Doménbiztonság és adatvédelem online workshop

Amikor doménünk felett más szerezheti meg a hatalmat

Dravecz Tibor, INTEGRITY Kft.

2020. október 15.

Az Internet infrastruktúra három fundamentális eleme:

Border Gateway Protocol (BGP)

routing információ kicserélését segíti az Interneten

Domain Name System (DNS)

hierarchikus, decentralizált adatbázis és címtár Internetre kapcsolódó számítógépek, szolgáltatás, erőforrások, és felhasználók számára

Network Time Protocol (NTP)

Internet hosztok időszinkronizációját biztosítja

"The *Domain Name Server*[1] (DNS) is the Achilles heel of the Web. The important thing is that it's managed responsibly."
Tim Berners-Lee

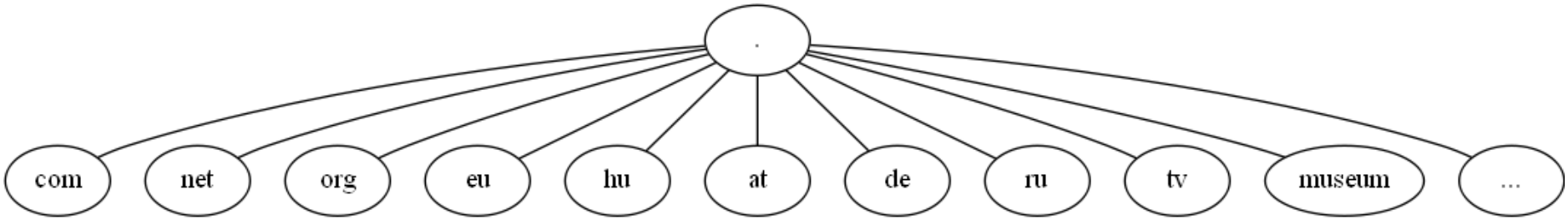
"There is nothing worse than a sharp image of a fuzzy concept."

Ansel Adams,

but, we have a fuzzy image of a fuzzy concept.

[1] Sic!

Felső szintű domainek (top level domains /TLDs/)



generic TLD (gTLD) (com, net, org, info, biz, bank, shop stb.)

sponsored TLD (sTLD) (asia, coop, jobs, museum, tel, travel stb.)

country code TLD (ccTLD)

speciális TLD-k (infratruktúra /.arpa/ és ICANN teszt TLD-k)

genericTLD státuszú ccTLD-k (.co, .nu, .tk, .tv stb.)

gTLD jellegű vagy ilyenként előszeretettel használt ccTLD (.io, de akár .is, .it stb.)

a kettő közötti átmenet (pl. .cn)

nemzeti jellegű ccTLD-k (.hu, .at, .ca, .de, .fr, .in, .jp, .ro, .ru, .uk, .us, .tw stb. és a .eu)

.com .net .org .edu .gov .int .mil

.arpa .テスト .परीक्षा

.eu (.ею, .ευ)

.hu (co.hu info.hu tm.hu gov.hu)

.at .hr .ro .rs (.срб) .si .sk .ua

.cz .ch .de .es .fr .nl .pl .uk (co.uk)

.cn .in .ru (.рф, .su) .us

.is .it

.io .tv .co .ml .mx .nu .tk

.info .biz .name

.bike . blackfriday .email .icu .mobi .porn .pub .shop

.aero .asia .coop .jobs .museum .puntcat .tel .travel .xxx

.bank .security .protection

.azure .google .symantec .toyota .budapest .london .москва .tirol

---

https://www.iana.org/domains/root/db 1616 top level domains (2020-10-10)

TLD-nként (különösen ccTLD-nként) többé-kevésbé eltérő lehet bármi, így

- **más domainregisztrációs szabályozás,**
- **más domainregisztrációs rend (policy),**
- **más regisztrátori rendszer, más regisztrátorok,**
- **más díjazás,**
- **más biztonsági rend (policy),**
- **más üzemeltetés, menedzsment (registry szinten),**
- **más környezet,**
- **más jogi szabályozás,**
- **más vitarendezési lehetőségek, eljárások,**
- **más felhasználás, más szokások, eltérő előzmények, különböző trendek,**
- **más és eltérő kockázatok.**

Bár a TLD-k jó része ún. ICANN-típusú regisztrációt alkalmaz vagy jórészt ennek mintáját követi.

