black hat ASIA 2020

OCTOBER 1-2, 2020
BRIEFINGS

Misuse of DNS
The Second Most Used Protocol

#BHASIA @BLACKHATEVENTS

Hello, Virtual Friend

- My name is Emilio and I’m hacker
- I like to play with packets, networks, electronics and 3D printers
- I presented security tools at various conferences (DEF CON, BlackHat Asia, Ekoparty, HITB, AV Tokyo, Code Blue, SECCON, etc)
- Sorry, I’m not a native programmer or English speaker :)
- UTC+9

Attacks on DNS

Server Side

- Buffer overflow
- Information Disclosure
- Flooding (DDoS/DoS)
- Amplification (DDoS/DoS)

Client Side

- Cache Poisoning/Spoofing
- Hijacking (MiTM)
- DNS Rebinding

Protocol

- Zone Transfers (remember this right?)
- Tunneling
- Command and Control (C&C)

Security on DNS

DNSSEC

- RFC 4033 dated 2005
- Root Signing, Key Mgmt, Validation, etc
- No encryption (privacy)
- Complex Implementation

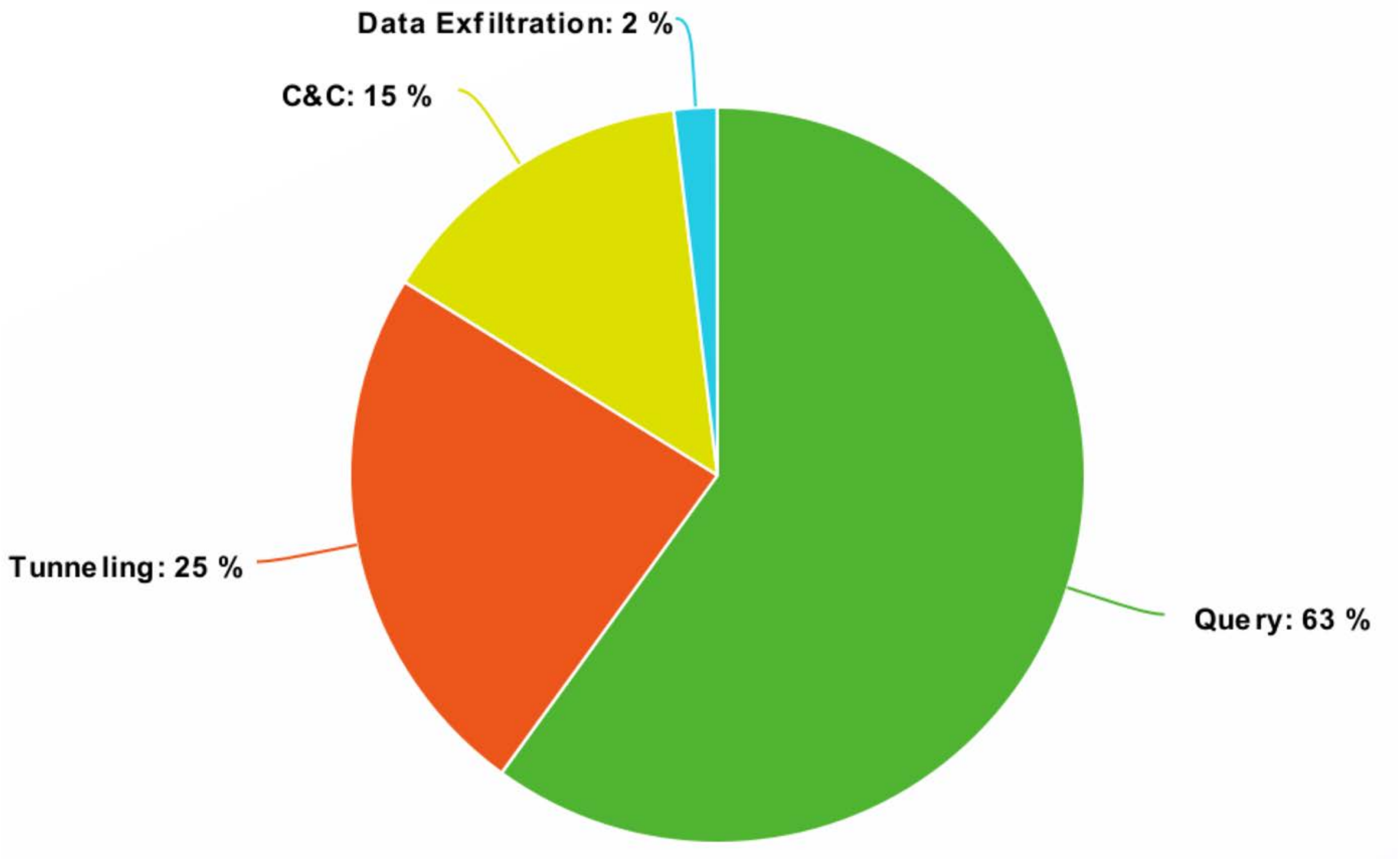
DNS over HTTPS (DoH)

- Prevent ISP Tracking (fail)
- Bypass enterprise filters
- Help Criminals?

DNS over TLS (DoT)

- Performance (TCP vs UDP)
- Allow ”opportunistic” (failback to plain DNS)

Estimated DNS Usage



Cover Channels

Tunneling

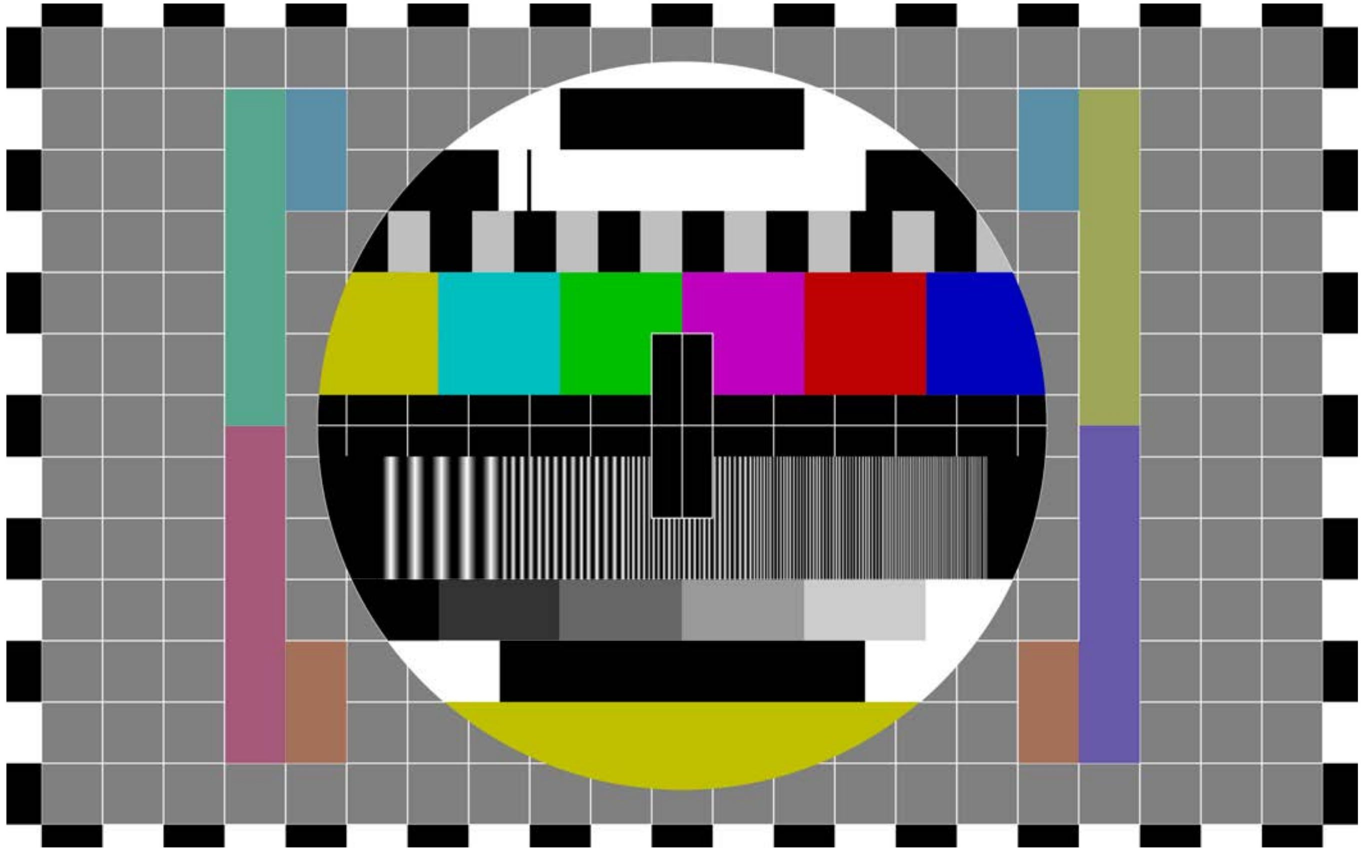
- Free Internet (Hotels, Airports, Planes)
- Avoid ISP Filters
- Encapsulate VPN traffic
- Bypass corporate firewalls

Command and Control (C&C)

- Botnets
- Malware updates
- Espionage
- Remote/Reverse shell
- State-Sponsors tools

Data Exfiltration

- Stealing
- Data Leak
- Unauthorized data transfers



Tools

DNS Exfiltration

- https://github.com/m57/dnsteal
- https://github.com/Arno0x/DNSExfiltrator
- https://github.com/krmaxwell/dns-exfiltration
- https://github.com/coryschwartz/dns_exfiltration
- http://requestbin.net/dns
- https://github.com/ytisf/PyExfil

DNS Tunneling / C&C

- https://dnstunnel.de/
- https://code.kryo.se/iodine/
- https://github.com/iagox86/dnscat2
- https://github.com/IncideDigital/Mistica
- https://github.com/averagesecurityguy/c2
- https://www.aldeid.com/wiki/Dns2tcp

Pros & Cons

We don't want this

- Short DNS TTL
- DNS TXT or NULL query type
- Long DNS label queries (FQDN)
- High volume requests from same IP
- Tons of NXDOMAIN answers
- Same sub/domain

We want this

- Control vs Data Architecture
- DNS NS query type
- Short (20-30 char) label query
- Many source IP queries
- No answer from data domains
- Multiple sub/domain for Data flow

Control & Data

- Threading (multiple files)
- Scalable
- Split flow (asymmetric)
- Not sequential
- Compress & AES-256 CTR
- Retransmission

Stealth

- DNS NS query type
- No state-full connections (FW/IPS)
- Random times between chunks
- Limit name request to 20-30 char
- Remember spoofing?
- No sequential packets, long live random

Can we do all that??

Proof of Life

DFEX

DNS File EXfiltration

https://github.com/ekiojp/dfex

Prevention & Detection

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

Conclusion

Next Steps:

- The “RTE” Method (Research-Test-Experiment)
- DDFEX – Distributed DNS File Exfiltration (scalable)
- Cloud Automation (ansible)
- C&C Manager for control domains
- Use control flow for C&C
- PowerShell client

Thanks for watching

Emilio

ekio_jp

https://github.com/ekiojp/dfex

https://dfex.dob.jp