



DNS v rukou útočníka. Reálné příklady použití tohoto protokolu v útoku

Jan Ryneš
Solutions Architect
Infoblox



DNS. Stejně jako kyslík, není
důležitý, dokud žádný nemáte



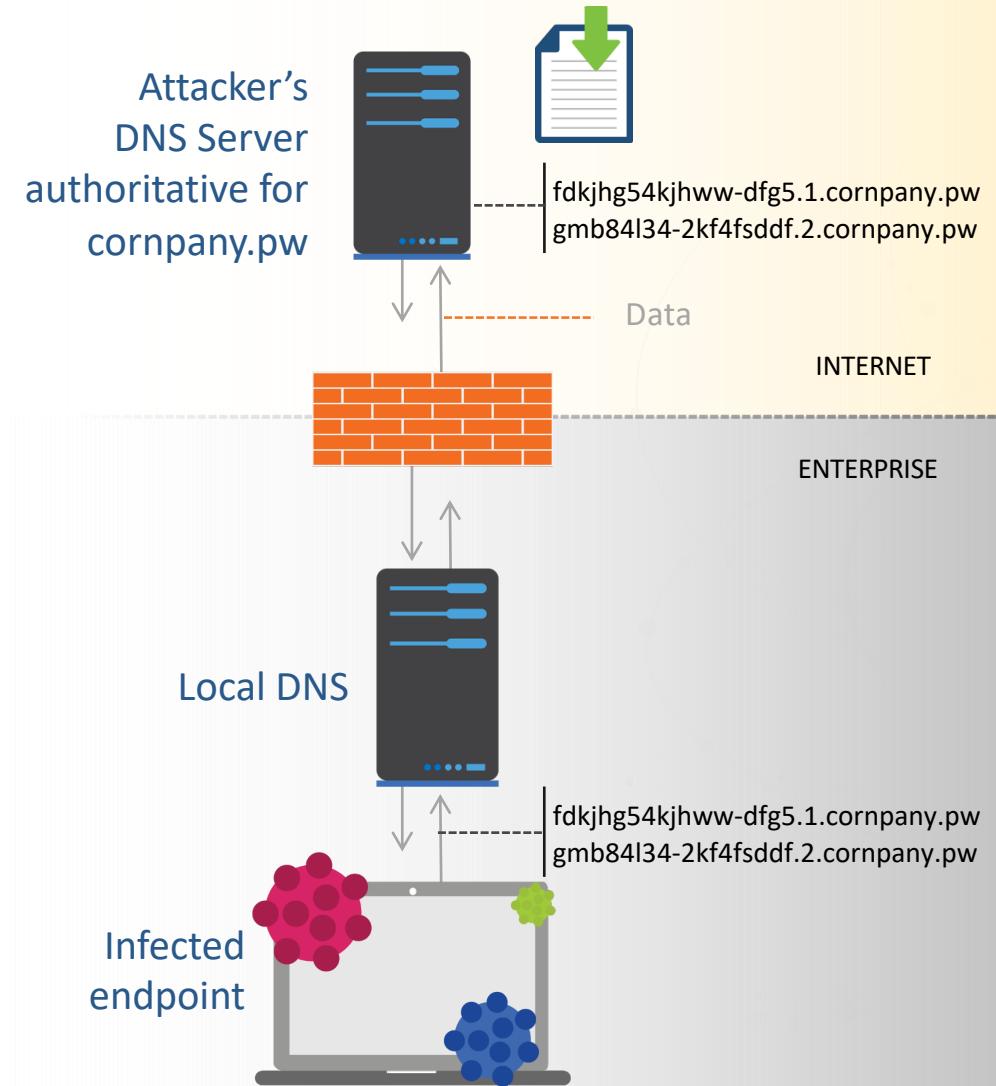
Jak Malware používá DNS?



DNS Jako transportní mechanizmus

Exfiltrace

- Útočník zaregistrouje doménu a nastaví autoritativní server DNS na internetu, aby fungoval jako koncový bod tunelu
- Data opouštějící vnitřní síť:
 - Šifrována veřejnými klíči
 - Překódována do a-z, 0-9, – a _ za použití algoritmů jako jsou
 - Hex, Base32, nebo modifikovaný Base64 (URL-Safe)
 - Rozdělena do částí až do 63 znaků (label limit)
 - Odeslána jako jednotlivé dotazy ve tvaru <část>.doména
- Dotazy mohou být odeslány přímo (pokud je dovoleno na firewall), skrze existující DNS server v síti nebo skrze Proxy (například ve tvaru http://<část>.doména)



AlinaPOS

- Point-of-Sale (POS) malware rodina

- Vzorek DNS dotazu:

yczA8vzDkO7I5OX86-SH-umQm5D6w8TN.analytics-akadns[.]com

yczA8vzDkO7I5OX86-SH-
umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYmp
uampqampqbk5mam5qampqampKdnZqamg.analytics-akadns[.]com

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



AlinaPOS

- Vzorek DNS dotazu:

yczA8vzDkO7I5OX86-SH-umQm5D6w8TN.analytics-akadns[.]com



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



AlinaPOS

- Vzorek DNS dotazu:

The screenshot shows a user interface for analyzing DNS queries. On the left, there's a sidebar titled "Recipe" with icons for save, folder, and delete. Below it, a section titled "From Base64" contains a dropdown menu for "Alphabet" set to "A-Za-z0-9-_". A list of options follows: "Standard (RFC 4648): A-Za-z0-9+/", "URL safe (RFC 4648 §5): A-Za-z0-9-_", "Filename safe: A-Za-z0-9+-", "itoa64: ./0-9A-Za-z=", "XML: A-Za-z0-9_.", and "v64: A-Za-z0-9_". On the right, the "Input" section shows the base64 string "yczA8vzDk07l50X86-SH-umQm5D6w8TN" with metrics "length: 32" and "lines: 1". The "Output" section shows the decoded string "ÉÌÀòüÃ. îåääüëä. úé... úÃÄÍ" with metrics "time: 1ms", "length: 24", and "lines: 1". There are also various icons for file operations like copy, paste, and refresh.

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



AlinaPOS

Recipe +

From Base64 (stop) II

Alphabet: A-Za-z0-9-_ ▼

Remove non-alphabet chars

XOR Brute Force (stop) II

Key length: 1 Sample length: 100

Sample offset: 0 Scheme: Standard

Null preserving Print key

Output as hex

Input length: 32
lines: 1 +

yczA8vzDk07l50X86-SH-umQm5D6w8TN

Output start: 5915 time: 3ms
end: 5948 length: 8924
length: 33 lines: 255 (stop) II

Key = a7: nkgU[d7IBCB[LC]N7<7]dcj
Key = a8: adhZTk8FMLMTCL/RA838Rkle
Key = a9: `ei[Uj9GLMLUBM.S@929Sjmd
Key = aa: cfjXVi:DONOVAN-PC:1:Ping
Key = ab: bgkYWh;EN0NW@0,QB;0;Qhof
Key = ac: e`l^Po<BIHIPGH+VE<7<Voha
Key = ad: dam_Qn=CHIHQFI*WD=6=Wni`
Key = ae: gbn\Rm>@KJKREJ)TG>5>TmjC
Key = af: fco]Sl?AJKJSDK(UF?4?Ulkb
Key = b0: y|pBLs ^UTUL[T7JY + Jst}
Key = b1: x}qCMr!_TUTMZU6KX!*!Kru|
Key = b2: {~r@Nq"\WVwNYV5H[")"Hqv.
Key = b3: z.sAOp#]VWVOXW4IZ#(#Ipw~
Key = b4: }xtFHw\$ZQPQH_P3N]\$/Nwpy
Key = b5: |yuGIV%[PQPI^Q20\%.%0vqx
Key = b6: .zvDJu&XSRSJ]R1L_&-&Lur{
Key = b7: ~{wEKt 'YRSRK\S0M^', 'Mtsz



AlinaPOS

- Vzorek DNS dotazu:
yczA8vzDkO7I5OX86-SH-
umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkpOemJ2cl5.iYm5uYm
puampqampqbk5mam5qampqampKdnZqamg.analytics-
akadns[.]com

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



Recipe



Input

length: 103
lines: 1



A
yczA8vzDk07l50X86-SH-
umQm5CQ2sXZhM_Sz5CQmZycmZ2dkpmTkp0emJ2c15.iYm5uYmpuampqampqbk5mam
5qampqampKdnZqamg

From Base64



Alphabet

A-Za-z0-9-_

Remove non-alphabet chars

XOR Brute Force



Key length
1

Sample length
100

Sample offset
0

Scheme
Standard

Null preserving Print key

Output as hex

Crib (known plaintext string)

Output

start: 14703 time: 10ms
end: 14789 length: 22184
length: 86 lines: 255



0033023222223;123222222:55222
Key = a9: `ei[Uj9GLMLUBM.S@9299s1p-
f{f99055044;0::7145>1122132333332:03233333;44333
Key = aa: cfjXVi:DONOVAN-
PC:1::pos.exe::366377839894276=22112010000019301000000877000
Key = ab:
bgkYWh;EN0NW@0,QB;0;;qnr/dyD;;277266928985367<33003101111108210
111111966111
Key = ac: e`l^Po<BIHIPGH+VE<7<<viu(c~c<<500511>5?>?
2410;44774676666667?567666666>11666
Key = ad: dam_Qn=CHIHQFI*WD=6==wht)b.b==411400?4>?
>3501:5566576777776>47677777?00777
Key = ae: gbn\Rm>@KJKREJ)TG>5>>tkw*a|a>>722733<7=
<=063296655645444445=745444444<33444
Key = af: fco]Sl?AJKJSDK(UF?4??ujv+'}`??633622=6=<
<172387744754555554<65455555=22555
Key = b0: y|pBLs ^UTUL[T7JY + jui4.b.),,)--")#"#.(-,'((++
(******#)******"-***
Key = b1: x}qCMr!_TUTMZU6KX!*!!kth5~c~!!(--(,,#("##/),-

Zdroj: [h](#)



DNS jako Transportní Mechanismus

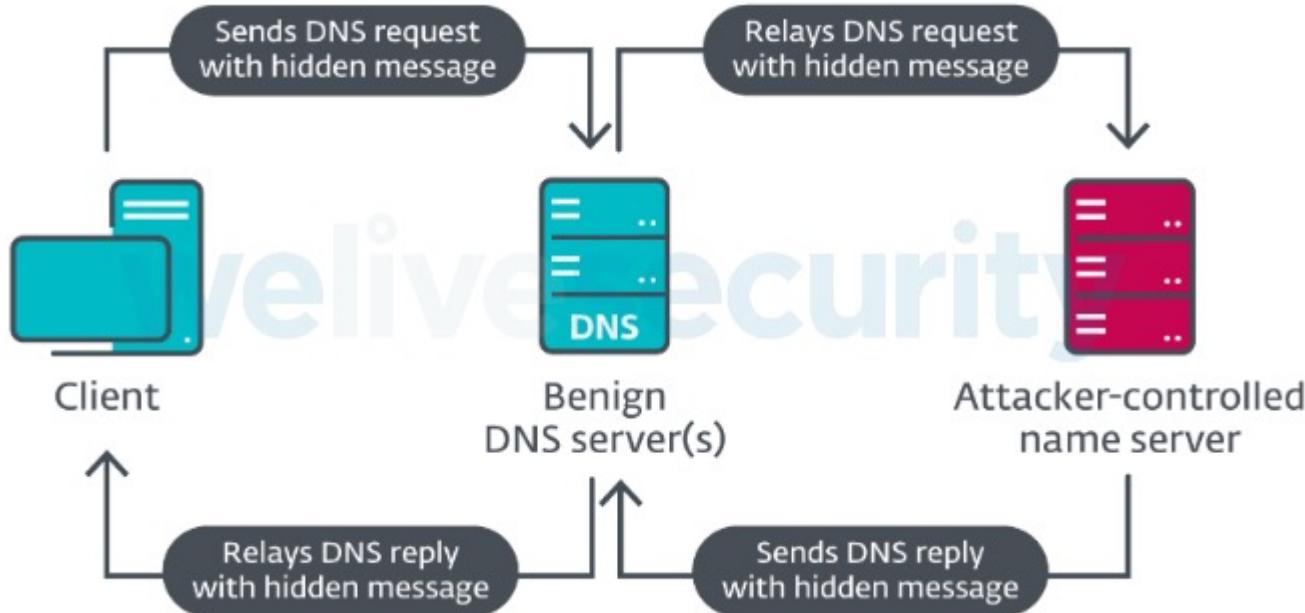
Infiltrace

- Funkce TCP lze napodobit zakódováním bloků dalšími daty, například kontrolním součtem a číslem paketu
- Data lze odeslat zpět v různých záznamech, např.
 - A - umožňuje 4 bytes (dostatek pro kód, např. 1.1.1.200 = resend packet 200)
 - AAAA - umožňuje 16 bytes
 - MX záznam : 2 bytes + domain name (255 bytes)
 - CNAME - dovoluje až do 110 bytes v Base32
 - TXT - umožňuje $N \times 220$ bytes v Base64 (až do RDATA limitu 64kB)
 - NULL - dovoluje až 256 bytes
- Pomocí TXT a NULL je přenos rychlejší, na úkor snazší detekce



InvisiMole

- cílené na malé množství vysoko postavených organizací vojenského sektoru a diplomatické mise ve východní Evropě
- Ke stahování (infiltrace) a spouštění nových škodlivých komponent bylo použito DNS
- Pomocí vlastního tunelovacího mechanismu a kódování base32 s vlastní abecedou [abcdefghijklmnopqrstuvwxyz123456789]
- Byly použity záznamy NULL a AAAA



a8ydrh37klb4xak1k1r4thm3aaaaaaaaaaaara2gaaaaaaaaaaaaagiaiaaa.aaaaaaaaaaaae.adstat[.]red
a8ym2np5fmbixcolmcy8eiylfiltgycolh1tarbrvaaaaaaaaaaaaalaaiaaa.aaaaaaaaaaaae.wlsts[.]net
a8yyqstx4kbpf32grsnnfoslbltgf3egvbaar7ymaaaaaaaaaaaaalaaiaaa.aaaaaaaaaaaae.amz-eu401[.]com
a8yfdt2riibpf32grsnnfoslbltgf3egvbaar7ymaaaaaaaaaaaaalaaiaaa.aaaaaaaaaaaae.update[.]xn--6frz82g
a8y3g5f2h2aaybyfplr4xcbaaaaaaaaaaaaahoraaaaaaaaaaaaagiaca.aaaaaaaaaaaae.153[.]re
a8yqykttelbixcolmcy8eiyfmcotvbolpcvarpy7aaaaaaaaaaaaalaaiaaa.aaaaaaaaaaaae.mx1[.]be

Entropy: 3.8 (or 4.3 w/o 16* „a”)



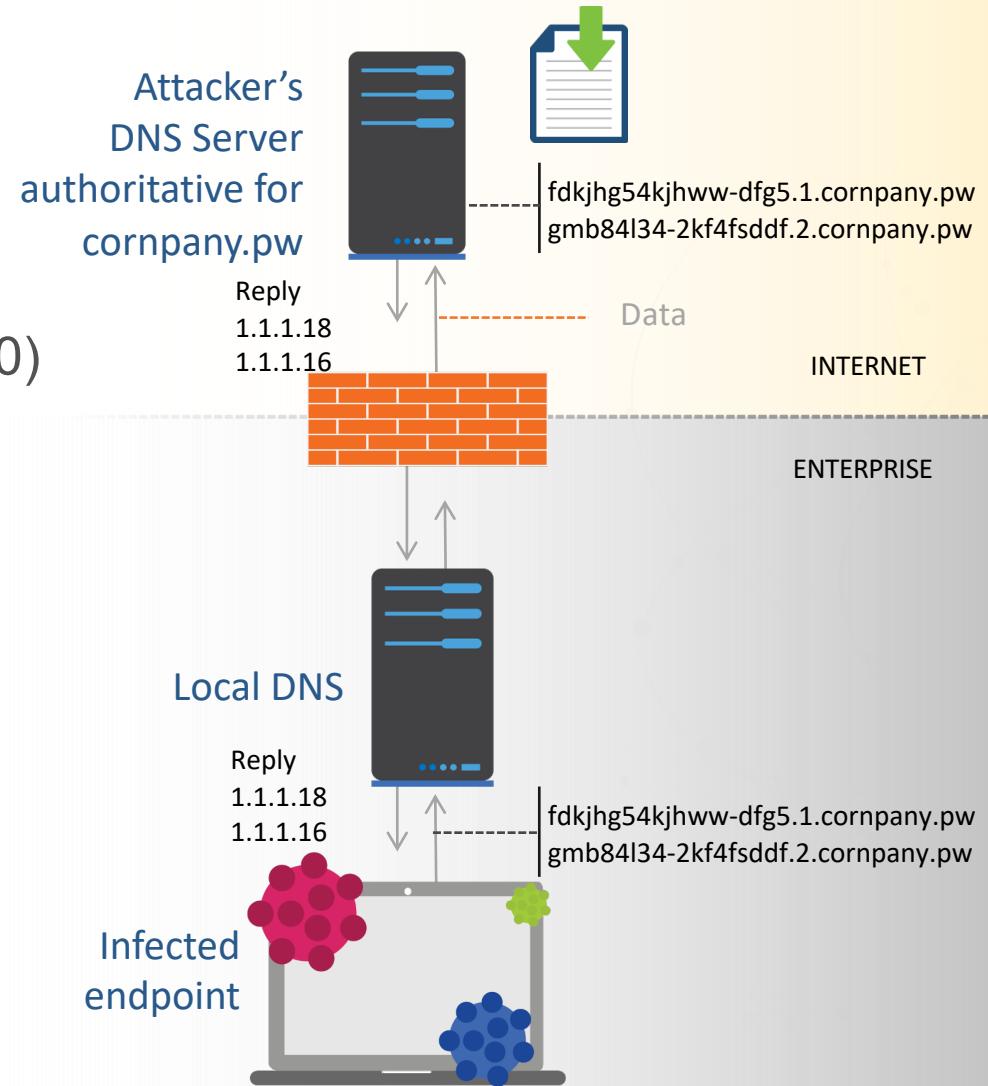
DNS as a Transport Mechanism

C2 a Tunelování

- Kombinace Exfilrace a Infiltrace
- Příklad užitečných kódů
 - A - Dovoluje 4 bytes
(Dostatek pro kód, např. 1.1.1.200 = resend packet 200)
- U tunelování nutné zasílat Keep a live pakety

taskType	taskType
21	netsh firewall show state
22	netsh firewall show config
23	schtasks /query /fo LIST /v
24	tasklist /v
16	ipconfig /all
17	route print
18	arp -A

Příklad: PowerSource / DNS Messenger



SombRAT / FiveHands

- Poprvé viděno od Vánoc 2020 do jara 2021
- Rovněž nasazen jako součást ransomwaru FIVEHANDS
- Počáteční přístup přes vzdálenou plochu pomocí ukradených přihlašovacích údajů nebo zero-day zranitelnost VPN
- SombRAT backdoor primárním účelem je stahovat a spouštět pluginy poskytované prostřednictvím serveru C2.
- Backdoor ve výchozím nastavení komunikuje s C2 prostřednictvím tunelu DNS

HOST	IP	LAST REPORT
b6feaf6c4a533ea958453e26f7ce.feticost.com	200.4.134.1	12/23/2020
b66ff4c0886525da50453221c9d9.feticost.com	106.153.172.132	12/23/2020
b56cf79e78d729a5534631228210.feticost.com	28.66.197.64	12/23/2020
b56cf71b778b2c5d53463122ab05.feticost.com	121.242.53.109	12/23/2020
b069f2bf28f31b9074182c2e0b56071b2dba6413b3ebe068a9f0c61155629b.feticost.com	198.80.94.124	12/23/2020
a77ee5b88ffffbc8d82150131dc4c0e3ef2.feticost.com	79.246.0.1	12/23/2020
a57ce7bdbaff67a45c55457e36b0a301532c52523df58c2ac33fd59c021aaa.feticost.com	103.173.0.1	12/23/2020
a27be0abf65b570717aac3858abea665b1592fab4411e860c756e2c2961db1.feticost.com	31.210.0.1	12/23/2020
9a43d8807a4d2ea743cb8dd63ee69fa133998e2389386e701247e81f592444.feticost.com	176.28.0.1	12/23/2020
964fd49da162acc1df793273be2af44c1d70eb9e74eca2bd3b55ff56039ed2.feticost.com	191.210.0.1	12/23/2020
8e57cc9294f9982875534b6c57698901cde3c9b23ff5ca0d8356f6e71ac02f.feticost.com	45.227.0.1	12/23/2020
8a53c887d1c20344e48031b218cedac4.feticost.com	23.252.0.1	12/23/2020

Zdroj: <https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>
<https://blogs.blackberry.com/en/2021/05/threat-thursday-sombrat-always-leave-yourself-a-backdoor>



DNS Hijacking

- **DarkHalo after SolarWinds: the Tomiris connection**

- Přesměrování na útočníkem kontrolované DNS servery
- Používáno pro kradení přihlašovacích údajů
- Použití Let's Encrypt certifikátů pro věrohodné kopie stránek

