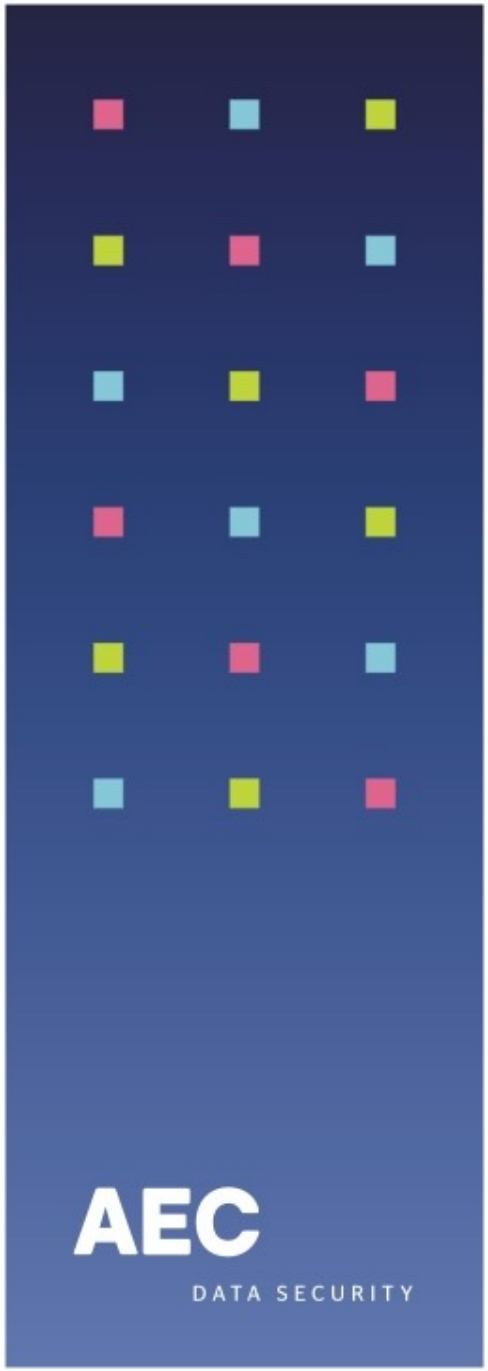
AEC
DATA SECURITY

Úvod do kybernetické (ne)bezpečnosti

Lukáš Bláha
Senior IT Security Consultant
25. 4. 2016

Bio

- V IT bezpečnosti více než 5 let
- Penetrační testy & testy sociálním inženýrstvím
- Implementace bezpečnostních technologií
- Mobilní technologie a trendy
- Zákazníci typu:
  - Finanční sektor
  - Telekomunikace
  - Energie
  - Farmacie
  - Ecommerce



Obsah

- Jaké jsou cíle útoků?
- Kdo a proč útočí?
- Jakým způsobem útočí?
- Jaké existují ochrany?
- Okénko do budoucnosti

Kdo byl napaden?

- Finanční sektor – JP Morgan Chase, Multi-Bank Cyberheist, Global Payments, Íránské banky, American Business Hack, Citigroup
- Telco – Vodafone, T-Mobile, AT&T
- IT – Adobe, Apple, HP, Kaspersky Lab, RSA, HBGary
- Web/e-commerce – AshleyMadison, CarPhone, Living Social, Linkedin, Twitter, Ebay, SnapChat
- Zdravotní organizace – Anthem, CareFirst, Premera
- Armáda – US Military, Stratfor, US Army
- Obchod – UPS, Target, Home Depot, Starbucks
- Vládní organizace – US OPM, Turecko, Sýrie, Austrálie, Jížní Afrika
- Průmysl & infrastruktura – Israel Power Plant (červ Stuxnet), Ukraine Energy Grid

Kdo a proč?

- Typy útočníků a jejich motivace
  - White Hat Hacker – „good guys“
  - Black Hat Hacker - finanční zisk
  - Script kiddie – zvědavost, sláva
  - Hacktivista - politický/společenský/náboženský zájem, odplata
  - Státem podporovaný hacker – „control cyberspace“, armádní cíle
  - Špión - konkurenční boj
  - Kyberterorista – šíření strachu a paniky

Kdo a proč?

- Dříve útoky jednotlivců za účelem osobní slávy
- Dnes specializované a velmi motivované skupiny útočníků, kteří mají dostatek zdrojů (peněz, znalostí, času)
- (ne)legální business - hacking na zakázku (445 miliard dolarů ročně)
- Malware-kity, botnety, exploit – komodita

]HackedTeam[

Hacking Team's clients are the governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE, many of whom have

Jak?

- Obecný scénář útoku:

  1. Získání přístupu – fyzicky, e-mailem, pomocí zranitelnosti síťové služby nebo aplikace. Zajištění vzdáleného přístupu do sítě.

  2. Prohledání sítě společnosti – hledání dalších zranitelných prvků.

  3. Kompromitace jednotlivých systémů – zajištění kontinuálního pokračování útoku v případě odhalení jednoho z bodů.

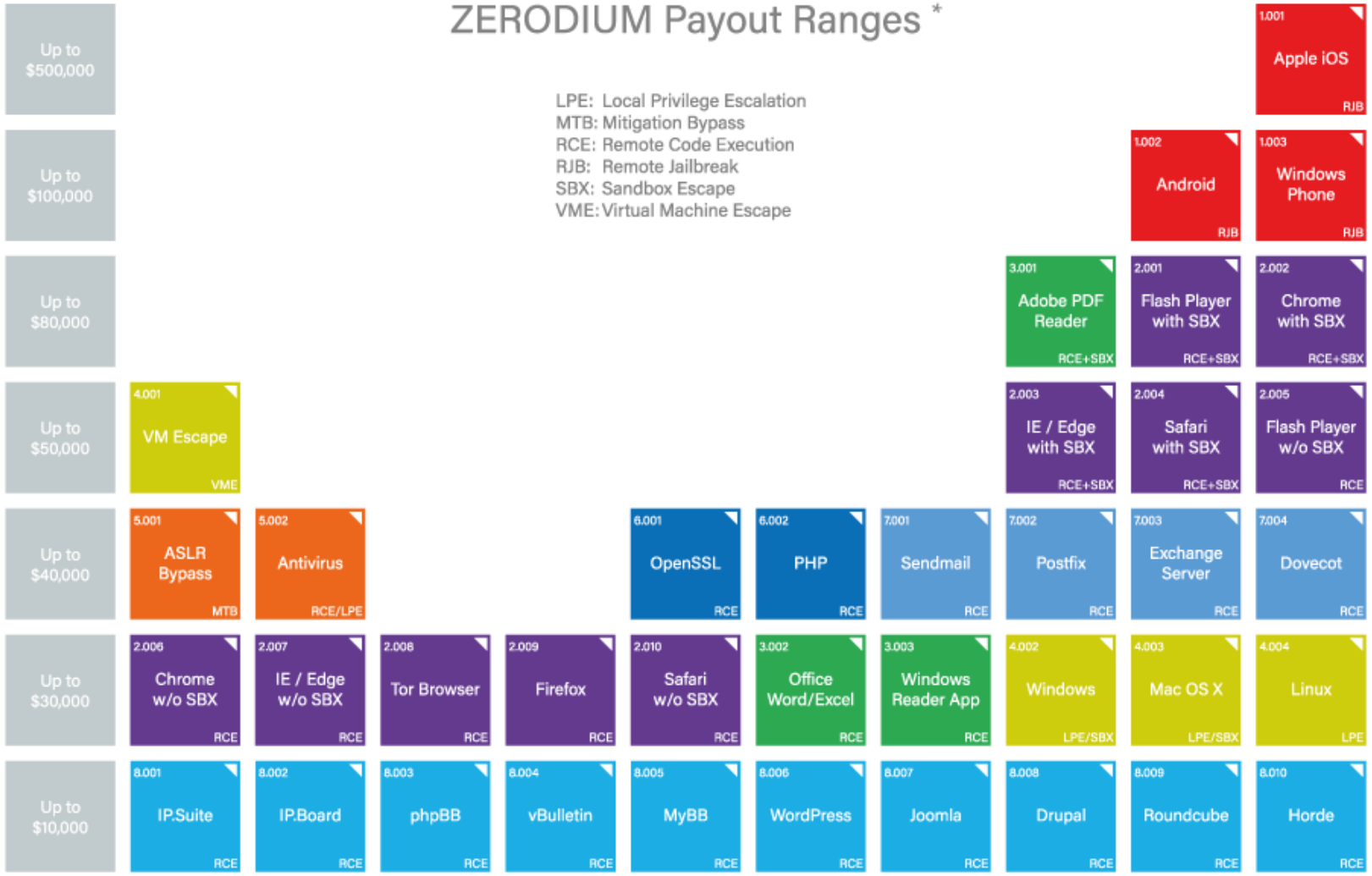
  4. Úplná kompromitace sítě (privilege escalation) – získání přístupových údajů k serverům, službám, aplikacím a nakonec i k účtům doménových administrátorů.

  5. Sběr a exfiltrace citlivých dat.

  6. Zahlazení stop – odstranění všech stop, které byly zanechány. Síť však zůstává kompromitována, aby se mohl útočník vrátit zpět.

Nejčastější vektory útoku

- Softwarové zranitelnosti – 0-day



Nejčastější vektory útoku

- Chyby ve webových nebo mobilních aplikacích – SQL Injection, XSS, chybná autentizace
- Špatná konfigurace – nedostatečné autentizační metody, slabá uživatelská hesla!!
- Malware
  - vir, červ, trojský kůň, rootkit, spyware, backdoor, keylogger
  - ransomware
  - malwaretising
- Sociální inženýrství
  - emailový – phishing
  - telefonický
  - fyzický
  - sociální sítě
- Inside job

Jak se bránit?

- Bezpečnostní (penetrační) testy
- Bezpečnostní hardening systémů
- Technologie
  - Firewall, Antimalware, AntiSpam, …
  - Security Information and Event Management
  - Vulnerability Management Systems
  - Web Application Firewall
  - Data Loss Prevention
  - Network Behavior Analysis
  - Mobile Endpoint Protection
- Vzdělávání koncových uživatelů v oblasti aktuálních bezpečnostních hrozeb
- Důkladná kontrola zaměstnanců

Budoucnost a trendy

- Internet of Things – lékařské přístroje, smart cars, smart home
- Mobilní zařízení - hlavní nástroj pro práci & zábavu
- Cílem budou i menší společnosti a jiné oblasti trhu (např. školství)
- Více útoků s jiným cílem než je finanční zisk – destrukce/vandalismus a politický/ideologický zájem
- Vznik nových zákonů, vyhlášek, regulací

WE NEED YOU

Děkuji za pozornost

Otázky?

Lukas.Blaha@aec.cz