Preventivní akce CSIRT.CZ v roce 2017

Pavel Bašta • email@nic.cz • 21. 06. 2017

CZ.NIC | SPRÁVCE DOMÉNY CZ

Proč?

- Je lepší problémům předcházet, než je řešit
- Známé případy z posledních let
  - Nezáplatované/neupgradované stroje → ransomware WannaCry
  - Nezabezpečené kamery → Botnet Mirai
  - Zranitelnosti PhpMyAdmin, JBosse, MySQL, MSSQL serveru, ElasticSearch, Apache Tomcat, Oracle Weblogic → botnet BondNet
  - Zranitelnost pluginu RevSlide pro WordPress → 100 000 webů šířících malware
  - Netgear Authentication Bypass → odhadem 10 000 routerů s pozměněnými DNS servery

Z čeho vycházíme

- Pasivně získaná data
  - V současnosti využívána v nástrojích Malicious Domain Manager (MDM) a PROKI
  - Dále v rámci incident handlingu
  - Nárazově z veřejně dostupných dat (shodan, pastebin)
- Aktivně získaná data
  - Honeypoty
  - Aktivní skenování sítí

Co už jsme dělali a děláme

- Malicious Domain Manager
- Skener webu
- Testování odolnosti sítě
- Honeypoty
- Zranitelné routery Asus
- Uniklé přihlašovací údaje
- Dostupné SCADA a další průmyslové řídící systémy

Co už jsme dělali a děláme

- Varování před útoky zaměřenými na uživatele z ČR
- Nenáhodné zdrojové porty DNS serverů
- Heartbleed
- ROM-0

Právní rámec

- Možný problém u aktivního skenování sítí
  - § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
    - (1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.
    - (2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a
    - a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
    - b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
    - c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
    - d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,
    - bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.

Právní rámec

- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
  - (1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
  - a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
  - b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,
  - bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.

Právní rámec

- Jak se lze bránit
  - § 30 Svolení poškozeného
    - (1) Trestný čin nespáchá, kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny.
    - (2) Svolení podle odstavce 1 musí být dáno předem nebo současně s jednáním osoby páchající čin jinak trestný, dobrovolně, určitě, vážně a srozumitelně; je-li takové svolení dáno až po spáchání činu, je pachatel beztrestný, mohl-li důvodně předpokládat, že osoba uvedená v odstavci 1 by tento souhlas jinak udělila vzhledem k okolnostem případu a svým poměrům.
    - (3) S výjimkou případů svolení k lékařským zákrokům, které jsou v době činu v souladu s právním řádem a poznatky lékařské vědy a praxe, nelze za svolení podle odstavce 1 považovat souhlas k ublížení na zdraví nebo usmrcení.

Právní rámec

- § 31 Přípustné riziko
  - (1) Trestný čin nespáchá, kdo v souladu s dosaženým stavem poznání a informacemi, které měl v době svého rozhodování o dalším postupu, vykonává v rámci svého zaměstnání, povolání, postavení nebo funkce společensky prospěšnou činnost, kterou ohrozí nebo poruší zájem chráněný trestním zákonem, nelze-li společensky prospěšného výsledku dosáhnout jinak.
  - (2) Nejde o přípustné riziko, jestliže taková činnost ohrozí život nebo zdraví člověka, aniž by jím byl dán k ní v souladu s jiným právním předpisem souhlas, nebo výsledek, k němuž směřuje, zcela zřejmě neodpovídá míře rizika, anebo provádění této činnosti zřejmě odporuje požadavkům jiného právního předpisu, veřejnému zájmu, zásadám lidskosti nebo se příčí dobrým mravům.

