cisco Live!

#CiscoLive

More Encryption, More Privacy, More Malware

David McGrew, PhD
Blake Anderson, PhD

BRKSEC-1898

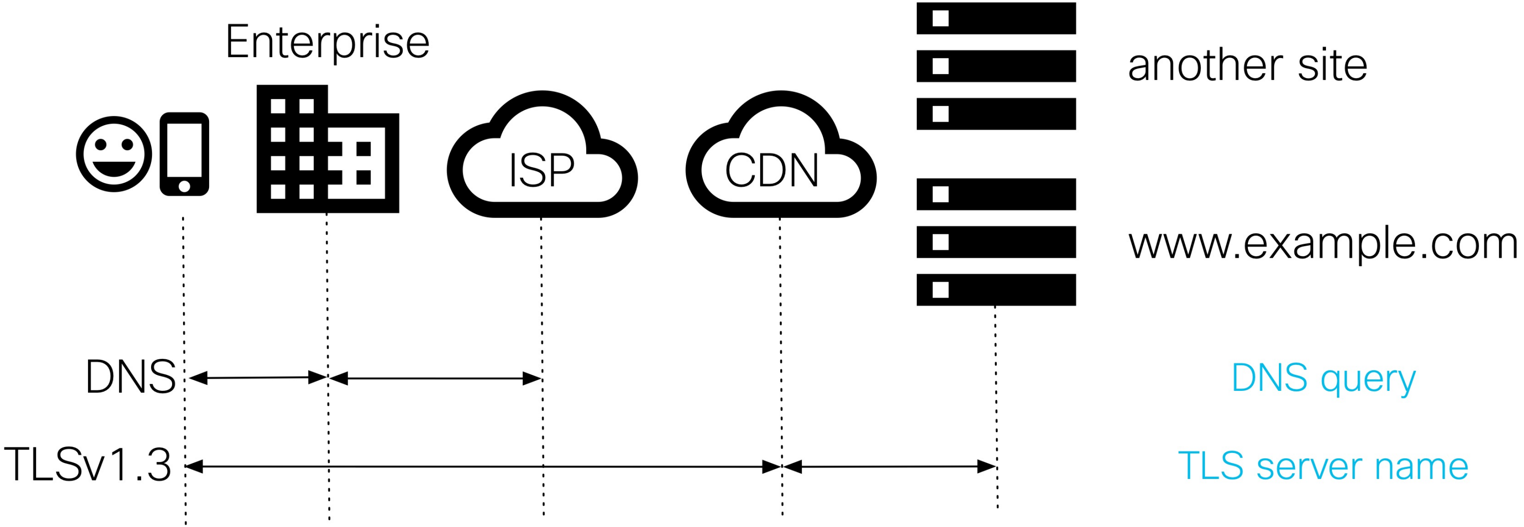
Agenda

- New encryption protocols
- How does this change visibility?
- Malware and Indicators of Compromise
- TLS Fingerprinting
- Conclusions

New Encryption Protocols

	Uses	Goals
TLSv1.3	Web Secure transport	Lower latency Only modern crypto Privacy against ISPs
DNS over HTTPS (DoH)	Domain name lookups	Privacy against ISPs
QUIC	Web Secure transport	Lower latency Multiplexing without blocking Connection migration

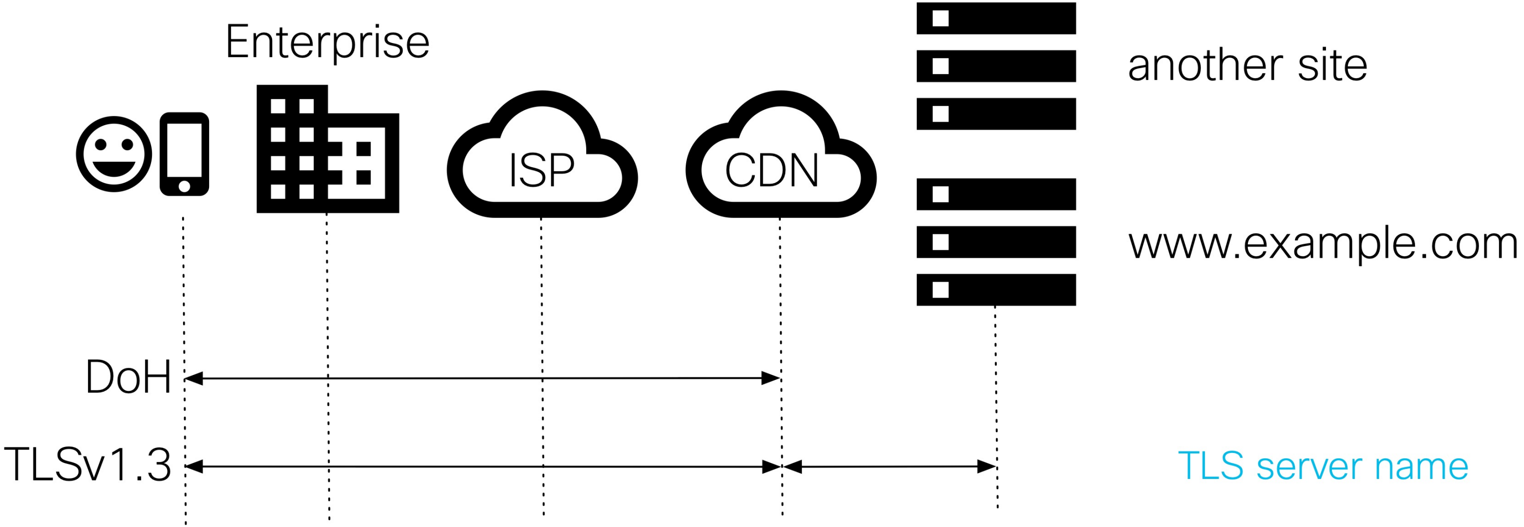
Secure Web with DNS



DNS query

TLS server name

Secure Web with DoH



How Does This Change Visibility?

