



Advanced IT infrastructure control:
Do it better, safer, easier and cheaper

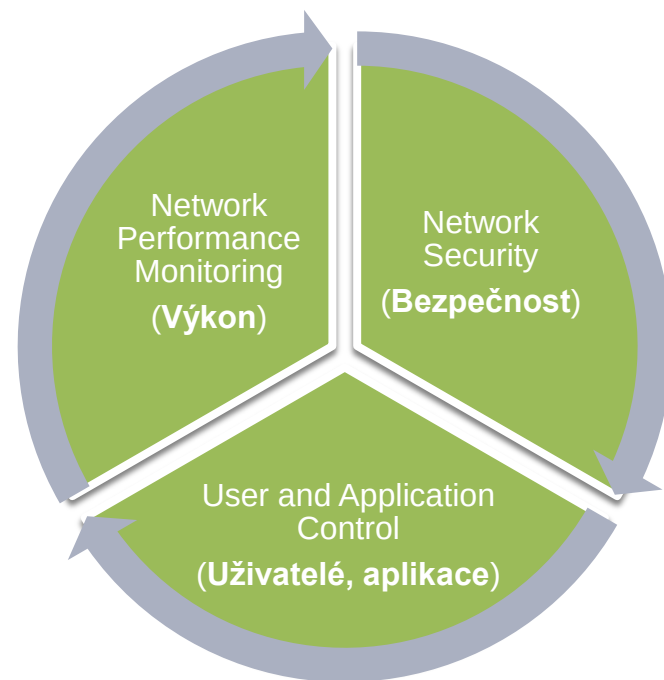
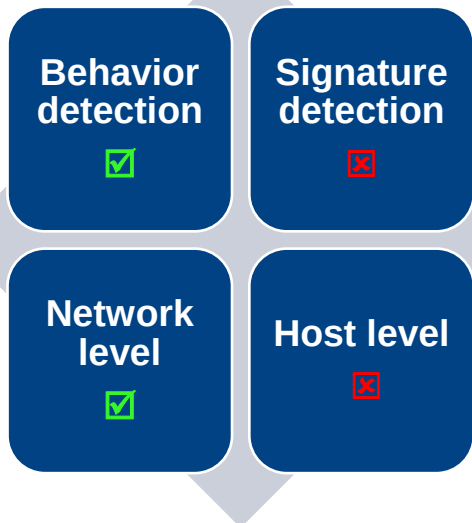
FlowMon ADS 3

Nová generace řešení pro analýzu provozu datové sítě

FlowMon ADS

Přehled produktu

- ▶ Řešení pro **automatickou analýzu provozu datové sítě**
- ▶ Určeno k detekci provozních a bezpečnostních problémů a podezřelých aktivit
- ▶ Založeno na automatické analýze provozu, strojovém učení a profilování chování





[Home](#) | [Gadgets](#) | [Apps & Web](#) | [News](#) | [Reviews & Features](#) | [Companies](#)

SECURITY

DNSChanger: FBI Warns Infected Computers Will Lose Web, Email Access in July

By **MATT PECKHAM** | [@mattpeckham](#) | April 23, 2012 | **8**

Summary

DNSChanger is a trojan that will change the infected system's Domain Name Server (DNS) settings, in order to divert traffic to unsolicited, and potentially illegal sites.

The trojan is usually a small file (about 1.5 kilobytes) that is designed to change the 'NameServer' Registry key value to a custom IP address. This IP address is usually encrypted in the body of a trojan. As a result of this change a victim's computer will contact the newly assigned DNS server to resolve names of different web servers.

DNS Changer

Stanice před infekcí

DNS Changer Check-Up - Clean - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Qualys BrowserCheck x DNS Changer Check-Up - Clean x +

www.dns-ok.us

Latest Headlines Kontrola malware DN... DNSChanger-Check-... Qualys BrowserCheck

DNS Changer Check-Up



DNS Resolution = **GREEN**

Your computer appears to be looking up IP addresses correctly!

Had your computer been infected with DNS changer malware you would have seen a red background. Please note, however, that if your ISP is redirecting DNS traffic for its customers you would have reached this site even though you are

<http://dns-changer.eu/en/check.php>

```
C:\cmd\cmd.exe

Connection-specific DNS Suffix . : 
Description . . . . . : VIA Rhine II Fast Ethernet Adapter
Physical Address. . . . . : 00-0A-E4-A2-BF-4B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.1.54
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.1.1
DHCP Server . . . . . : 10.0.1.1
DNS Servers . . . . . : 10.0.1.1
Lease Obtained. . . . . : Friday, May 18, 2012 12:03:12 PM
Lease Expires . . . . . : Saturday, May 19, 2012 12:03:12 PM

C:\cmd>_
```

DNS Changer

Stanice po infekci



DNS Changer Check-Up



DNS Resolution = **RED**

Your computer is using the DNS Changer nameservers and is therefore probably infected.

It is extremely difficult to remove this particular malware from your system but we may be able to help. For suggestions on how to fix this problem please visit <http://www.dcwg.org/fix/>.

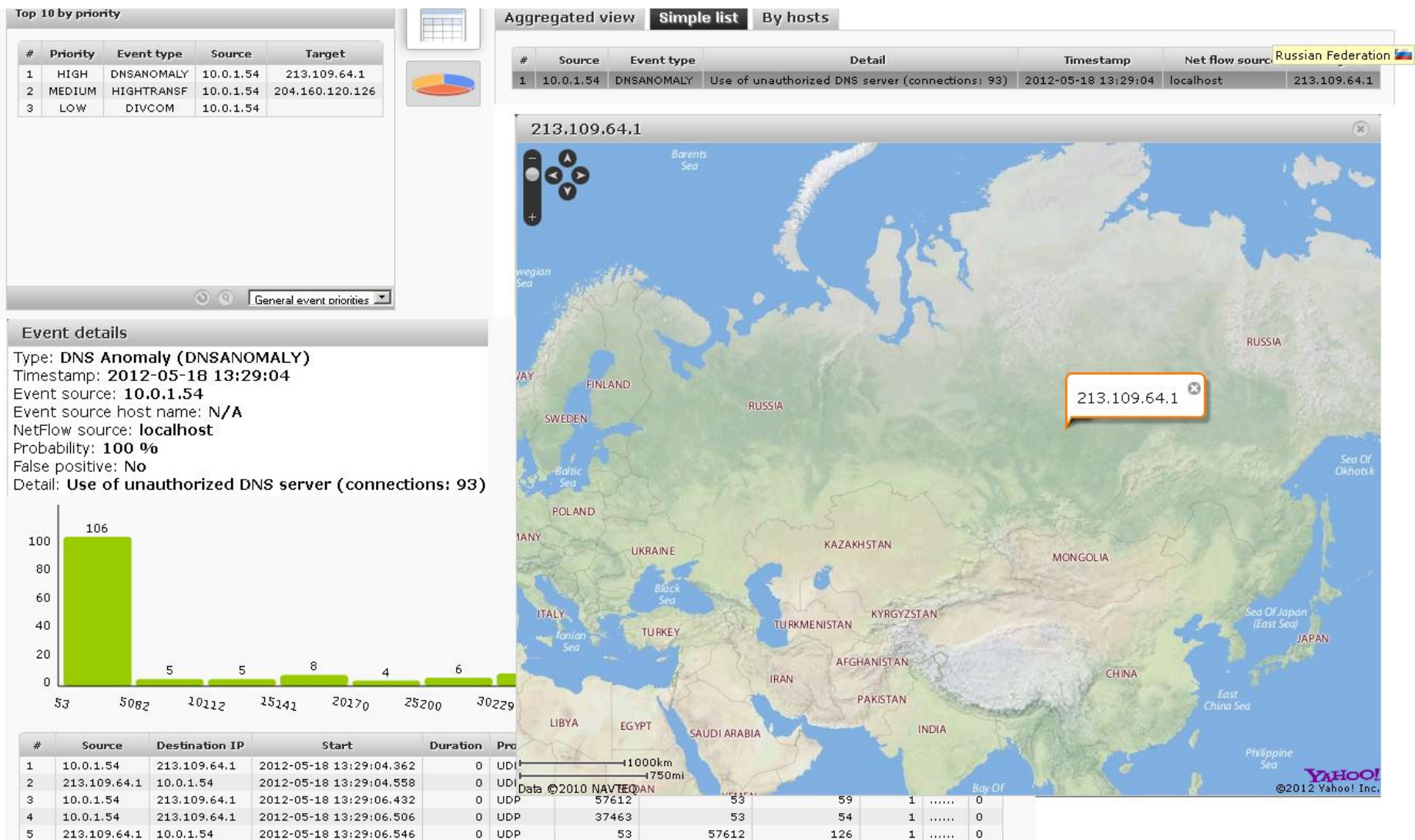
```
C:\cmd\cmd.exe

Connection-specific DNS Suffix . : .cz
Description . . . . . : VIA Rhine II Fast Ethernet Adapter
Physical Address. . . . . : 00-0A-E4-A2-BF-4B
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 10.0.1.54
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.1.1
DHCP Server . . . . . : 10.0.1.1
DNS Servers . . . . . : 213.109.64.1
                        213.109.79.254
Lease Obtained. . . . . : Friday, May 18, 2012 9:55:22 AM
Lease Expires . . . . . : Saturday, May 19, 2012 9:55:22 AM

C:\cmd>
```


