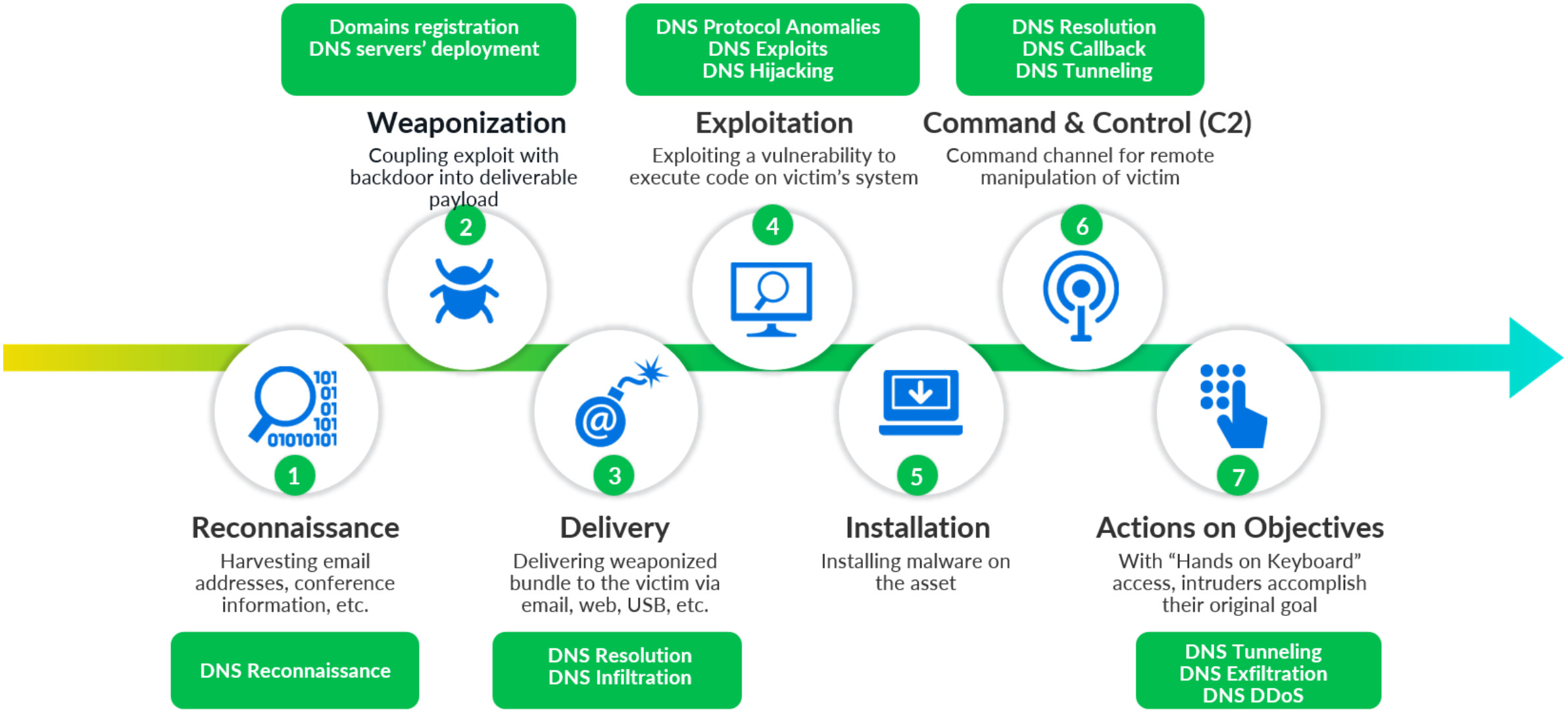
Verticum Networks

DNS – Veszélyforrás vagy védekezési lehetőség?

Hankó Péter – hanko.peter@verticum.net

Hogyan élnek vissza a DNS protokollal?



C2 kommunikáció DNS tunnelinggel

- **Hamis biztonságérzet**

  Zártnak gondolt zónából is lehetséges internet irányú adatforgalom

- **Kétirányú kommunikáció**

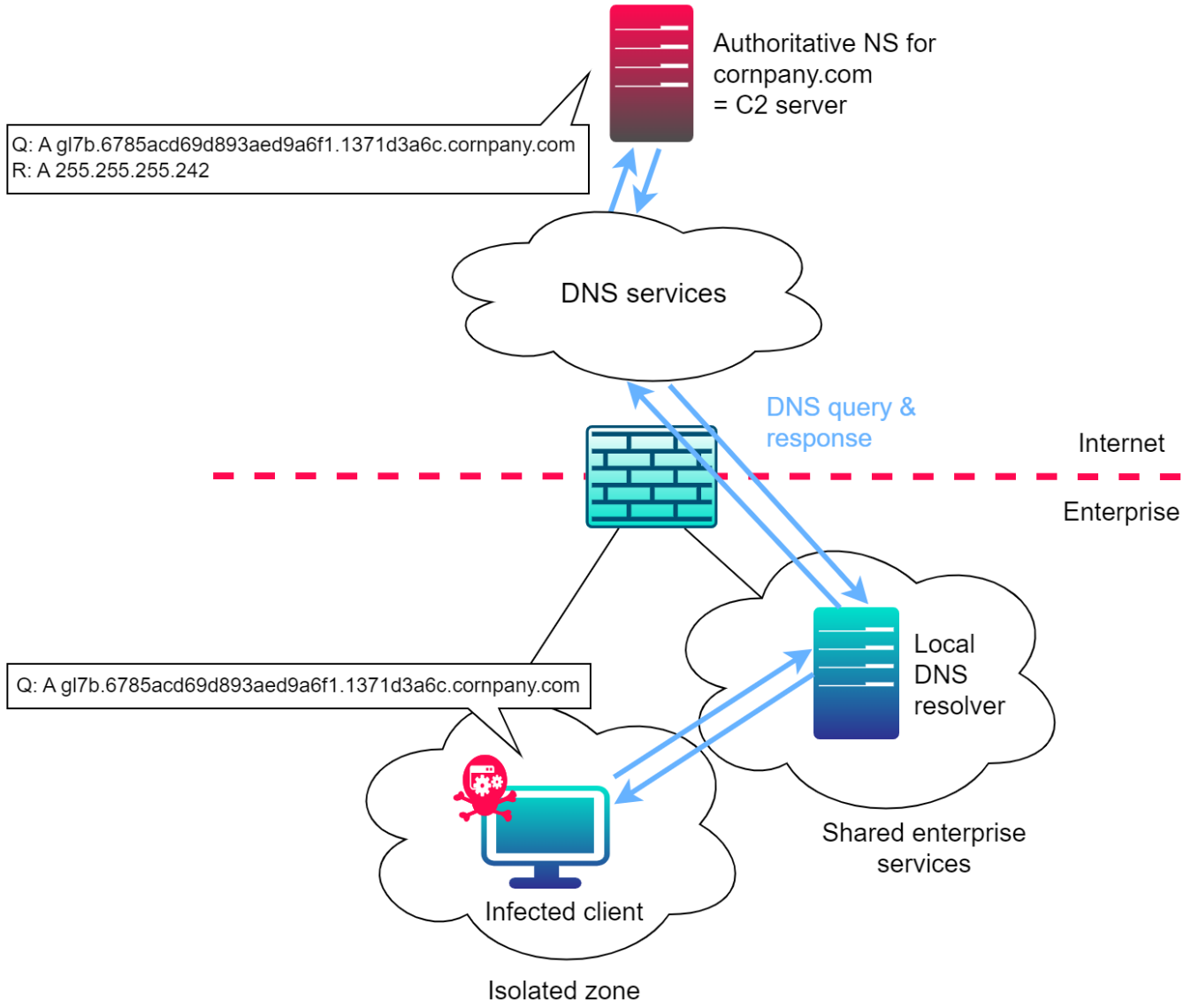
  Data exfiltration
  Data infiltration

- **Gyakran használt rekordok**

