SECURITY 2013

21. ročník konference o bezpečnosti v ICT

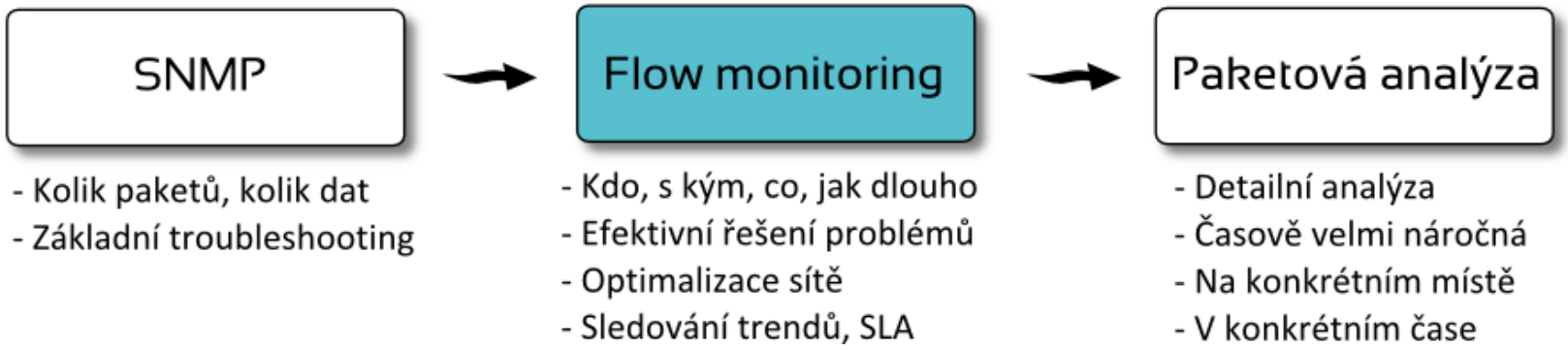
FlowMon ADS – praktické aplikace a případové studie

Pavel Minařík

INVEA-TECH, a.s.

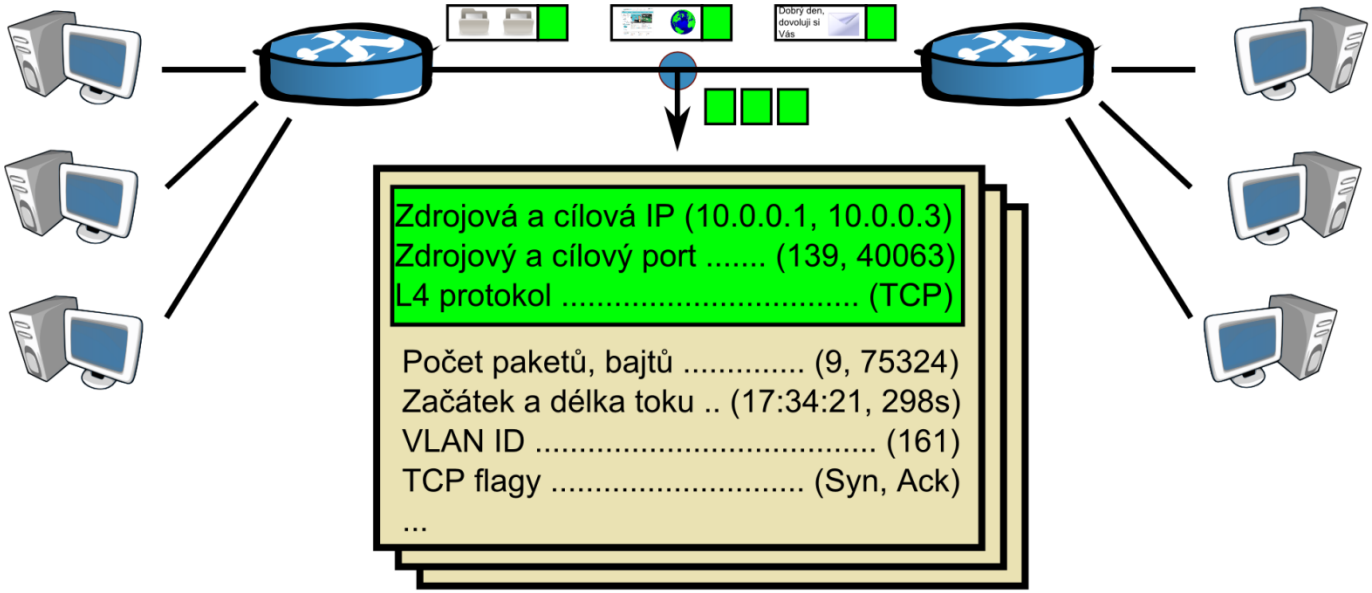
Monitoring sítě

- SNMP (monitoring)
  - pouze na úrovni základních čítačů, chybí detailní informace
- **Datové toky** (next generation monitoring)
  - detailní přehled o dění v síti
- Paketová analýza
  - velmi detailní, ale časově velmi náročná



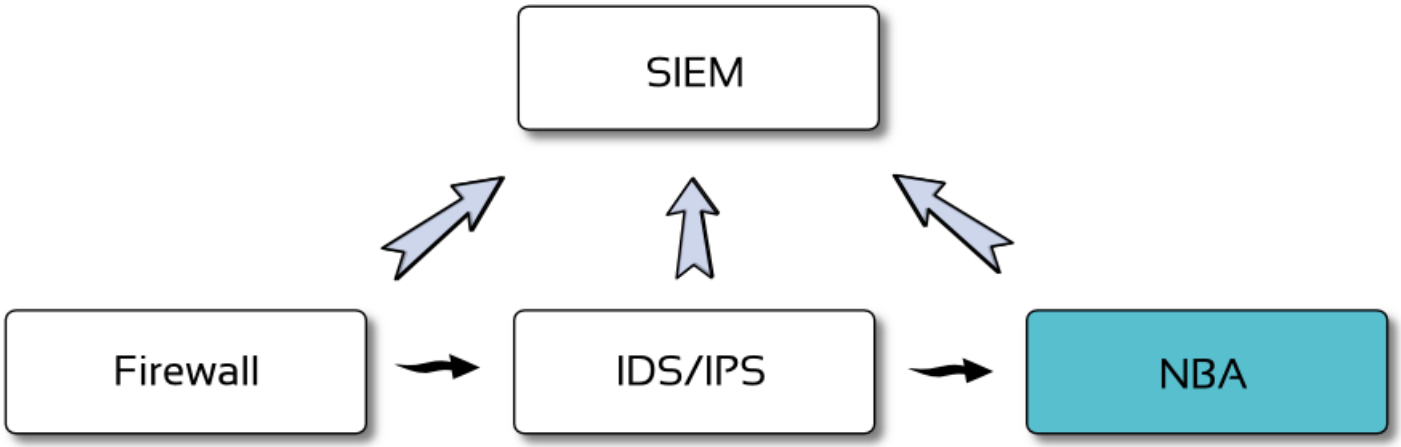
Datové toky

- Analyzují se pouze hlavičky paketů, obsah paketů není monitorován ani uchováván
- Moderní metoda monitorování sítí
- NetFlow jako nejrozšířenější standard, podpora u celé řady výrobců



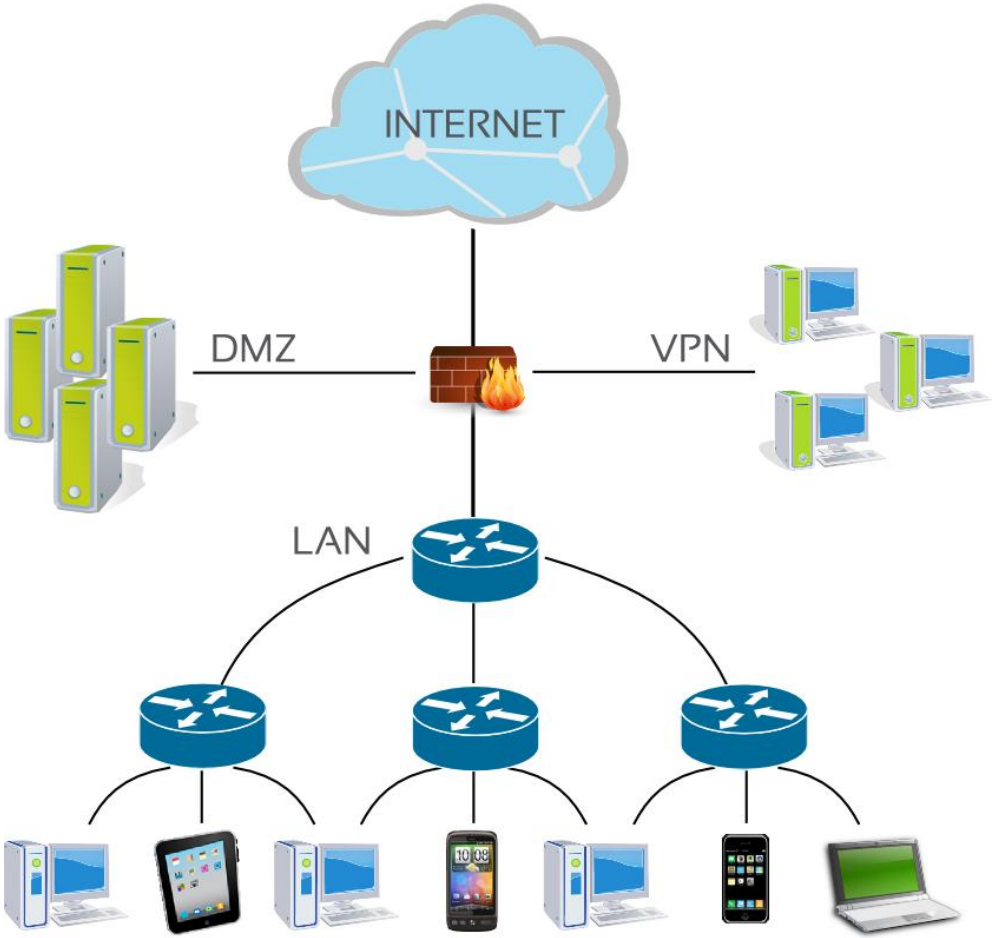
Bezpečnostní nástroje

- Firewall
- IDS/IPS
- Antivir
- **Network Behavior Analysis (NBA)**
- SIEM (log management)



Bezpečnost - trendy

- Obrana perimetru je nutná, nikoliv však postačující



Proč NBA?

- Počet napadených organizací neustále roste a tyto útoky mívají fatální následky
- Nejedná se pouze o útoky na velké společnosti, ale ty jsou nejvíce vidět
- ČR: státní správa, banky a pojišťovny

BUSINESS CENTER Jun 3, 2011 6:58 pm

Sony Hacked Again: How Not to Do Network Security

DigiNotar Compromised, Removed as Trusted CA

September 9th, 2011 Goto comments Leave a comment

IT Security & Network Security News

Japan's Largest Defense Contractor Hit by Cyber-Attackers

LinkedIn Twitter 5 Facebook 3 +1 0 Share 8

By: Fahmida Y. Rashid
2011-09-19
Article Rating: ☆☆☆☆☆ / 0

Proč NBA?

- Eurostat report, únor 2011
  - 84% počítačů v Evropě je chráněno anti-malware programem
  - 31% počítačů v Evropě je nakaženo nějakým typem malware

eurostat newsrelease

21/2011 - 7 February 2011

8 February 2011: Safer Internet Day

Nearly one third of internet users in the EU27 caught a computer virus

84% of internet users use IT security software for protection

Hlavní principy NBA

- Technologie je flexibilní, vysoce škálovatelná a jednoduchá na nasazení
- Nevyžaduje žádné zásahy do infrastruktury

Behavior detection ☑

Signature detection ☒

Network level ☑

Host level ☒

Hlavní principy NBA

- Sledování chování a jeho změna v čase
  - Provozní problémy, malware, botnety, …
- Aplikace metod strojového učení a heuristik
  - Skype, TOR, Bittorent, ICQ, TeamViewer, …
- Aplikace rozhodovacích stromů pro sledování útoků v čase
  - SSH, RDP, Telnet, …
- Vyhledávání shluků podobně se chovajících stanic a tzv. outlierů
  - Nežádoucí aplikace, malware, botnety, …

Technologie NBA v praxi

- Pokročilý malware – příklad DNS Changer

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

Home | Gadgets | Apps & Web | News | Reviews & Features | Companies

SECURITY

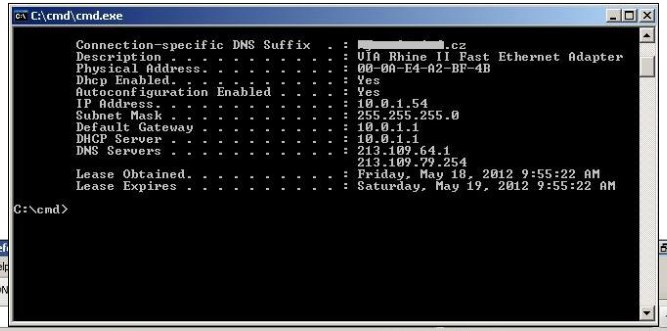
DNSChanger: FBI Warns In
Computers Will Lose Web, F
Access in July

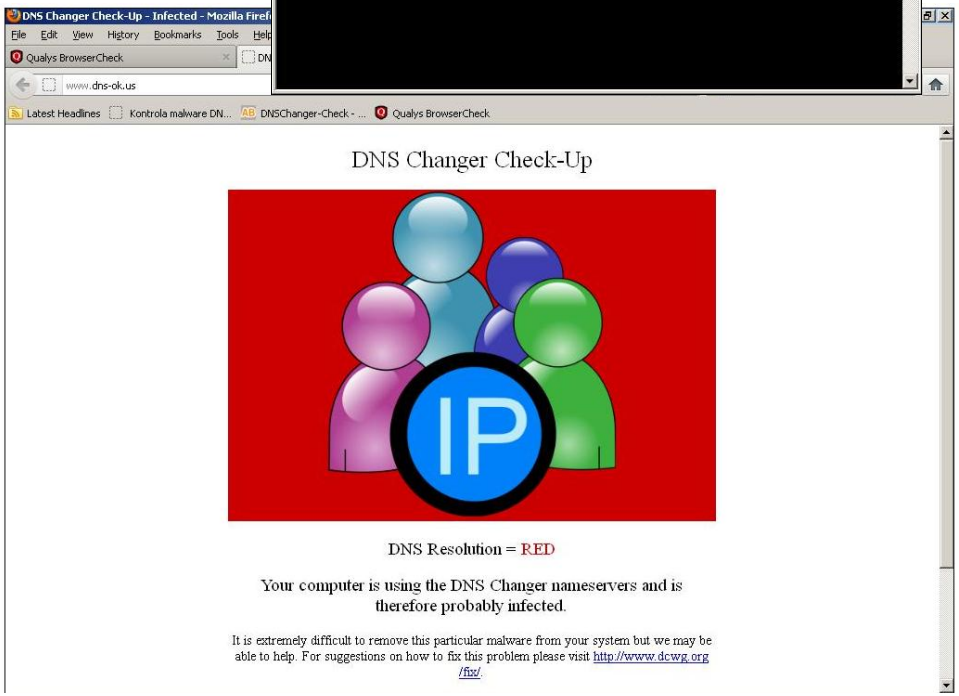
By MATT PECKHAM | @mattpeckham | April 23, 2012 | 8

Summary

DNSChanger is a trojan that will change the infected system's Domain Nam
traffic to unsolicited, and potentially illegal sites.

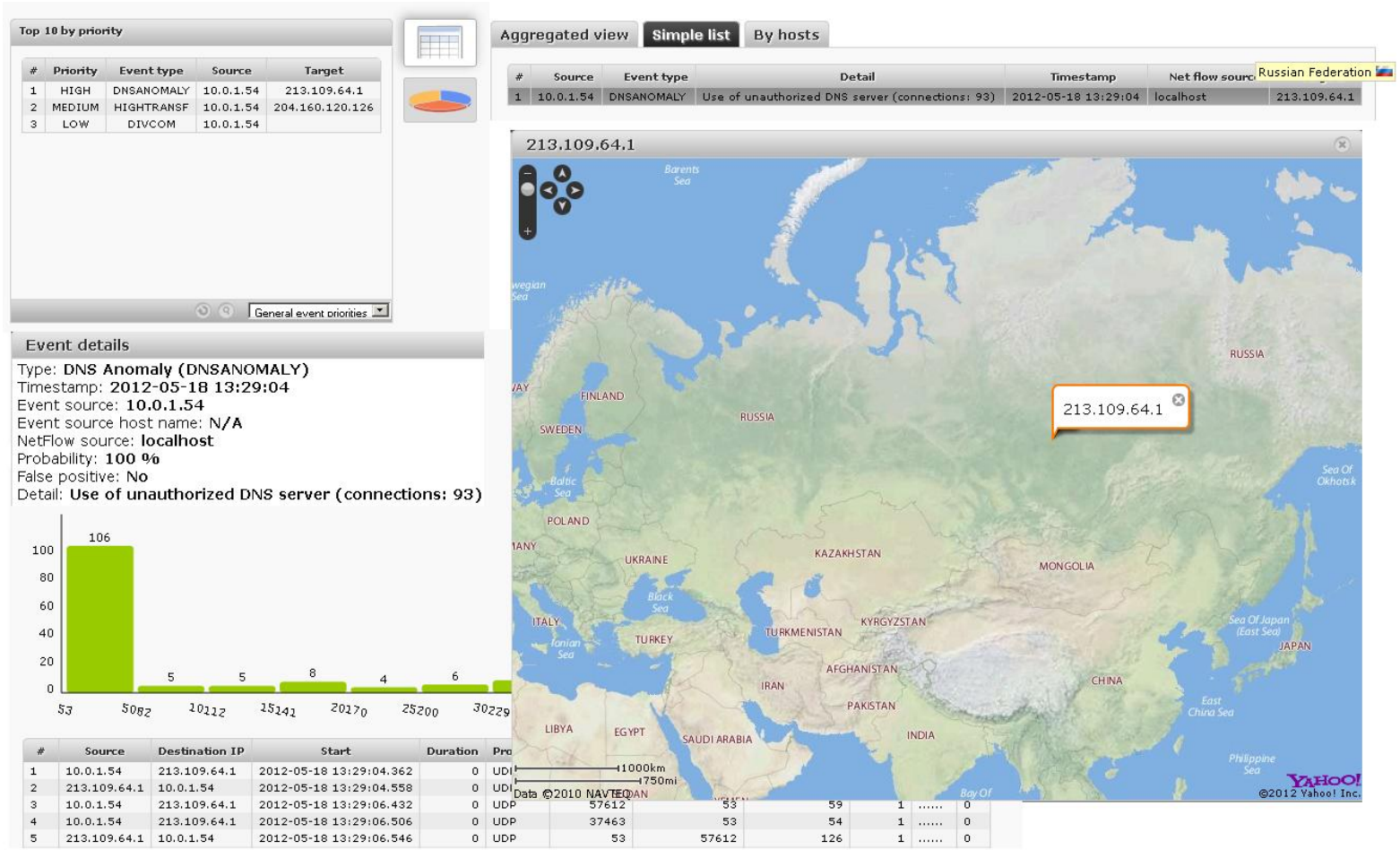
The trojan is usually a small file (about 1.5 kilobytes) that is designed to cha
custom IP address. This IP address is usually encrypted in the body of a troj
computer will contact the newly assigned DNS server to resolve names of di





Technologie NBA v praxi

- Pokročilý malware – příklad DNS Changer



Technologie NBA v praxi

- Úniky dat – malware/zaměstnanci

Malware from Peru Reportedly was sending AutoCAD Drawings to China

by SUNITHBABU (ONLINE) *on* JUNE 26, 2012

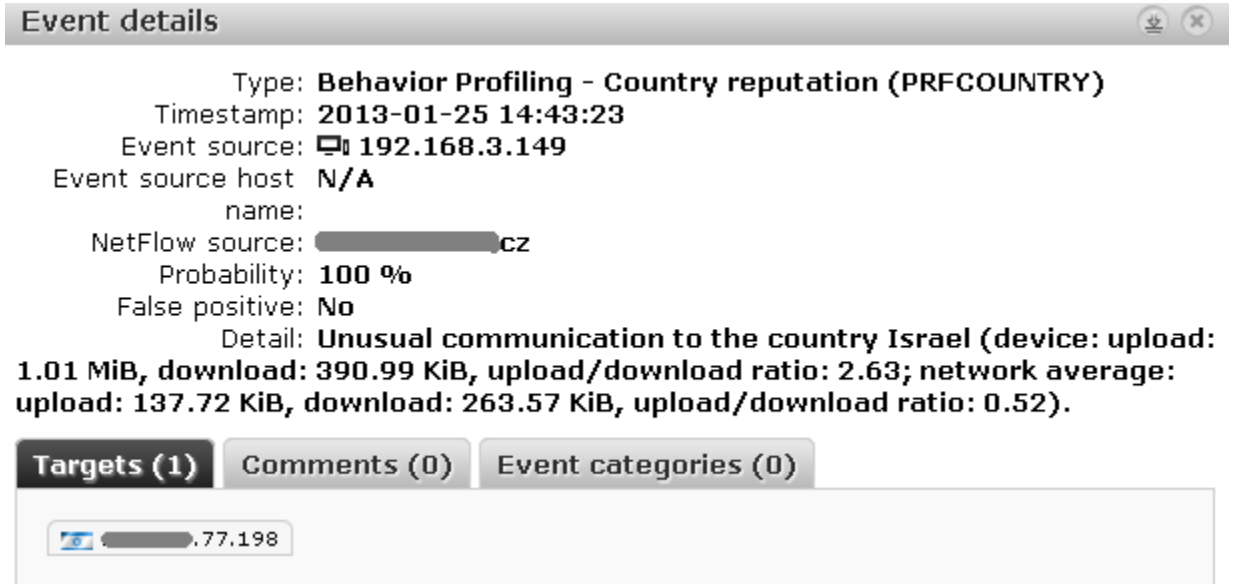
ESET, one of the developer of security solutions for home and corporate use, yesterday announced it has uncovered and helped thwart a worm that targets AutoCAD drawings. Tens of thousands of AutoCAD drawings, primarily from users in Peru and a few other Spanish-speaking nations, reportedly were leaking at the time of the discovery.

0 Tweet

ACAD/Medre.A a Malware worm was stealing AutoCAD files from infected computers and sending them to e-mail accounts in China. ESET worked with Tencent, the owner of the domain that hosted the suspect e-mail addresses; the Chinese National Computer Virus Emergency Response Center; and Autodesk to stop the file transmissions, the company reports. The e-mail accounts associated with the malware were blocked, preventing further data leakage.

Technologie NBA v praxi

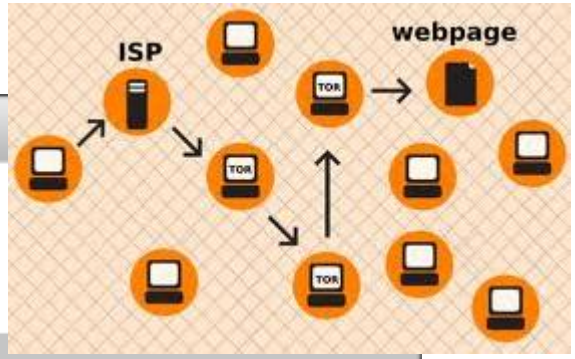
- Úniky dat – malware/zaměstnanci



#	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	98.13[redacted] 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)

Technologie NBA v praxi

- Nežádoucí aktivity, skrývání identity
  - The Onion Router (TOR)
  - Vhodné pro obcházení politik a omezení



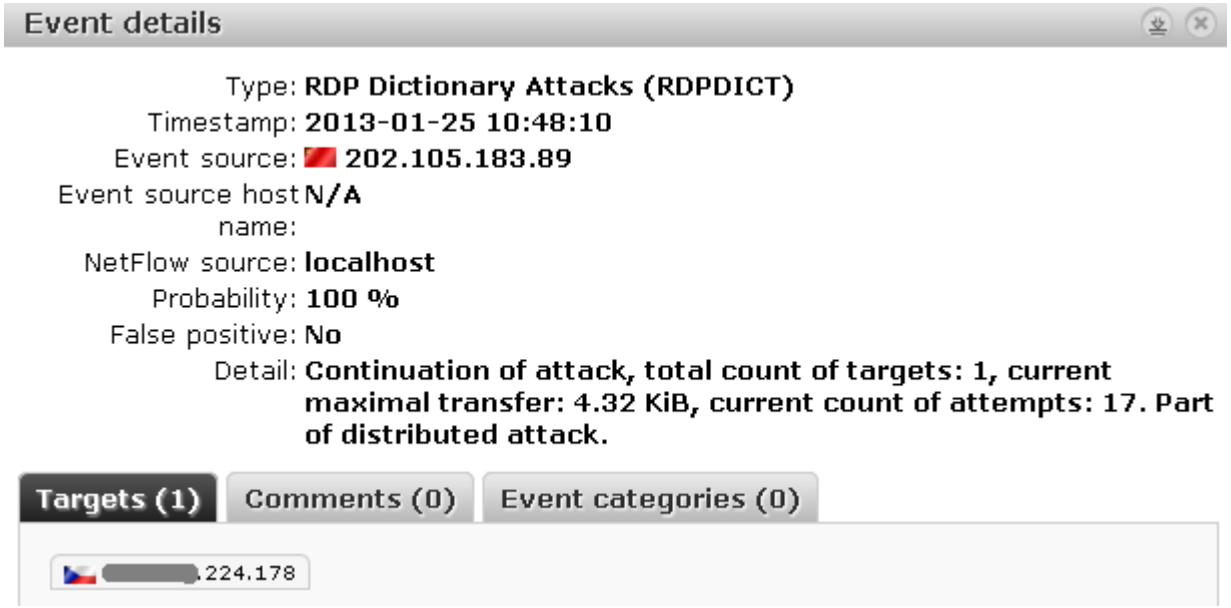
Event details

Type: **The Onion Router (TOR)**
Timestamp: **2012-05-09 13:06:59**
Event source: **10.0.1.25**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **75 %**
False positive: **No**
Detail: **Tor communication, unique onion routers: 51**

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.0.1.25	TOR	Tor communication, unique onion routers: 51	2012-05-09 13:06:59	localhost	31.31.74.162, 38.229.70.61, 46.165.196.73, 46.166.147.126, 50.7.240.10, 50.115.125.54, 62.75.186.116, 62.220.136.253, 70.33.208.83, 74.125.232.246, , ...

Technologie NBA v praxi

- Útoky na síťové služby



#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	140.121.70.70	SSHDICT	End of attack (unsuccessful), summary: Total count of targets: 1, maximum transferred: 1.14 KiB, total count of attempts: 56, duration of attack: 274.57 seconds. Single attack..	2013-01-30 13:59:57	[redacted].cz	192.168.3.110
2	140.121.70.70	SSHDICT	Continuation of attack (unsuccessful), total count of targets: 1, current maximal transfer: 1.13 KiB, current count of attempts: 28. Single attack..	2013-01-30 13:57:46	[redacted].cz	192.168.3.110
3	140.121.70.70	SSHDICT	Start of attack (unsuccessful), count of targets: 1, maximum transferred: 1.14 KiB, count of attempts: 28. Single attack..	2013-01-30 13:55:27	[redacted].cz	192.168.3.110

Technologie NBA v praxi

- SPAM, kde se bere?

#	Detail	Timestamp	Net flow source	Targets
1	Mail count: 1270, network average: 414.50	2012-10-24 21:48:46		12.102.252.75, 17.172.36.33, 17.172.36.34, 24.71.223.11, 46.255.224.55, 64.8.71.15, 64.12.90.65, 64.12.90.66, 64.12.90.98, 64.12.138.161, , ...
2	Mail count: 1386, network average: 259.50	2012-10-24 21:38:52		12.102.252.75, 17.172.36.32, 24.71.223.11, 64.8.71.15, 64.12.90.34, 64.12.90.65, 64.12.90.66, 64.12.90.97, 64.12.138.161, 64.18.5.10, , ...
3	Mail count: 545, network average: 130.00	2012-10-24 21:23:41		12.102.252.75, 24.71.223.11, 64.8.71.15, 64.12.90.1, 64.12.90.34, 64.12.90.97, 64.12.90.98, 64.18.5.11, 64.59.134.8, 64.9 Canada
4	Mail count: 2181, network average: 593.50	2012-10-24 21:18:40		12.102.252.75, 17.172.36.32, 17.172.36.34, 24.71.223.11, 38.102.228.17, 62.211.72.32, 64.8.71.15, 64.12.90.1, 64.12.90.33,

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.8.1.236	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 169, targets: 56, port list: 443, 80, 13392, 1756, 3245, 5722, 7244, 11066, 11811, 13190, 13580, 14217, 14942, 19135, 20015, 20223, 20933, 21429, 22417, ...)	2012-12-11 10:35:07	localhost	1.82.88.72, 2.103.32.169, 2.132.56.167, 31.46.161.145, 37.142.121.172, 46.119.207.231, 46.191.203.63, 46.241.146.163, 61.53.97.41, 61.142.42.167, ...
2	10.8.1.236	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 403, targets: 121, port list: 443, 80, 12350, 13392, 1024, 1663, 1685, 2396, 4802, 5805, 6718, 6894, 7324, 7716, 8900, 10126, 11399, 12033, 12363, ...)	2012-12-11 10:30:04	localhost	5.79.180.249, 5.166.175.130, 14.221.13.45, 24.1.97.218, 24.134.171.181, 31.218.245.94, 37.110.10.36, 41.101.14.54, 41.177.18.14, 42.119.66.234, ...
3	10.8.1.236	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 225, targets: 82, port list: 443, 12350, 2082, 3595, 5984, 6038, 7924, 7963, 8213, 9232, 10272, 11191, 14124, 14905, 15648, 17243, 17564, 17779, 18773, ...)	2012-12-11 10:25:00	localhost	2.134.83.95, 5.9.138.194, 5.9.139.3, 14.220.221.3, 24.52.82.175, 31.11.80.167, 31.210.218.91, 37.79.17.109, 39.113.14.115, 41.97.111.203, ...
4	10.8.1.236	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 155, targets: 53, port list: 443, 12350, 80, 13392, 12351, 33033, 8023, 16321, 17247, 21823, 22530, 22584, 34117, 45127, 45129, 46878, 50218, 51613, 51876, ...)	2012-12-11 10:21:43	localhost	5.152.5.33, 31.11.80.167, 31.192.153.186, 37.6.250.21, 46.147.151.193, 46.152.68.35, 46.241.130.202, 50.142.79.70, 65.55.223.12, 77.238.195.68, ...

Technologie NBA v praxi

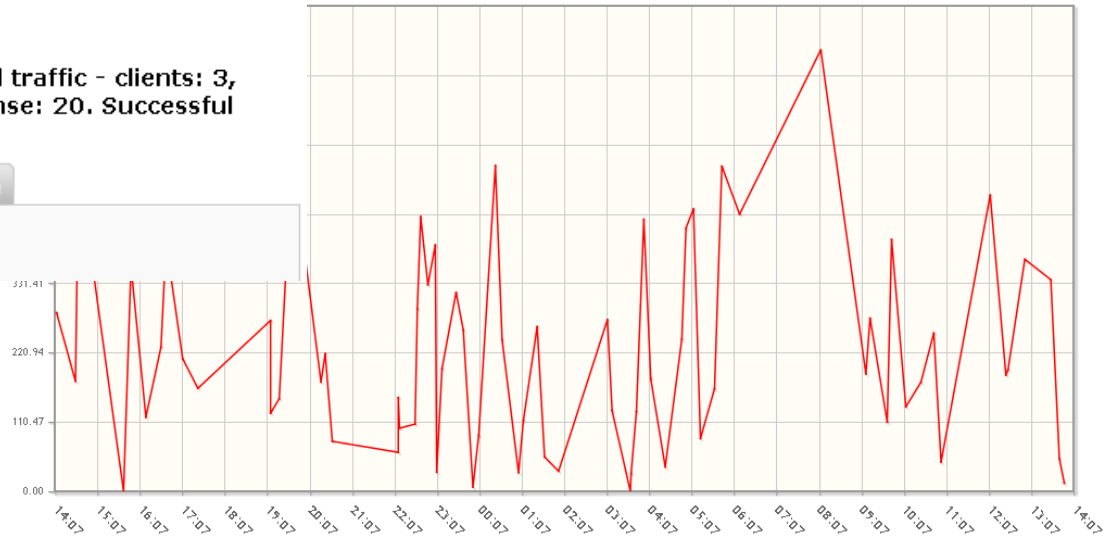
- Provozní problémy
  - Nezjistitelné běžnými dohledovými prostředky
  - Výpadky, latence, špatné konfigurace

Event details

Type: **Service not available (SRVNA)**
Timestamp: **2012-08-31 06:54:48**
Event source: **10.66.1.21**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **100 %**
False positive: **No**
Detail: **Unavailable services (TCP: 8888). Unsuccessful traffic - clients: 3, rejected connections: 96, connections without response: 20. Successful traffic - clients: 0, connections: 0.**

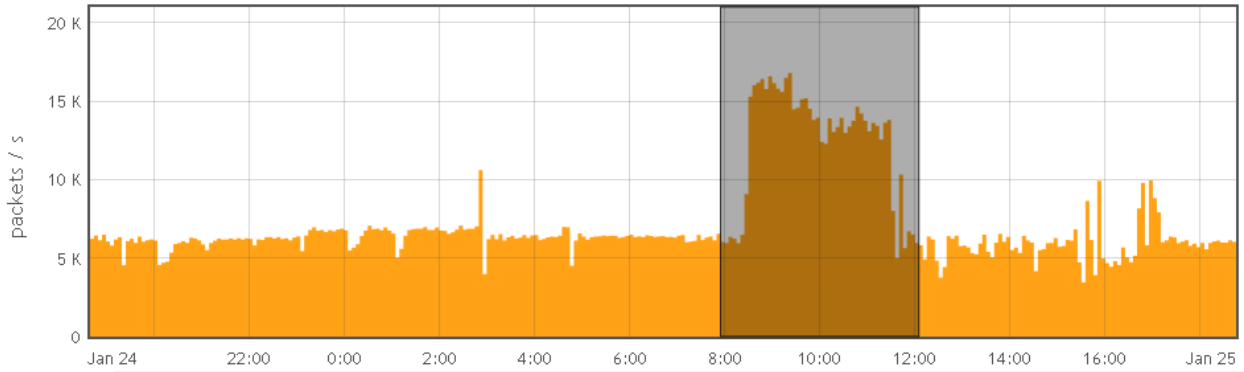
Targets (3) | Comments (0) | Event categories (0)

10.65.5.117 | 10.66.2.36 | 10.66.2.47



Technologie NBA v praxi

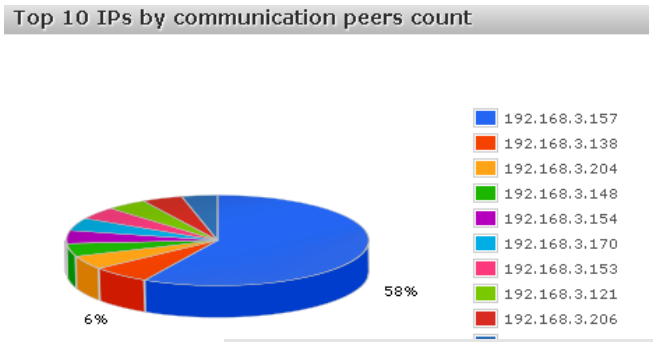
- Anomálie zatížení datové sítě
  - Zahlcení pakety, toky, vytížení linky, …

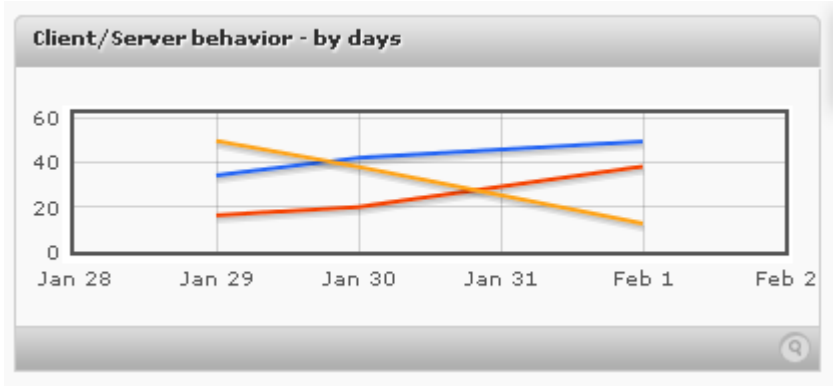


Color	Start Time - first seen	Duration	Protocol	Any Port	Flows	Input Packets	Input Bytes	Packets per second	Bits per second	Bytes per package
1	01/25/2013 - 7:54:40 AM	4h, 6m, 52s	any	shilp	204 (84.6%)	121.47 M (100.0%)	113 GB (100.0%)	8200	65528526	998
2	01/25/2013 - 8:25:51 AM	3h, 9m, 48s	any	1016	80 (33.2%)	109.4 M (90.1%)	101.53 GB (89.9%)	9605	76583215	996
3	01/25/2013 - 8:16:32 AM	3h, 45m	any	881	90 (37.3%)	9.48 M (7.8%)	9.05 GB (8.0%)	702	5758429	1024
4	01/25/2013 - 11:36:09 AM	10m, 48s	any	1015	6 (2.5%)	1.73 M (1.4%)	1.6 GB (1.4%)	2669	21245977	994
5	01/25/2013 - 7:54:40 AM	21m, 37s	any	798	10 (4.1%)	863.03 K (0.7%)	831.98 MB (0.7%)	665	5380111	1010
6	01/25/2013 - 7:59:13 AM	4h, 9s	any	domain	9 (3.7%)	38 (0.0%)	2.32 KB (0.0%)	0	1	62
7	01/25/2013 - 8:20:29 AM	5m, 22s	any	sunrpc	12 (5.0%)	33 (0.0%)	1.78 KB (0.0%)	0	45	55
8	01/25/2013 - 8:16:17 AM	0s	any	878	2 (0.8%)	32 (0.0%)	21.31 KB (0.0%)	63	344980	681
9	01/25/2013 - 8:20:29 AM	5m, 22s	any	935	12 (5.0%)	12 (0.0%)	1.05 KB (0.0%)	0	26	90
10	01/25/2013 - 8:22:38 AM	1m, 44s	any	722 ?	4 (1.7%)	10 (0.0%)	496 B (0.0%)	0	37	49
								Flows 241	Bytes 113 GB	Packets 121.47 M

Technologie NBA v praxi

- Skutečné chování stanic v síti
  - Poskytované a využívané služby, servery, změny chování





Service details as provided by servers

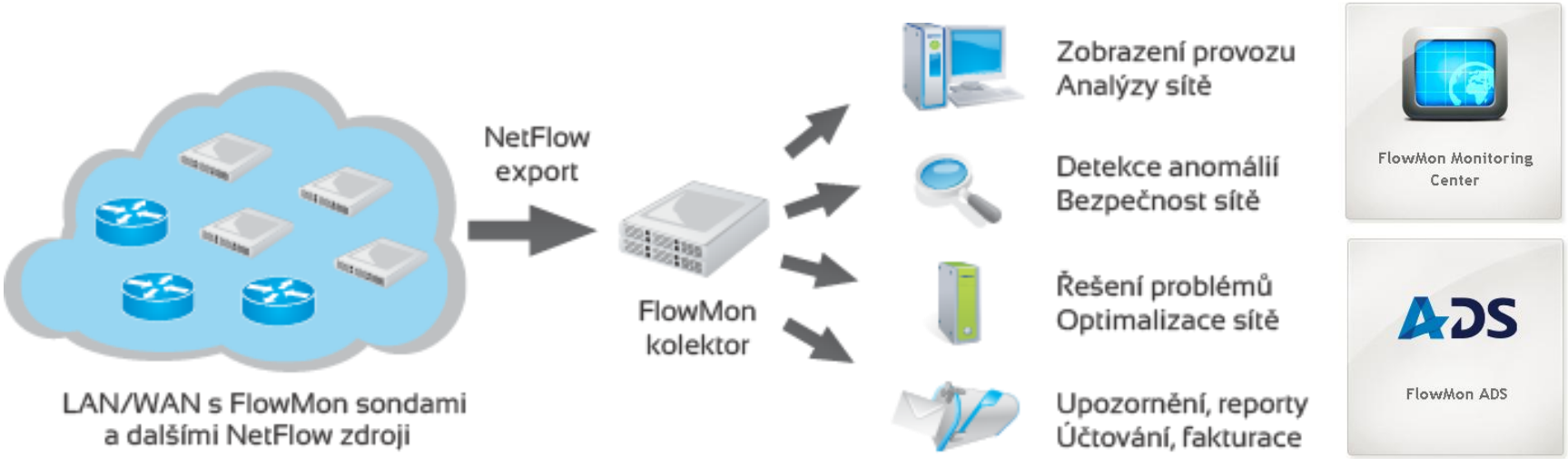
Protocol/port: **TCP/902**
Service name: **vmware**
Description: **VMWare Authentication service | IDEAFARM-CHAT**

Source data | Chart

#	IP address	Transferred (MiB)	Custom service name
1	192.168.3.107	216.39	vmware
2	192.168.3.106	6.52	vmware

Možnosti nasazení NBA

- Sondy měřící zájmový provoz a generující NetFlow na jeden nebo více kolektorů.
- Kompatibilní s NetFlow technologiemi třetích stran (routery, kolektory).



Zkušenosti s NBA

- Ing. Róbert Turcer, CIO, FERONA Slovakia:
  - Implementácia sondy bola vykonaná rýchlo a bez vplyvu na prevádzku našich ICT systémov
  - Na základe nasnímaných dát sa podarilo odhaliť niekoľko nebezpečne sa správajúcich počítačov v našom systéme
  - Po overení týchto informácií sme zistili, že zariadenia skutočne vykazovali prítomnosť škodlivého softvéru, prípadne chybnú konfiguráciu

Zkušenosti s NBA

- Jan Svatoš, ředitel IT, AVE CZ:
  - Řešení FlowMon nám poskytlo kompletní přehled o dění v naší síti a umožnilo nám rozkrýt veškeré komunikace v reálném čase, ale i řadu týdnů zpět.
  - Díky těmto klíčovým informacím jsme objevili řadu nežádoucích stavů v sítí – ať již v podobě chyby v kancelářském softwaru na několika stanicích nebo chyby při komunikaci s tiskovým serverem.
  - Díky optimalizaci struktury provozu jsme výrazně snížili vytížení především MPLS sítě. To nám přináší měsíční úsporu v řádu desetitisíců korun.

Zkušenosti s NBA

- Ing. Jaroslav Šmíd, GŘ HZS ČR:
  - Hlavní předností, kterou spatřujeme ve srovnání s jinými nástroji, je orientace na celkové chování aktivních prvků, od serverů až po koncové uživatelské stanice na síti. To nám umožňuje detekovat a reagovat na dosud neznámé nebo specifické hrozby.
  - Zařízení šetří čas našim správcům počítačový sítí při odhalování a řešení problémů v síti.

Shrnutí

- Technologie NBA je celosvětový trend
  - Není otázkou zda, ale kdy…
- Gartner: *„Pokud máte Firewall a IDS/IPS, zvažte jako další krok implementaci NBA.“*
- Uvedené příklady použití a případové studie vychází z nasazení původního řešení českého řešení **FlowMon** společnosti **INVEA-TECH**
- Vyzkoušejte si přínosy technologie NBA ve Vaší vlastní datové síti

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Pavel Minařík
INVEA-TECH, a.s.
minarik@invea.cz