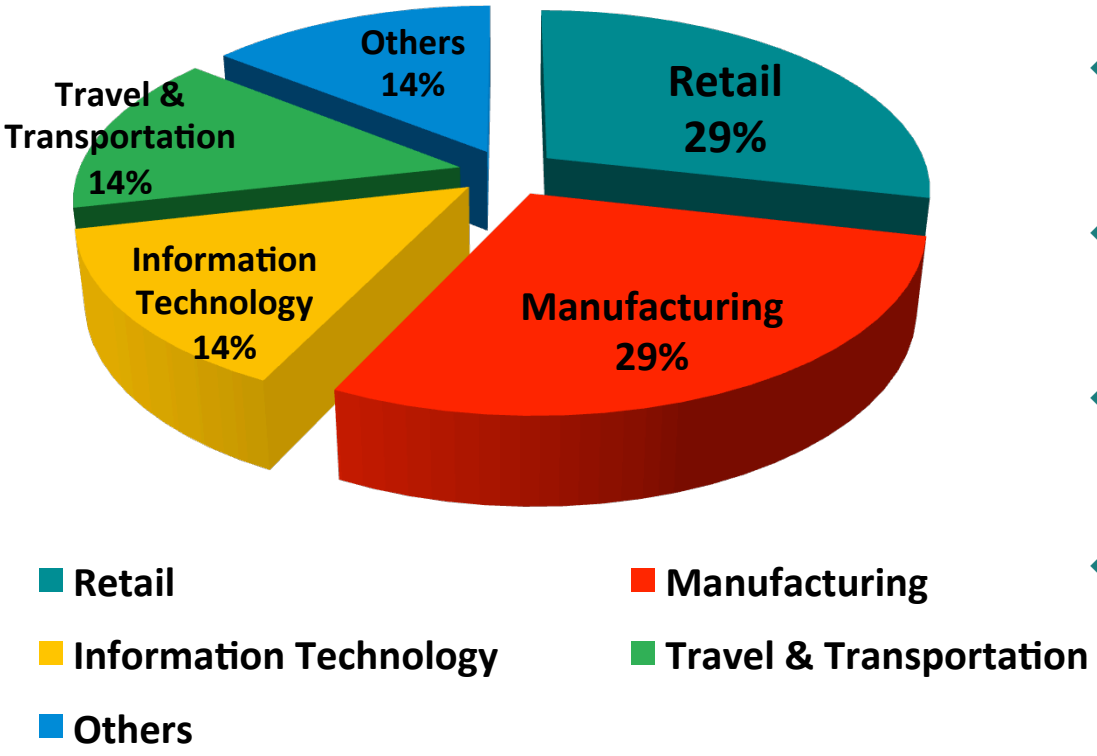


IN US IT RU BG DE IL AT FR HU GR EG
BE CA PL ES PK MU CN HK GB BH TW SG

Group ZA01

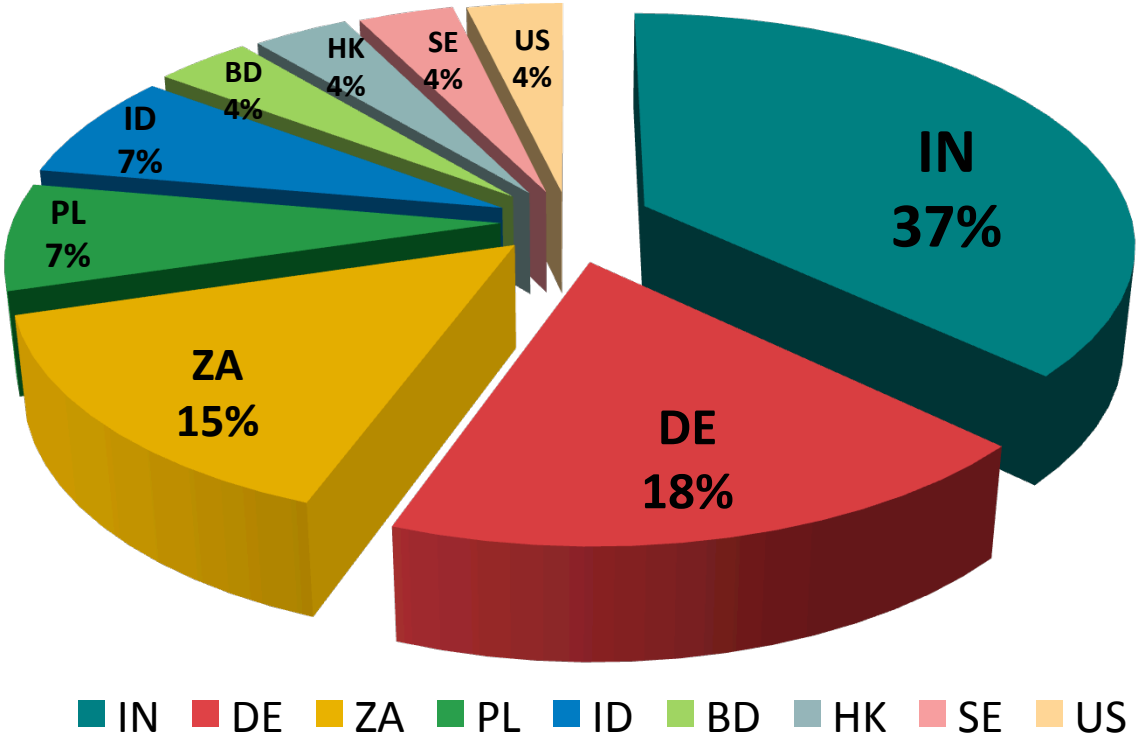
Group Name	ZA01
Nationality/ Location	SOUTH AFRICA, KWAZULU-NATAL, DURBAN
Victim #	27
Stolen credentials	pop3:28 ftp:3 http:20
Malware used	Zeus
Server owned	3
Technique	Spear phishing -- attachment
Feature	Your Order.exe drop.exe drops.exe

Group ZA01 – Victims by industry



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

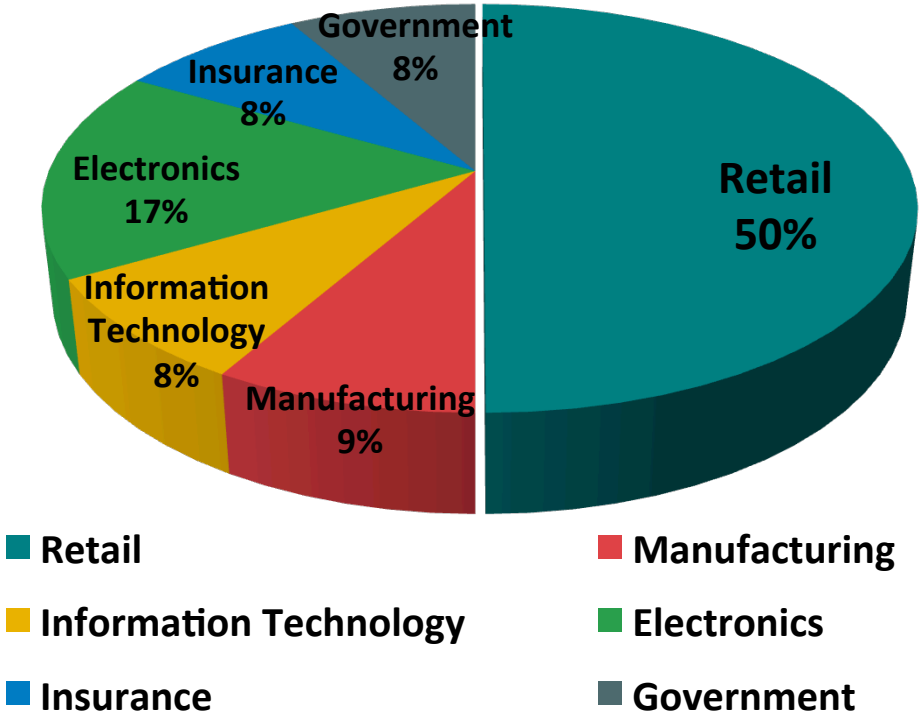
Group ZA01 – Victims by country



Group ID01

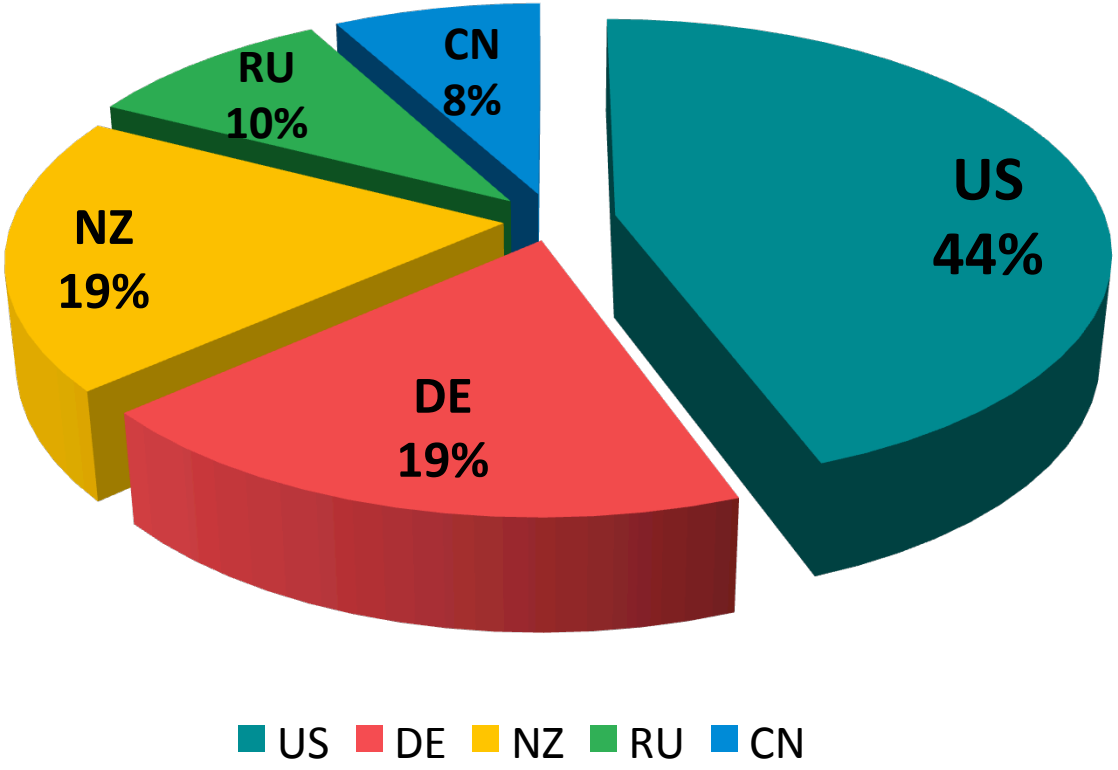
Group Name	ID01
Nationality/ Location	INDONESIA
Victim #	100
Stolen credentials	pop3:22 ftp:31 http:10
Malware used	Zeus
Server owned	3
Technique	Spear phishing -- attachment Phishing
Feature	

Group ID1 – Victims by industry



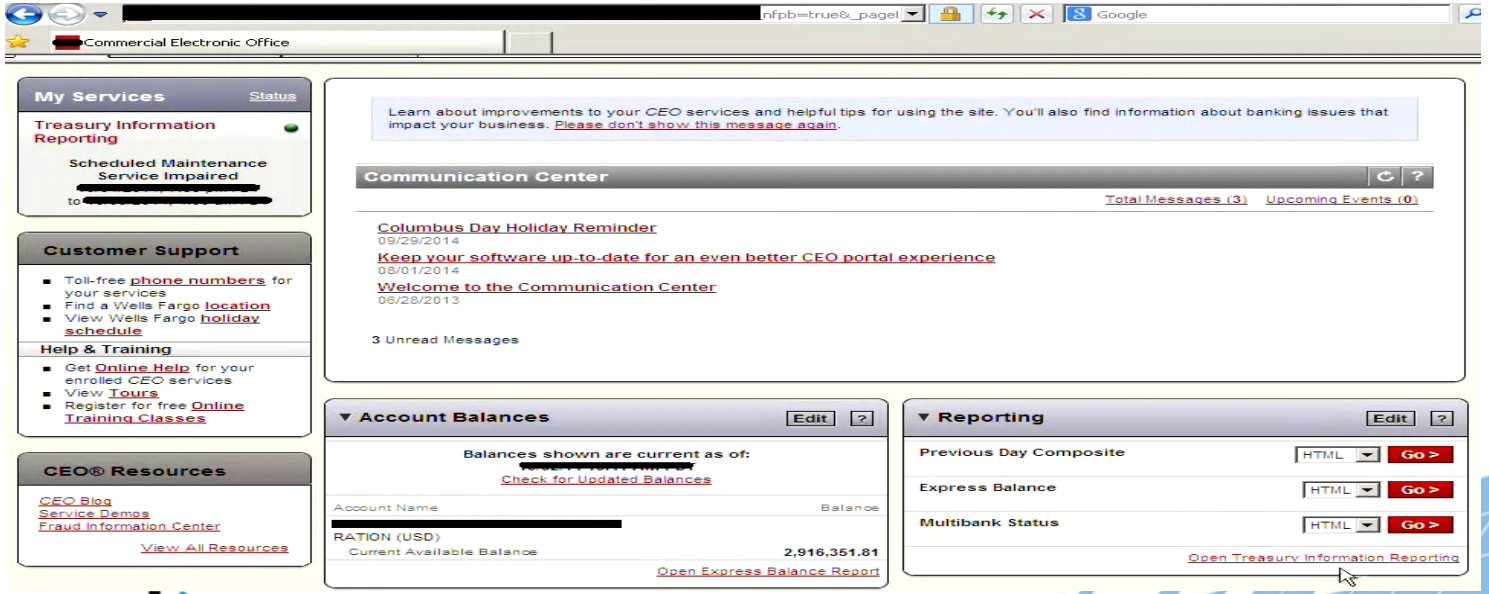
- Aviation Equipment Company
- India's electrical equipment manufacturer
- European flying committee

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.



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

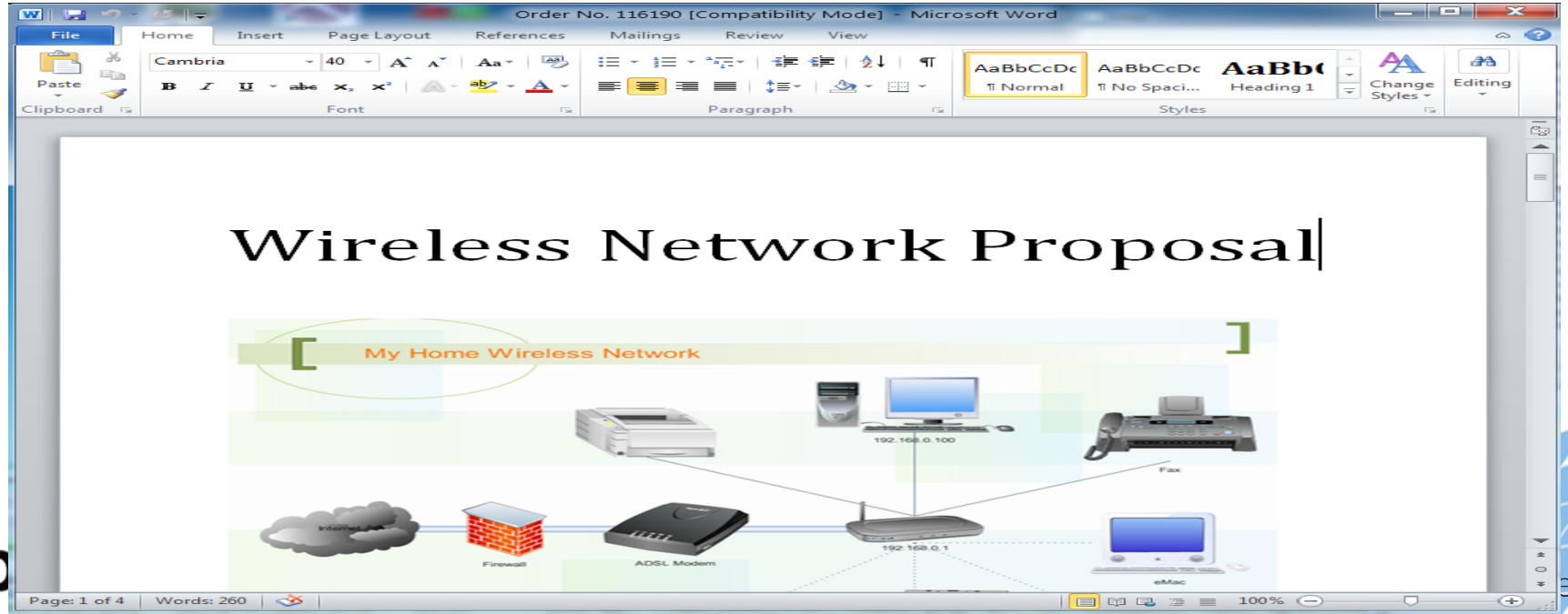
#RSAC

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 **likkkke.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 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 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($_GET["
                 sitename"]) && isset($_GET["password"])&& isset($_GET["pcname"])
                 )
172          {
173              foreach($_GET as $key => $value)
174              {
175                  $data[$key] = query($value);
176              }
177              $result = mysql_query("SELECT id FROM `logs` WHERE `app` = '".
                     urldecode($data["app"])."' AND `url` = '".urldecode($data["
                     sitename"])."' AND `username` = '".urldecode($data['username
                     '])."' AND `password` = '".urldecode($data['password'])."';"
                     );
178              if (mysql_num_rows($result) == 0)
179              {
180                  $results = mysql_query("INSERT INTO `logs` (`id`, `app`, `
                         url`, `username`, `password`, `pcname`, `date`, `ip`)
181                                          VALUES (NULL ,'".urldecode($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

```
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');
```

```
                    url`, `username`, `password`, `pcname`, `date`, `ip`)
181                                 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