Jó és rossz TLD-k

- Milyen szempontból jók és rosszak az egyes TLD-k?
  - Gyanúsként vagy rosszként kezelik domainünket?
  - Adott biztonsági kozkázatai lehetnek egy bizonyos TLD-nek.
  - Más az értéke, presztizse (legmagasabb: com).
  - Miért akarunk domaint regisztrálni, illetve használni az adott TLD alatt?

TLD-nként eltérő és más jellegű a

- kockázat
- biztonság
  - másfélék lehetnek sérülékenységek, eltérő veszélyek
- jogbiztonság
- adminisztráció (igénylés, fenntartás)

Amikor doménünk felett más szerezheti meg a hatalmat

The 10 Most Abused Top Level Domains

As of 11 October 2020 the TLDs with the worst reputations for spam operations are:

1	.fit	Badness Index: 5.32	Domains seen: 8,291 Bad domains: 5,164 (62.3%)
2	.viajes	Badness Index: 3.62	Domains seen: 138 Bad domains: 107 (77.5%)
3	.webcam	Badness Index: 3.14	Domains seen: 122 Bad domains: 86 (70.5%)
4	.fail	Badness Index: 2.98	Domains seen: 411 Bad domains: 226 (55.0%)
5	.tk	Badness Index: 2.91	Domains seen: 34,651 Bad domains: 10,844 (31.3%)
6	.cf	Badness Index: 2.81	Domains seen: 12,773 Bad domains: 4,285 (33.5%)
7	.email	Badness Index: 2.77	Domains seen: 13,439 Bad domains: 4,433 (33.0%)
8	.work	Badness Index: 2.76	Domains seen: 58,322 Bad domains: 16,560 (28.4%)
9	.loan	Badness Index: 2.74	Domains seen: 462 Bad domains: 232 (50.2%)
10	.rest	Badness Index: 2.65	Domains seen: 3,799 Bad domains: 1,393 (36.7%)

The 10 Worst Botnet Countries

As of 10 October 2020 the world's worst botnet infected countries are:

1	Egypt	Number of Bots: 1614017
2	China	Number of Bots: 1529910
3	India	Number of Bots: 1186445
4	United States of America	Number of Bots: 968418
5	Viet Nam	Number of Bots: 649158
6	United Kingdom of Great Britain and Northern Ireland	Number of Bots: 443978
7	Iran (Islamic Republic of)	Number of Bots: 395217
8	Brazil	Number of Bots: 384190
9	Indonesia	Number of Bots: 304520
10	Thailand	Number of Bots: 284082

Spamhaus

com = 3.9% bad (score 0.48)
net = 8.3% bad (score 0.86)
org = 1.9% bad (score 0.15)

arpa = 0.0% bad (score 0.00)
edu = 0.0% bad (score 0.00)
mil = 0.0% bad (score 0.00)
gov = 0.2% bad (score 0.00)
int = 2.4% bad (score 0.00)

info = 5.6% bad (score 0.48)
biz = 15.6% bad (score 1.29)

shop = 3.1% bad (score 0.20)
icu = 8.9% bad (score 0.80)
top = 27.8% bad (score 2.54)
email = 33.0% bad (score 2.77)
fit = 62.3% bad (score 5.32)

bank = 0.0% bad (score 0.00)
security = 0.0% bad (score 0.00)
coop = 0.1% bad (score 0.00)

hu = 0.1% bad (score 0.00)
eu = 3.3% bad (score 0.23)

kp = 0.0% bad (score 0.00)
eg = 0.0% bad (score 0.00) (No.1 *)
ch = 0.1% bad (score 0.00)
cz = 0.1% bad (score 0.00)
sk = 0.2% bad (score 0.00)
si = 0.2% bad (score 0.00)
se = 0.2% bad (score 0.01)
rs = 0.3% bad (score 0.00)
at = 0.3% bad (score 0.01)
es = 0.3% bad (score 0.01)
de = 0.3% bad (score 0.02)
vn = 0.4% bad (score 0.01) (No.5 *)
tw = 0.5% bad (score 0.02)
kr = 0.7% bad (score 0.03)
fr = 0.9% bad (score 0.06)
be = 1.2% bad (score 0.07)
nl = 1.5% bad (score 0.11)
ro = 0.5% bad (score 0.02)
uk = 0.5% bad (score 0.04)
pl = 0.9% bad (score 0.05)
in = 2.2% bad (score 0.16)
jp = 3.5% bad (score 0.23)
ru = 3.8% bad (score 0.33)
cn = 18.0% bad (score 2.09)
us = 20.1% bad (score 1.83)

cf = 33.5% bad (score 2.81)
tk = 31.3% bad (score 2.91)
ml = 27.5% bad (score 2.35)
fm = 7.4% bad (score 0.23)
cc = 3.7% bad (score 0.24)
co = 1.7% bad (score 0.12)
tv = 0.8% bad (score 0.03)
io = 0.6% bad (score 0.03)
nu = 0.5% bad (score 0.01)
mx = 0.4% bad (score 0.01)

