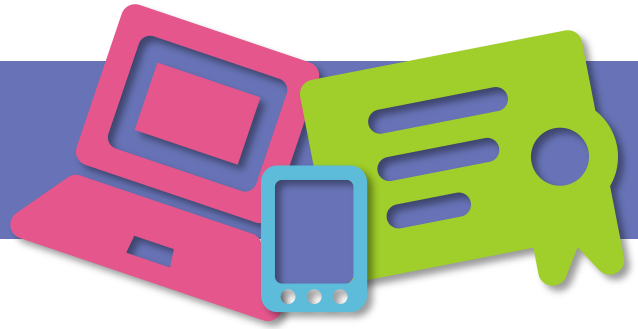
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Boj s cielenými útokmi

Daniel Hetényi

Trend Micro

Ponemon 2012: Priemerná cena útoku $8.9M

EMC: Cena útoku na RSA $66M

IANS Survey: 50% dotazovaných boli obeťami cieleného útoku

Verizon 2013: 75% útokov vyžadovalo minimálne znalosti

…. Ale extra vysoké náklady / znalosti na detekciu a ochranu

Neférový súboj s útočníkmi

ÚTOČNÍCI

- ✓ Lacné nástroje
- ✓ Nájdu miesto prieniku
- ✓ Zameranie na konkrétny cieľ
- ✓ Nízky postih pri neúspechu

OBRANA

- ✗ Drahé zdroje na obranu
- ✗ Veľa bodov na bránenie
- ✗ Bránim sa voči všetkému
- ✗ Vysoký postih pri neúspechu

Ekonomika útoku

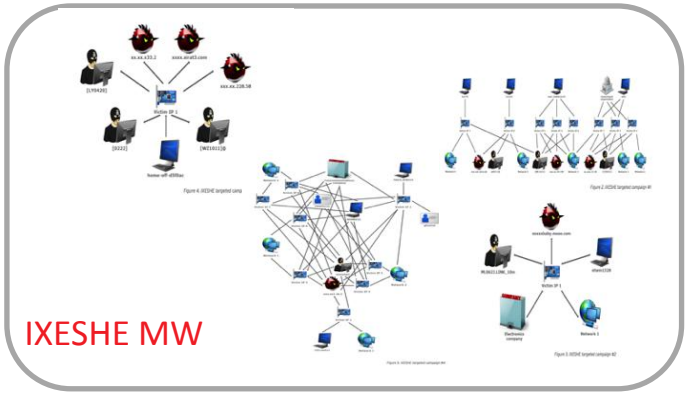
Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per update

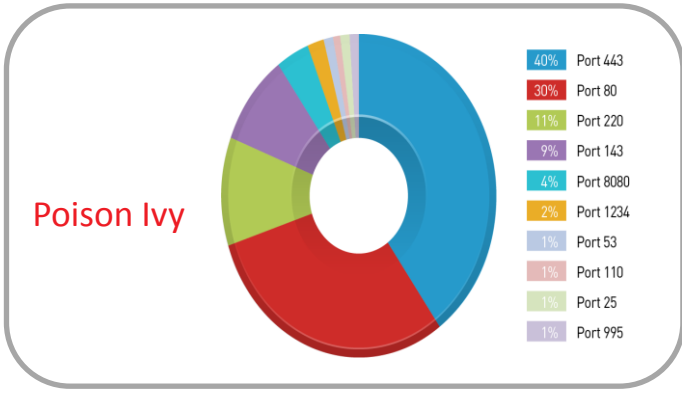
Table 7: Botnet prices

Offering	Price
1-time security software checking	US$0.15-0.20
1-week subscription	US$10
1-month subscription	US$25-30