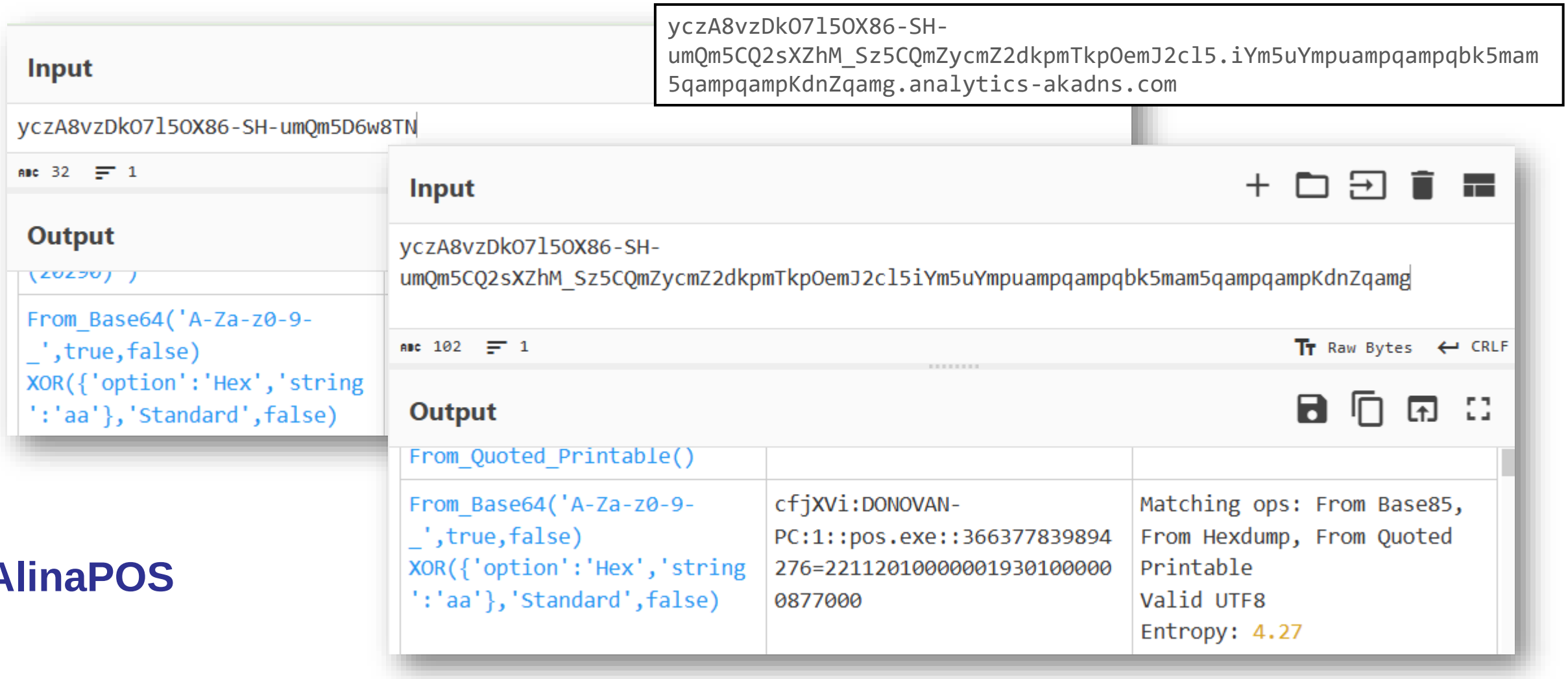
  A, AAAA, TXT,
  NULL, CNAME, MX, SOA*, NS

```
dig +short owa365.bid SOA
ns13.value-domain.com. hostmaster.owa365.bid.
1579278658 16384 2048 1048576 2560

ping 1579278658
Pinging 94.33.225.66 with 32 bytes of data...
```