Spamhous badness score:

$$\left(\frac{D_b}{D_t}\right) \log(D_b)$$

where

- D_b is the number of bad domains detected
- D_t is the number of active domains observed

https://www.spamhaus.org/statistics/tlds/

* Worst Botnet Country

Fontos szolgáltatások vagy önmagában is értékes nevek

nem értékes domének:	**minek-kell-nekem-ez-a-domain.com** **veletlenul-regisztraltam-magamnak.eu** **semmi-ertelme-nincs-1234567890.hu**	**árvíztűrőütvefúrógép.hu**
értékes domének, melyek azonban nincsenek 'éles' használatban:	**Még nem elindult cég, szolgáltatás, termék neve, melyben azonban nagy potenciál, illetve érték van; fontos védjegy, de aktívan domainként éppen nem használt.** **Jól hangzó általános név, vagy pl. egy kétbetűs string, mely értékes a domaintulajdonosnak, de éppen nincs használatba.**	
értékes szolgáltatások (már emiatt is értékes a maga domain is):	**Fontos szolgáltató cégneve; jelentős szolgáltatás; fontos portál stb.**	**police.hu, katasztrofavedelem.hu otp.hu, cib.hu, aegon.hu, google.hu, index.hu, nic.hu, eon.hu, bookline.hu, libri.hu, mol.hu, atomeromu.hu, visa.hu, ibm.com, amazon.com, visa.com, eurid.eu, wikipedia.org, nytimes.com, facebook.com**

Kockázat, sérülékenység

ICANN

Nyilvántartók (Registries) (pl. com: VERISIGN, hu: ISZT Nonprofit Kft., eu: Eurid)

Regisztrátorok (Registrars)

Közvetítők (Resellers)

Domainigénylők/használók (Registrants)

Tényleges domainhasználók[2] + harmadik felek (pl. felhasználók)

Más szereplők:

- **Authoritatív DNS-szolgáltatók**
  - **felsőbb szintű DNS-szolgáltatók (hu: ISZT Nonprofig Kft. + CDNS és Rcodezero)**
- Távközlési szolgáltatók, hálózatüzemeltetők
- Hoszting szolgáltatók
- Más szolgáltatók (tűzfal, IDS, DDoS védelem, monitoring stb.)
- További szereplők: tanácsadók, auditorok stb.
- Hatóságok, bíróságok, jogalkotás.

[2] akik konkrétan saját célra használnak adott domaint

DNS biztonság

Authoritatív DNS és DNS-feloldás:

authoritatív és resolver (rekurzív) DNS szerverek

Jelen esetben csak az authoritatív DNS szolgáltatás és a domain biztonság kérdésével foglalkozunk!

DNS	Domain
1. Root DNS zóna ('.') 1.1. TLD zóna (pl. hu.) 1.1.1. domain zóna (pl. domen.hu) 1.1.1.1. zónaadatok (esetleg delegált zónák) (pl. A, MX, CNAME, TXT stb. rekordok)	1.) ICANN 2.) Registry 3.) Regisztrátor 4.) Közvetítő (opc.) 5.) Tulajdonos

Domain portfolió

Kockázat értékelés	Mit ér meg nekünk egy domain biztonsága?
Kockázat kezelés	Ignoráltuk a kockázatot.
Domain portfolio management	Kinek van ilyen?
Szervezeti szabályozás	Domainnevek ebből kimaradtak.
Személyi felelősségek	nem hosszabbított domain nevek névszerver nem hosszabbított domainneve
Üzletfolytossági terv (BCP) **Katasztrófaterv (DRP)**	minden működik, csak éppen semmi
Contingency Planning	Mit kezdjünk most ezzel?
Biztonsági tervezés, biztonsági politika	Hallotunk már a DNS spoofingról meg az DNS amplifikációs támadásról is. De erről még nem. - Erre nem gondoltunk. Ezt is védeni kellett volna?
Dokumentáció	Fogalmunk sincs ki a felelős, honnan tudjuk?
Monitorozás, riasztások	Valami baj van, de nem tudunk róla. Rendszerünk észleli, de nincs intézkedés.
Ellenőrzés, audit	Erre nem is gondoltunk! Ezzel nem számoltunk! Ez nem úgy van, ahogy kéne!