Table 8: Security software checking prices

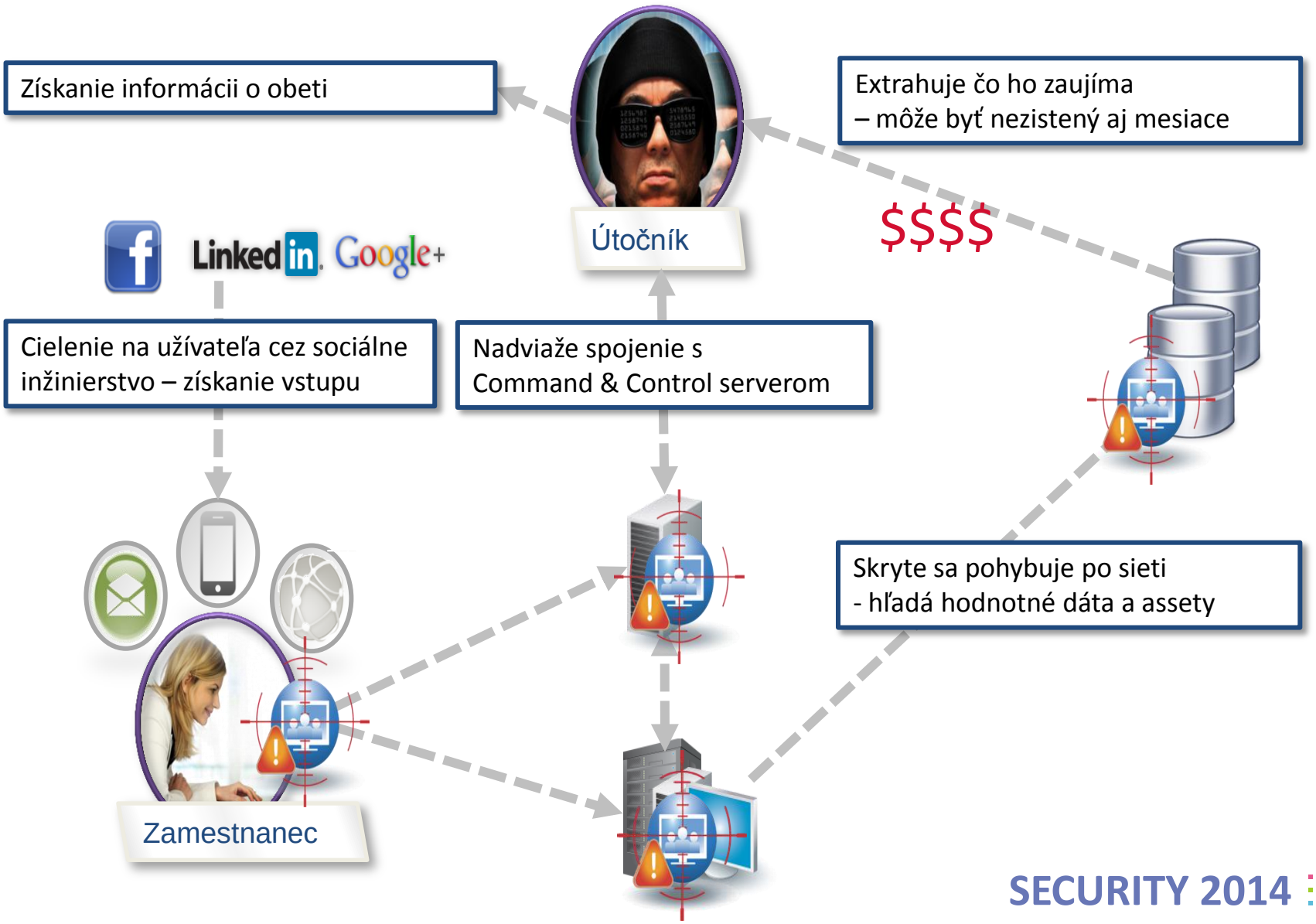
Pokročilé maskovacie techniky



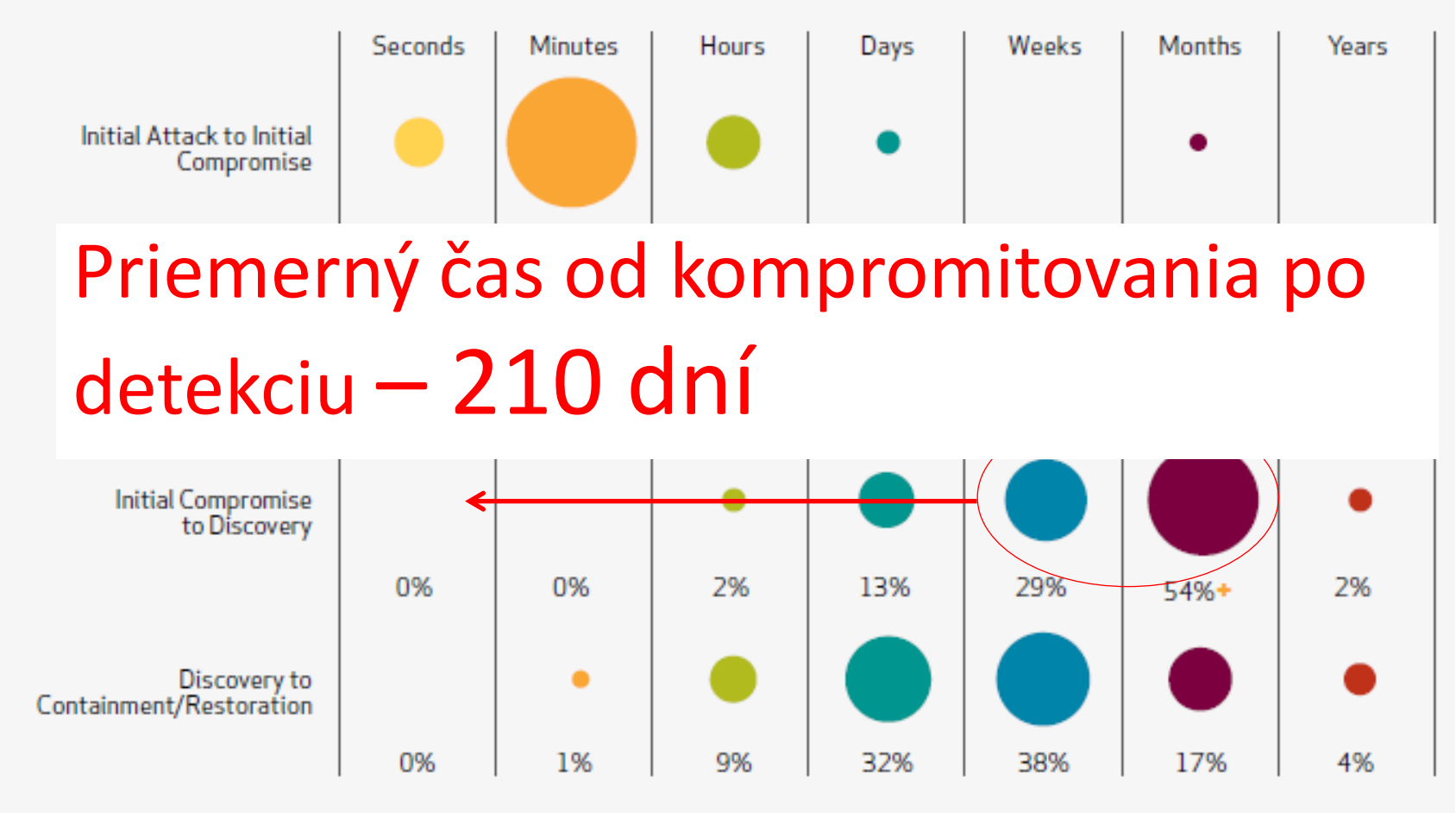


- Útoky z legitímnych kanálov
- Neštandardné komunikácie k C&C serverom
- Rôzne typy protokolov, aplikácií a metód

Anatómia cieleného útoku



Ako dlho sú útoky schované



Priemerný čas od kompromitovania po detekciu – 210 dní

Source: Verizon Data Breach Investigations Report 2012

1. Detekcia – Bod vstupu

1. Signatúrový antimalware scan
2. Emulujte neznáme súbory v sandboxe:
   1. Analýze podrobte **všetky** tipy súborov
   2. Využite vlastné prostredie ako sandbox

      (napr. Win 7, Adobe Reader 10, Java 1.6, MS Office 2013)
3. Ak podrobná simulácia kódu preukáže škodlivé správanie kódu, nastavte si obranu
   - Škodlivé správanie = zhadzuje kód bezpečnostné nastavenia, pristupuje na nebezpečné URL, začína sa propagovať, mení registre, systémové DLL, snaží sa zneužiť nejakú zraniteľnosť …