DNS exfiltration példa



AlinaPOS

https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-alina-pos-malware.pdf

Malware C2 over DNS jellegzetességek

- **PYSA / Mespinoza ransomware, Vermilion Strike**
  DNS TXT rekordok az elsődleges csatorna, ha nem megy, átáll HTTP-re
- **ALPHV BlackCat ransomware**
  Nagy adatforgalom: 7 nap alatt kb. 6 millió query, 1 GB adat kiszivárogtatása
- **FiveHands ransomware / SombRAT backdoor**
  A backdoor DNS tunnelen keresztül tölti le a futtatandó pluginokat a C2 szerverről.
- **Symbiote**
  Lopott belépési adatok továbbítása DNS queryknek álcázva. Berkeley Packet Filtert telepített – ha a gépen packet capture-t indítottak, a gyanús forgalmat kiszűrte a pcap-ből.
- **APT34 Saitama backdoor, Sunburst**
  Lassú, random késleltetésű csomagok, hiba esetén több órás szünet
- **InvisiMole**

```
aa8ydrh37klb4xaklklr4thm3aaaaaaaaaaara2gaaaaaaaaaaaaaaaagiaiaa.aaaaaaaaaaae.adstat.red
a8ym2np5fmbixcolmcy8eiyfiltgycolhltarbrvaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaae.wlsts.net
a8yyqstx4kbpf32grsnnfoslbltgf3egvbaar7ymaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaae.amz-eu401.com
a8yfdt2riibpf32grsnnfoslbltgf3egvbaar7ymaaaaaaaaaaaaaaaalaaiaa.aaaaaaaaaaae.update.xn--6frz82g
```

DGA – Domain Generation Algorithm

- A botok nem fixen bedrótozott IP címen vagy domainnéven veszik fel a kapcsolatot a C2 központtal.
- Domainnevek legyártása algoritmussal, majd a bot addig próbálkozik, míg az első válaszolót meg nem találja.
- Domainnév generálása időbélyeg alapján: adott név használata adott időablakban.
- Dictionary DGA: a felhasználandó domainnevek előállítása szótárból.

Dictionary 1:		**Dictionary 2:**		**Suppobox malware domains:**
face		gone		facegone.net
walk		road		walkroad.net
weak		dont		sellfool.net
sell	+	fool	→	weakheat.net
deep		heat		deepaunt.net
ball		aunt		facethey.net.
push		they		pushaunt.net
both		lift		walklift.net
		goes		facegoes.net

DGA domainek: mennyi lehet belőlük?

Bamital 197,000 | 1	Fobber 2,000 | 2	Mewsei 1,984 | 1	Pykspa 2 775,342 | 2	Simda 11,528 | 12
Banjori 421,390 | 30	Geodo 90,232 | 2	Murofet 1 4,063,680 | 2	QakBot 385,000 | 1	Suppobox 98,304 | 3
Bedep 3,806 | 4	Gameover DGA 6,182,000 | 2	Murofet 2 262,000 | 1	Ramdo 3000 | 3	Szribi 2,949 | 1
Conficker 125,118,625 | 3	Gameover P2P 262,000 | 1	Necurs 3,551,232 | 6	Ramnit 18,000 | 18	Tempedreve 204 | 1
CoreBot 18,160 | 2	Gozi 16,963 | 9	Nymaim 65,040 | 3	Ranbyus 64,400 | 7	TinyBanker 81,930 | 90
Cryptolocker 1,108,000 | 1	Hesperbot 178 | 3	Pushdo 124,021 | 4	Redyms 34 | 1	Torpig 17,610 | 2
DirCrypt 420 | 14	Kraken 300 | 1	Pushdo TID 6,000 | 1	Rovnix 10,000 | 1	UrlZone 10,009 | 6
Dyre 592,000 | 1	Matsnu 3,346 | 2	Pykspa 1 22,764 | 1	Shifu 1,554 | 2	VolatileCedar 170 | 1