Domain és DNS biztonsági szolgáltatások

Kik nyújtják:

- nyilvántartók (Registries) (pl. hu: ISZT Nonprofit Kft., eu: Eurid)
  - pl. Registry Lock, Whois
- regisztrátorok (Registrars)
  - pl. Registrar Lock, MFA stb.
- közvetítők (opcionális)
- DNS üzemeltetők (adott DNS hierarchia szintjén)
  - pl. DNSSEC, Anycast DNS, MFA stb.
- és más kapcsolódó szolgáltatások és szolgáltatók (részben opcionálisok, pl. fejlesztés, rendszermérnöki szolgáltatások, tanácsadás, oktatás, audit stb.)

Registry Lock és Registrar Lock

Registrar Lock - bizonyos nem kívánt műveletek ellen véd

Domain Status: **clientDeleteProhibited** https://icann.org/epp#clientDeleteProhibited
Domain Status: **clientTransferProhibited** https://icann.org/epp#clientTransferProhibited
Domain Status: **clientUpdateProhibited** https://icann.org/epp#clientUpdateProhibited

Registry Lock - bizonyos nem kívánt műveletek ellen véd

Domain Status: **serverDeleteProhibited** https://icann.org/epp#serverDeleteProhibited
Domain Status: **serverTransferProhibited** https://icann.org/epp#serverTransferProhibited
Domain Status: **serverUpdateProhibited** https://icann.org/epp#serverUpdateProhibited

Registrar Lock - regisztrátor szintjén véd, illetve regisztrátor váltás ellen is védhet

Registry Lock - regisztrátor szintje felett implementált védelem

Részleges és teljes zárolás ('zár', 'lock')

Példa: **teljes** registry lock: **.HU domainzár**
részleges registry lock: (ún. 1F, illetve 2F, azaz **1-, illetve 2-faktoros**) **megerősítéses eljárás** a .HU regisztrációs rendszerben

Kapcsolattartók és jóváhagyók

- **értesítési kontaktok**
- **jogosultak (változás jóváhagyók)**

Értesítéseket és riasztásokat a **lehető legszélesebb kör** kapja!
Jellemzően csoportcímek alkalmazandók.

Változást csak a **lehető legszűkebb kör** kezdeményezhessen és hagyhasson jóvá

- ugyanakkor mindig biztosítani kell, hogy szükséges változást végre lehessen hajtani.

Változtatásra jogosult személyek, accountok és adataik (pl. email cím, telefonszám) szenzitív adatok, szigorúan titkosan kellene ezen adatokat kezelni! (Whoisban nem jelenhetnének meg!)

Tervezetlenség, szabályozatlanság, dokumentálatlanság, ellenőrzés, belső felügyelet, és audit hiánya

'Set and forget' domain regisztráció és fenntartás

'Set and forget' DNS üzemtetés

Nem kielégítő, nem biztonságos, nem megbízható névszerver-szolgáltatás

Registry Lock nem előfizetett

DNSSEC nem alkalmazott

DKIM, DMARC, … **és még sok más fontos és hasznos dolog nem alkalmazott (vagy nem jól implementált)**

A kisebb és a nagyobb baj (kár)

Nem kívánt (csalárd) tulajdonos átírás

versus

nem kívánt (csalárd) authoritatív névszerver-módosítás

és ami többek közt erre vezethet:
a nem kívánt (csalárd) regisztrátorváltás


3

Robin Hood 'igazságot' tesz

Robin Hood nagyon megharagudott a …Shop webáruházra,

- nem akarja kirabolni, csak meg akarja büntetni.

Elhatározta (D)DOS támadást zúdít a webáruházra,

- azonban látja, hogy magát a webáruházat nehéz hatásosan letámadni.

Látja azonban, hogy a …Shop névszervereit érdemes lehet DDOS-olni[4]:

Name	Type	TTL	Section	NameHost
…shop.hu	NS	600	Answer	ns.xxxshop.hu
…shop.hu	NS	600	Answer	secondary.szolgaltato.hu

[3] https://upload.wikimedia.org/wikipedia/commons/c/c8/Robin_shoots_with_sir_Guy_by_Louis_Rhead_1912.png
[4] DNSSEC nincs, de most csupán DDoS a cél, most erre ne gyúrjunk, mondja Robin magában.