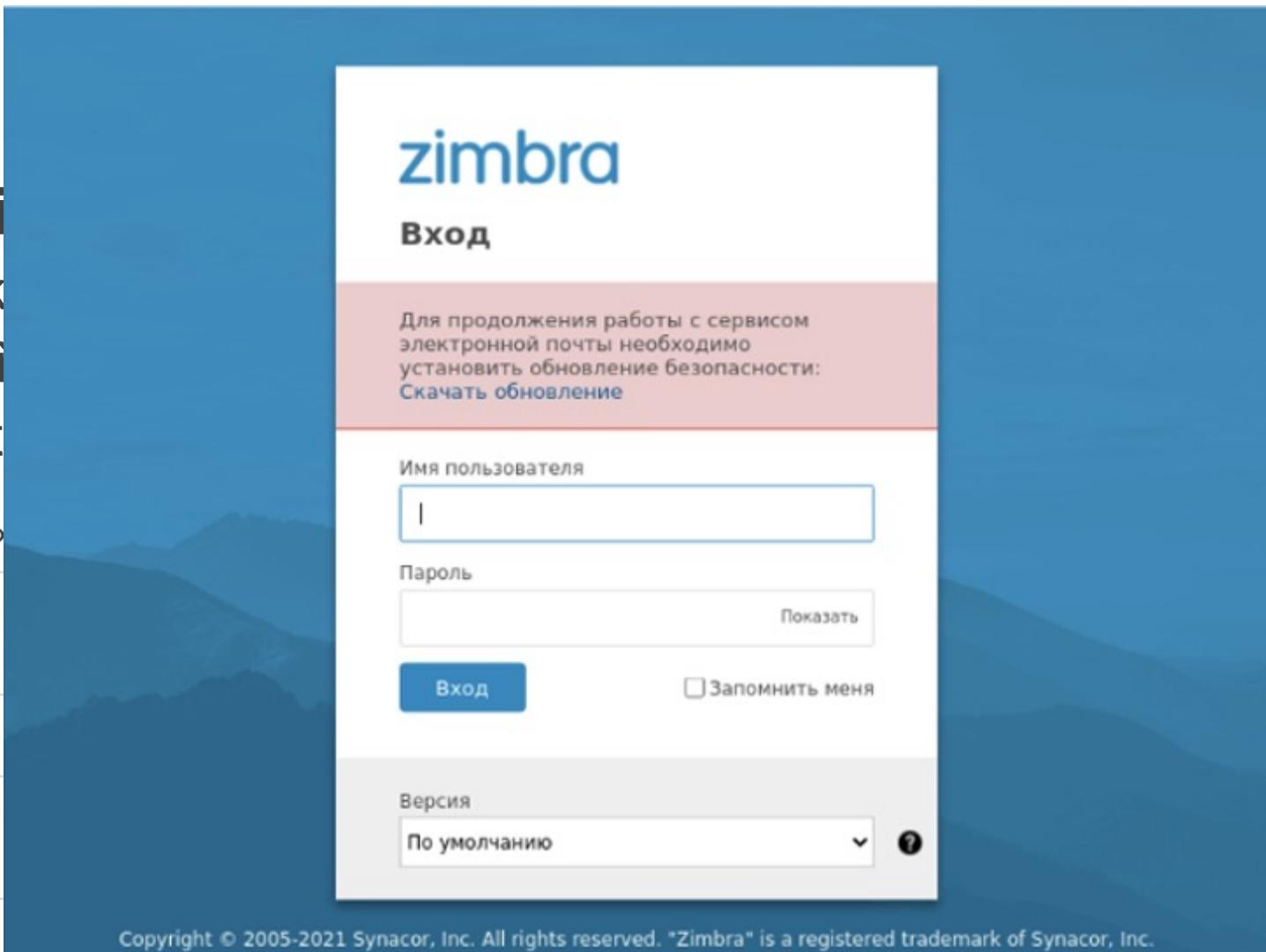
Zone	Period during which the authoritative servers were malicious	Hijacked domains
mfa.***	December 22–23, 2020 and January 13–14, 2021	mail.mfa.*** kk.mfa.***
invest.***	December 28, 2020 to January 13, 2021	mail.invest.***
fiu.***	December 29, 2020 to January 14, 2021	mx1.fiu.*** mail.fiu.***
infocom.***	January 13–14, 2021	mail.infocom.***



DNS Hijacking

- DarkHalo after SolarWinds
 - Přesměrování na útočník
 - Používáno pro kradení přihlašovacích údajů
 - Použití Let's Encrypt certifikátů

Zone	Period during which the authorizations were issued
mfa.***	December 22–23, 2020 and January 13–14, 2021
invest.***	December 28, 2020 to January 13, 2021
fiu.***	December 29, 2020 to January 13, 2021
infocom.***	January 13–14, 2021



Techniky útoků na DNS servery

DNS reflection/DrDoS attacks	Using third-party DNS servers (mostly open resolvers) to propagate a DoS or DDoS attack
DNS amplification	Using a specially crafted query to create an amplified response to flood the victim with traffic
TCP/UDP/ICMP floods	Denial of service on layer 3 or 4 by bringing a network or service down by flooding it with large amounts of traffic
DNS-based exploits	Attacks that exploit bugs or vulnerabilities in the DNS software
DNS cache poisoning	Corruption of DNS server cache data with a rogue domain or IP
Protocol anomalies	Causing the server to crash by sending malformed DNS packets and queries
Reconnaissance	Attempts by hackers to get information on the network environment before launching a DDoS or other type of attack
DNS tunneling	Tunneling of another protocol through DNS port 53 for malware insertion and/or data exfiltration
DNS hijacking	Modifying the DNS record settings to point to a rogue DNS server or domain
NXDomain attack	Attacks that flood DNS server with requests for non-existent domains, causing it to send NXDomain (non-existent domain) responses
Phantom domain attack	Attacks where a DNS resolver is forced to resolve multiple non-existent domains, causing it to consume resources while waiting for responses

■ DNS-specific Exploits

■ Volumetric/DDoS Attacks





Populární nástroje útočníků



Nástroje

Tools

- NSTX
- DNSCat2
- Iodine
- TUNS
- Dns2TCP
- Heyoka
- OzymanDNS
- DNS_TXT_Pwnage

Platforms

- Cobalt Strike
 - Komerční produkt
- Nishang framework
 - Volně dostupné
- Vermilion Strike
 - Pro Windows i Linux