```
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["
```

Specific user agent

```
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');
```

```
                    url`, `username`, `password`, `pcname`, `date`, `ip`)
181                 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

```
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["
```

Specific user agent

```
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

```
                    url`, `username`, `password`, `pcname`, `date`, `ip`)
181                 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

```
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["
```

Specific user agent

```
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

```
                    url`, `username`, `password`, `pcname`, `date`, `ip`)
181                 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

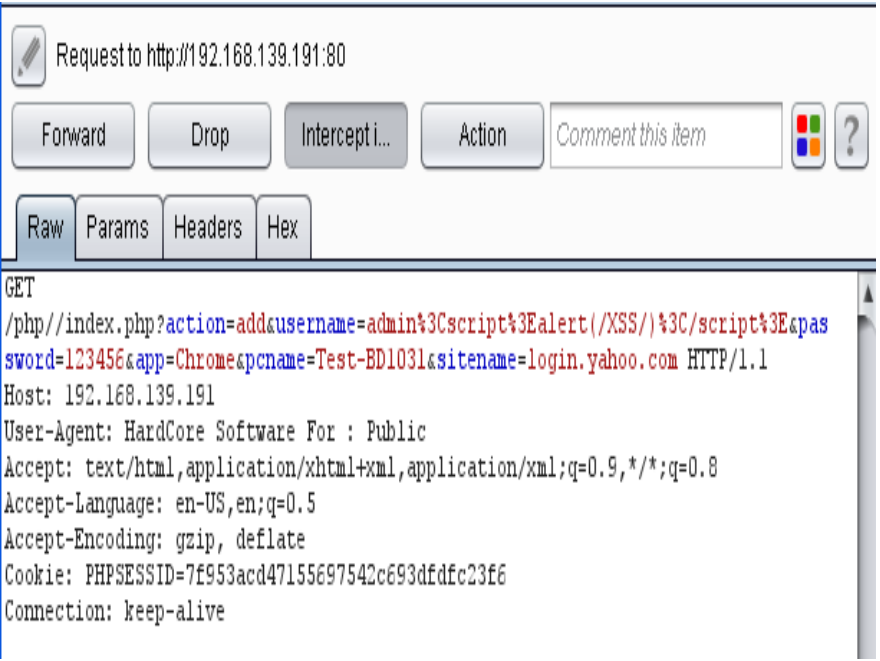
```
359     if ($total > 0)
360     {
361         $result = mysql_query("SELECT * FROM `logs` ORDER BY `date` ".$_
                SESSION['order']." LIMIT ".($logsperpage*$_SESSION["page"])." ,
                ".$logsperpage.";");
362         $i = 0;
363         $fetched = mysql_num_rows($result);
364         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++;
```

ISR stealer persistent cross site scripting

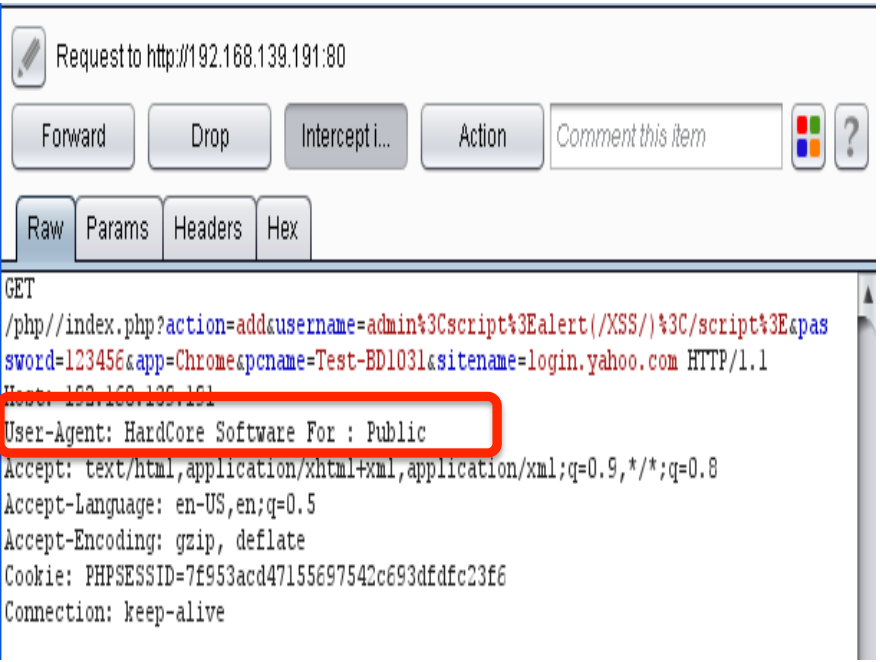
- Source & sink: index.php

```
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++;
```

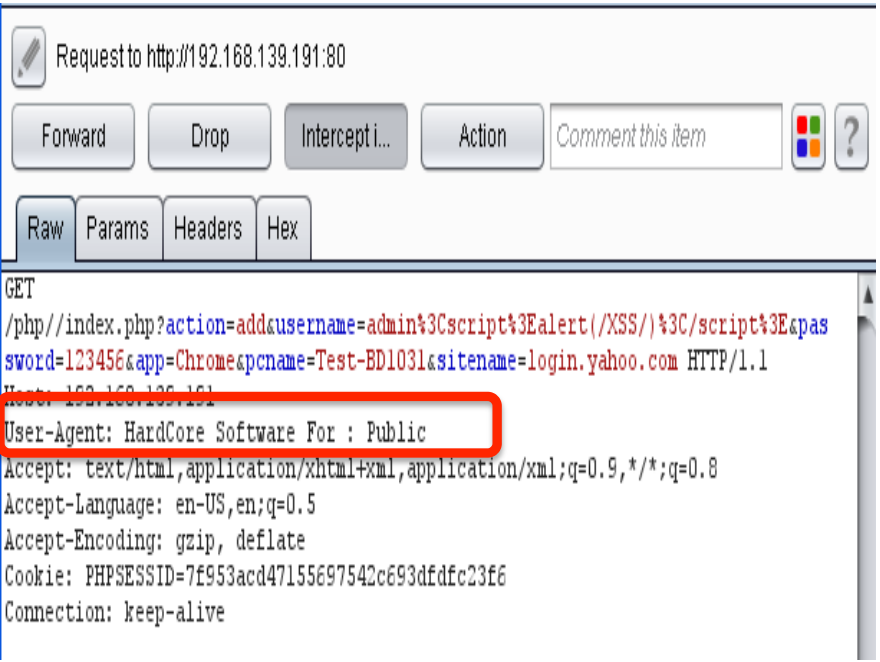
ISR stealer persistent cross site scripting

