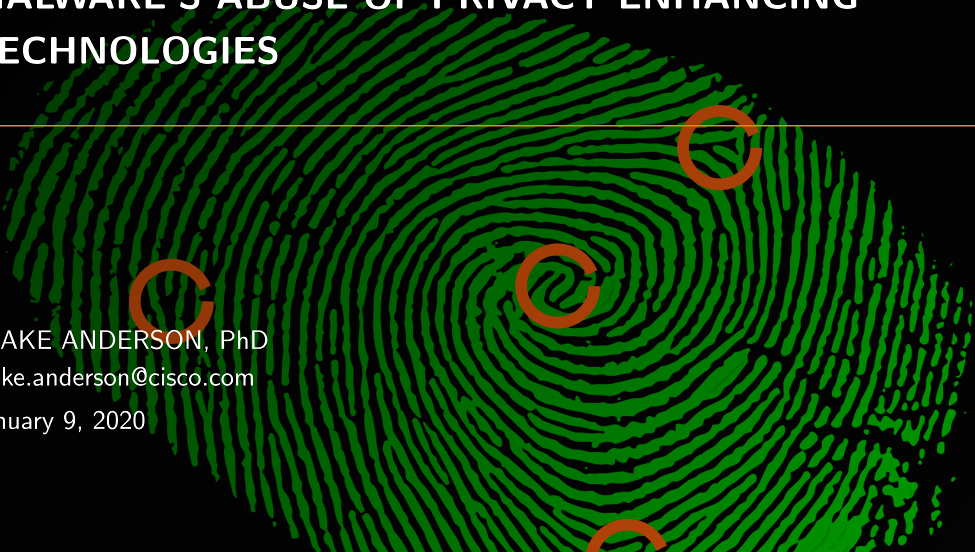
MALWARE'S ABUSE OF PRIVACY ENHANCING TECHNOLOGIES



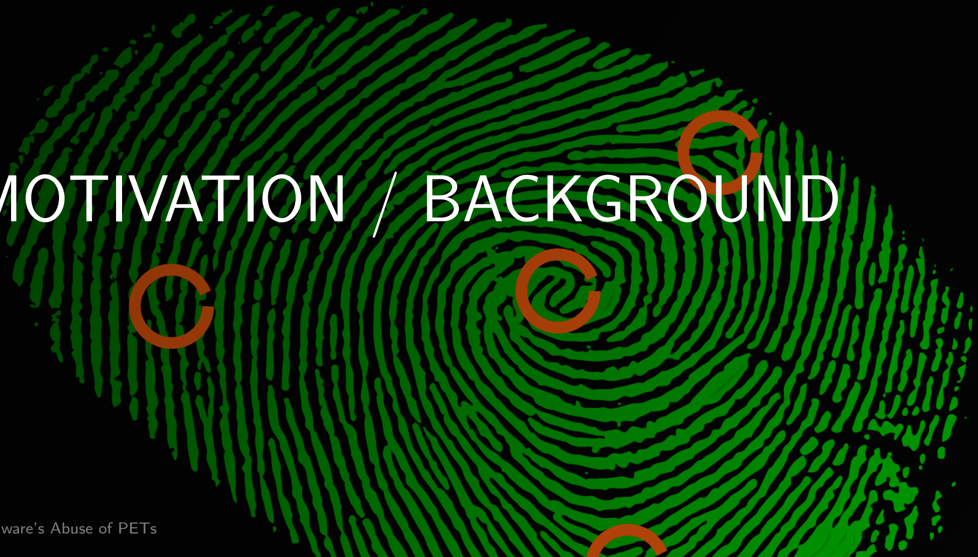
BLAKE ANDERSON, PhD
blake.anderson@cisco.com

January 9, 2020

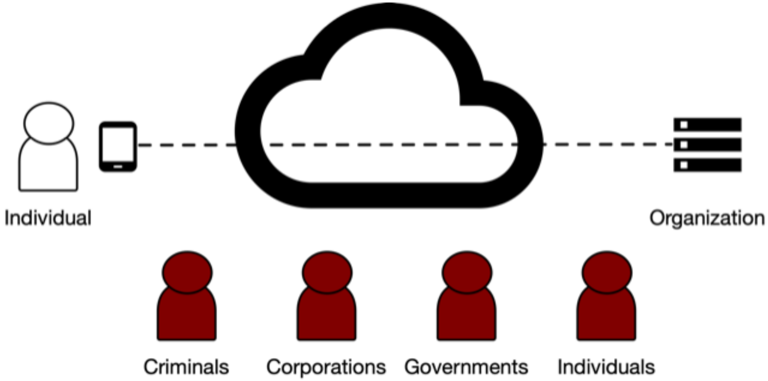
OUTLINE

- Motivation / Background
- General malware PET's trends
- Malware's abuse of censorship circumvention tools
- Future trends