Další techniky a taktiky



Look-a-like domény

TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES

TLD swap phishlabs.tech

Omission phshlabs.com

Subdomains phish.labs.com

Transposition phsihlabs.com

Typosquatting phishlav.com

Insertion phishxlab.com

Hyphenation phish-labs.com

Homoglyph phishlābs.com

Repetition phishllabs.com

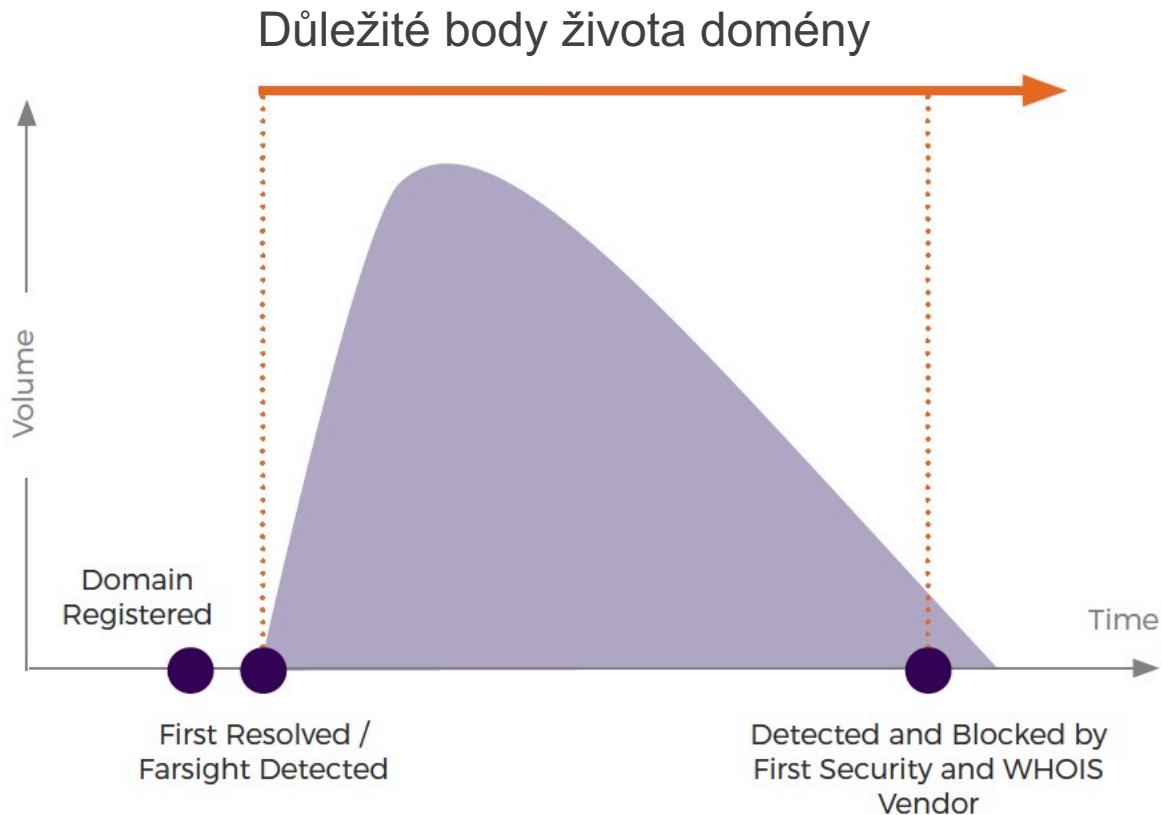
Vowel-swap phishlebs.com

Replacement ph1shlabs.com

Addition phishlabss.com



Phishing kampaně



Lookalike – partial match



DATUM 14/06/2021

SLEDOVACÍ KÓD BUDE ZASLÁN PO
PROVEDENÍ PLATBY!

CELKOVÁ ČÁSTKA: 53,47 KČ

ZPŮSOB PLATBY :

Kreditní karta

PLATIT A POKRAČOVAT

ZRUŠIT

Ceskapostapay[.]com

192[.]64[.]117[.]221 Malicious Activity!

Effective URL: [https://ceskapostapay\[.\]com/payment/Package>Select-payment-method.php?NAME_PATH=track_yy_dl24&SCREEN=identification_contrat...](https://ceskapostapay[.]com/payment/Package>Select-payment-method.php?NAME_PATH=track_yy_dl24&SCREEN=identification_contrat...)

WHOIS Record (Created)	2021-06-14T01:40:11+00:00
Policy_NewlyObservedDomains	2021-06-14T01:44:32.000Z
MalwareDownload_Generic	2021-06-15T05:51:33.037Z

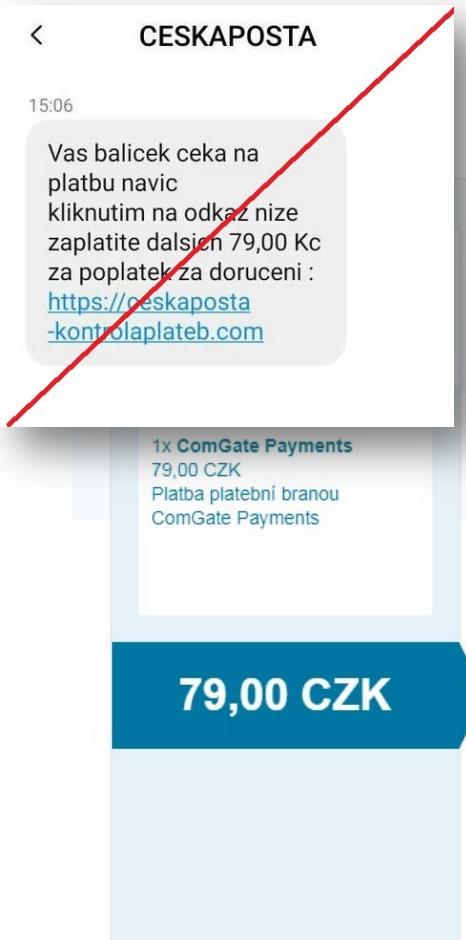
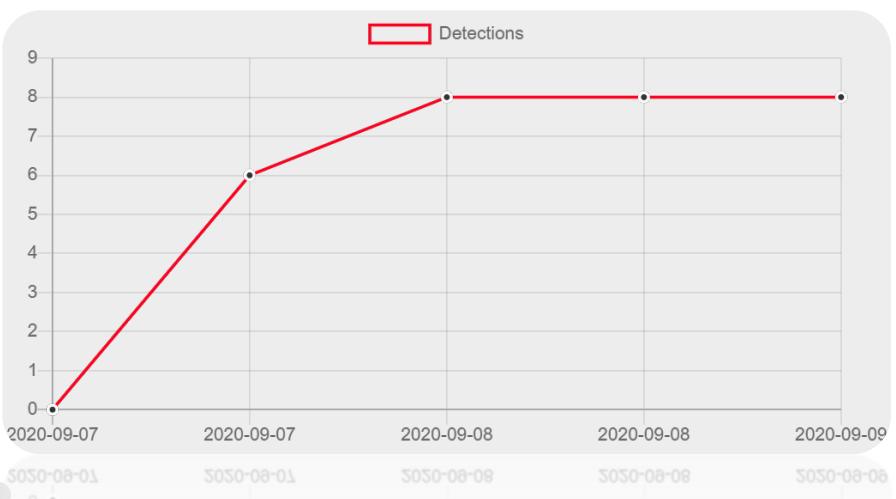


Nové domeny - smishing

Domain Name: ceskaposta-kontrolaplateb[.]com

Creation Date: 2020-09-05 14:42 CET

First Query: 2020-09-05 14:52 CET



Bezpečná online platba



Vaše platební údaje nikdy nesdílíme s obchodníkem. V adresním řádku prohlížeče si prosím ověřte, že se nacházíte na stránce platebnibrana.csob.cz a že zelená ikonka zámečku indikuje bezpečné spojení.

Številka kartice
Veljavnost
CVC/CVV

Zaplatit 79,00 CZK

Česká pošta **Verified by MasterCard** **VISA** **SecureCode**

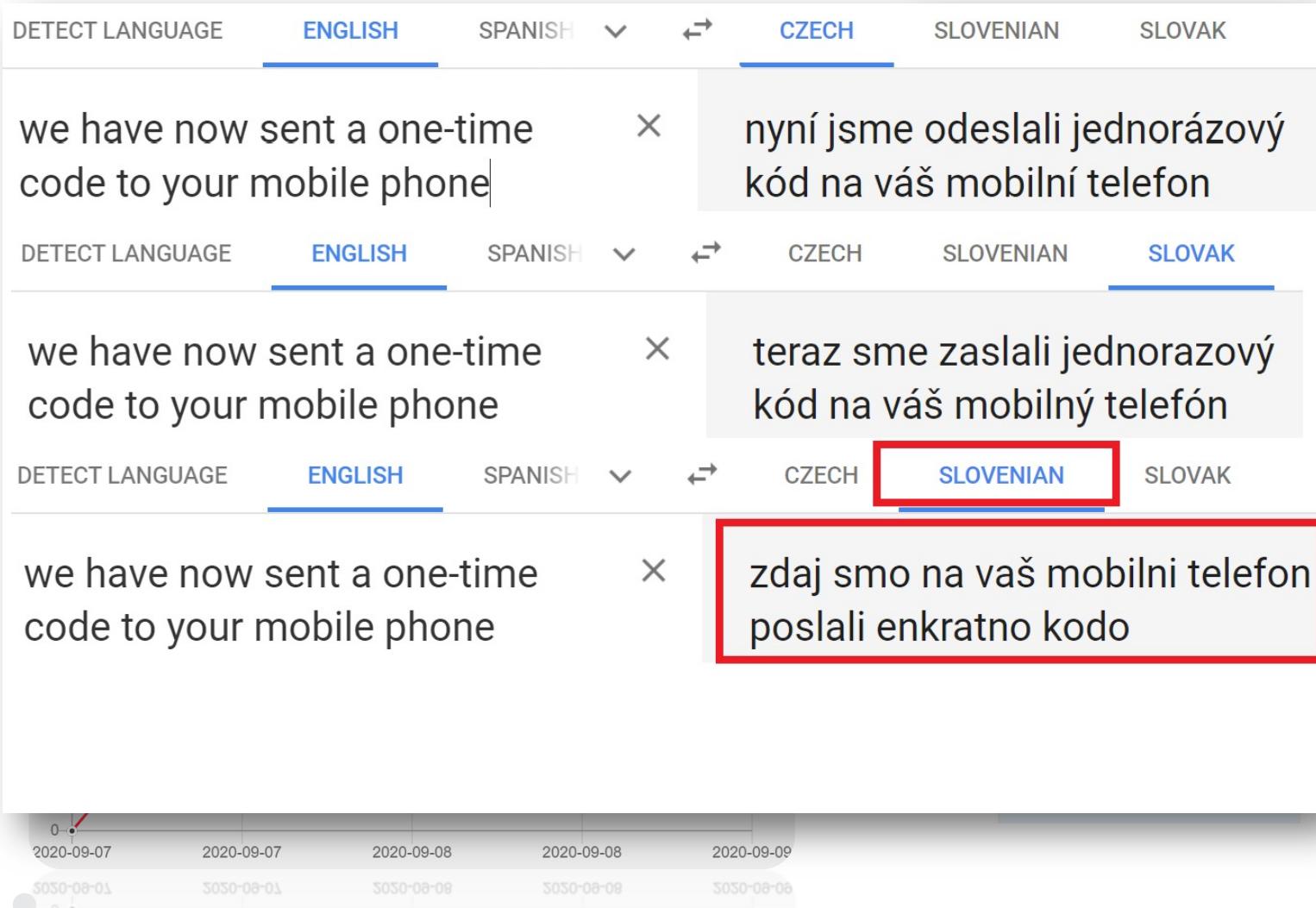
Potrditev z enkratno kodo
Zdaj smo na vaš mobilni telefon poslali enkratno kodo.
Vnesite kodo, ki ste jo prejeli po telefonu za izvedbo transakcije, in
pritisnite "Potrdi".

Spletna trgovina:	transakcija
Zneselek:	79,00 CZK
Datum:	09/07/2020 07:46:32 pm
Številka kartice:	XXXX XXXX XXXX XXXX
Dostop do kode prek besedilnega sporočila:	<input type="text"/>
	Potrdite

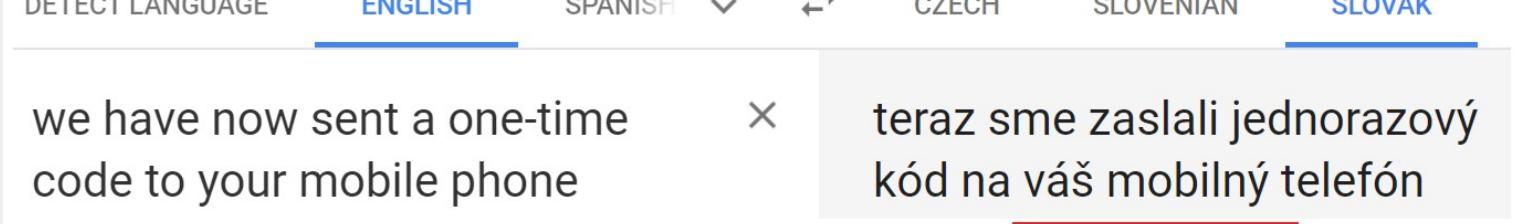
SMS screenshot from: <https://manipulatori.cz/pozor-na-podvod-sms-zprava-se-tvari-jako-zprava-od-ceske-posty/>



Nové domeny - smishing

Detect Language English Spanish 

we have now sent a one-time code to your mobile phone  nyní jsme odeslali jednorázový kód na váš mobilní telefon

Detect Language English Spanish 

we have now sent a one-time code to your mobile phone  teraz sme zaslali jednorazový kód na váš mobilný telefón

Detect Language English Spanish 

we have now sent a one-time code to your mobile phone  zdaj smo na vaš mobilni telefon poslali enkratno kodo





SMS screenshot from: <https://manipulatori.cz/pozor-na-podvod-sms-zprava-se-tvari-jako-zprava-od-ceske-posty/>



Kolik domén je generováno DGA?

Bamital 197,000	Fobber 2,000	Mewsei 1,984	Pykspa 2 775,342	Simda 11,528
Banjori 421,390	Geodo 90,232	Murofet 1 4,063,680	QakBot 385,000	Suppobox 98,304
Bedep 3,806	Gameover DGA 6,182,000	Murofet 2 262,000	Ramdo 3000	Szribi 2,949
Conficker 125,118,625	Gameover P2P 262,000	Necurs 3,551,232	Ramnit 18,000	Tempedreve 204
CoreBot 18,160	Gozi 16,963	Nymaim 65,040	Ranbyus 64,400	TinyBanker 81,930
Cryptolocker 1,108,000	Hesperbot 178	Pushdo 124,021	Redyms 34	Torpig 17,610
DirCrypt 420	Kraken 300	Pushdo TID 6,000	Rovnix 10,000	UrlZone 10,009
Dyre 592,000	Matsnu 3,346	Pykspa 1 22,764	Shifu 1,554	Virut 15,335,008

Součet unikátních domén: **159 712 234** nebo 34 593 609 bez Conficker

ke konci roku 2015

Zdroj: DGArchive, Daniel Plohmann, 2016



Kolik domén je generováno DGA?

- Machine Learning Classifiers které se zaměřují na identifikaci malware rodiny za pomoci zjištěných DGA domény.

```
"domain": "61r3oz17bdx9lmtmdr9o7q2b.biz",
"property": "MalwareC2DGA_GameoverZeusV2",
"class": "MalwareC2DGA",
"threat_level": 100,
```

Bamital 197,000	Fobber 2,000	Mewsei 1,984	Pykspa 2 775,342	Simda 11,528
Banjori 421,390	Geodo 90,232	Murofet 1 4,063,680	QakBot 385,000	Suppobox 98,304
Bedep 3,806	Gameover DGA 6,182,000	Murofet 2 262,000	Ramdo 3000	Szribi 2,949
Conficker 125,118,625	Gameover P2P 262,000	Necurs 3,551,232	Ramnit 18,000	Tempedreve 204
CoreBot 18,160	Gozi 16,963	Nymaim 65,040	Ranbyrus 64,400	TinyBanker 81,930
Cryptolocker 1,108,000	Hesperbot 178	Pushdo 124,021	Redyms 34	Torpig 17,610
DirCrypt 420	Kraken 300	Pushdo TID 6,000	Rovnix 10,000	UrlZone 10,009
Dyre 592,000	Matsnu 3,346	Pykspa 1 22,764	Shifu 1,554	Virut 15,335,008

Součet unikátních domén: **159 712 234** nebo 34 593 609 bez Conficker

ke konci roku 2015

Zdroj: DGArchive, Daniel Plohmann, 2016



Slovníkové DGA

Slovník 1:

face
walk
weak
sell
deep
ball
push
both



Slovník 2:

gone
road
dont
fool
heat
aunt
they
lift
goes



Suppobox malware domains:

facegone.net.

walkroad.net.

weakdont.net.

sellfool.net.

weakheat.net.

deepaunt.net.

facethey.net.

ballpull.net.

pushaunt.net.

walklift.net.

bothfive.net.

facegoes.net.

Dictionary DGA	Example Family	Example Domain
Wordlist	Suppobox	facegone.net
Permutation	VolatileCedar	dotnetexplorer.info





Co si z toho odnést?

1. DNS je jen způsob odesílání a přijímání nějakých dat - může to být Cokoliv (tj. Adresa serveru C2, úkoly k provedení, škodlivý kód, citlivá data atd.)
2. DNS resolvers sloužit jako proxy



Q&A



Děkuji za pozornost

Jan Ryneš
Solutions Architect
jrynes@infoblox.com
+420 731 591 259