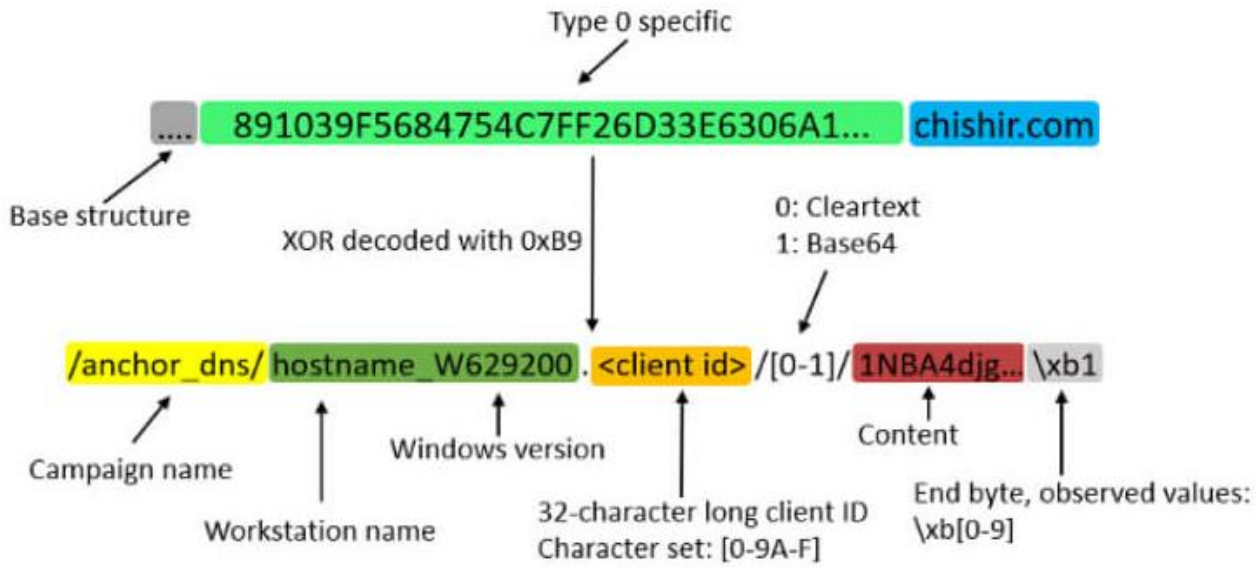
Sum of unique domains: 143,584,257 or 18,465,647 without Conficker

Daniel Plohmann: DGArchive – A Deep Dive into Domain Generating Malware (2015)
https://www.botconf.eu/wp-content/uploads/formidable/2/OK-P06-Plohmann-DGArchive.pdf