DNS Changer

Detekováno ve FlowMon ADS

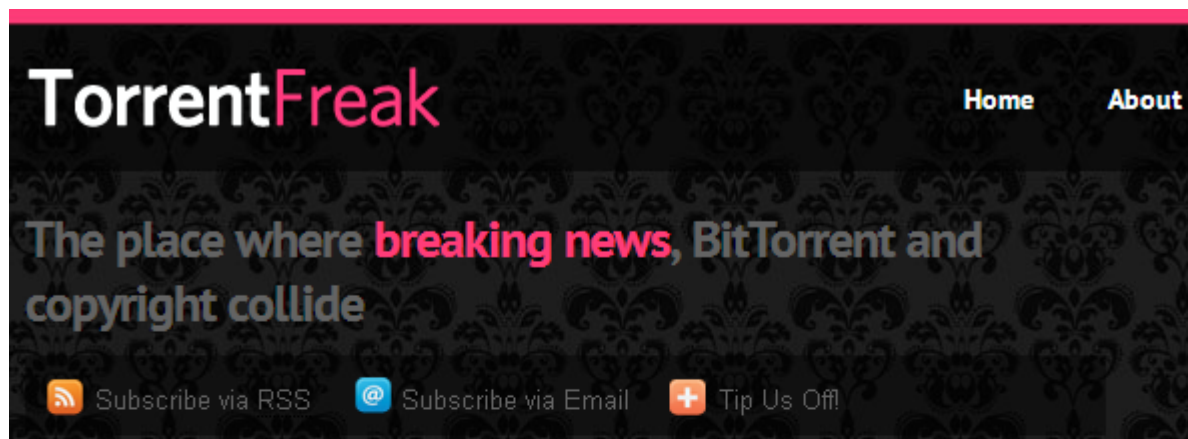


DNS Changer

Shrnutí

- ▶ **Z pohledu uživatele naprosto transparentní a neviditelné**
- ▶ Umožňuje přesměrovat provoz k podvodným stránkám a službám, **phishing!!!**
 - ▶ 7 osob z Estonska a Ruska bylo obviněno, prostřednictvím viru DNS Changer vydělali **\$14 mil.** během 5 let
- ▶ Může být snadno přehlédnut antivirem, existuje mnoho způsobů modifikace DNS
- ▶ Vážná hrozba sledovaná i FBI
 - ▶ http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

	Tradiční metody a přístupy	FlowMon ADS
Obsah paketů (L7)	Legitimní DNS dotaz	neřeší
Flow data (L3/L4)	neřeší	Použití nelegitimních DNS serverů
Profil chování	neřeší	Významně se odlišuje od ostatních PC v síti



How To Encrypt BitTorrent Traffic

 Ernesto

 April 16,
2006

 302

 bittorrent,
rc4_encryption,
traffic_shaping

 Print

More and more ISP's are limiting and throttling BitTorrent traffic on their networks. By throttling BitTorrent traffic the speed of BitTorrent downloads decrease, and high speed downloads are out of the question.

The list of ISP's that limit BitTorrent traffic, or plan to do so is growing every day, and according to the BBC, the 'bandwidth war' has begun.

Are you not sure if your traffic is being throttled Check the list of bad ISP's.

But there is a solution. Encrypting your torrents will prevent throttling ISP's from shaping your traffic. I will explain how to enable encryption in **Azureus**, **uTorrent**, and **Bitcomet**, the three most popular torrent clients.

Současné hrozby

Šifrovaný provoz P2P sítí

- ▶ Fáze 1 – řada neúspěšných spojení k poskytovatelům obsahu
- ▶ Fáze 2 – souběžné stahování dat, nestandardní porty
- ▶ Fáze 3 – současné končení stahování z řady zdrojů
- ▶ **Analýza obsahu není nutná!**

	Tradiční metody a přístupy	FlowMon ADS
Obsah paketů (L7)	neznámý, zašifrováno	neřeší
Flow data (L3/L4)	neřeší	Lze detekovat specifické chování
Profil chování	neřeší	Řada komunikačních partnerů a zemí

Současné hrozby

The Onion Router

- ▶ Nástroj pro zajištění anonymity na síti Internet
- ▶ Může maskovat nežádoucí aktivity a aplikace ...
- ▶ Používán pro přístup k blokovánému obsahu
- ▶ V aktuální verzi odolný proti analýze obsahu přenášených dat (L7)



The screenshot shows the Tor Project website. At the top left is the Tor logo, which consists of the word 'Tor' in a stylized purple font with a yellow onion bulb integrated into the letter 'o'. To the right of the logo are three navigation links: 'Home' (highlighted with a yellow background), 'About Tor', and 'Documentation'. Below the navigation bar is a large green banner with the text 'Anonymity Online' in white. Underneath this text is the phrase 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' in a smaller white font. On the left side of the banner is a small illustration of a yellow onion bulb. To the right of the onion is a purple button with the text 'Download Tor' and a small downward arrow icon. On the right side of the banner, there is a list of three bullet points, each preceded by a right-pointing arrow: 'Tor prevents anyone from learning your location or browsing habits.', 'Tor is for web browsers, instant messaging clients, remote logins, and more.', and 'Tor is free and open source for Windows, Mac, Linux/Unix, and Android'.

Tor

[Home](#) [About Tor](#) [Documentation](#)

Anonymity Online

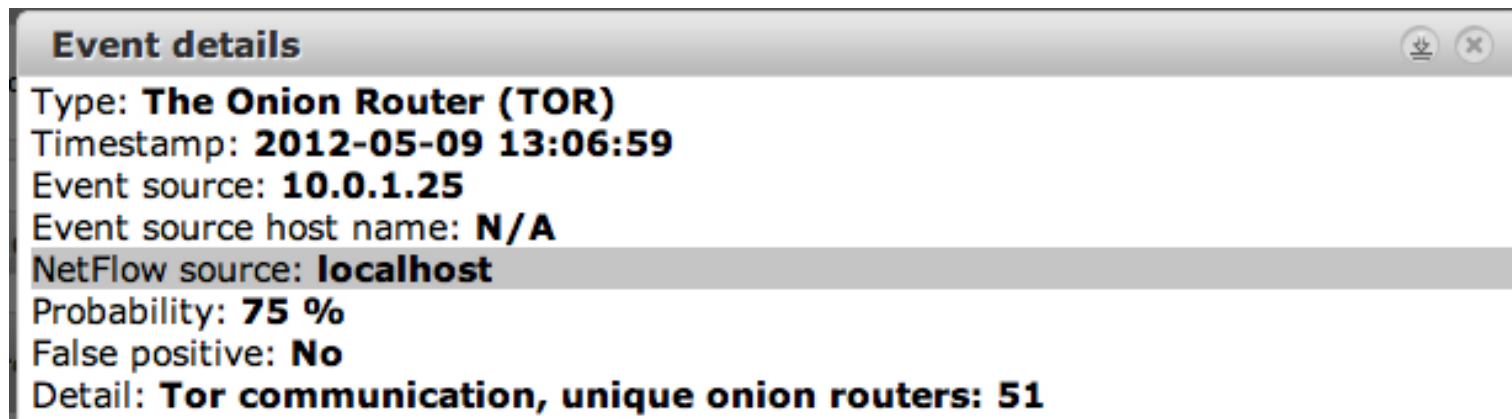
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

 [Download Tor](#) ↓

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Současné hrozby

The Onion Router



	Tradiční metody a přístupy	FlowMon ADS
Obsah paketů (L7)	neznámý, zašifrováno	neřeší
Flow data (L3/L4)	neřeší	Pravděpodobnostní heuristický algoritmus
Profil chování	neřeší	V závislosti na míře využití řada unikátních partnerů

Současné hrozby

Řada dalších ...

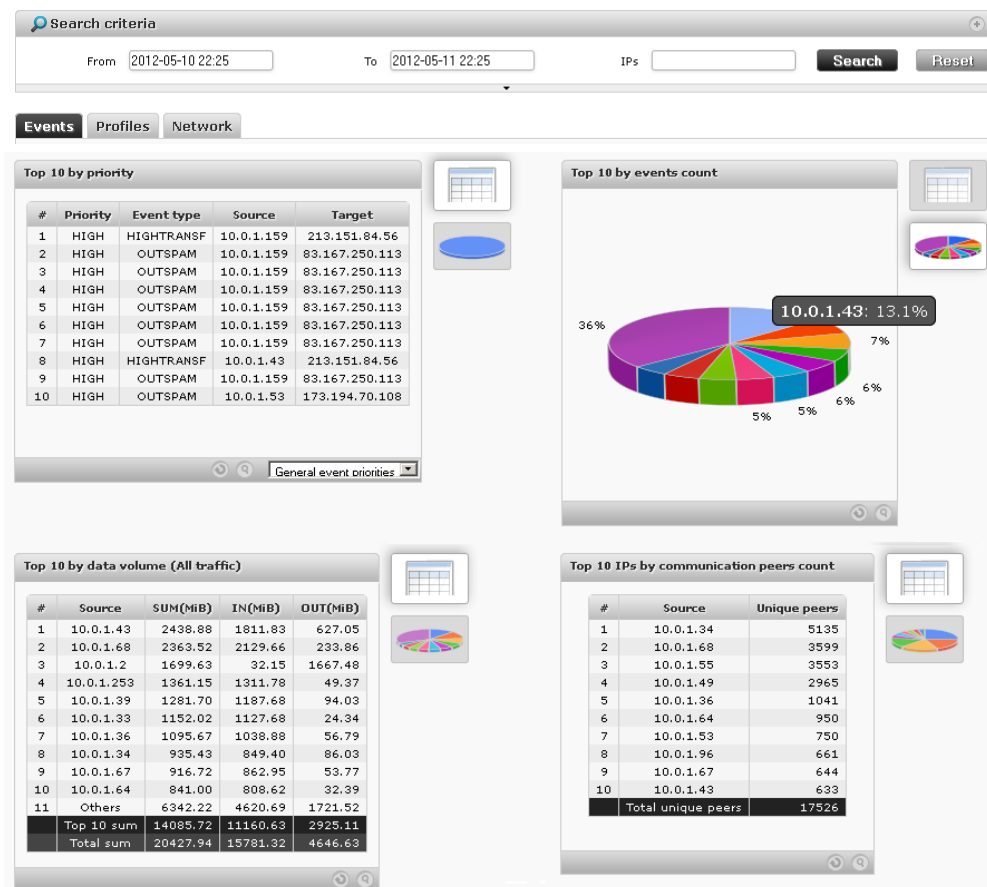
- ▶ Útoky (slovníkové útoky proti síťovým službám, útoky DoS/DDoS, útoky typu DNS amplification, ...)
- ▶ Nežádoucí aplikace, které mohou ohrozit bezpečnost sítě (TeamViewer, Skype, ICQ, MS Messenger, ...)
- ▶ Porušení bezpečnostních politik (obcházení proxy, úniky dat, ...)
- ▶ Bezpečnost není jediná věc, na které záleží (výpadky služeb, konfigurační problémy, tunelování IPv6 v IPv4 sítích, ...)