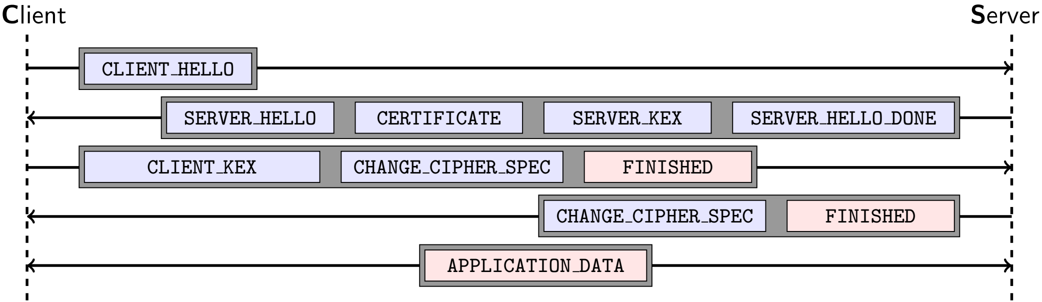
MOTIVATION / BACKGROUND



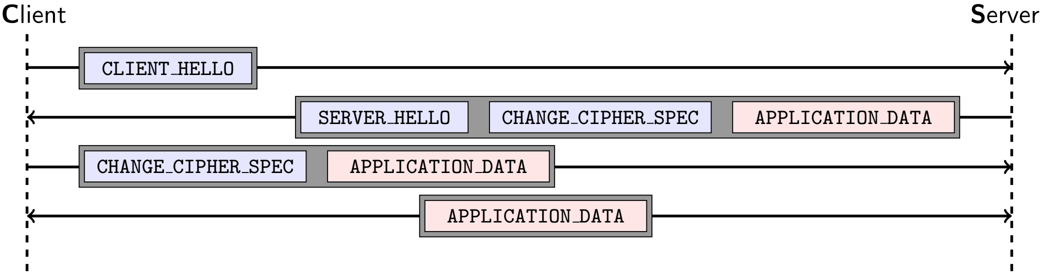
NETWORK THREAT LANDSCAPE



TLS 1.2


Client
Server
CLIENT_HELLO
SERVER_HELLO
CERTIFICATE
SERVER_KEX
SERVER_HELLO_DONE
CLIENT_KEX
CHANGE_CIPHER_SPEC
FINISHED
CHANGE_CIPHER_SPEC
FINISHED
APPLICATION_DATA

TLS 1.3


Client
Server
CLIENT_HELLO
SERVER_HELLO
CHANGE_CIPHER_SPEC
APPLICATION_DATA
CHANGE_CIPHER_SPEC
APPLICATION_DATA
APPLICATION_DATA

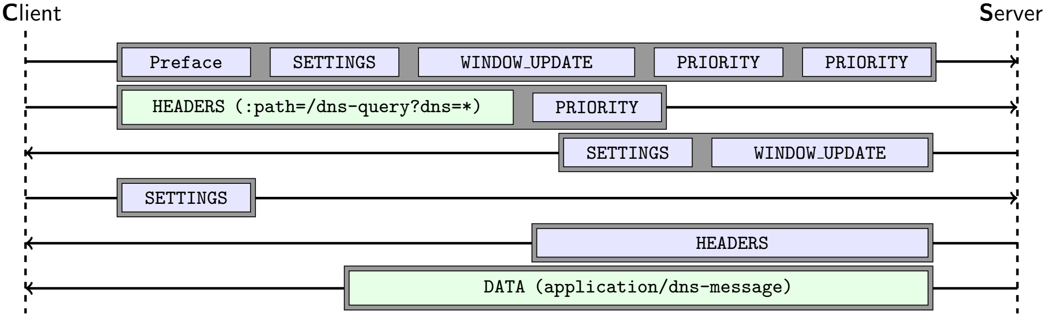
TLS CLIENT_HELLO

```
HandshakeType:      01
Length              0001fc
ProtocolVersion:    0303
ClientRandom:       a19fdbf3...
SessionID:          06d18594...
CipherSuites:       0a0a...000a
CompressionMethods  0100
Extensions:         0000...
```