C2 over DNS detektálása – statikus eszközök

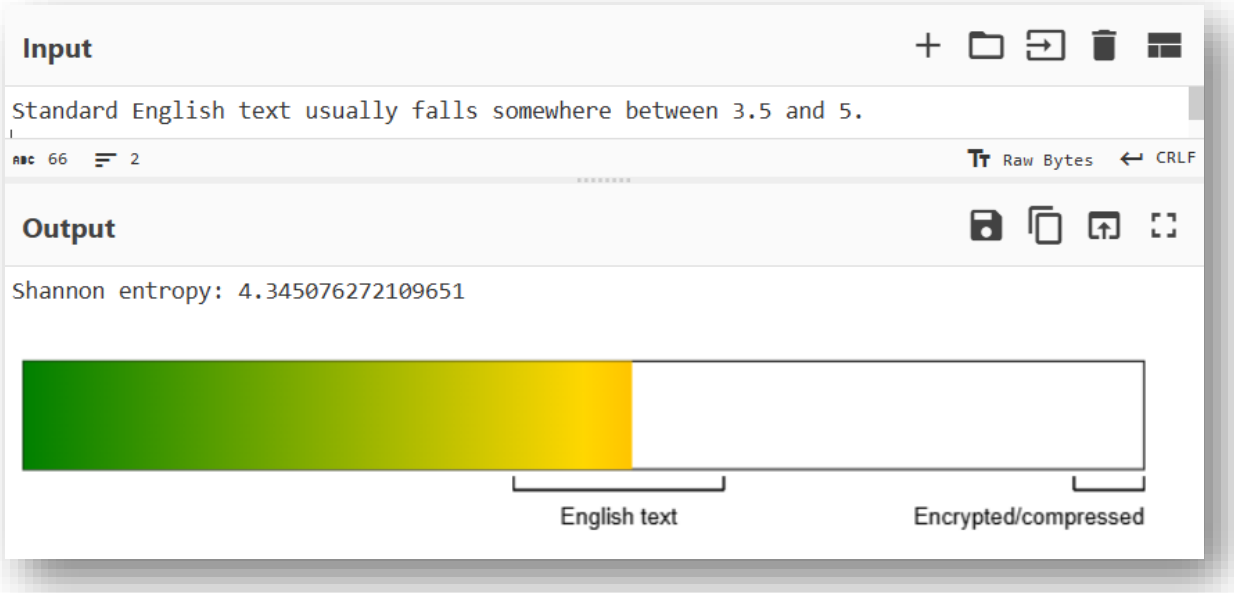
- **Reputációs listák**
  - Gyanús vagy rosszindulatú tevékenységhez kapcsolt domainnevek, illetve IP címek listái
  - Lookalike domainek
  - DNS szervereken Response Policy Zone (RPZ) formájában alkalmazható: a zónához, illetve annak rekordjaihoz akciót társítunk: allow, block (NXdomain, error), redirect
  - RPZ-k létrehozhatók lokálisan vagy letölthetők feedek formájában (zone transfer)