Právní rámec

- „Riziko musí být postoupeno za účelem, dosažení společensky nutných či potřebných hodnot, očekávaný výsledek musí být rentabilní ze společenského hlediska. Riziko je společensky prospěšné, jestliže se jeho podstoupením zvyšuje celková společenská efektivnost a produktivita práce, jestliže dochází k osobním, časovým a materiálním úsporám – je přitom samozřejmé, že výhoda, o kterou se usiluje, nesmí být neoprávněná.
  - *ŠÁMAL, Pavel a kol. Trestní zákoník I. § 1 až 139. Komentář. 2. vydání. Praha: C. H. Beck, 2012. s. 428.*

Co chystáme v roce 2017

- Ověřovací fáze provozu systému PROKI
- Sken CMS
- Hledání kompromitovaných webů

Ověřovací fáze provozu systému PROKI

- Dvě hlavní funkce
  - Automatizované rozesílání informací o incidentech pocházejících ze sítí v ČR
    - Veřejné i neveřejné zdroje
    - Služba pro správce z koncových sítí
    - Pouze informace relevantní pro ČR
    - Agregace informací do jedné zprávy
  - Analytické funkce
    - Především pro potřeby CSIRT.CZ
    - Některé výstupy budeme předávat partnerům

Ověřovací fáze provozu systému PROKI

- Důležité informace
  - 1x týdně agregované informace do každé sítě
  - Agregace podle abuse mailu
  - Posíláno na abuse kontakt
  - Možnost požádat o vyřazení ze zasílání i o změnu e-mailové adresy
  - Ne všechny typy incidentů vyžadují stejnou pozornost
  - Uvítáme zpětnou vazbu

Ověřovací fáze provozu systému PROKI

- Formát

```
- time_detected - čas, kdy byl incident detekován
- ip - ip adresa vykazující popisované chování
- class - třída incidentu
- type - typ incidentu (jedna třída může obsahovat více typů)
- time_delivered - čas, kdy byl incident zaregistrován systémem PROKI
- country_code - kód země
- asn - číslo autonomního systému
- description - dodatečný popis incidentu, pokud je dostupný
- malware - rodina nebo název malwaru, pokud je dostupný
- feed_name - název zdrojového feedu
- feed_url - odkaz na zdrojový feed
- original_base64 - původní záznam ze zdrojového feedu kódovaný base64
```

PROKI
PREDIKCE A OCHRANA PŘED KYBERNETICKÝMI INCIDENTY

Projekt „**Predikce a ochrana před kybernetickými incidenty (PROKI)**“ (*VI20152020026*) je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.

CZ.NIC | SPRÁVCE DOMÉNY CZ

Skenování CMS

- Content Management System
  - Joomla, Drupal, WordPress...
  - Častá příčina napadení webových stránek
  - Analýza společnosti Sucuri z roku 2016
    - 75 % z napadených webů běželo na WordPressu
    - Více než 50 % pak bylo provozováno na neaktuální verzi
    - 1/3 napadení také přes neaktualizované pluginy

Skenování CMS

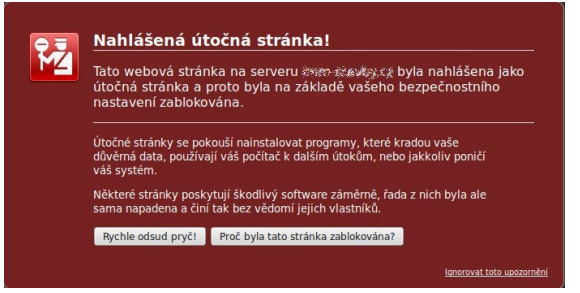
- Tento rok test verzí CMS
- Podle výsledků bychom do budoucna rozšířili skenování o hledání zranitelných pluginů
- Načtení hlavní stránky webu
- Hledání meta tagu Generator
- Následně sada testů pro bližší identifikaci verze
- User-agent "csirt.cz CMS seeker"

Skenování CMS

- V rámci přípravy otestováno cca 100000 domén
  - Cca 45 procent webů používá nějaké CMS
  - 3% WordPress 4.6.6
  - 2% WordPress 4.4.10
  - WordPress 3.3.2
  - WordPress 3.0.1
  - 2,8 % Joomla 1.5

Hledání kompromitovaných webů

- Cílem vyhledat napadené stránky šířící malware o kterých nevíme
- Synergie projektů Turris, Malicious Domain Manager (MDM)
- MDM dodává informace o nebezpečných zahraničních IP do Turrisu, Turris nás informoval o podezřelém chování „turistů“
- Budeme hledat pokusy o spojení na IP které známe, případně na jakékoliv zahraniční IP adresy
- Proof of Concept



Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz