

SECURITY 2012



20. ročník konference o bezpečnosti v ICT

Zpracování pokročilých útoků

(Behaviorální analýza *aneb Co se nám to tu vlastně děje?*)

Michal Drozd

Senior consultant

AEC

DATA SECURITY





Něco z tisku ... ☺

■ Hacking & Malware business

- Mediální kauzy
 - RSA, Sony, Shady Rat, LM, ...
 - OTE, Letiště Brno, MPSV, ...
 - ACTA

- Zveřejněné vs. Nezveřejněné

■ Zdroje napadení

- Profesionálové
- Amatéři - Skript kiddies

■ Moderní útoky

- APT a nové techniky.
- Zero-day exploits, personalizace.
- Signature resistant.

15. února 2012



SECURITY 2012



Co lze ještě získat...

- Úroveň zabezpečení.
- Úroveň útočníka.
- Specifikace aktiv.
 - Banking
 - Telco
 - Industry
 - Logistika
 - Government

Sun
Tzu's
THE
ART
OF
WAR



Citát: „Celé válečnictví stojí na podvodech“.
Sun Tzu, 500 př.n.l



Vektory útoku

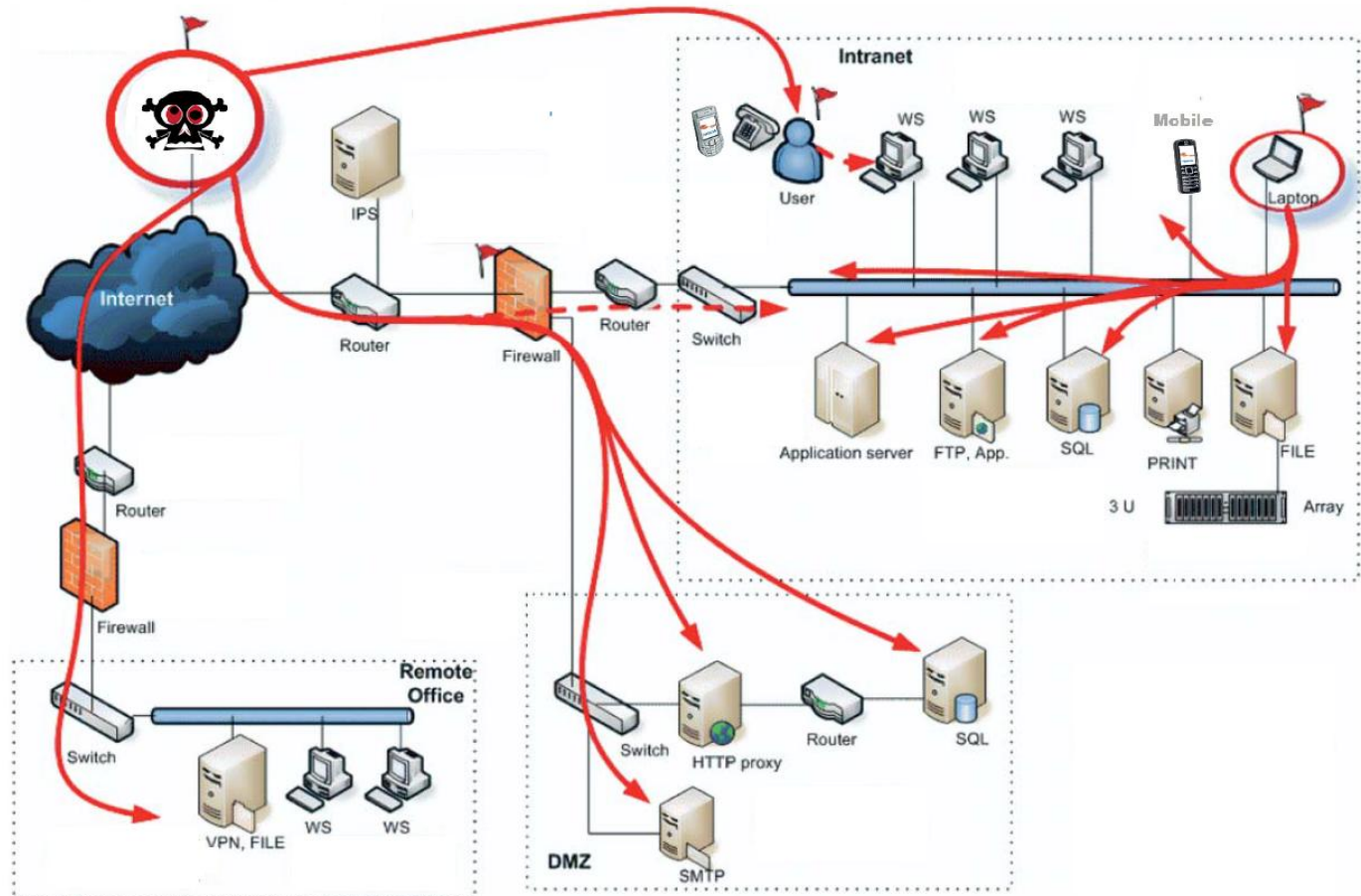
■ Vektory napadení

■ Vnější perimetr

- Služby
- Web
- VPN

■ Vnitřní síť

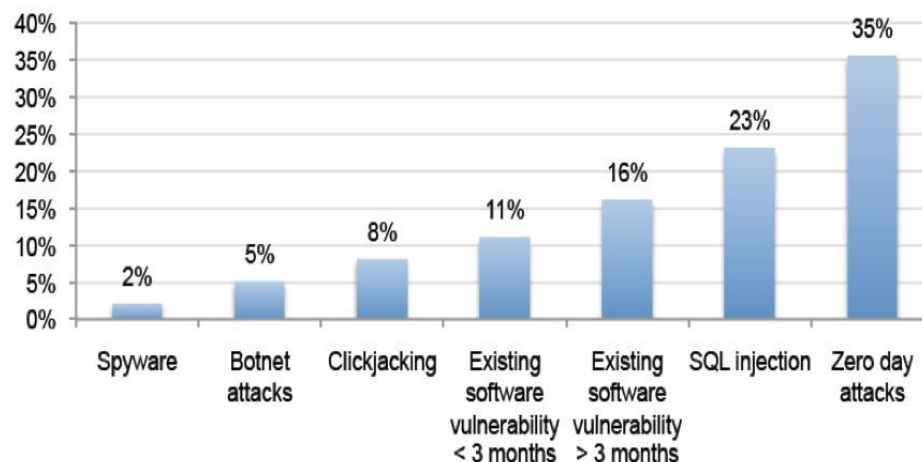
■ Uživatelé



Efektivní způsoby napadení

- Vnější perimetr.
- Intranet.
 - Web
 - Data Injection.
 - Zero-day exploits.
 - Passwords.
 - Běžné služby
 - Passwords.
 - Zero-day exploits.

- Uživatelé
 - Trojanizace
 - Web.
 - Mediální soubory.
 - Socialing.





Aktuální obrana – Antimalware

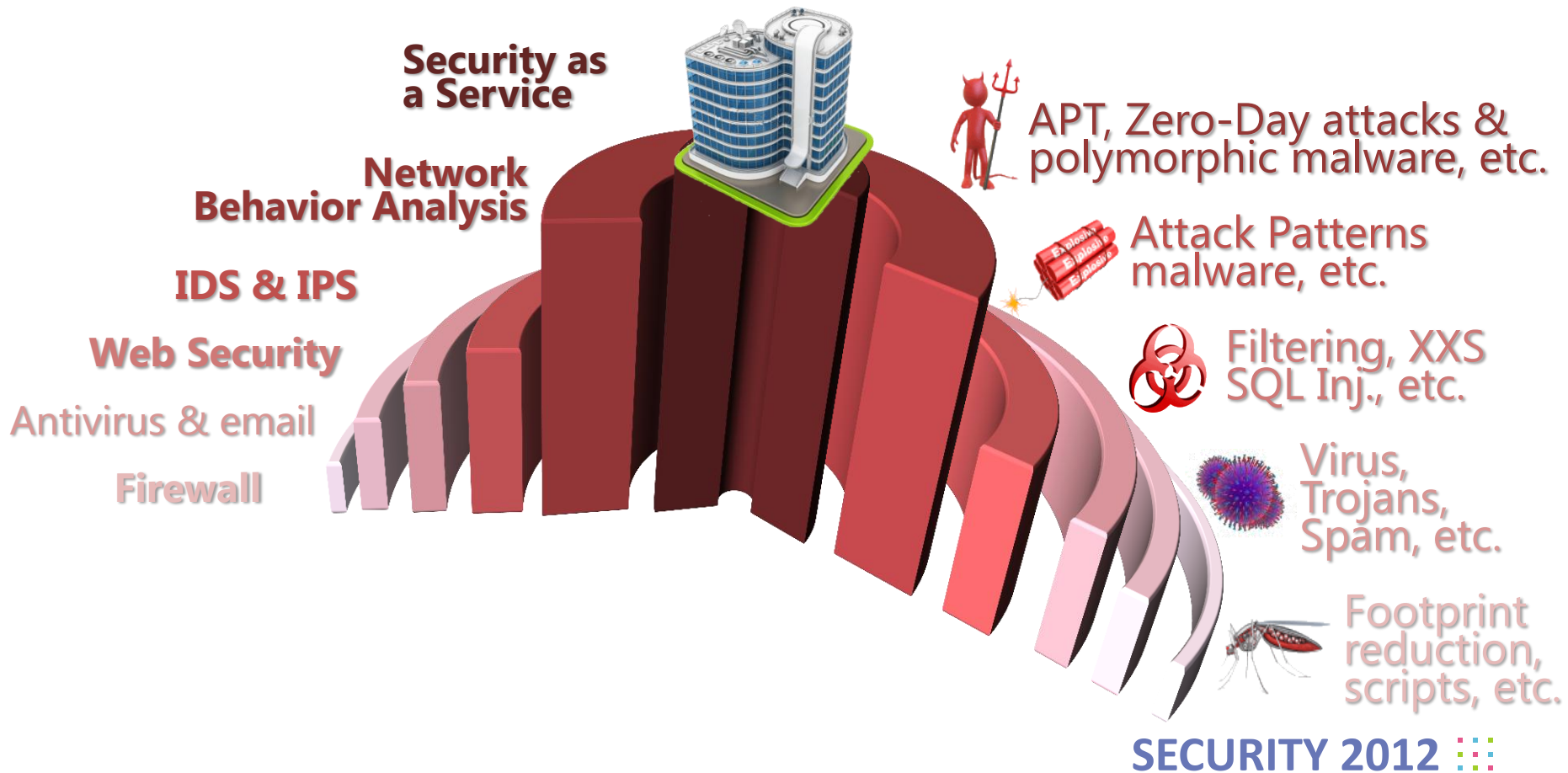
- Signatures based
 - Antivir (rok 1988)
 - IDS & IPS (rok 1985)
- Signatures free
 - SIEM, DLP, Web security.
 - Firewall
 - **Behavioral analysis based**
 - NBA - Network Behavioral Analysis (2002)
 - ADS - Anomaly Detection System (1998)
- Nedostatky





Způsoby obrany

- Rozdělení detekce útoků pro jednotlivé technologie





NBA – popis technologie

- Detekce na základě statistických metod
- Designové cíle
 - Chránit klienty Predikováním a Diagnózou útoků/anomálií
 - Zbavit se závislosti na signaturách
 - Založeno na analýze síťových dat (netflow, dump)
 - Nabídnout inteligentní pohled na velké množství dat



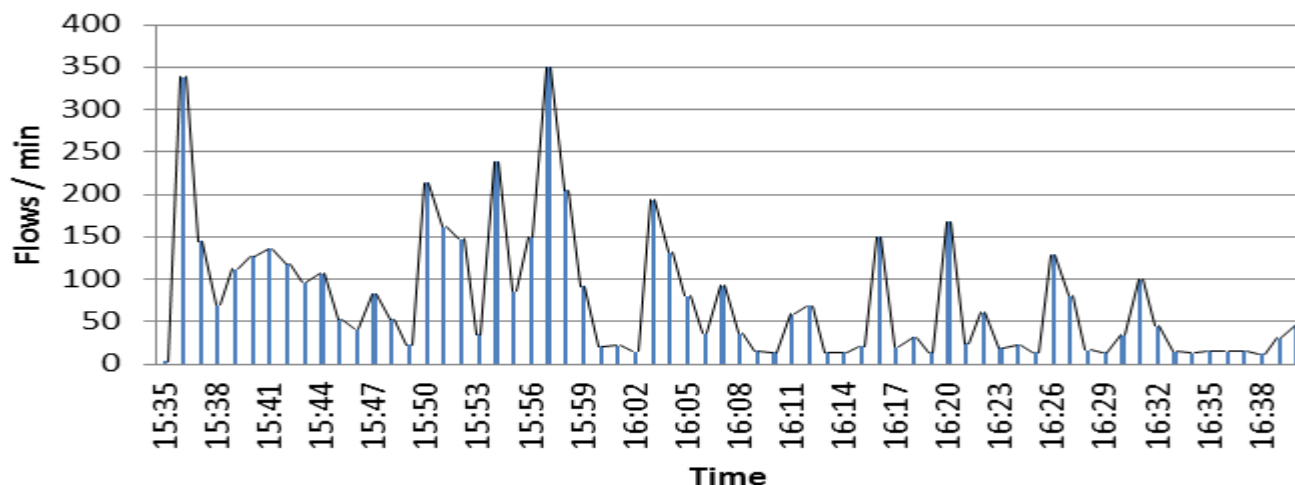


Princip detekce – komunikace malware

■ Netflow - http komunikace

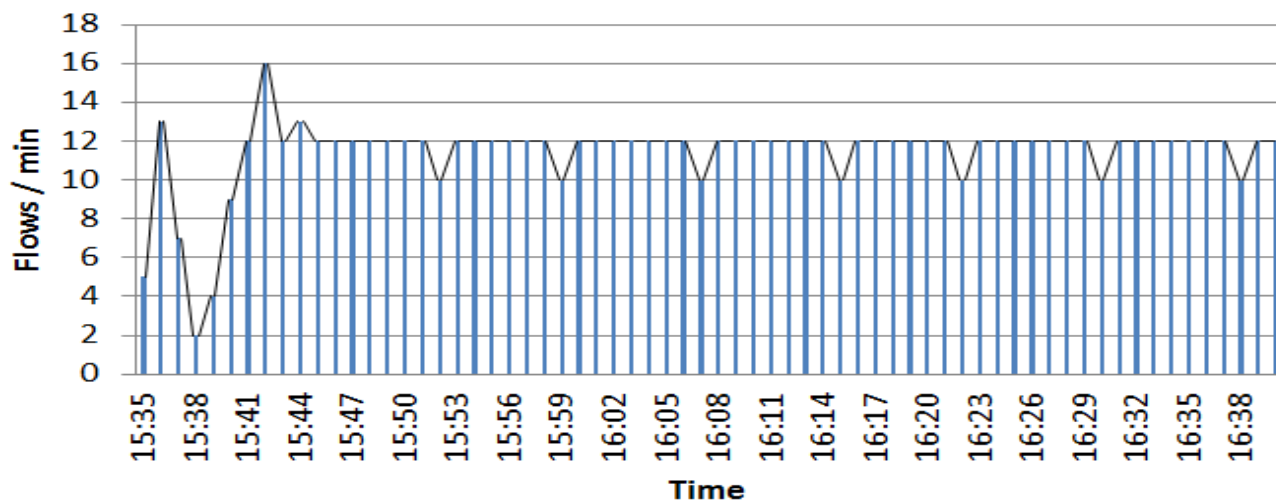
■ Legální

■ user



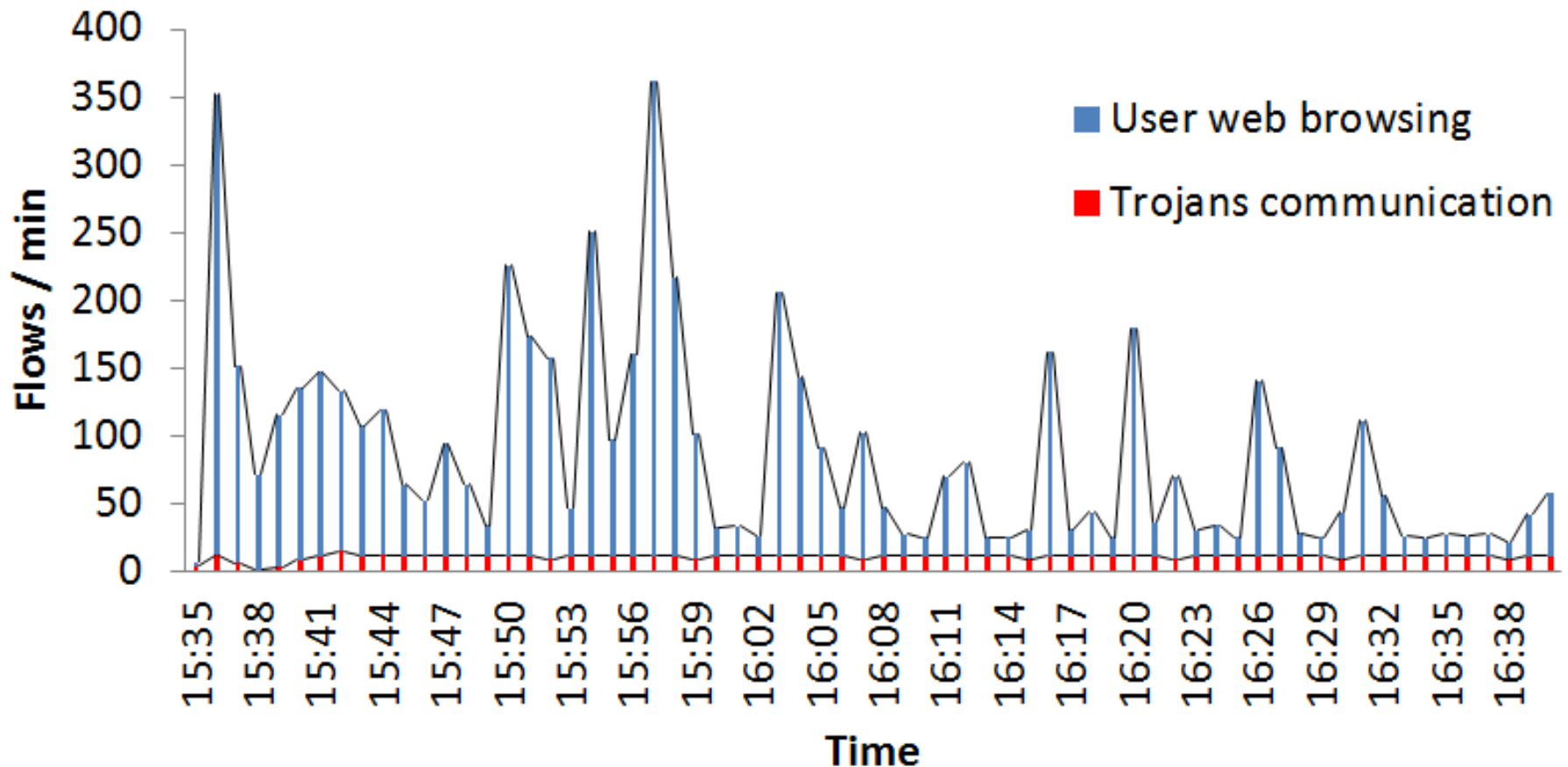
■ Nelegální

■ trojan



Princip detekce – komunikace malware

■ Výsledné spojení obou grafů





Vendors

- AdvaICT – FlowMon ADS
- Arbor Networks – PeakFlow X
- Cognitive Security - Cognitive Analyst
- LanCope - StealthWatch
- McAfee – NUBA & NTBA
- Plixer – Scrutinizer & Flowalyzer
- Q1 Labs (IBM) - QRadar
- RSA - NetWitness



- FlowMon ADS



Cognitive Security

- Cognitive Analyst
- Ocenění Česká hlava 2010 za přínos v AI



■ NetWitness



Důležité vlastnosti

- Detekční metody
 - Založené na pravidlech
 - Založené na umělé inteligenci
- Klasifikace provozu
 - Klasifikace pouze anomálií
 - Klasifikace celého provozu
- Možnosti nasazení
 - Dodaný HW
 - Vlastní zdroje
- Ostatní aspekty
 - Přehlednost GUI
 - Jednoduchost nasazení
 - Cena licence a doplňků (HW sondy)





Závěrem

- S NBA jsme začali v roce 2010
- Velké množství zkušenosti
 - Brýle do vnitřní sít
 - Relativně jednoduché rozhraní, nutný skill (puška)
- Velmi pozitivní výsledky
 - Detekce
 - APT
 - Řada kompromitovaných zařízení
 - Útoky ve vnitřní síti
 - Dohled nad uživateli, outsourcingem a procesy
- NBA je nutnou součástí kvalitního monitoringu



Cisco 2Q11 Global Threat Report

- *“[If] you’re not seeing APT attacks in your organization, it is probably not that they are not occurring or that you’re safe. It’s more likely that you may need to rethink your detection capabilities”*
 - [Cisco 2Q11 Global Threat Report]

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Michal Drozd

AEC, spol. s r. o.

michal.drozd@aec.cz