Csak két névszerver van (anycast nem alkalmazott).
Miért is 600 a TTL az NS rekordnál?
Miért is BIND 4-es az első névszerver? (És miből gondolhatom ezt?)

- A lényeg, hogy ez infók talán még jól jönnek. És még pár további ígéretes dologra felfigyel Robin, az előbbieknél fontosabbakra is.

Előzetes tesztek szerint a hosztok elérése igen jó, gyorsak a válaszidők, de a primary talán különösen érzékeny lehet a DoS támadásra, de a secondary is remény szerint lebéníthatónak tűnik a hálózatának elárasztásával,

- igaz, ezzel nem csak az …Shop, hanem a (névszerver, hoszting stb.) szolgáltatójának és ügyfeleinek is odavágunk (járulékos veszteség, mi több Robin úgy gondolja, hogy megérdemli a büntetést a szolgáltató is).

Sobri Jóska nem Robin Hood, Ő rabolni akar!

(Az Előadó szárnypróbálgatása, mint krimiíró.)

https://upload.wikimedia.org/wikipedia/commons/c/c9/Sobri_J%C3%B3ska_igazi.png

Sobri Jóska nem egy képzett hacker, nemrég szabadult, csak szabadulása előtt tanulta meg a net alapjait a börtönben.

Ezért nem akar valami csavaros támadást, úgy gondolja, hogy egyszerűen csak lenyúlja a TotálBank domainjét, a TOTALBANK.HU-t, és ezen akció után akár nyugdíjba is mehet.

Annyi esze van, hogy ha magának vagy másnak átíratná, akkor ezzel biztos túl gyorsan lebukna, ezért CSAK REGISZTRÁTORVÁLTÁST tervez, Magyar TotálBank Nyrt. nevén hagyja a totalbank.hu-t, de az új regisztrátornál már Ő fog rendelkezni a DOMAIN AUTHORITATÍV NÉVSZERVEREI felett.

Látja Sobri, hogy DNSSEC sincs, de az egyszerűbb útra tesz, elsőre regisztrátorváltással kíván próbálkozni.

A regisztrátorváltás sikere nem reménytelen (okirathamisításban és social engineeringben bízik), szerencsére REGISTRY LOCK nincs a domainhez beállítva.

Mindazonáltal a TOTALBANK.HU domain felett, ha átveszi egy időre hatalmat, akkor noha sok felhasználó belépési adatait meg tudja szerezni, ez még nem elég pénzlenyúláshoz.

De hát ott vannak a bank ügyfelei, akik sokan olyan 2FA eljárást alkalmaznak, melyben az egyik faktor (az ügyfelek jó részénél) telefonszám alapú.

Jóska kigondolja, hogy a bank sok ügyfelének telefonszámát meg kellene előre szerezni, méghozzá éppen megfelelő időpontra

- akkor, amikor a TOTALBANK.HU domain felett át tudja venni a hatalmat. Persze ismeri a SIM kártyás trükköt, de ez félő egyre kevésbé lesz használható, hát kigondol mást (itt nem írjuk le mit :-)

Előkészületek

A támadó okosan nem írja más nevére a domainnevet;

- **regisztrátorváltás?**
- **vagy csak a megfelelő account megszerzése?**

A támadó közvetlen anyagi hasznot, ezen felül információt (személyes és üzleti adatokat) is kíván szerezni.

A támadó több szinten is támadást szervez.

D-nap, H-óra **Támadás indul! - Minden terv szerint, pontos időzítéssel.**

Mennyi idő alatt észleli a TotálBank a támadást, milyen reakcióidővel képes válaszolni?

Ha a regisztrátorváltást Sobri Jóska sikeresen végrehajtja,

- akkor a TotálBank **már mindenképpen veszteséget** szenved el,
  - a kérdés, hogy gyors és megfelelő reakciójában **mennyire tudja ezt enyhíteni**, mit tud maga megoldani, mit segíthetnek neki szolgáltatói, többekközt:
    - volt regisztrátora már jobbára semmit,
    - új regisztrátora és a domain nyilvántartó szervezet,
    - Internet hozzáférés-szolgáltatók … , hatóságok, …

    mit, hogyan és milyen gyorsan tudnak segíteni.

További károk H+N óra múltán.

"The horrific damage of 9/11 did not end when those buildings came down." - Kirsten Gillibrand

Ajánlott olvasmányok

https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

https://blog.talosintelligence.com/2019/04/seaturtle.html

https://krebsonsecurity.com/2020/03/phish-of-godaddy-employee-jeopardized-escrow-com-among-others/

https://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf