
# DNS File EXfiltration


Emilio / @ekio_jp

# Information:
# New HITB Q&A system

- Using “Slido App” to vote best question
- Free swag from HITB (yay!)
- Interactive, ask question anytime (answer maybe later)
- Don’t worry, go ahead and put your question out!
- Extra swag from me too（笑）

https://dfex.dob.jp

# Hello, Friend

- My name is Emilio or **エミリオ** and I'm hacker
- I like to play with packets, networks, electronics and 3D printers
- I presented tools at various conferences (DEF CON, BlackHat Asia, HITB, AV Tokyo, SECCON, HamaSec, Hacker's Party, etc)
- Sorry, I'm not a native programmer or English speaker ☺

https://dfex.dob.jp

# DNS File EXfiltration?

**What?**
- Using DNS protocol as a “Covert Channel”
- Unauthorized Files Transfer (in a polite way)

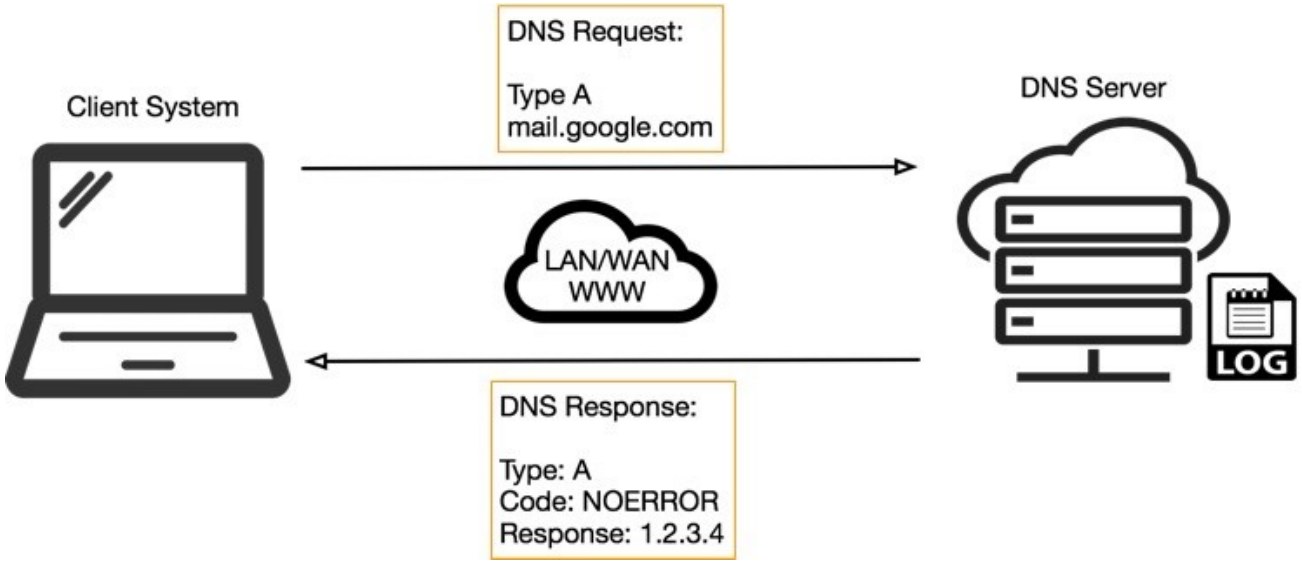
**When?**
- A post-exploitation technique
- Used in restricted networks (NG Firewalls, IPS, Proxies)

**How?**
- The good old fashion “HIPS” (Hide In Plain Sight)

https://en.wikipedia.org/wiki/Covert_channel

https://dfex.dob.jp

# DNS traffic




https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

# Existing Tools

DNS Exfiltration

- *dnsteal v2.0*
  https://github.com/m57/dnsteal
- *DNSExfiltrator*
  https://github.com/Arno0x/DNSExfiltrator
- *dns-exfiltration*
  https://github.com/krmaxwell/dns-exfiltration
- *dns_exfiltration*
  https://github.com/coryschwartz/dns_exfiltration
- *Requestbin*
  http://requestbin.net/dns

