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

FlowMon ADS 3

Nová generace řešení pro analýzu provozu datové sítě

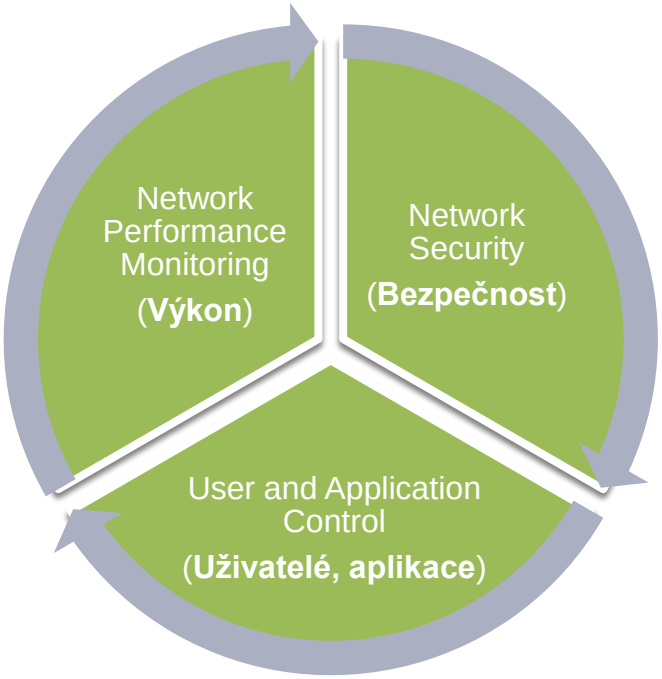
ADVAiCT

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

Behavior detection ☑	Signature detection ☒
Network level ☑	Host level ☒



DNS Changer

TIME Techland
News and reviews about gadgets, gear, apps and the web

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

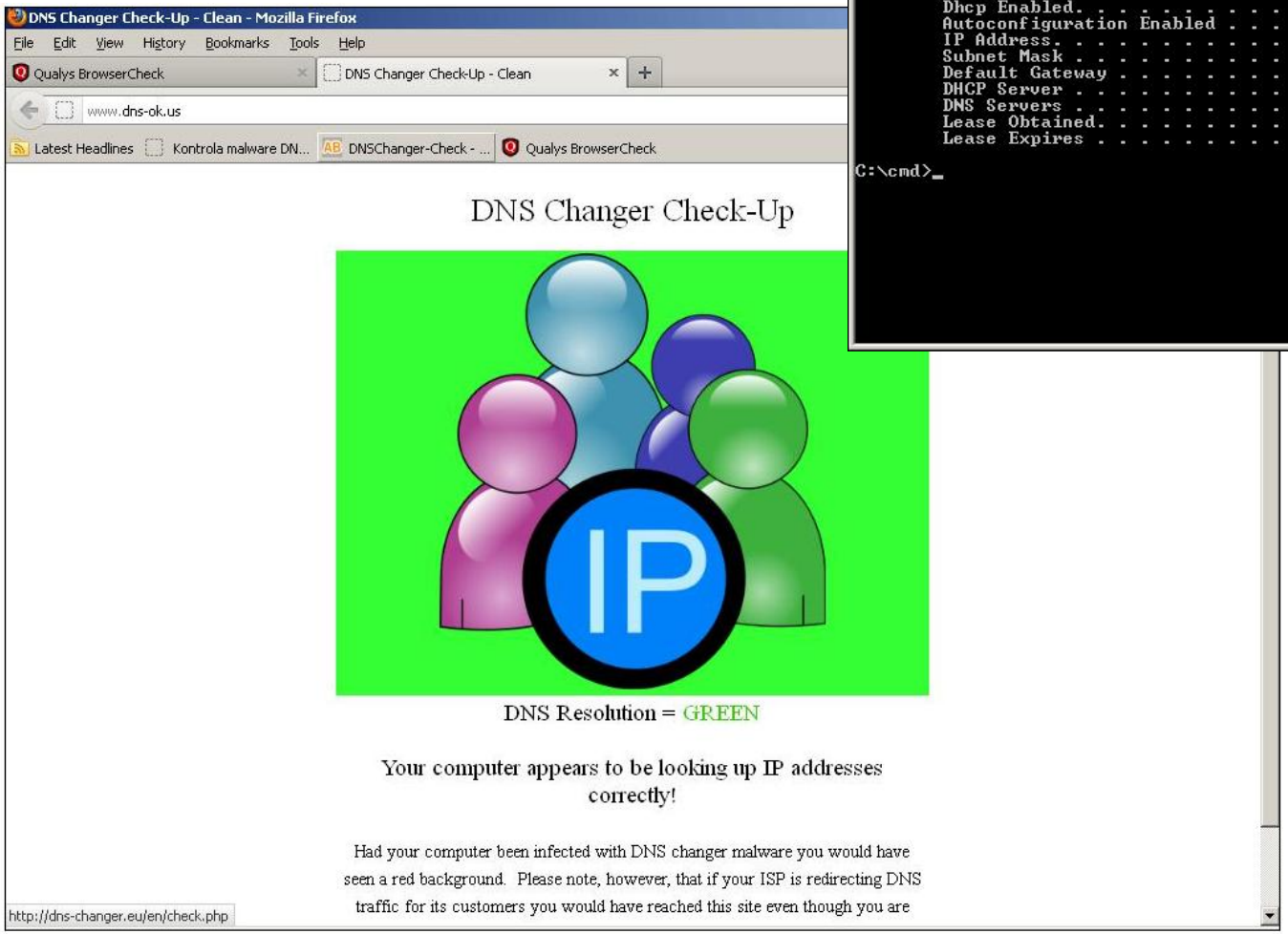
Summary

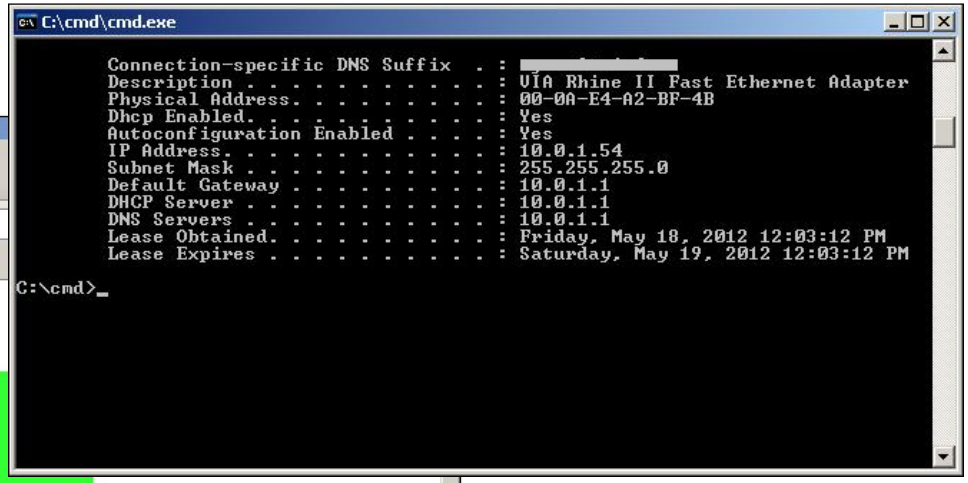
DNSChanger is a trojan that will change the infected system's Domain Name Server (DNS) settings, in order to divert traffic to unsolicited, and potentially illegal sites.

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 webservers.

DNS Changer

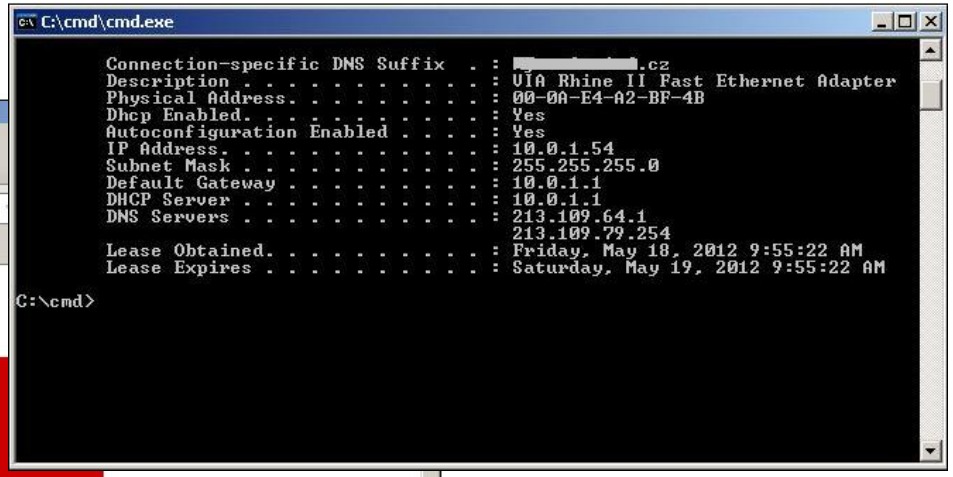
Stanice před infekcí

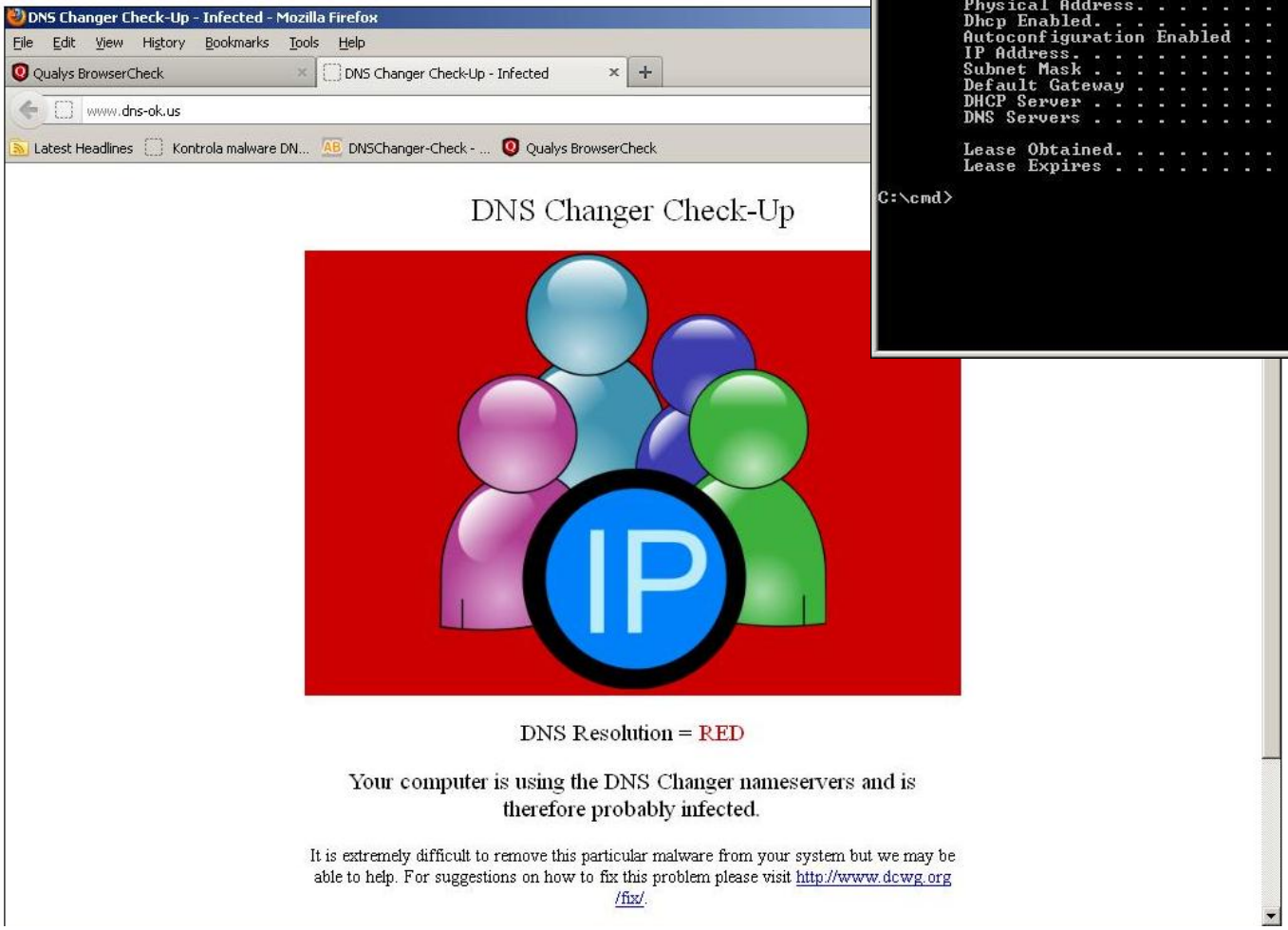




DNS Changer

Stanice po infekci





DNS Changer

Detekováno ve FlowMon ADS

Top 10 by priority

#	Priority	Event type	Source	Target
1	HIGH	DNSANOMALY	10.0.1.54	213.109.64.1
2	MEDIUM	HIGHTRANSF	10.0.1.54	204.160.120.126
3	LOW	DIVCOM	10.0.1.54	

General event priorities

Aggregated view | Simple list | By hosts

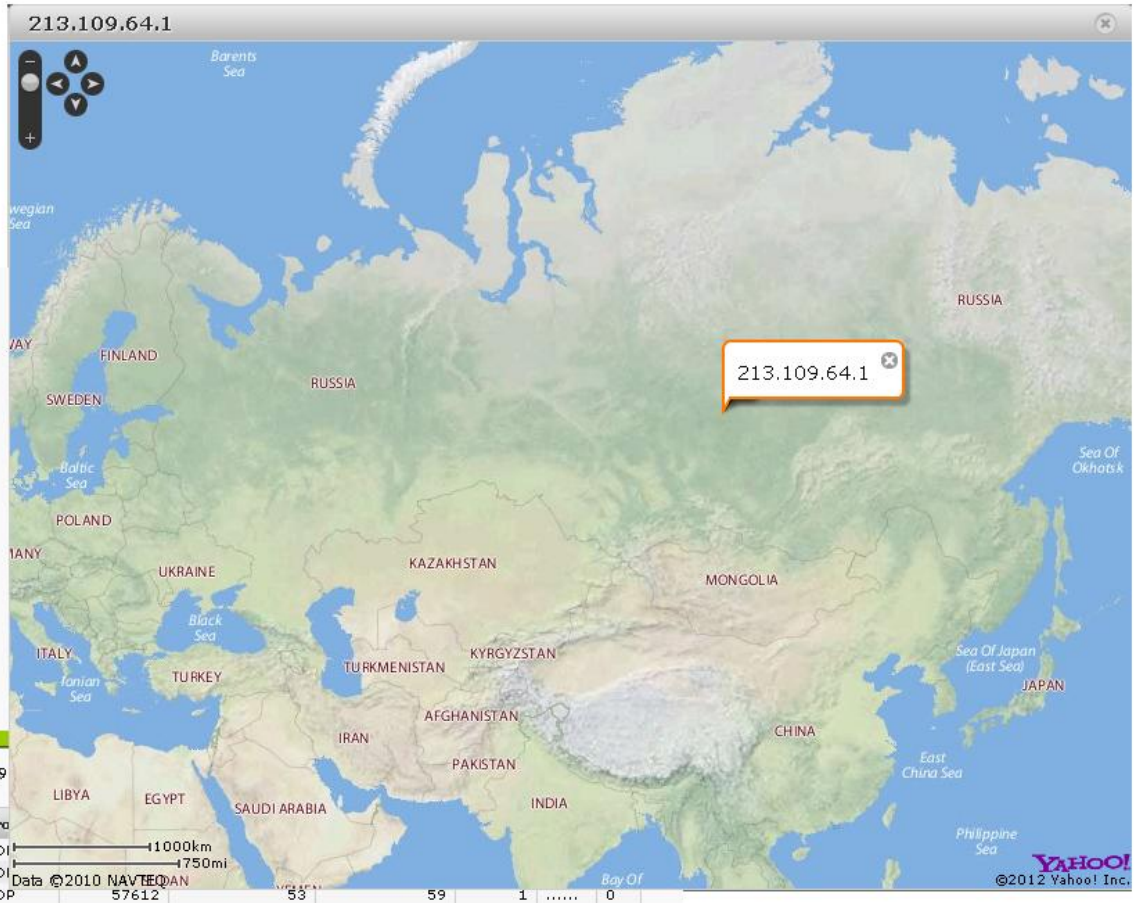
#	Source	Event type	Detail	Timestamp	Net flow sourc	
1	10.0.1.54	DNSANOMALY	Use of unauthorized DNS server (connections: 93)	2012-05-18 13:29:04	localhost	213.109.64.1

Russian Federation

Event details

Type: **DNS Anomaly (DNSANOMALY)**
Timestamp: **2012-05-18 13:29:04**
Event source: **10.0.1.54**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **100 %**
False positive: **No**
Detail: **Use of unauthorized DNS server (connections: 93)**

#	Source	Destination IP	Start	Duration	Pro						
1	10.0.1.54	213.109.64.1	2012-05-18 13:29:04.362	0	UDI						
2	213.109.64.1	10.0.1.54	2012-05-18 13:29:04.558	0	UDI						
3	10.0.1.54	213.109.64.1	2012-05-18 13:29:06.432	0	UDP	57612	53	59	1	.....	0
4	10.0.1.54	213.109.64.1	2012-05-18 13:29:06.506	0	UDP	37463	53	54	1	.....	0
5	213.109.64.1	10.0.1.54	2012-05-18 13:29:06.546	0	UDP	53	57612	126	1	.....	0