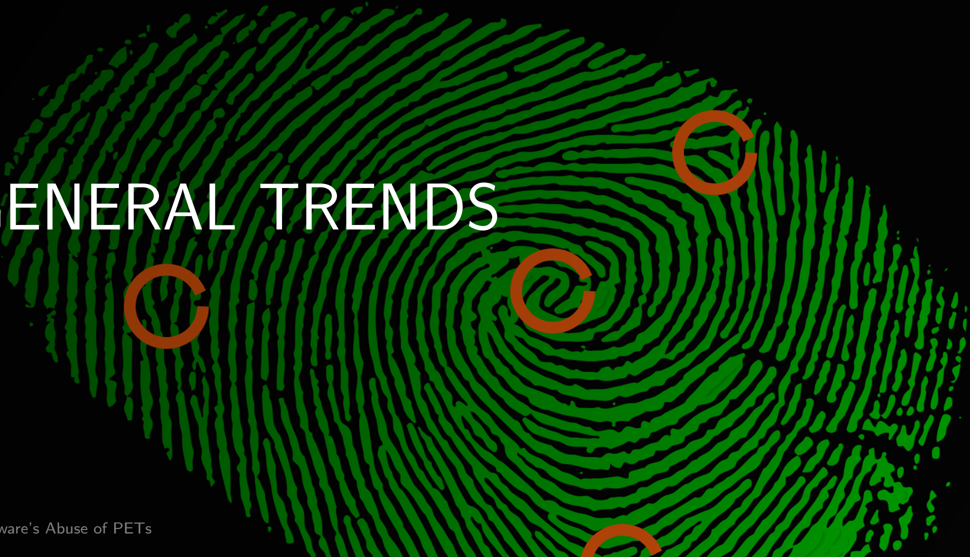
TLS CLIENT_HELLO FINGERPRINTING

$$a : \begin{bmatrix} \texttt{ProtocolVersion:} & \texttt{0303} \\ \texttt{CipherSuites:} & \texttt{0a0a...000a} \\ \texttt{Extensions:} & \texttt{0000...} \end{bmatrix} \rightarrow \begin{bmatrix} \texttt{Process:} & \texttt{chrome.exe} \\ \texttt{Version:} & \texttt{76.0.3809.132} \\ \texttt{SHA-256:} & \texttt{5616...9acc} \\ \texttt{Category:} & \texttt{browser} \\ \texttt{OS:} & \texttt{WinNT} \\ \texttt{OSversion:} & \texttt{10.0.17134} \\ \texttt{OSedition:} & \texttt{Enterprise} \end{bmatrix}$$

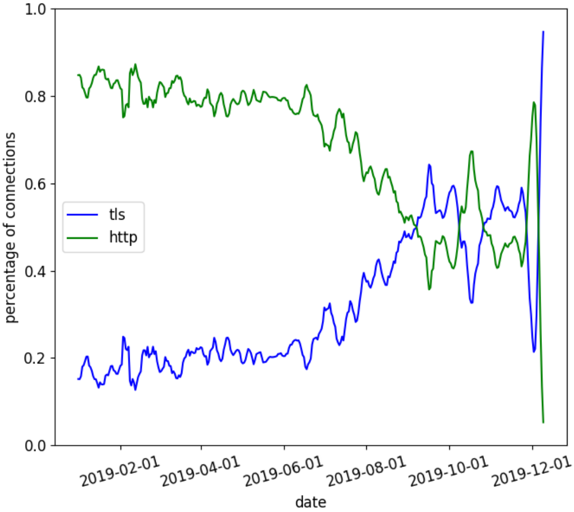
DNS-OVER-HTTPS



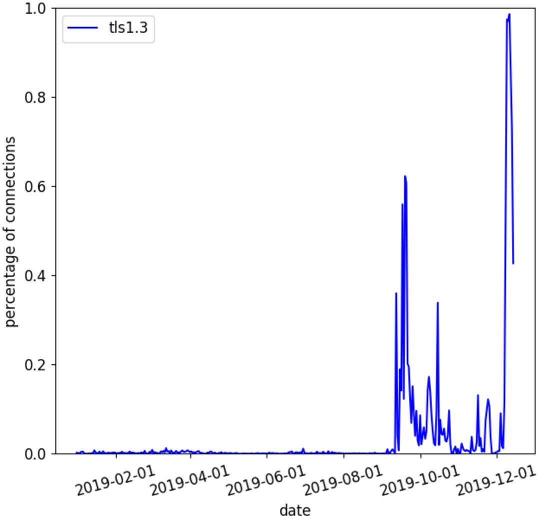
GENERAL TRENDS



MALWARE'S TLS USAGE

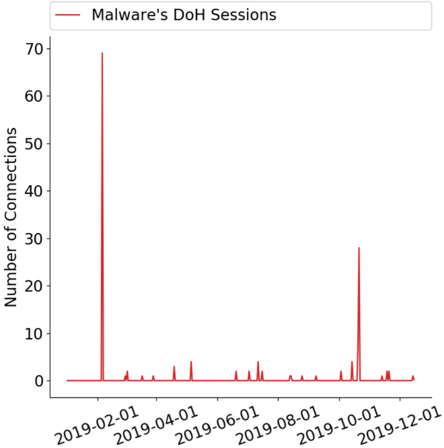


MALWARE'S TLS 1.3 USAGE



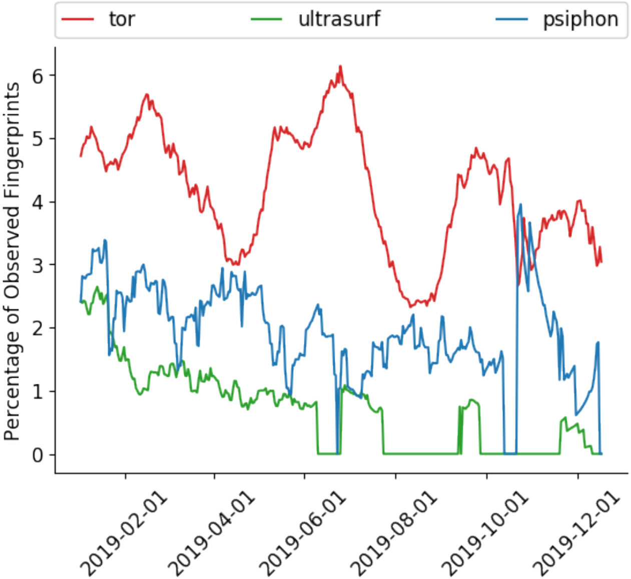
MALWARE'S DNS-OVER-HTTPS USAGE

- Currently, there are only a handful of malware-initiated DoH connections
- In the same dataset, we observed ∼1 million DNS flows per day



MALWARE'S ABUSE OF CENSORSHIP CIRCUMVENTION TOOLS

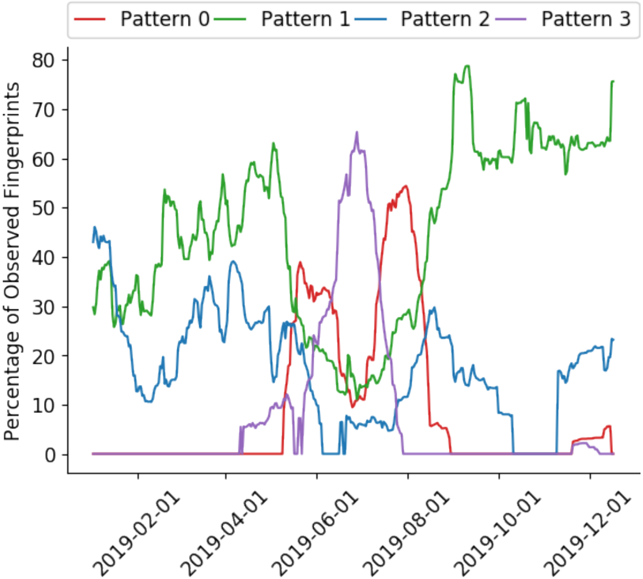
MALWARE'S ABUSE OF CENSORSHIP CIRCUMVENTION TOOLS



PSIPHON'S TLS FINGERPRINTS

- Randomly mimics Chrome/Firefox/Safari/iOS fingerprints
  - https://github.com/refraction-networking/utls/ → u_parrots.go
- Destinations typically use a word-based DGA
- Common fingerprints often omit popular extensions (`server_name`)

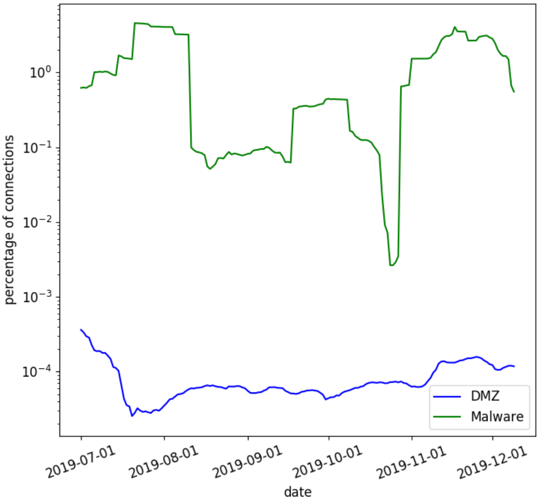
MALWARE'S ABUSE OF FINGERPRINT RANDOMIZATION