DNS Tunneling

- https://dnstunnel.de/
- https://code.kryo.se/iodine/
- https://github.com/iagox86/dnscat2

Tools look like this

https://dfex.dob.jp

# What we wish

- AES 256-CTR Encryption
- Retransmission Capabilities
- Error free (CRC)
- Threading Support
- Speed? (back to 4800 bauds!)
- Multiple sub/domain (avoid IOC)
- Stealthy
- One-way packets*

Tools we want

* Unless retransmission

https://dfex.dob.jp

# Avoiding Detection

Things we don't want:

- Short DNS TTL
- DNS TXT records
- Long DNS FQDN queries
- High volume requests from same IP
- Same sub/domain

Things we do want:

- Control vs Data sub/domains
- DNS NS query type
- No answer from data domains
- Multiple sub/domains for control and data
- Limit name request to 20-30 char

https://dfex.dob.jp

# DFEX Algorithm

Steps:

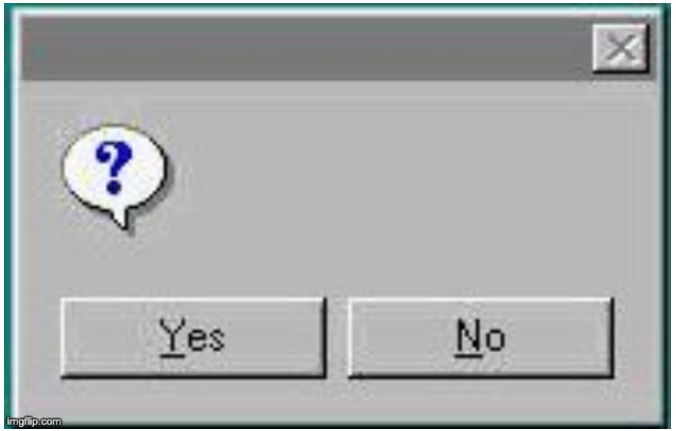
1) File CRC32
2) File ID generation
3) Compress file (zlib)
4) Generate key (hashed passphrase)
5) Encrypt file with AES-256 CTR
6) Apply base32 with custom padding
7) Split file into 20-30 characters chunks
8) Generate SRC IP's list for spoofing
9) Send control DNS packet (ID, CRC32, total pkts)
10) Send data DNS packet (ID, pkt seq, 20-30 char)
11) Repeat 10) till completed
12) Send control re-transmission packet
13) If DNS 'A' answer, re-send data seq X pkt
14) Send control re-transmission packet
15) Holdtime expired and file transfer completed


https://dfex.dob.jp

# Are these queries suspicious?

d15d5hi91tsj9x.cloudfront.net

efa2f1adkf9fjdncu8dbsowd5f.cloudwatch.net




https://dfex.dob.jp

# Well.....

tango~$ nslookup **d15d5hi91tsj9x.cloudfront.net**
Server: 8.8.8.8
Address: 8.8.8.8#53

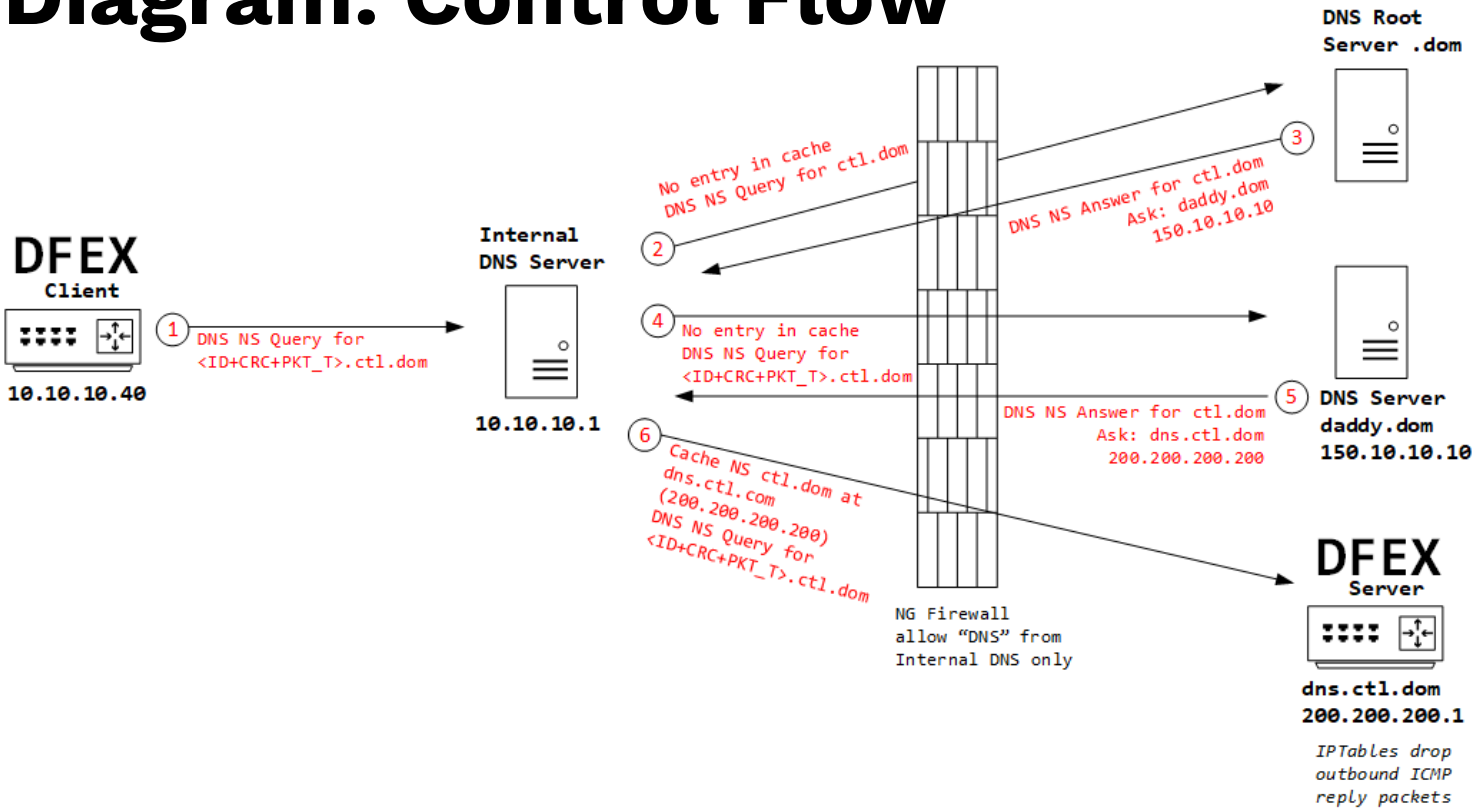
Non-authoritative answer:
Name: d15d5hi91tsj9x.cloudfront.net
Address: 13.249.146.100
Name: d15d5hi91tsj9x.cloudfront.net
Address: 13.249.146.31
Name: d15d5hi91tsj9x.cloudfront.net
Address: 13.249.146.18
Name: d15d5hi91tsj9x.cloudfront.net
Address: 13.249.146.13

# However.....

tango~$ nslookup **efa2f1adkf9fjdncu8dbsowd5f.cloudwatch.net**
Server: 8.8.8.8
Address:  8.8.8.8#53

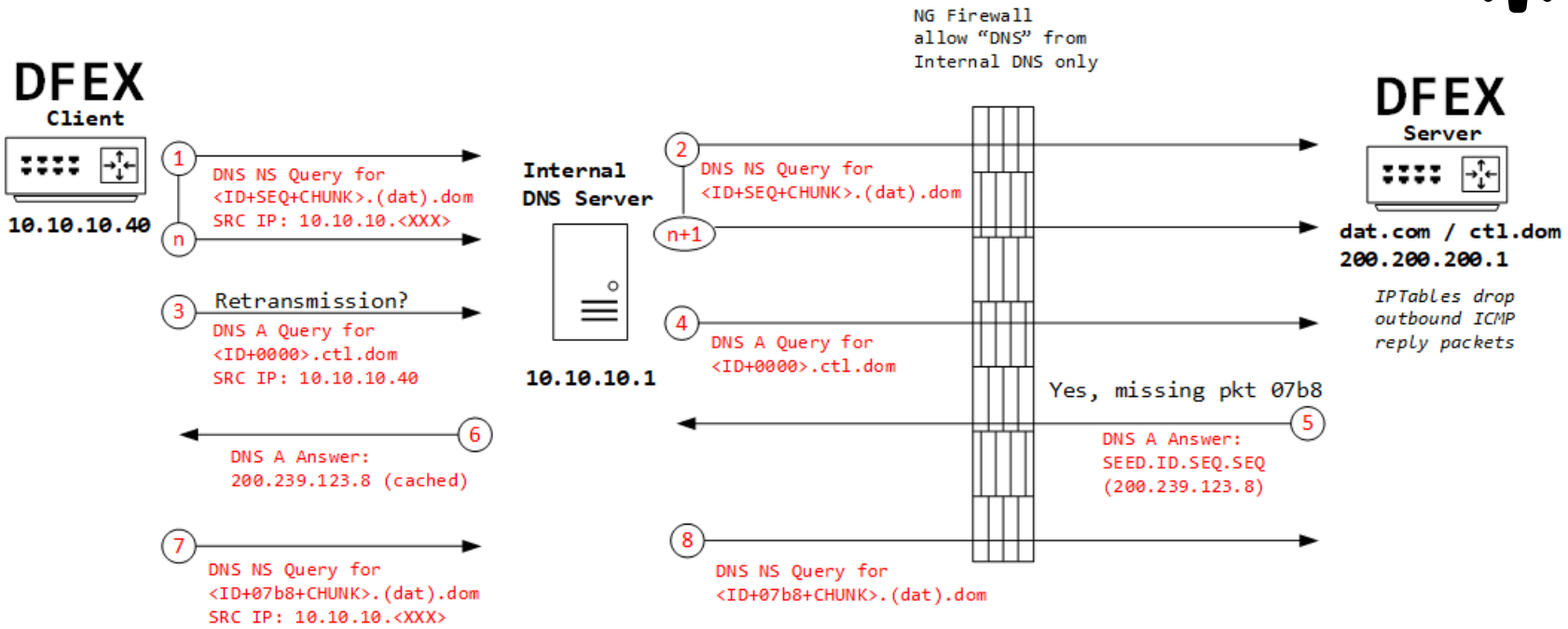
** server can't find efa2f1adkf9fjdncu8dbsowd5f.cloudwatch.net: NXDOMAIN