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:46:40	localhost	74.114.28.110
2	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:41:39	localhost	74.114.28.110
3	10.0.1.55	SCANS	horizontal TCP SYN scan (attempts with response: 21, attempts without response: 94, targets: 110, port list: 6881)	2012-05-09 11:37:48	localhost	27.130.215.94, 31.37.244.126, 31.150.26.23, 49.0.3.222, 62.82.217.58, 62.168.45.106, 67.81.64.156, 71.192.37.125, 77.65.47.91, 77.100.222.129, , ...
4	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:36:35	localhost	74.114.28.110
5	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:31:32	localhost	74.114.28.110
6	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:24:55	localhost	74.114.28.110
7	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:20:30	localhost	74.114.28.110
8	10.0.1.55	SCANS	horizontal TCP SYN scan (attempts with response: 24, attempts without response: 78, targets: 102, port list: 6881)	2012-05-09 11:17:55	localhost	37.6.190.131, 37.15.187.111, 37.17.113.24, 37.55.101.210, 41.141.93.88, 41.145.34.97, 41.201.191.45, 41.221.105.69, 46.12.143.36, 46.13.13.81, , ...
9	10.0.1.73	ONLINEMSG	www.meebo.com	2012-05-09 11:16:44	localhost	74.114.28.110
10	10.0.1.55	SCANS	horizontal TCP SYN scan (attempts with response: 20, attempts without response: 87, targets: 107, port list: 6881, 6882)	2012-05-09 11:12:42	localhost	2.25.13.238, 2.101.4.177, 2.235.40.109, 31.181.59.45, 46.13.16.120, 46.13.56.144, 46.13.71.2, 46.25.29.173, 46.27.1.113, 46.44.59.126, , ...

FlowMon ADS

Dashboard

- Okamžitá indikace problémů
- Zobrazení formou tabulky/grafu
- Detaily a drill down na vyžádání
- Události
 - Top 10 událostí dle priority
 - 10 nejnovějších událostí
 - Top 10 nejčastějších typů událostí
 - Top 10 IP adres dle počtu událostí
- Profily chování (top uživatelé)
 - Top 10 IP adres dle objemu dat
 - Top 10 IP adres dle počtu spojení
 - Top 10 IP adres dle komunikačních partnerů
 - Top 10 IP adres dle cílových zemí
- Chování celé sítě
 - Top 10 využívaných služeb
 - Top 10 poskytovaných služeb
 - Top 10 zemí



- ▶ Útoky (skenování portů, slovníkové útoky, DoS, Telnet)
- ▶ Anomálie provozu (DNS, multicast, vysoká variabilita komunikace)
- ▶ Anomálie chování IP adres (změna profilu chování)
- ▶ Nežádoucí aplikace (P2P sítě, on-line komunikátory, TOR, TeamViewer)
- ▶ Malware (viry, spyware, botnety, komunikace s adresami na blacklistech)
- ▶ Pošta (odchozí SPAM, nelegitimní poštovní servery)
- ▶ Provozní problémy (zpoždění, přetížení, reverzní DNS záznamy, výpadky služeb)
- ▶ Potenciální úniky dat (upload na veřejné servery, webová úložiště)
- ▶ Porušení bezpečnostních politik (obcházení proxy serveru, neznámá zařízení)
- ▶ Specifické metody (sledování senzorové sítě)

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.1.1.84	UPLOAD	Uploaded: 38.83 MiB, downloaded: 0.57 MiB, ports: 80	2012-05-10 11:43:34	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
2	10.1.1.84	UPLOAD	Uploaded: 243.48 MiB, downloaded: 4.07 MiB, ports: 80	2012-05-10 11:37:19	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
3	10.1.1.84	UPLOAD	Uploaded: 199.97 MiB, downloaded: 4.49 MiB, ports: 80	2012-05-10 11:33:47	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
4	10.1.1.84	UPLOAD	Uploaded: 232.03 MiB, downloaded: 4.38 MiB, ports: 80	2012-05-10 11:28:32	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
5	10.1.1.84	UPLOAD	Uploaded: 197.11 MiB, downloaded: 3.74 MiB, ports: 80	2012-05-10 11:24:10	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)

FlowMon ADS

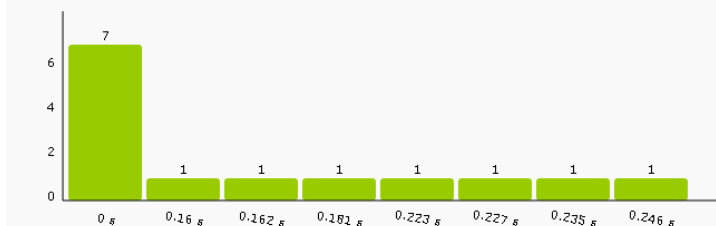
Analytické možnosti

- Určeny k průzkumu a analýze provozu, který způsobil událost
 - Grafická reprezentace přenosů dat na síti
 - Uzly reprezentují IP adresy
 - Hrany reprezentují přenosy dat mezi IP adresami
 - Vizualizace je živá a interaktivní, detaily a další provoz je dostupný na vyžádání
- Export důkazů pro budoucí použití

Type: **Instant Messaging (INSTMSG)**
Timestamp: **2012-05-11 15:48:45**
Event source: **10.0.1.87**
Event source host name: **N/A**
NetFlow source: **localhost**
Detail: **Skype protocol (Skype), unique servers: 1**

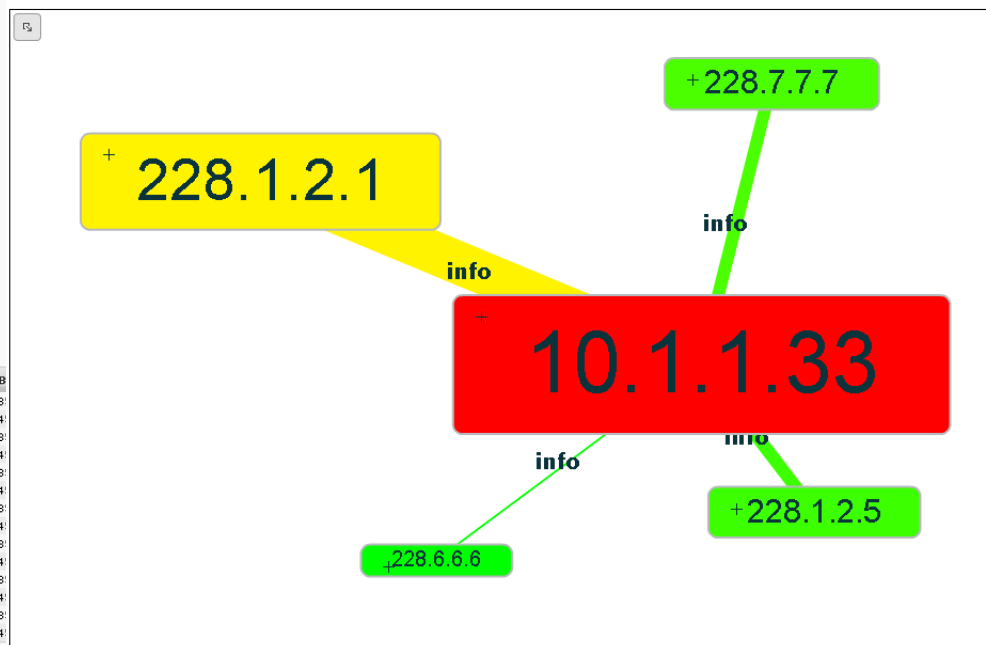
[Save as text file](#)