2. Detekcia – Command & Control

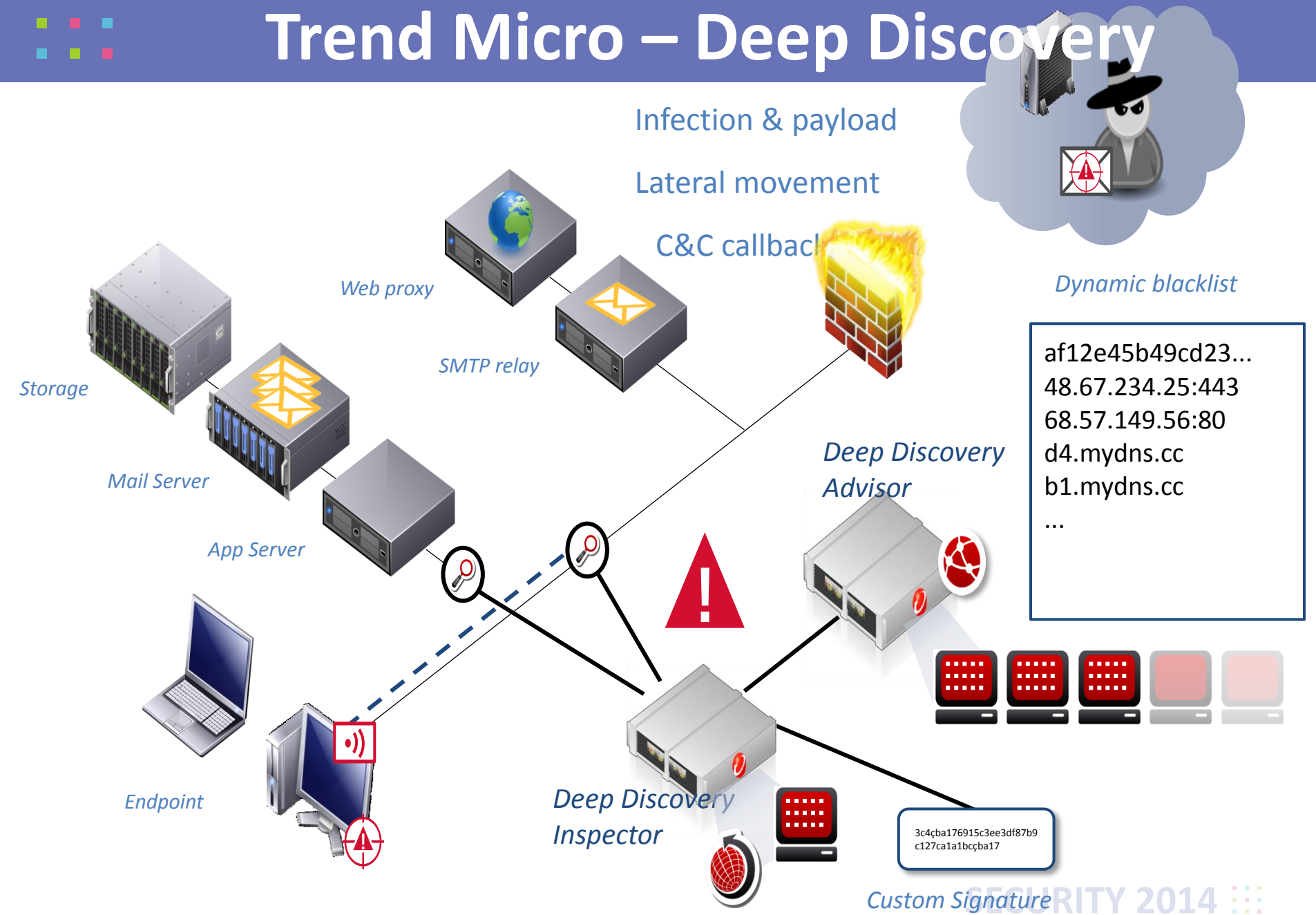
1. Zistite komunikáciu kódu “domov”
2. Monitorujte všetky protokoly
3. Sledujte aj interné C&C servre
4. Z emulácie neznámych súborov získate nové C&C servery určené na cielený útok
5. Nastavte si IP a URL blacklisty na webových, emailových bránach, firewalloch alebo routroch, endpointových ochranách

3. Detekcia – Laterálne pohyby

Zabráňte prieniku útočníka hlbšie do infraštruktúry

1. Zistite podozrivú komunikáciu
   - Sken siete, sken serverov na zraniteľnosti, propagácia kódu
2. Zistite podozrivé stavy v sieti
   - Brute force útoky, útoky na DNS servre, Active Directory
3. Tieňte zraniteľnosti na kritických službách

Trend Micro – Deep Discovery



Trend Micro – Deep Discovery

- **Na mieru šitá detekcia**
  - Detekuje celý útočný cyklus
  - Sandboxy sú prispôsobiteľné na vlastné prostredie
  - Emulujeme ďaleko viac ako Microsoft prostredie (android, mac, ..)
  - Inšpekcia 100+ protokolov
- **Na mieru šitá obrana**
  - Ochrana na sieti, na koncových zariadeniach a serverov s custom signatúrami
  - Integrácia s poprednými SIEM riešeniami
  - Podrobný popis hrozieb s vysvetlením, čo robia
- **Nízke náklady:**
  - 1 zariadenie na záchyt všetkej sieťovej komunikácie a rôzne prevedenia
- **Expertíza:**
  - 25 rokov v IT bezpečnosti a 1.300 výskumníkov

SECURITY 2014

Útok na Južnú Kóreu

- Opakované sofistikované útoky na vlády a firmy
- Útok v 03 – 2013 ochromil časť bánk, vlády a médií

Trend Micro Deep Discovery chránilo úspečne viac polovicu bánk, 80 vládnych inštitúcií a mnohé firmy

Čo môžete spraviť ešte dnes

- **Získajte obrázok o vašej bezpečnosti**
  - Zapožičanie riešenia na detekciu cielených útokov
  - Zapája sa pasívne (span port) za už existujúce obrany
  - 2 týždne zber dát
  - Kompletný obrázok, či sa vás niekto snaží kompromitovať alebo už ste kompromitovaní, aké útoky sa použili
- **Osobná konzultácia** s Trend Micro

ku kybernetickej bezpečnosti

Špeciálny bónus

Získajte **zadarmo** licenciu

Trend Micro Titanium Maximum Security

v hodnote 1.500 Kč!

Ochránite ňou až 3 domáce zariadenia na 1 rok.

Za vizitku na stánku Trend Micro.

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Daniel Hetényi

Trend Micro

Daniel_Hetenyi@trendmicro.com