# Diagram: Control Flow



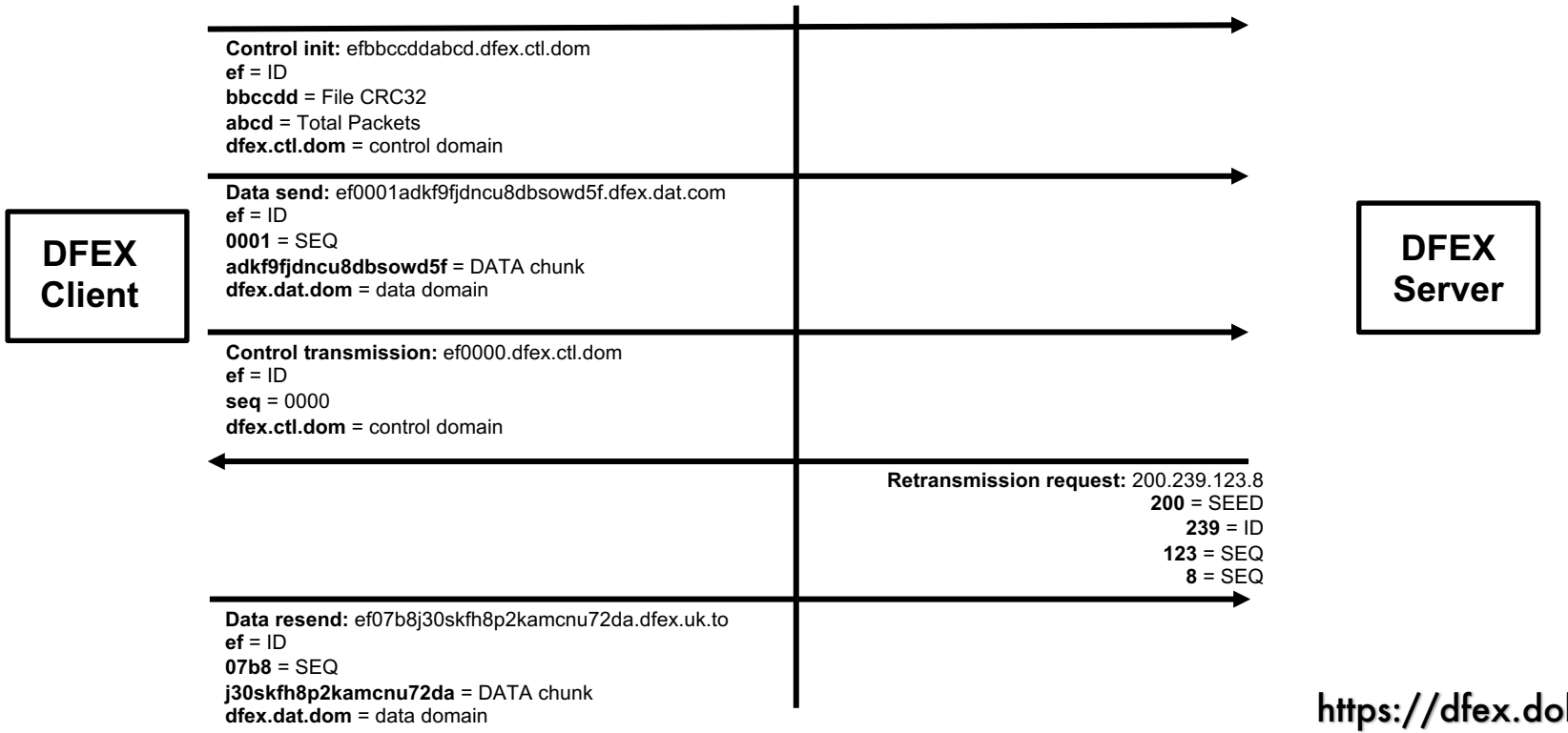

https://dfex.dob.jp

# Diagram: Data Flow



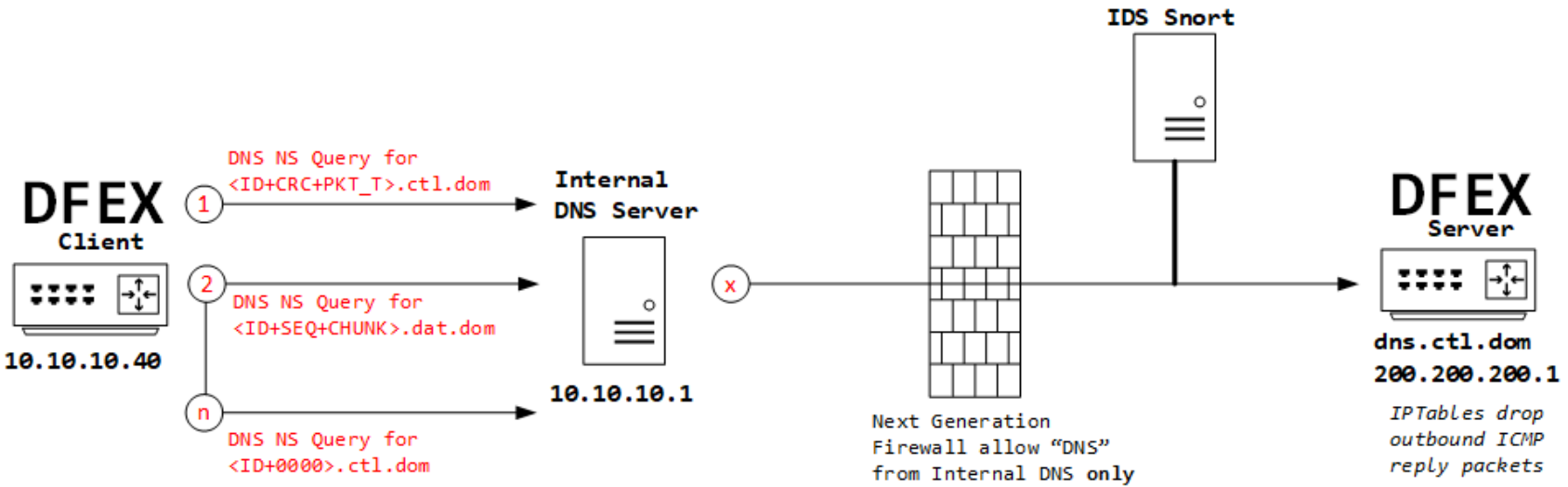

https://dfex.dob.jp

# Packet Example




https://dfex.dob.jp

# Demo Infra (MACCHERONI)




https://dfex.dob.jp

# Proof of Concept or go away

https://dfex.dob.jp

# Performance

Example:

- 120Kb file
- ~1900 packets (20 Characters)
- Source network (/24)
- 5 Data Domains
- 1 Control Domain

Results:

- ~270 seconds
- 1-2 query per IP for Data Domain
- 1 query (total) for Control Domain
- 4.8kbps file transfer speed

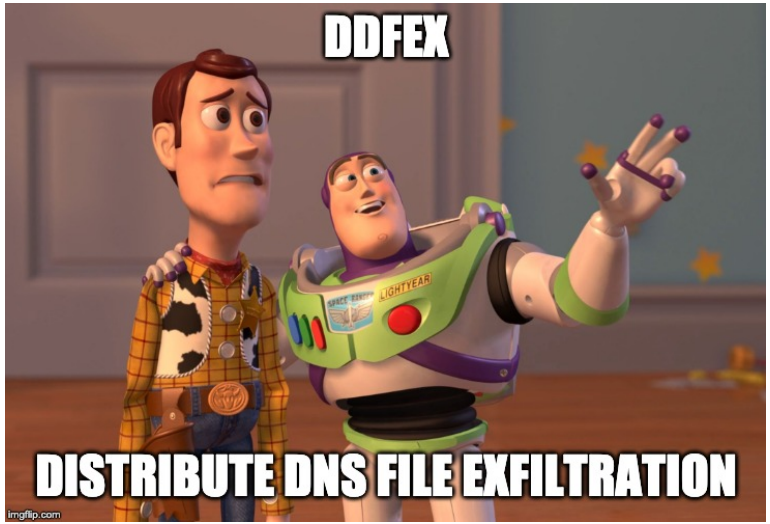

https://dfex.dob.jp

# Limitations

- Up to 255 simultaneous files
- ~4Mb file size
- Retransmission TTL (caching)

# The Future

- DDFEX – Distributed DNS File EXfiltration
- Cloud Automation
- C&C Manager




https://dfex.dob.jp

# Conclusion

Prevention & Detection:

- Don’t allow DNS external query ☺
- Use DNS Sinkhole
- DNS log analytics (ie, Splunk) and smart SOC people
- Entropy analytics methods using same smart SOC people
- DNS Cloud Services (ie, Umbrella/CloudFlare)

https://dfex.dob.jp

# Questions?

# Before I forget...
# Disclaimer:

The tool is provided for educational, research or testing purposes
Using this tool against network/systems without prior permission is illegal
The author is not liable for any damages from misuse of this tool, techniques or code

# Thanks!

 Emilio

 ekio_jp

 https://github.com/ekiojp/dfex

 https://dfex.dob.jp