Count of flows due to Duration



#	Source	Destination IP	Start	Duration	Protocol	Source port	Destination port	Transferred (B)
1	10.0.1.87	193.120.199.16	2012-05-11 15:44:00.684	0.246	TCP	3911	12350	8
2	193.120.199.16	10.0.1.87	2012-05-11 15:44:00.735	0	TCP	12350	3911	4
3	10.0.1.87	193.120.199.16	2012-05-11 15:45:35.452	0.235	TCP	3911	12350	8
4	193.120.199.16	10.0.1.87	2012-05-11 15:45:35.506	0	TCP	12350	3911	4
5	10.0.1.87	193.120.199.16	2012-05-11 15:47:10.912	0.162	TCP	3911	12350	8
6	193.120.199.16	10.0.1.87	2012-05-11 15:47:10.963	0	TCP	12350	3911	4
7	10.0.1.87	193.120.199.16	2012-05-11 15:48:45.787	0.223	TCP	3911	12350	8
8	193.120.199.16	10.0.1.87	2012-05-11 15:48:45.837	0	TCP	12350	3911	4
9	10.0.1.87	193.120.199.16	2012-05-11 15:50:22.738	0.227	TCP	3911	12350	8
10	193.120.199.16	10.0.1.87	2012-05-11 15:50:22.792	0	TCP	12350	3911	4
11	10.0.1.87	193.120.199.16	2012-05-11 15:51:57.999	0.160	TCP	3911	12350	8
12	193.120.199.16	10.0.1.87	2012-05-11 15:51:58.054	0	TCP	12350	3911	4
13	10.0.1.87	193.120.199.16	2012-05-11 15:53:32.745	0.181	TCP	3911	12350	8
14	193.120.199.16	10.0.1.87	2012-05-11 15:53:32.797	0	TCP	12350	3911	4

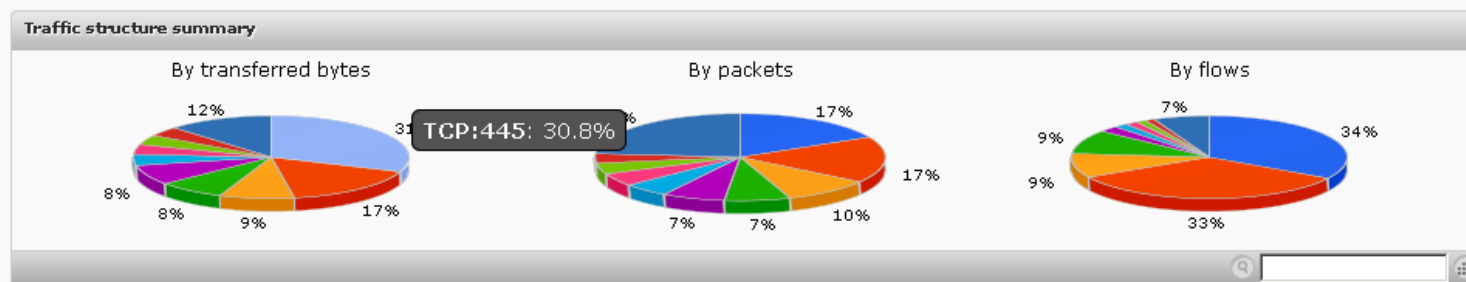
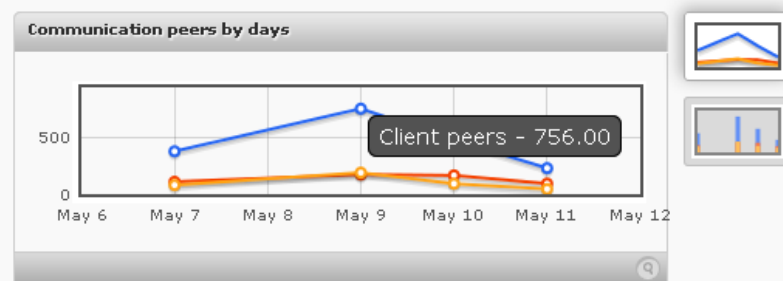
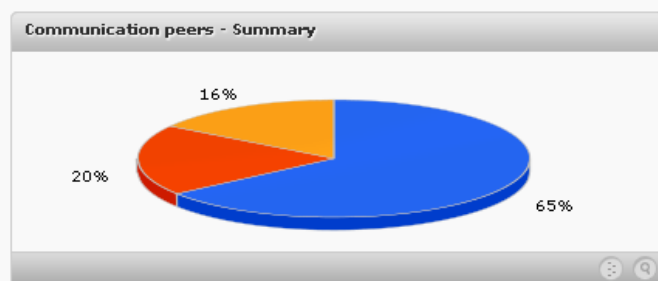
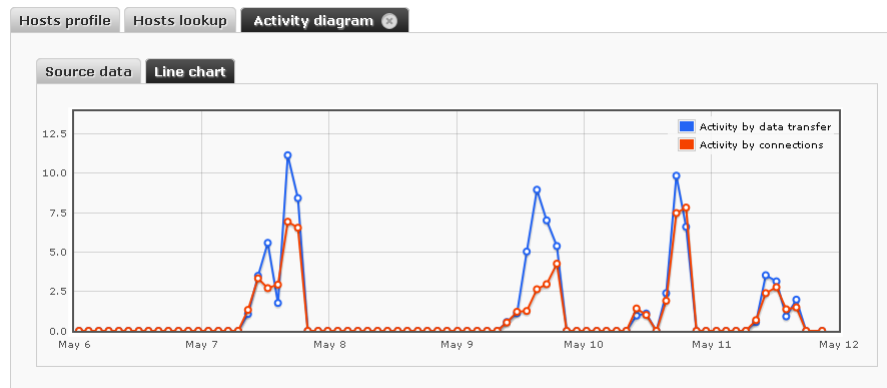
Event type	Timestamp	Source	Resolved source IP	Detail	Probability	Net flow source	False positive
Multicast traffic (MULTICAST)	2012-05-11 16:24:14	10.1.1.33	N/A	Reserved, attempts: 63	100 %	localhost	No