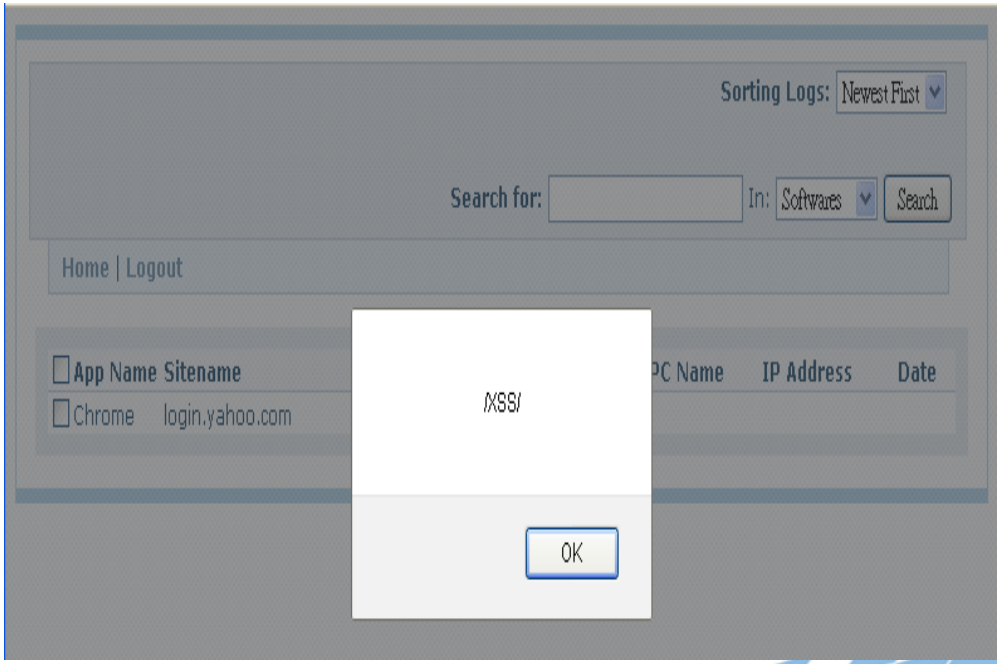


ISR stealer persistent cross site scripting



ISR stealer persistent cross site scripting



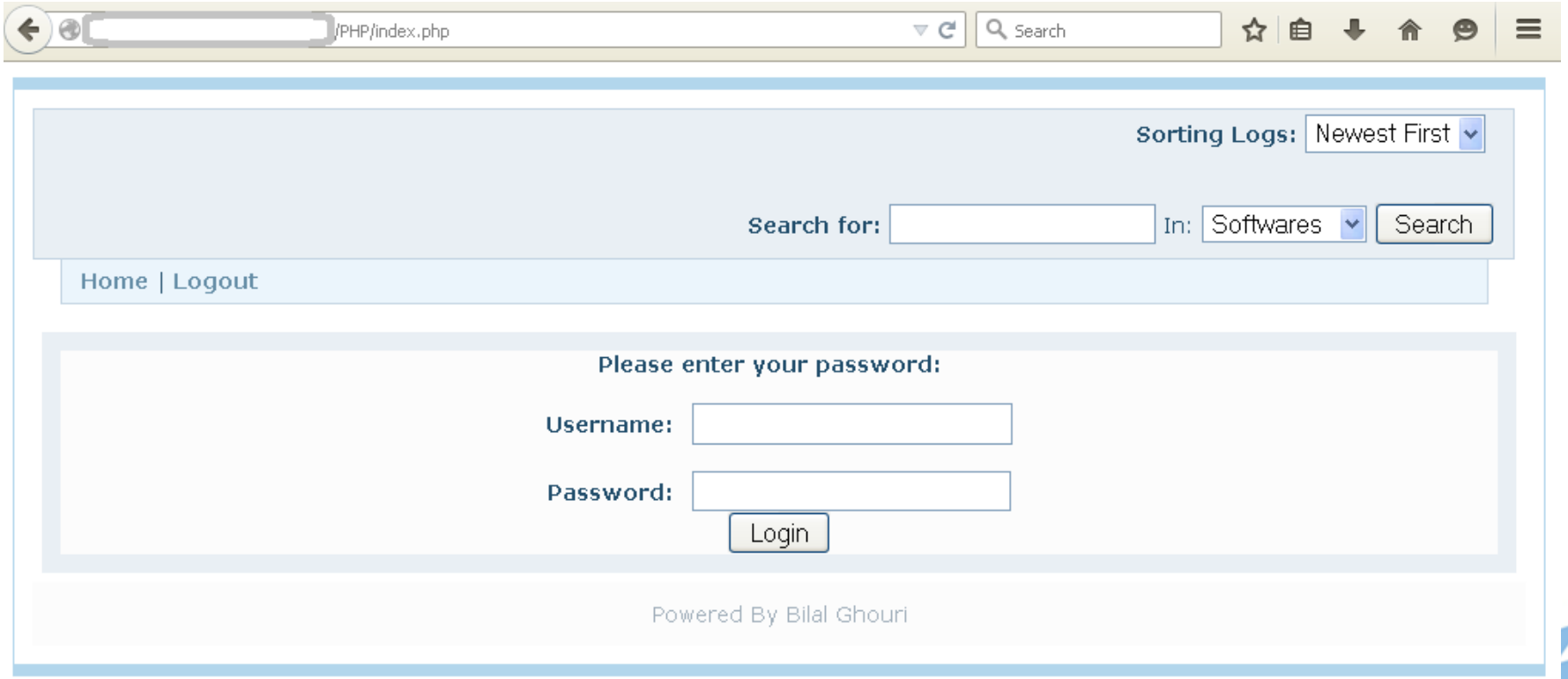


Campaign attribution

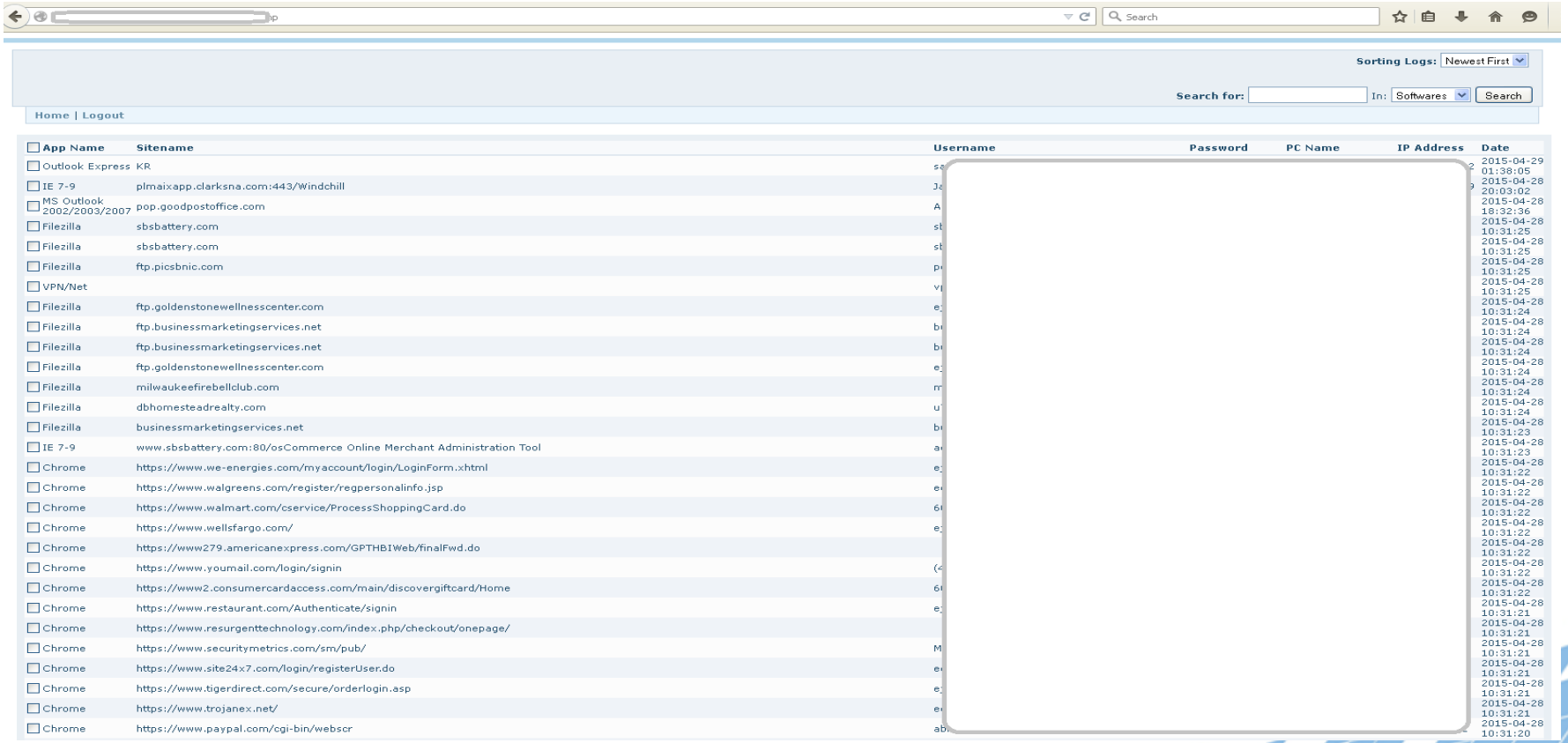
- USER_AGENT:
  - Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.118 Safari/537.36 OPR/28.0.1750.51
- IP addresses:
  - 41.220.69.115 - AS 29465 (Nigeria)
  - 41.220.69.185 - AS 29465 (Nigeria)

