WPAD a bezpečnost v DNS

Viktor Kustein, Gransy s.r.o.

1. Kdo jsme a co děláme?

- Poskytovatel hostingu a doménových služeb.
- Vlastní ICANN akreditace.
- Zákazníky máme od koncových uživatelů po registry.
- AnycastDNS.

2. Čeho chceme docílit?

„Nechceme být jen doménový registrátor, ale chceme být i poskytovatel, který se angažuje při zajišťování stability a bezpečnosti Internetu.“

3. Co pro to děláme?

- Automatizujeme registrace.
- Podporujeme DNSSEC všude, kde to jde.
- Poskytujeme AnycastDNS (například pro KE a BA ccTLD).
- Provozujeme vlastní checker dns.app.

4. Co pro to ještě budeme dělat?

- Připravujeme protected Anycast public DNS (46.8.8.8), bude se snažit ochránit uživatele před škodlivými doménami.
- Provozujeme Public Static DNS a síť proxy serverů, na kterých analyzujeme a vyhledáváme právě tyto škodlivé domény.
- Chceme sestavit vlastní CSIRT tým a získat akreditaci.

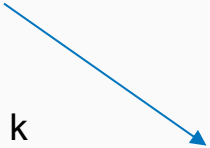
WPAD

1. WPAD

- **Web Proxy Autodiscovery Protocol** (WPAD). Je to metoda, kterou využívá většina webových prohlížečů k automatickému zjištění umístění proxy serveru.
- Po startu prohlížeče se automaticky spustí dotaz na vyhledání serveru wpad.lokalni_domena, a poté se zkusí stáhnout soubor wpad.dat. Když takový soubor na serveru je, daný prohlížeč jej stáhne a spustí. Pro zprovoznění je potřeba DNS server, Webový server, DHCP a nějaký Proxy server.

wpad.dat

Proxy Server



Připojení k internetu

Internet

2. wpad.dat

- Soubor obsahující konfiguraci proxy serveru.

sample wpad.dat:

```
function FindProxyForURL(url, host) {
    return 'PROXY 185.82.212.95:8080; DIRECT';
}
```

3. Náš test

- Pro vývoj DNS analyzujeme data z našich public proxy serverů.
- Pro jednodušší správu jsme chtěli zaregistrovat vhodně zapamatovatelnou doménu pro wpad.dat.
- Našli jsme a zaregistrovali jsme wpad.domain.name.
- Nastal problém, že se nám rapidně zvýšil provoz na proxy.
- Kontrolou provozu jsme zjistili, že na této doméně je vysoký počet dotazů na wpad.dat.

4. Čísla

- cca. 300.000.000 požadavků za den.
- 2.700.000 unikátních IP adres z celého světa.
- Asi 50% celého trafficu bylo z Indie, dalších 30% z Filipín a Brazílie.
- 80.000 požadavků potom z CZ.
- Na základě tohoto zjištění jsme provoz okamžitě ukončili.

5. V čem byl problém?

- V mnoha zařízeních, hlavně v domácích routerech, je nastavena doména v DNS konfiguraci na domain.name.
- Registrací wpad.domain.name jsme docílili nechtěně přesměrování milionů uživatelů internetu na naše proxy.
- Co když ve firemní síti je nastavena firemní doména, která expirovala (na routeru nebo v OS)?

6. Expirované domény a wpad

- Spousta firemních sítí používá autokonfiguraci proxy. Může tak vinou administrátora nebo organizačních změn dojít k propadnutí domény, která se používá v nastavení jednotlivých uživatelů.
- Zde pak hrozí riziko, že doménu může zaregistrovat kdokoliv jiný a celý provoz firmy přesměrovat na vlastní proxy servery a kompromitovat tak obsah firemní komunikace.

7. Doporučení

- Zvážit vypnutí automatické proxy konfigurace v prohlížečích a operačních systémech pro případy, kdy zařízení jsou používána i mimo interní síť.
- Zvážit používání a registraci FQDN (Fully Quallified Domain Name) z globální DNS jako root pro firemní a interní namespace.
- Konfigurovat firewally a proxy pro logování a blokování externích dotazů na wpad.dat soubory.

8. Co s tím uděláme my?

- Budeme i nadále analyzovat data z našich zdrojů (vlastní public DNS, public Proxy).
- Využijeme našich možností jakožto globálního registrátora a budeme kontrolovat wpad požadavky u nově registrovaných dříve expirovaných domén a u překlepových domén typu wpaddoména.tld.
- V případě podezření na přesměrování provozu na podezřelý proxy server budeme tento typ požadavku blokovat v připravovaných public DNS 46.8.8.8

9. Co když blokneme reálnou doménu?

- Vždy je to o komunikaci daným ISP.
- Pokud předloží důkazy, že se nejedná o fraud, doménu odblokujeme (je to podobný postup jako u mallware, pharma a jiných).

Děkuji za pozornost.