Kybernetické hrozby

Existuje komplexní řešení?

Pavel Minařík

minarik@invea.com

Hlášení incidentu

28.5. 9:00 …

Nevím, co se děje
Většina z nás se nedostane na Internet
Ale informační systém je funkční
Ve školící místnosti je vše v pořádku

Hlášení incidentu

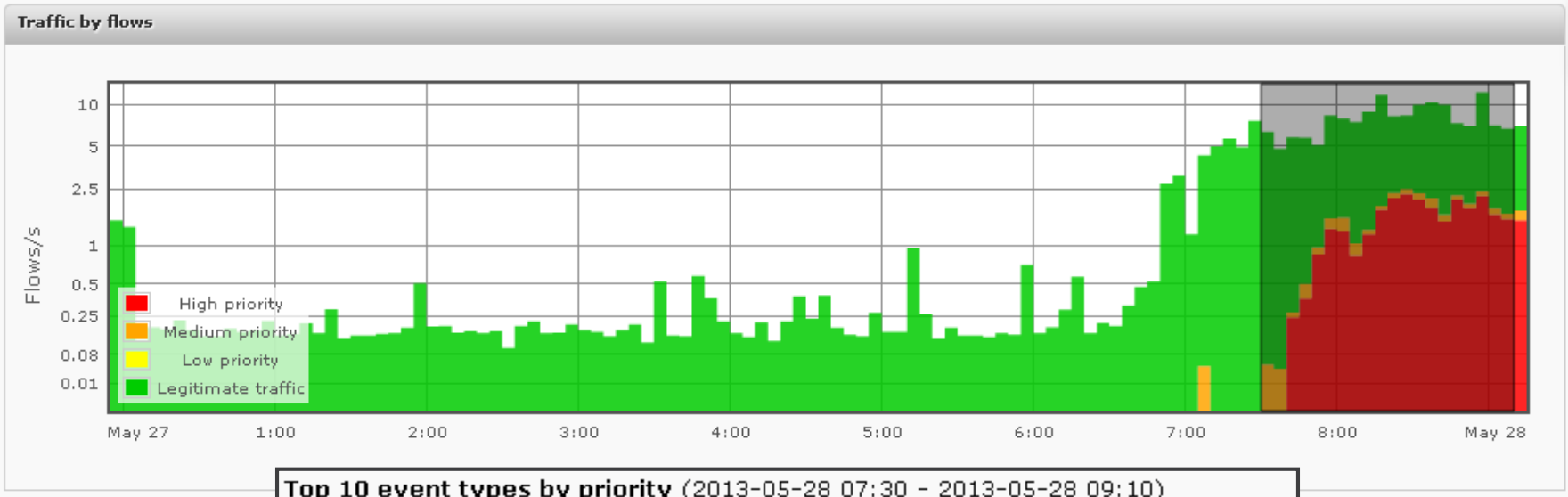
28.5. 9:00 …

To je teda zvláštní …
Žádné hlášení ze Zabbixu nemám
Servery i VPN jsou dostupné
Musím se na to podívat, ozvu se zpět

Hledání příčiny problému

28.5. 9:10 …

78 port skenů?
DNS anomálie?



Top 10 event types by priority (2013-05-28 07:30 - 2013-05-28 09:10)

HIGH	SCANS	78
MEDIUM	DNSANOMALY	91

Hledání příčiny problému

28.5. 9:10 …

Podívejme se na ty skeny
Ok, uživatelům nejede web
Souvisí s tím ty DNS anomálie?