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

ISR Stealer admin panel



ISR Stealer admin panel

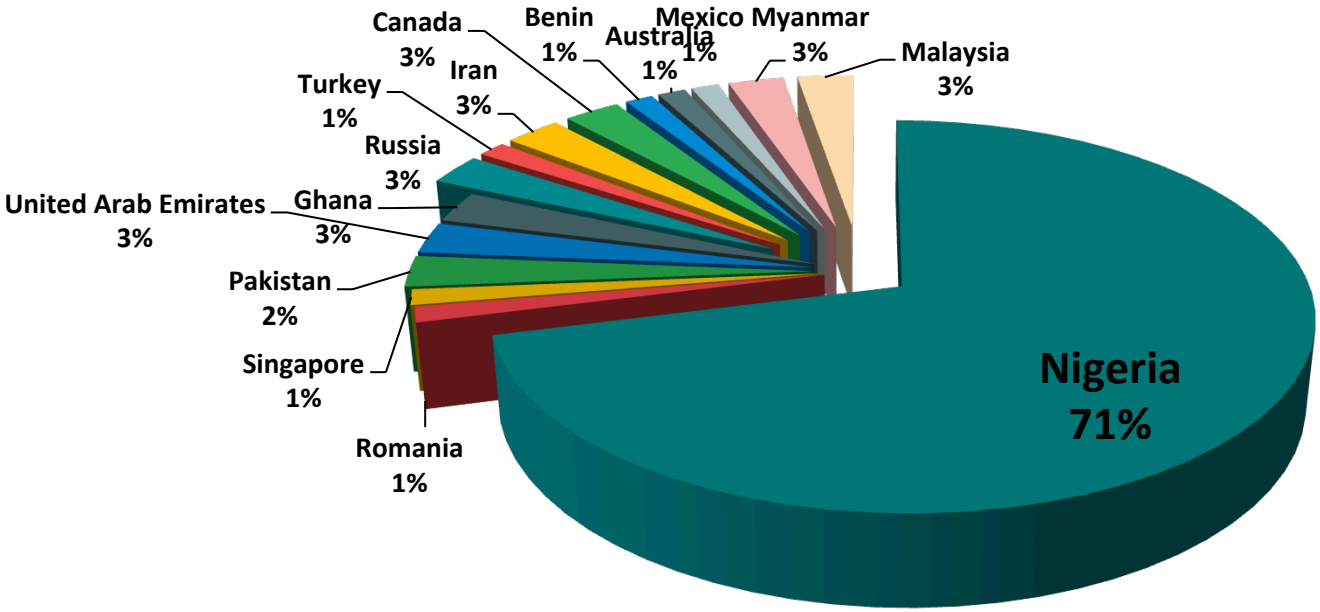


App Name	Sitename	Username	Password	PC Name	IP Address	Date
Outlook Express	KR					2015-04-29 01:38:05
IE 7-9	plmaixapp.clarksna.com:443/Windchill					2015-04-28 20:03:02
MS Outlook 2002/2003/2007	pop.goodpostoffice.com					2015-04-28 18:32:36
Filezilla	sbsbattery.com					2015-04-28 10:31:25
Filezilla	sbsbattery.com					2015-04-28 10:31:25
Filezilla	ftp.picsbnic.com					2015-04-28 10:31:25
VPN/Net						2015-04-28 10:31:25
Filezilla	ftp.goldenstonewellnesscenter.com					2015-04-28 10:31:24
Filezilla	ftp.businessmarketingservices.net					2015-04-28 10:31:24
Filezilla	ftp.businessmarketingservices.net					2015-04-28 10:31:24
Filezilla	ftp.goldenstonewellnesscenter.com					2015-04-28 10:31:24
Filezilla	milwaukeefirebellclub.com					2015-04-28 10:31:24
Filezilla	dbhomesteadrealty.com					2015-04-28 10:31:24
Filezilla	businessmarketingservices.net					2015-04-28 10:31:23
IE 7-9	www.sbsbattery.com:80/osCommerce Online Merchant Administration Tool					2015-04-28 10:31:23
Chrome	https://www.we-energies.com/myaccount/login/LoginForm.xhtml					2015-04-28 10:31:22
Chrome	https://www.walgreens.com/register/regpersonalinfo.jsp					2015-04-28 10:31:22
Chrome	https://www.walmart.com/cservice/ProcessShoppingCard.do					2015-04-28 10:31:22
Chrome	https://www.wellsfargo.com/					2015-04-28 10:31:22
Chrome	https://www279.americanexpress.com/GPTHBIWeb/finalFwd.do					2015-04-28 10:31:22
Chrome	https://www.youmail.com/login/signin					2015-04-28 10:31:22
Chrome	https://www2.consumercardaccess.com/main/discovergiftcard/Home					2015-04-28 10:31:22
Chrome	https://www.restaurant.com/Authenticate/signin					2015-04-28 10:31:21
Chrome	https://www.resurgenttechnology.com/index.php/checkout/onepage/					2015-04-28 10:31:21
Chrome	https://www.securitymetrics.com/sm/pub/					2015-04-28 10:31:21
Chrome	https://www.site24x7.com/login/registerUser.do					2015-04-28 10:31:21
Chrome	https://www.tigerdirect.com/secure/orderlogin.asp					2015-04-28 10:31:21
Chrome	https://www.trojanex.net/					2015-04-28 10:31:21
Chrome	https://www.paypal.com/cgi-bin/webscr					2015-04-28 10:31:20

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

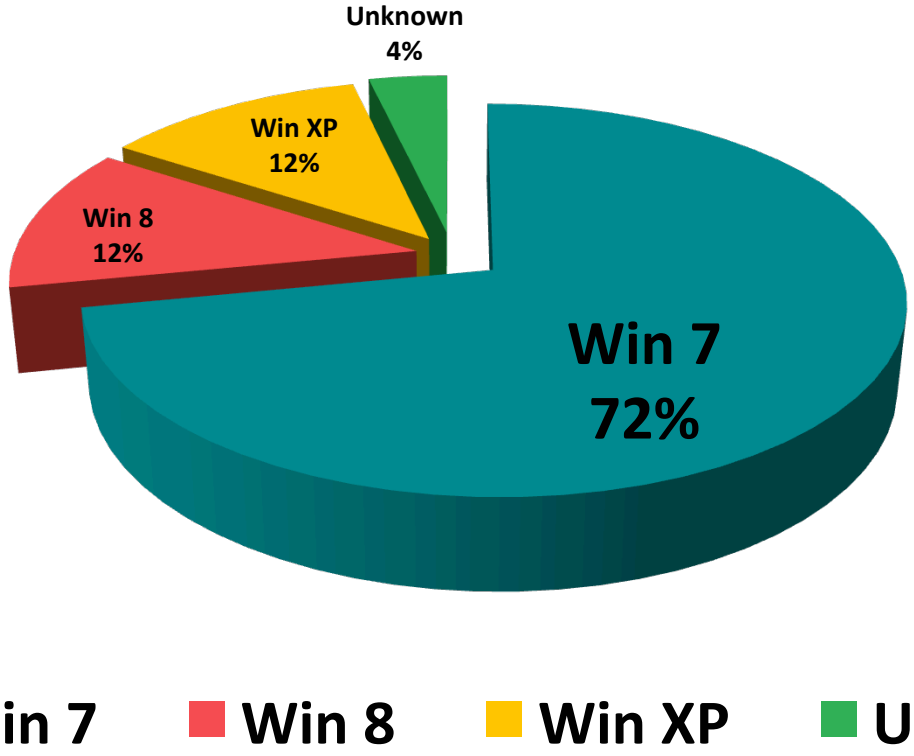
Actors by country



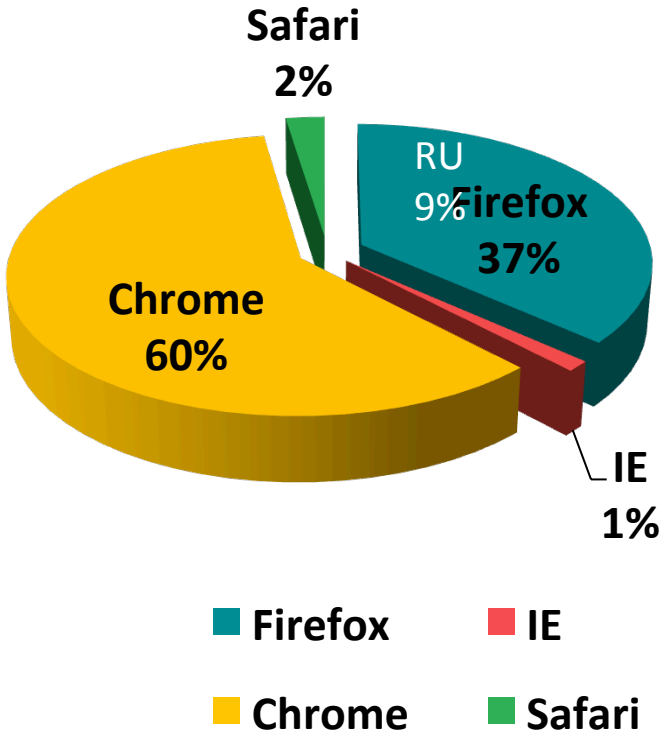
Nigeria ASN
29465
36873
37076
37127
37148

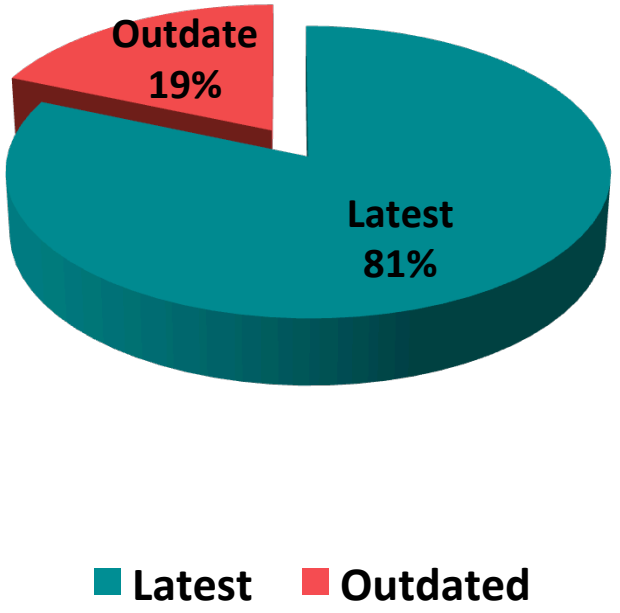
Nigeria
Romania
Singapore
Pakistan
United Arab Emirates
Ghana
Russia
Turkey
Iran
Canada
Benin
Australia
Mexico
Myanmar
Malaysia

Actors by OS



Actors by browser and by flash version



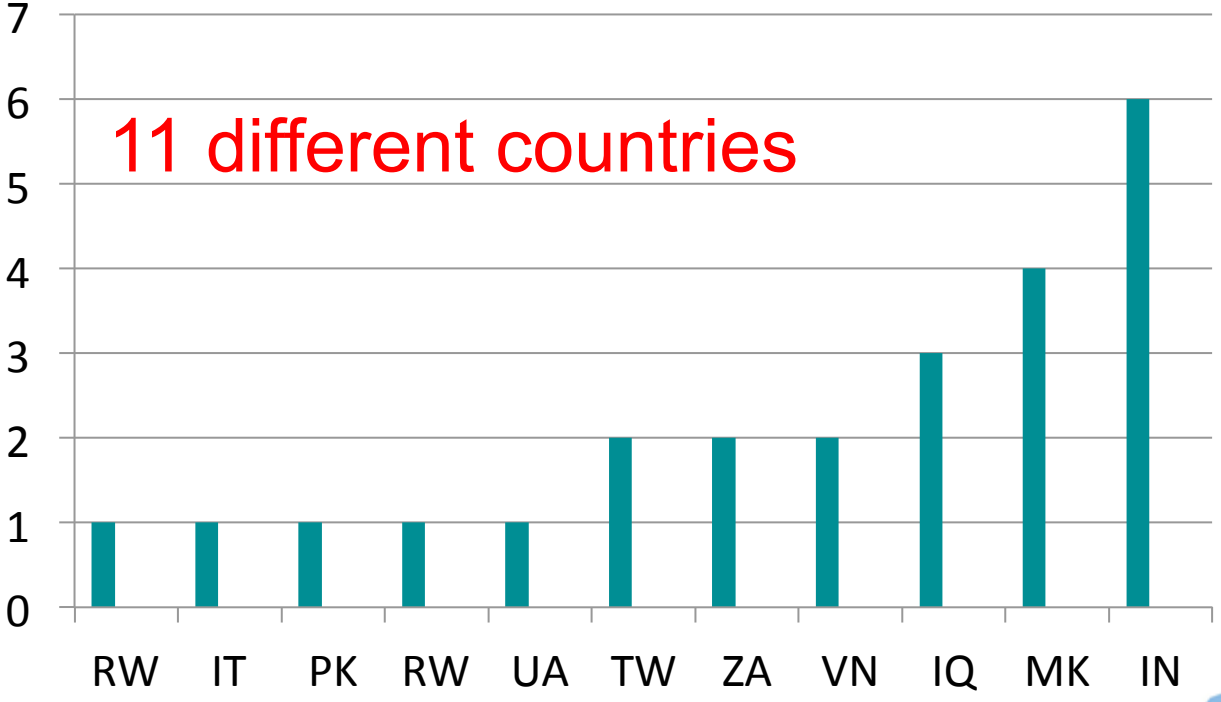


Nigerian gang evolution

- 2014: Traditional attachment techniques
  - Executable files (exe, scr) compressed within a Zip file
  - Purchase_Order.zip or Payment Advice pdf.zip etc.
  - Malware: Zeus / IceIX / 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, environt 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