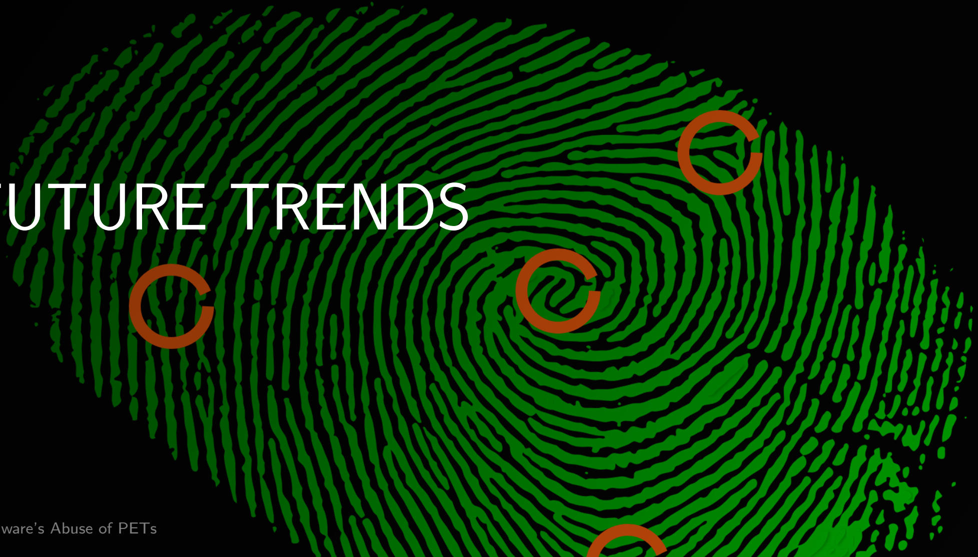
APPROXIMATE MATCHING

- `(0303)(009dc02c0005)((0000)(002b)(002d))`
- `(0303)(cca9000f0003c009)((0000)(002b)(002d))`
- Approximate matching can help!
  - Edit distance is an intuitive measure

MALICIOUS VS BENIGN TOR USAGE

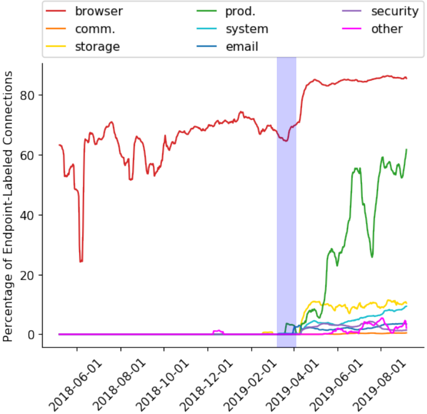


FUTURE TRENDS



TLS 1.3 - OS X

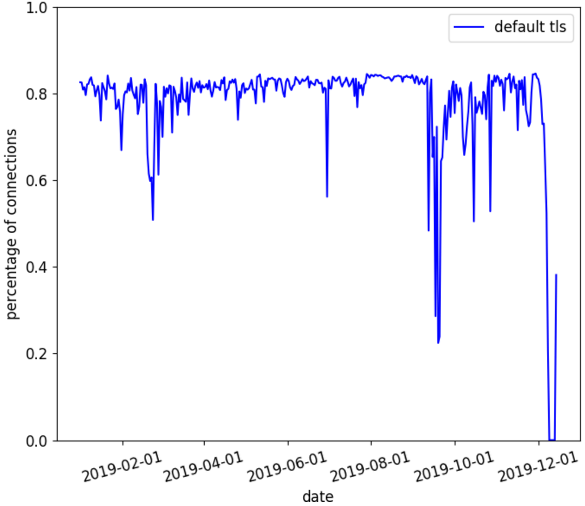
- Chrome/Firefox were initially the only applications supporting 1.3
- March 2019: MacOS 10.14.4/CoreTLS turn 1.3 on by default



DNS-OVER-HTTPS - Windows 10

- Enabling support sometime this year
- Will use the system's DNS configuration
- Will enforce DoH usage to DNS servers' supporting DoH

MALWARE AND SYSTEM DEFAULTS



CONCLUSIONS

- Malware continues to evade detection through:
  - TLS 1.0-1.3
  - Tor
  - More advanced obfuscation techniques
- As privacy enhancing technologies are turned on by default, malware's adoption will quickly follow
- https://github.com/cisco/mercury

THANK YOU!

cisco