DNS Changer

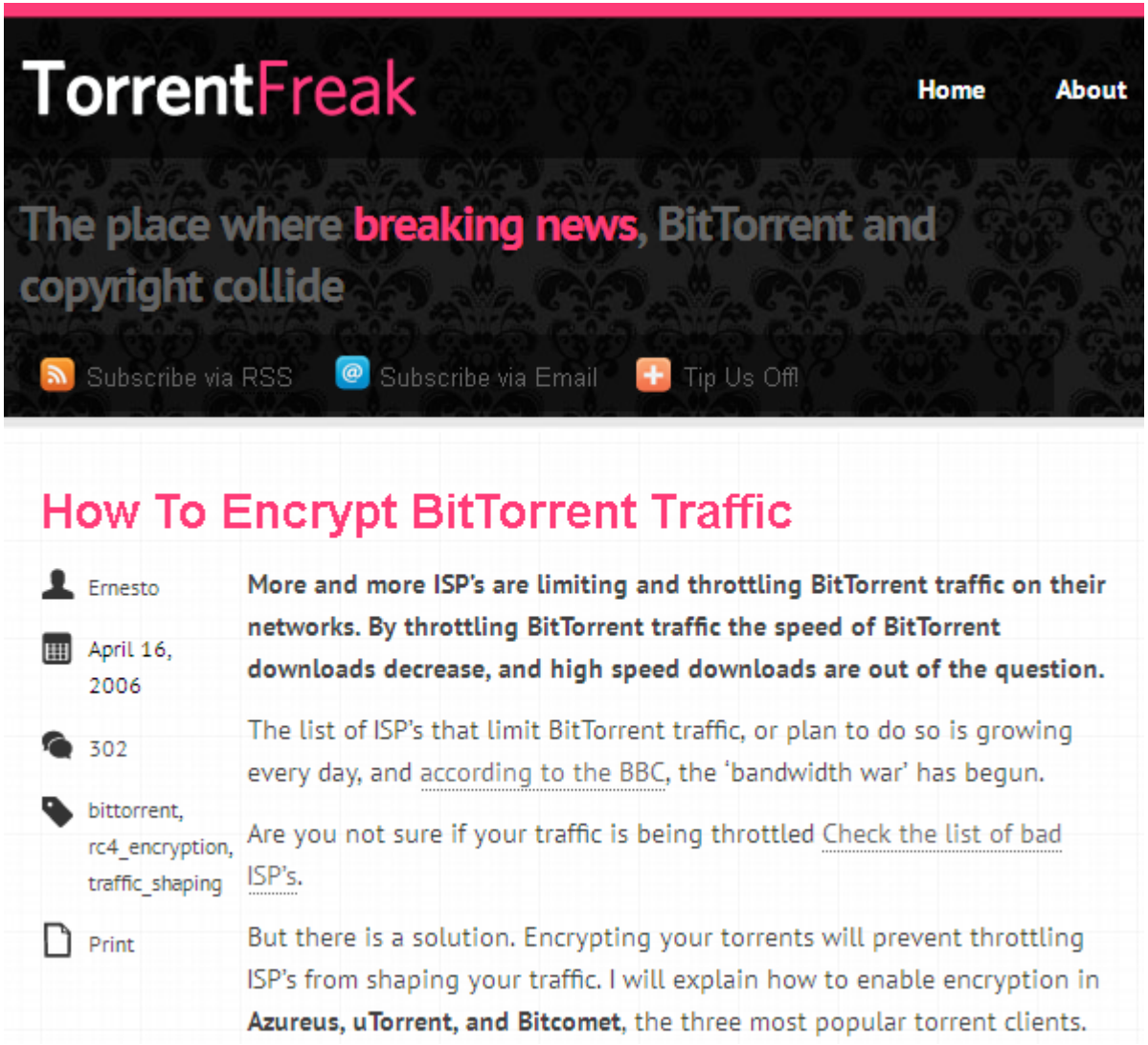
Shrnutí

- **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 Charger 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

Současné hrozby

Šifrovaný provoz P2P sítí



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

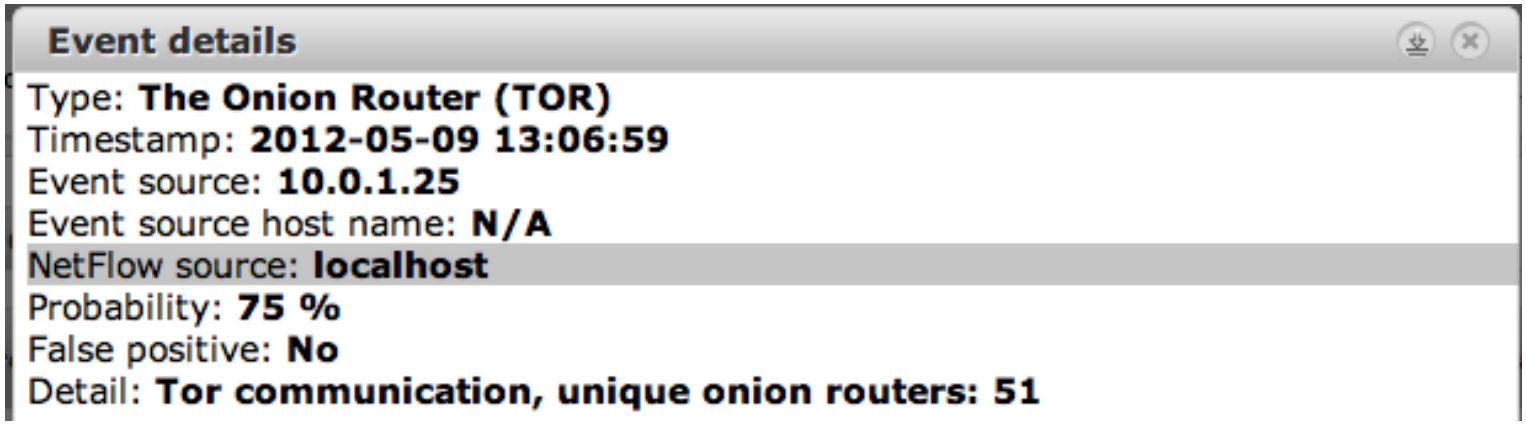
Současné hrozby

The Onion Router

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

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 …

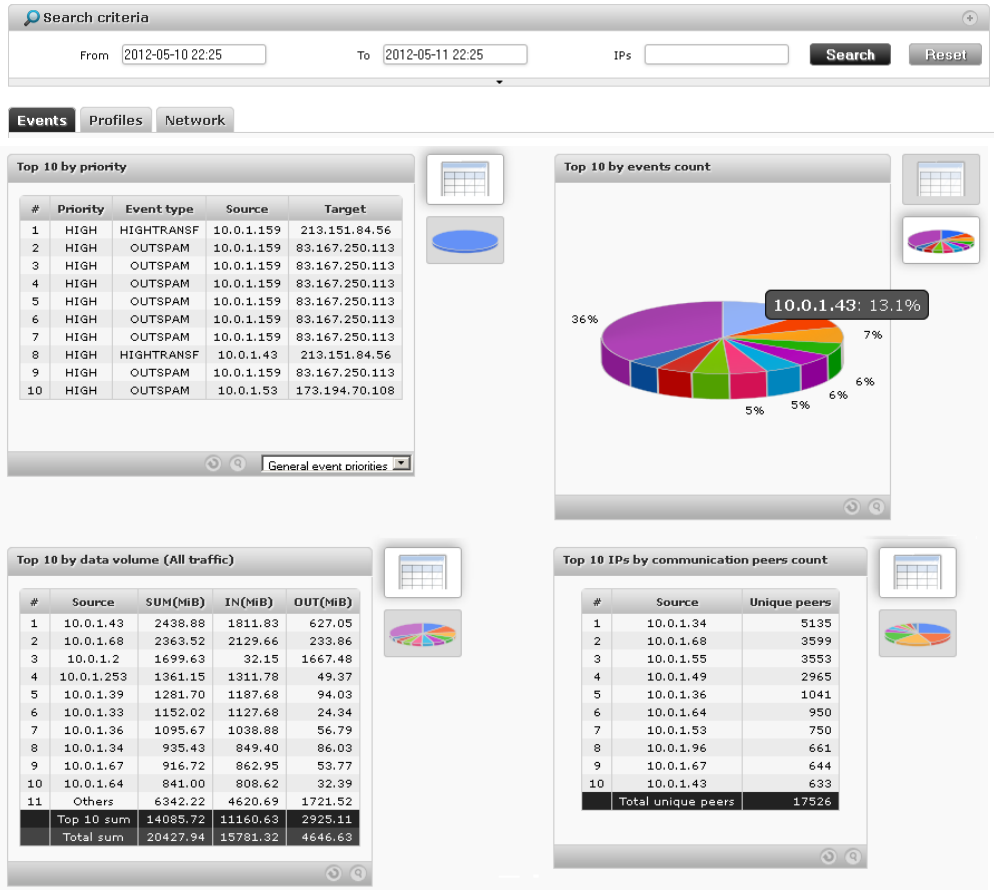
- Útoky (slovníkové útoky proti síťovým službám, útoky DoS/DDoS, útoky typu DNS amplification, …)
- Nežádoucí aplikace, které mohou ohrozit bezpečnost sítě (TeamViewer, Skype, ICQ, MS Messanger, ...)