- **Szignatúrák**
  - IOC, illetve DNS payload mintázatok alapján történő szűrés



C2 over DNS detektálása – dinamikus eszközök

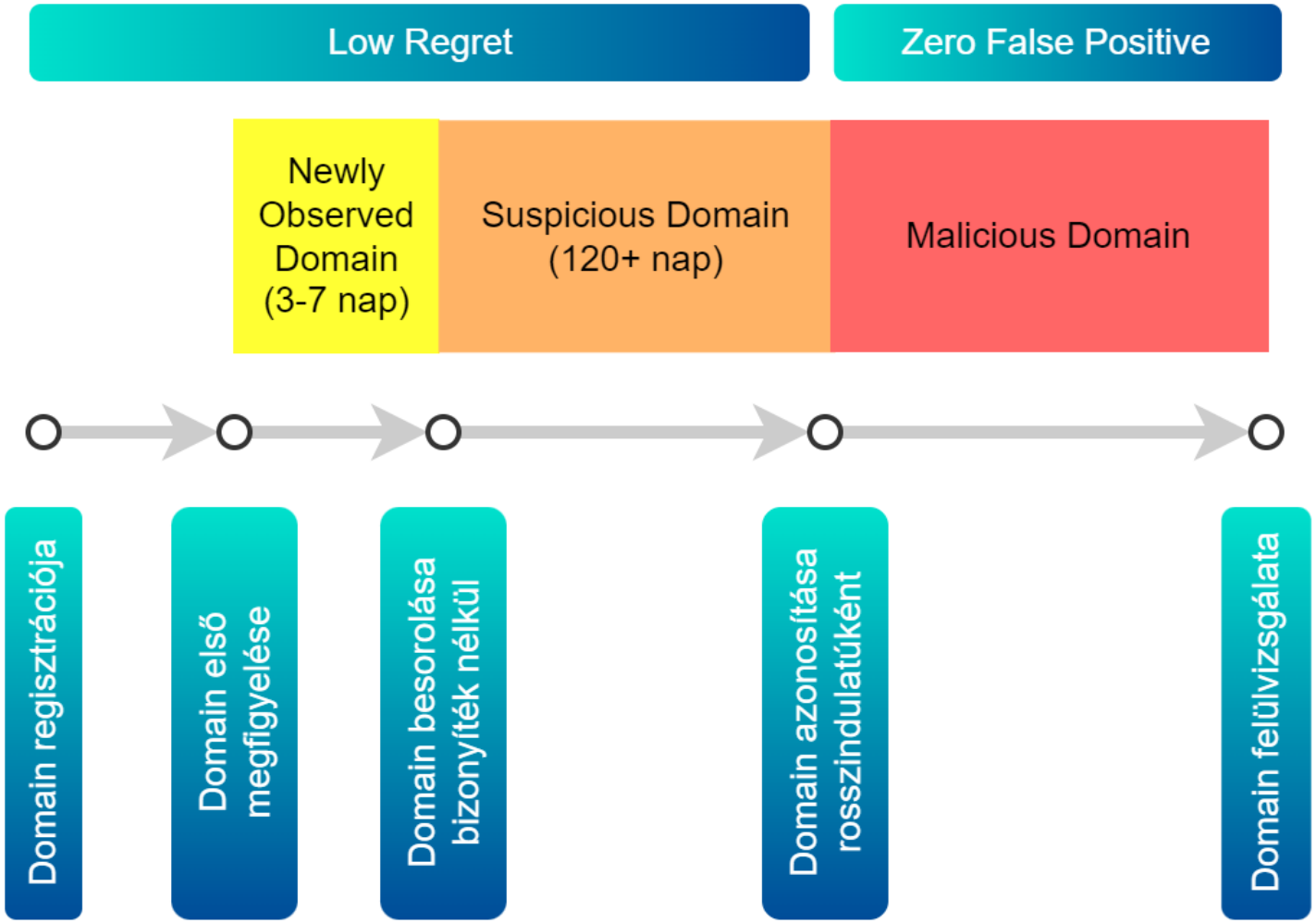
- **Lexikális analízis**
  - nem természetes nyelvi szótárakra épül, de azok jellegzetességeit keresi
  - betűk és egyéb karakterek (számok, jelek) aránya
  - HEX (a-f) karakterek aránya
  - magánhangzó-mássalhangzó arány
- **N-gram analízis**
  - 2-, 3-, 4-karakteres szekvenciák (2-, 3-, 4-gram) eloszlásának vizsgálata
- **Entrópia**
  - A magasabb érték nagyobb információtartalmat, egyúttal kisebb redundanciát jelent.
  - Magas érték kódolt tartalom, pl. DNS tunneling indikátora lehet.



C2 over DNS detektálása – dinamikus eszközök

- **Kumulatív entrópia**
  - a névfeloldási kérések és válaszok együttes entrópiájának számítása és statisztikája
- **Gyakoriság**
  - milyen gyakran mennek kérések ugyanattól a klienstől azonos domainre
  - milyen a kérések időbeli eloszlása
- **Méret**
  - a nagyobb payload méret nagyobb adatforgalmat jelent
- **Újdonságdetektálás**
  - cache-miss gyakorisága általában és kliensre lebontva
  - korábban elő nem forduló domainnév detektálása
- **AS számok szerinti eloszlás**
  - az AS számok mennyiségének megugrása malware tevékenységet jelezhet (pl. Fast Flux)

Domainek besorolási életciklusa



- Threat score
- Risk score
- Confidence score

https://github.com/JHUAPL/Low-Regret-Methodology/blob/main/README.md#introduction

Trendek

- Jelentős invesztíció a Threat Intelligence-be (erős teamek és technológiák)
- Piaci konszolidáció
- A Security SaaS szolgáltatásoknak köszönhetően sokkal több adat megy át a gyártók kezén
  - hatalmas bázis az adatbányászathoz, gépi tanuláshoz
  - pontosabban megismerik az ügyféligényeket
  - hatékonyabban tudják megtervezni a szoftverfejlesztést
- Mesterséges intelligencia

Verticum Networks

DNS Security Workshop

2024. november 13.

9:00–11:00

→ rendezveny@verticum.net
Verticum Networks Zrt.
1044 Budapest, Óradna utca 4.