#	Source	Event type	Detail	Timestamp	NetFlow source	Targets	Priority
1	192.168.0.27	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 169, targets: 55, port list: 443, 80, 33033, 12350, 40040, 5222).	2013-05-28 09:09:57	mirror_core	64.4.23.142, 64.4.23.149, 64.4.23.150, 64.4.23.152, 64.4.23.154, 64.4.23.156, 64.4.23.159, 64.4.23.162, 65.55.223.16, 65.55.223.17, …	HIGH
2	192.168.0.27	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 196, targets: 54, port list: 443, 80, 33033, 12350, 40040, 5222).	2013-05-28 09:05:18	mirror_core	64.4.23.141, 64.4.23.147, 64.4.23.152, 64.4.23.158, 65.55.223.13, 65.55.223.15, 65.55.223.16, 65.55.223.18, 65.55.223.22, 65.55.223.31, …	HIGH
3	192.168.0.35	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 99, targets: 31, port list: 80, 443, 33033, 12350, 40028).	2013-05-28 09:05:15	mirror_core	64.4.23.148, 64.4.23.151, 64.4.23.159, 64.4.23.166, 65.55.223.13, 65.55.223.19, 65.55.223.20, 91.190.218.52, 91.190.218.56, 91.190.218.57, …	HIGH
4	192.168.0.24	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 97, targets: 36, port list: 443, 80).	2013-05-28 09:05:09	mirror_core	74.125.224.0, 74.125.224.1, 74.125.224.2, 74.125.224.3, 74.125.224.4, 74.125.224.5, 74.125.224.6, 74.125.224.7, 74.125.224.8, 74.125.224.9, …	HIGH
5	192.168.0.49	SCANS	chaotic TCP SYN scan (attempts with response: 0, attempts without response: 74, targets: 27, port list: 443, 80, 33033, 12350, 5222, 40010).	2013-05-28 09:05:03	mirror_core	64.4.23.152, 65.55.223.16, 65.55.223.32, 65.55.223.37, 66.220.151.99, 69.171.241.10, 91.190.218.52, 91.190.218.53, 91.190.218.55, 91.190.218.61, …	HIGH

Hledání příčiny problému

28.5. 9:15 …

Jaký DNS server se používá?
192.168.0.53? To je notebook!
No asi už tuším…

192.168.0.53 As source: 0 As target: 8

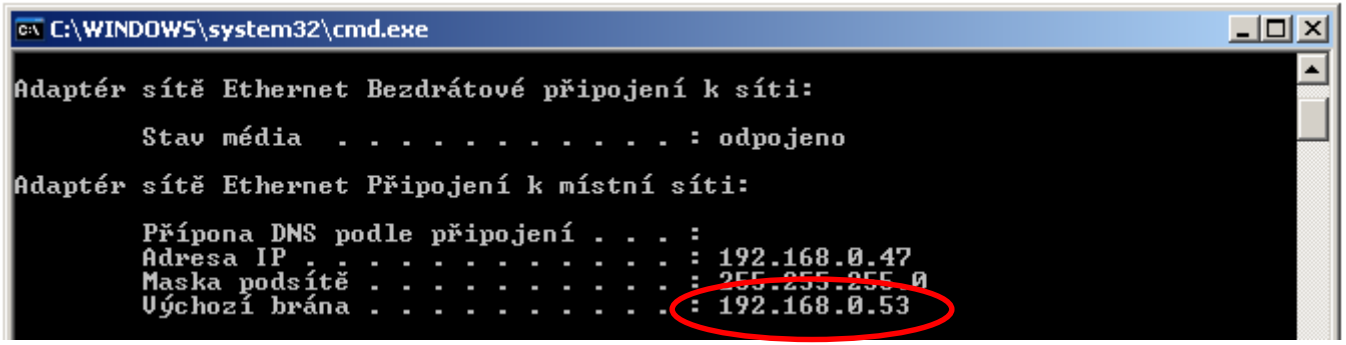
DNSANOMALY 0 8

#	Detail	Timestamp	NetFlow source	Source
1	Use of unexpected DNS server (with response, connections: 1, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:26	mirror_core	192.168.0.14
2	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:17	mirror_core	192.168.0.23
3	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:06:04	mirror_core	192.168.0.22
4	Use of unexpected DNS server (with response, connections: 6, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:44	mirror_core	192.168.0.24
5	Use of unexpected DNS server (with response, connections: 3, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:42	mirror_core	192.168.0.35
6	Use of unexpected DNS server (with response, connections: 6, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:23	mirror_core	192.168.0.20
7	Use of unexpected DNS server (with response, connections: 5, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:23	mirror_core	192.168.0.49
8	Use of unexpected DNS server (with response, connections: 9, commonly used DNS servers: 192.168.0.1).	2013-05-28 09:05:18	mirror_core	192.168.0.27

Hledání příčiny problému

28.5. 9:15 …

Zdá se, že máme v síti nový DHCP server
Ale to je notebook Novákové…



Hledání příčiny problému

28.5. 9:20 …

Tak se na to podívejme…
Notebook o sobě prohlašuje, že je DHCP server

▼ Filter

```
src ip 192.168.0.53 and proto udp and port 67
```

AND <None>

Process | Export to CSV

Start Time - first seen	Duration	Protocol	Source IP address	Source Port	Destination IP address	Destination Port	TCP Flags	TOS	Packets	Bytes	Packets per second	Bits per second	Bytes per package	Flows
2013-05-28 09:13:39.982	144.353	UDP	192.168.0.53	bootps	255.255.255.255	bootpc	.....	0	28	9330	0	517	333	1
2013-05-28 09:16:36.213	55.402	UDP	192.168.0.53	bootps	255.255.255.255	bootpc	.....	0	16	5340	0	771	333	1
									Flows 2		Bytes 14.33 KB			Packets 44

Hledání příčiny problému

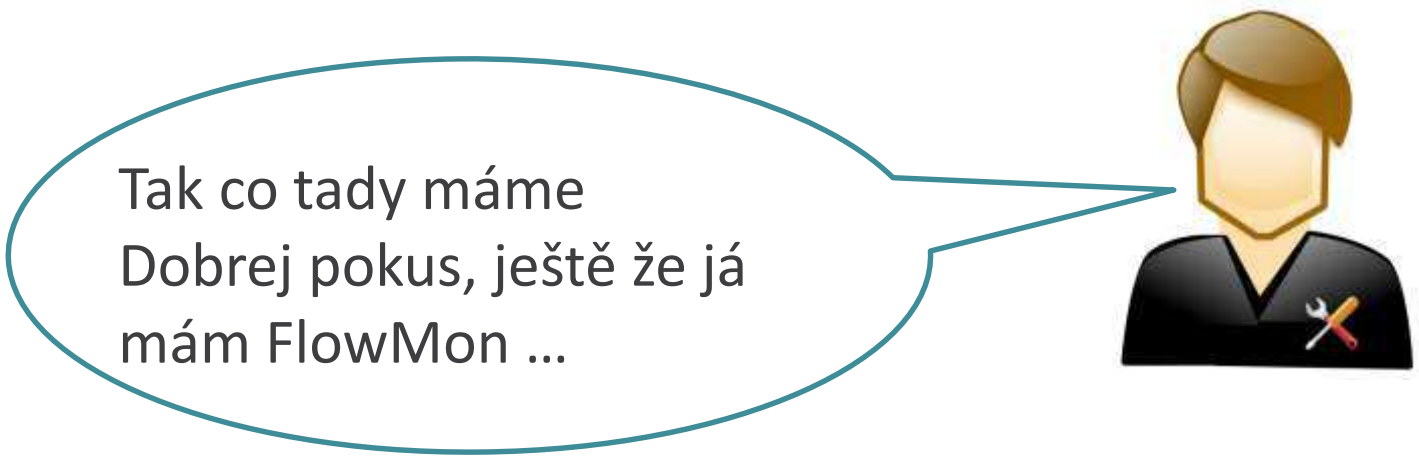
28.5. 9:25 …

Odpojte notebook Novákové!
Je to příčina problému
Asi bude zavirovaný
A restartujte svoje počítače

Nechápu
Aha? Ok
Řeknu to ostatním

Nudná obnova notebooku

29.5. 08:00 …



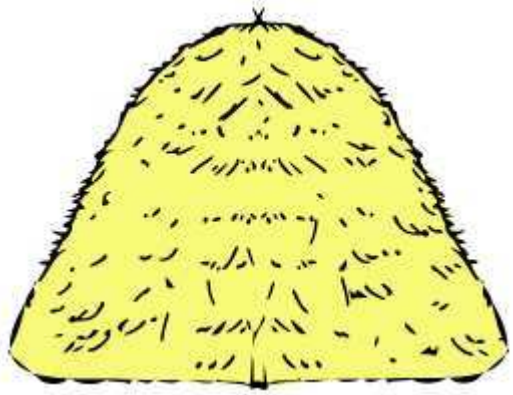
Co kdyby…

- Malware opravdu fungoval?
  - 192.168.0.X <-> 192.168.0.53 <-> 192.168.0.1 <-> Internet
  - Z pohledu uživatele je všechno v pořádku, ale
  - Malware by měl přístup k veškerému provozu
  - Mimo jiné k přihlašovacím údajům a jiným citlivým datům

- IT nemonitorovalo síťový provoz?
  - Pravděpodobně by problém řešili hodiny, ne 20 minut
  - Pokud by malware fungoval, ani by se to nedozvěděli

Shrnutí

- Neztrácejte čas hledáním pověstné jehly v kupce sena
  - Monitorujte síť
  - Buďte proaktivní
  - Buďte o krok napřed



- Běžné prostředky chrání jen do určité míry
  - Firewall, IDS, Antivirus, …
  - Potřebujete nástroje pro monitorování a analýzu provozu datové sítě, řízení přístupu do sítě a log management

Řešte problém komplexně

INVEATECH

Network visibility & security

Perimeter security

End point security

Gartner

Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time.

Recommendations

- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier.

TIME Techland

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

63%
OF THE ORGANIZATIONS IN OUR RESEARCH ARE INFECTED WITH BOTS

CHECK POINT 2013 SECURITY REPORT

The DATACENTER Journal

Attaining Network Visibility in the Era of Big Risk and Big Data

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

O společnosti INVEA-TECH

- Český inovativní výrobce řešení pro monitorování a analýzu provozu datové sítě (**FlowMon**)
- Fakta
  - Založena v roce 2007, sídlo v Brně
  - Silné VaV zázemí (MU, VUT Brno, CESNET)
  - 40+ zaměstnanců
- Ocenění
  - Zařazena do reportů Gartner od roku 2010
  - Deloitte CE Technology Fast 50 (již 2x)
  - Partnerství: Cisco, Check Point
  - 500+ zákazníků (ČR, Evropa, Japonsko, USA)

Gartner Research ID Number: G00208386

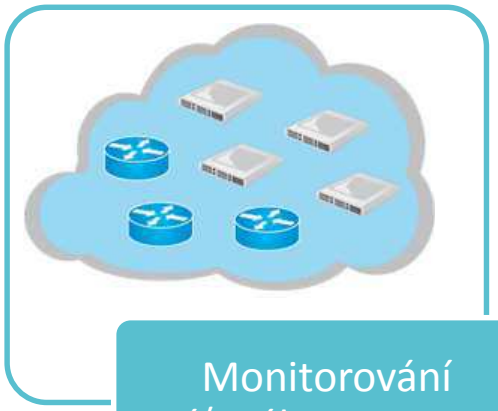
CISCO DEVELOPER Registered

vmware PARTNER TECHNOLOGY ALLIANCE

Check Point SOFTWARE TECHNOLOGIES LTD.

CERTIFICATE OF Deloitte. ACHIEVEMENT

FlowMon architektura



Monitorování síťového provozu

FlowMon Sondy

- samostatné pasivní zdroje statistik ze sítě - NetFlow / IPFIX data

FlowMon Kolektor

- úložiště, vizualizace a vyhodnocení síťových statistik

FlowMon ADS

- detekce anomálií, behaviorální analýza

Z pohledu uživatele

- **Monitorování provozu v síti** (NetFlow/IPFIX)
  - Kompletní viditelnost do dění v síti
  - Real-time a historická data pro LAN & WAN & komunikaci do Internetu
  - Optimalizace správy a provozu sítě
  - Efektivní troubleshooting

- **Bezpečnost datové sítě** (NBA, NBAD)
  - Jediný způsob, jak detekovat pokročilé hrozby
  - Založeno na behaviorální analýze
  - Detekce pokročilého malware, zero-day útoků, podezřelých přenosů dat, změn chování a dalších incidentů

Z pohledu uživatele

- **Záznam provozu v plném rozsahu**
  - Na vyžádání při řešení problémů a incidentů
  - Distribuovaná architektura
  - Podpora sítí 1G/10G/40G

- **Monitorování výkonu aplikací**
  - Sledování uživatelských transakcí bez SW agentů
  - Rozlišení zpoždění aplikace/sítě, sledování SLA
  - Určeno pro moderní (HTTP/HTTPS) aplikace

- **Ochrana přede útoky DDoS**
  - Detekce volumetrických útoků
  - Aktivní řízení směrování provozu a mitigace

Otázky?

INVEATECH

INVEATECH

High-Speed Networking Technology Partner

Pavel Minařík
minarik@invea.com
+420 733 713 703

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com