- Porušení bezpečnostních politik (obcházení proxy, úniky dat, …)
- Bezpečnost není jediná věc, na které 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



FlowMon ADS

Události

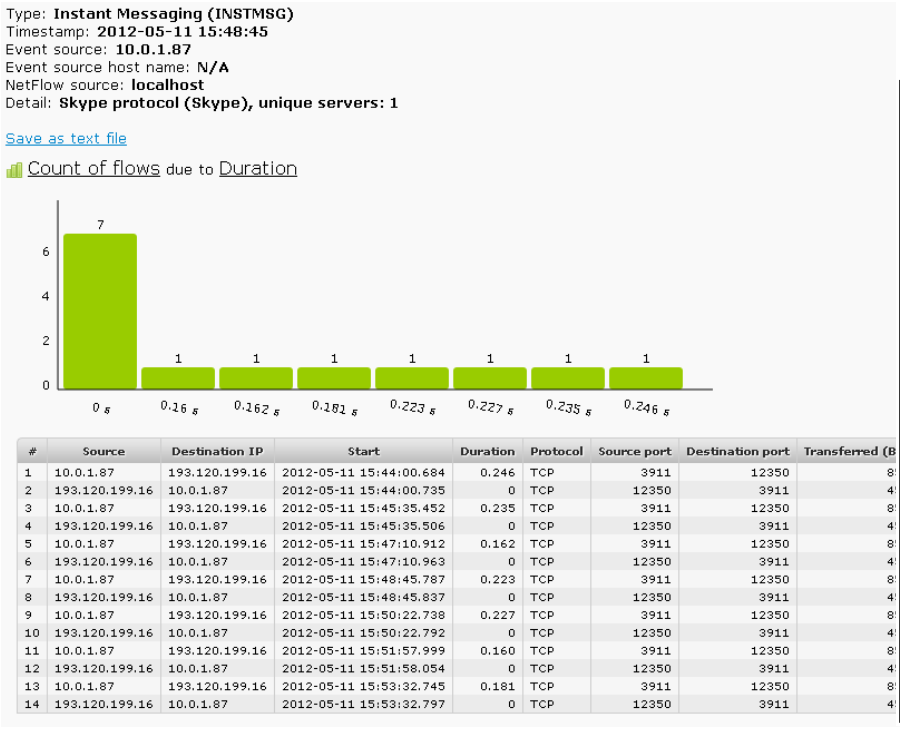
- Útoky (skenování portů, slovníkové útoky, DoS, Telnet)
- Anomálie provozu (DNS, multicast, vysoká variabilita komunikace)
- Anomálie chování IP adres (změna profilu chování)
- Nežádoucí aplikace (P2P sítě, on-line komunikátory, TOR, TeamViewer)
- Malware (viry, spyware, botnety, komunikace s adresami 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)

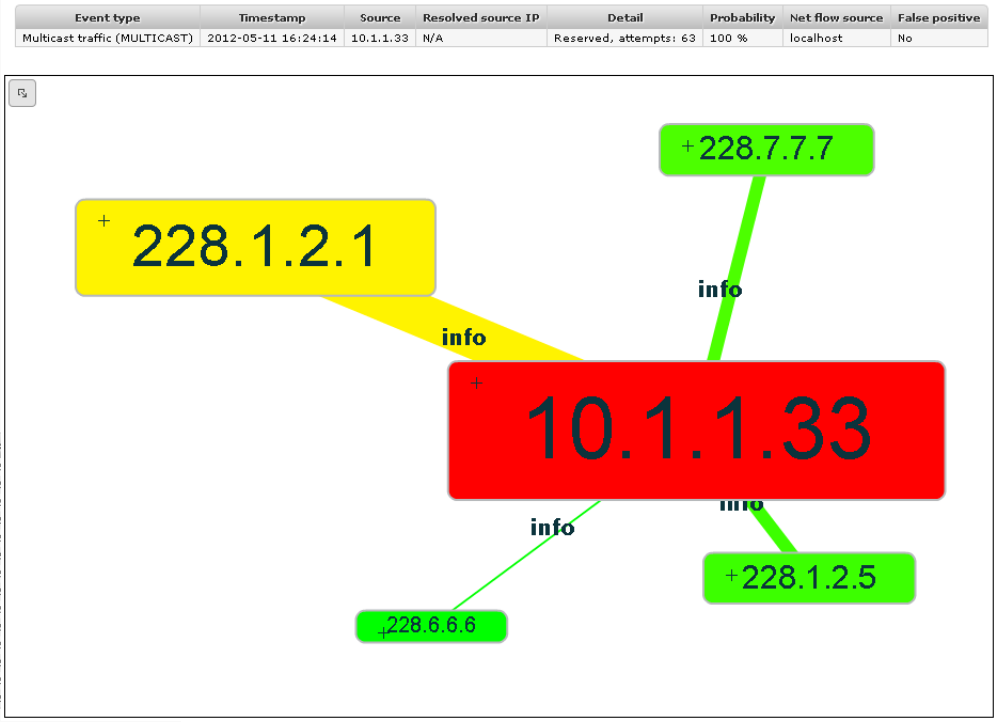
#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.1.1.84	UPLOAD	Uploaded: 38.83 MiB, downloaded: 0.57 MiB, ports: 80	2012-05-10 11:43:34	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
2	10.1.1.84	UPLOAD	Uploaded: 243.48 MiB, downloaded: 4.07 MiB, ports: 80	2012-05-10 11:37:19	localhost	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 United States 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 povoz je dostupný na vyžádání
- Export důkazů pro budoucí použití

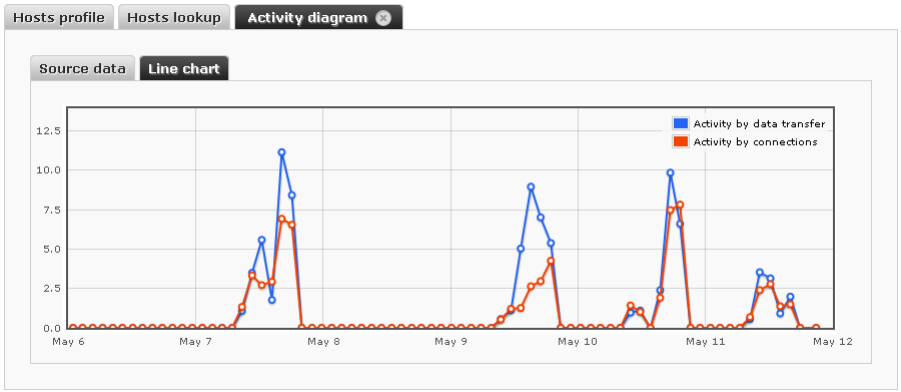


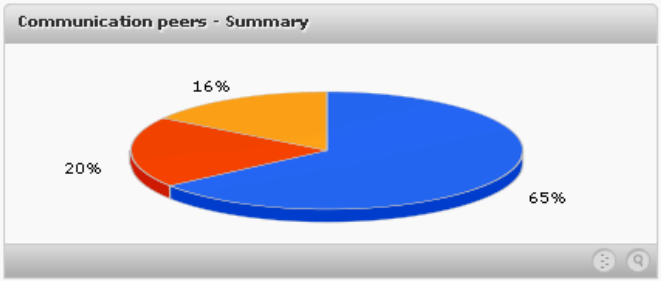


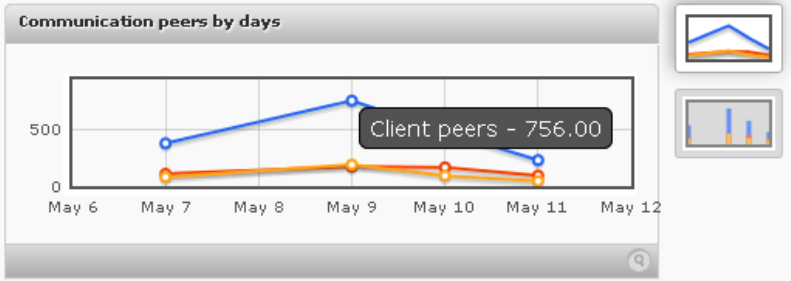
FlowMon ADS

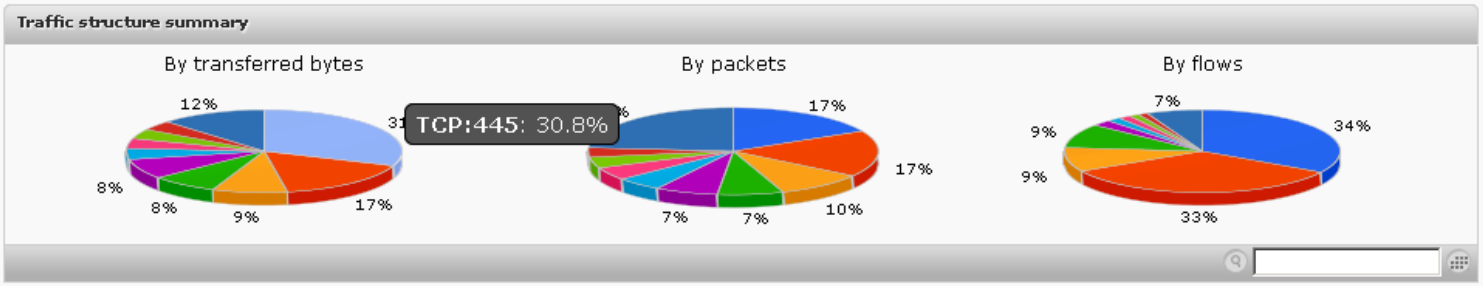
Profily chování

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





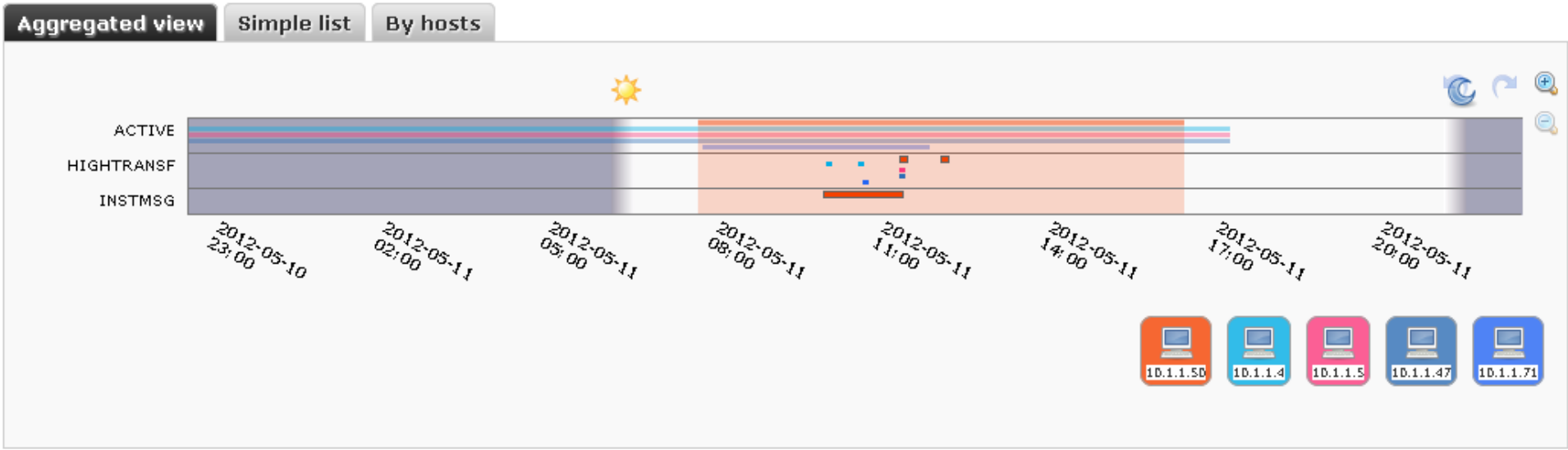




FlowMon ADS

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



FlowMon ADS

Srovnání s tradičním přístupem

	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