FlowMon ADS

Profily chování

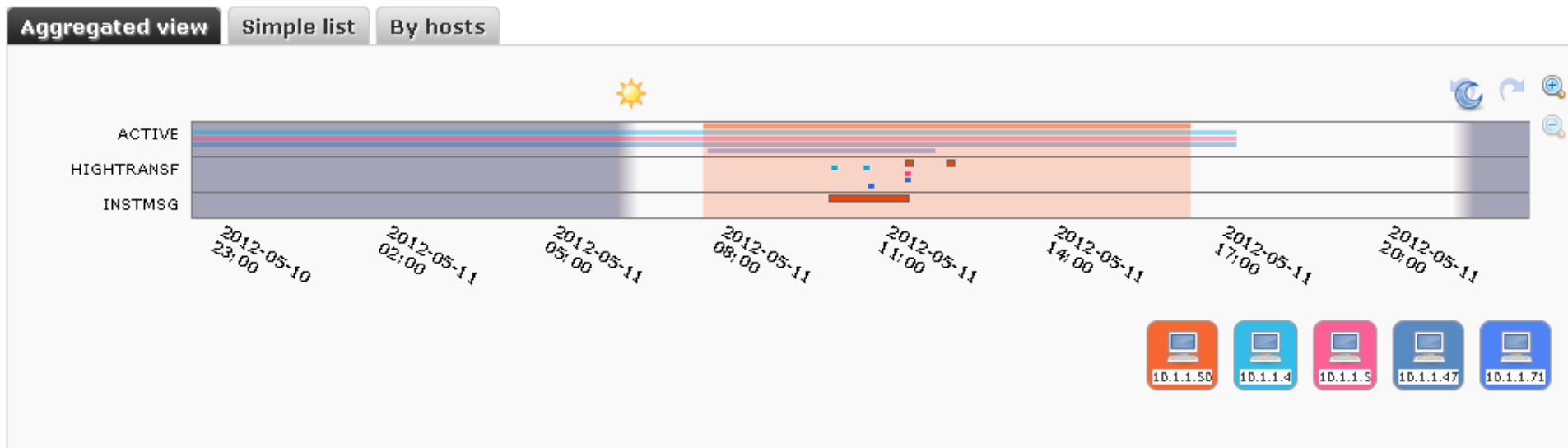
- Obecná role zařízení – klient/server
- Objem provozu
- Unikátní komunikační partneři
- Využívané a poskytované služby
- Celkový poměr aktivity IP adresy
- Vyhledávání klientů/serverů
- Vyhledávání služeb



FlowMon ADS

Pokročilé funkce

- ▶ Agregovaná vizualizace
 - ▶ Aktivita zařízení a trvání událostí na časové ose
- ▶ Podpora DHCP
 - ▶ Identita IP adresy je ověřena a uložena v okamžiku vygenerování události
- ▶ Podpora PROXY
 - ▶ Korelace NetFlow dat na obou stranách proxy serveru
- ▶ Podpora SIEM systémů
 - ▶ Export událostí protokolem Syslog nebo SNMP



	Tradiční metody a přístupy	FlowMon ADS
Místo instalace	Perimetr	LAN, datové centrum, perimetr
Metoda detekce	Analýza L7, na základě signatur	Analýza L3/L4, statistika, chování
Druh hrozeb	Známé hrozby	Známé L3/L4 a neznámé hrozby
Rozsah	Bezpečnostní hrozby	Bezpečnostní, provozní a výkonnostní problémy

- Cílem FlowMon ADS je doplnit a rozšířit schopnosti tradičních nástrojů pro ochranu sítě a detekci anomálií!

Kontakt

AdvaICT, a. s.

Jundrovská 618/31, 624 00 Brno

tel.: +420 511 112 170,

info@advaiCT.com, www.advaiCT.com



Správa IT infrastruktury:
lépe, snadněji, bezpečněji a levněji