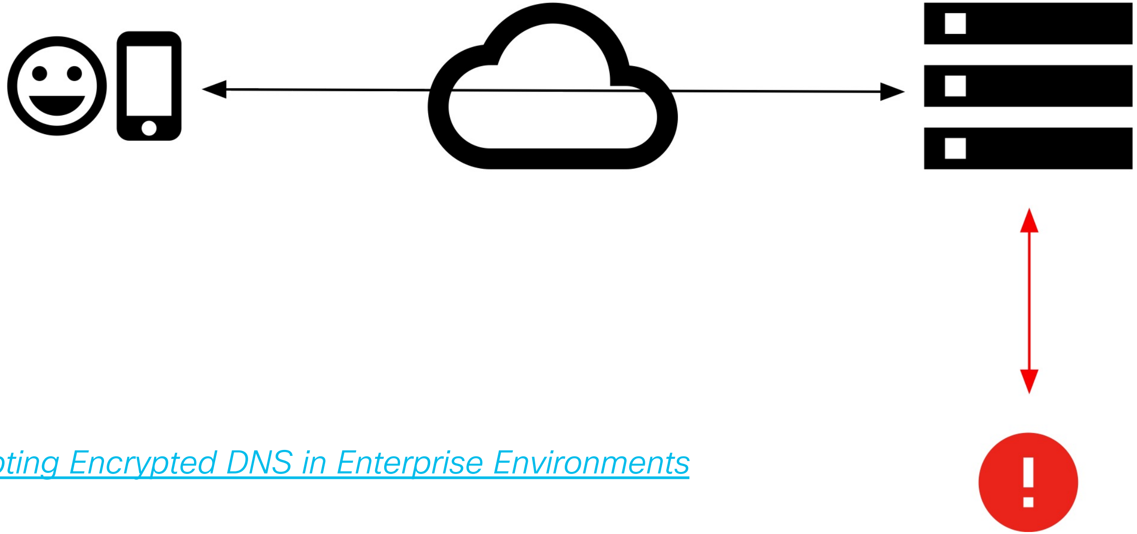
Server Name Visibility

	DNS Query	TLS Server Name	TLS Server Certificate
DNS + TLSv1.2	Clear	Clear	Clear
DNS + TLSv1.3	Clear	Clear	†Encrypted
DNS + QUIC	Clear	Clear	†Encrypted
DoH + TLSv1.2	Encrypted	Clear	Clear
DoH + TLSv1.3	Encrypted	Clear	†Encrypted
DoH + TLSv1.3 + ECH	Encrypted	Encrypted	†Encrypted

†Can be obtained through scanning

Communication Privacy Benefits and Pitfalls

Privacy benefit against
ISPs and local Govt

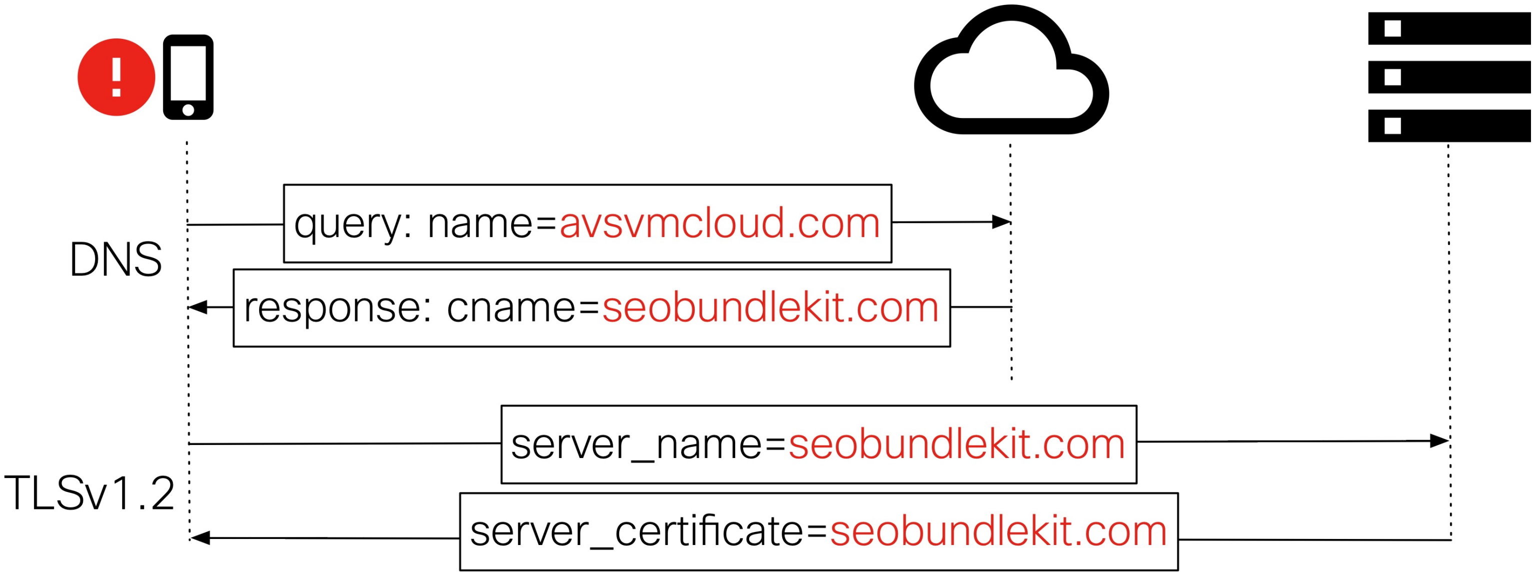


Threat against
Data Privacy

[Adopting Encrypted DNS in Enterprise Environments]()

Malware and Indicators of Compromise (IoCs)

Hunting Sunburst Malware



DNS

query: name=avsvmcloud.com

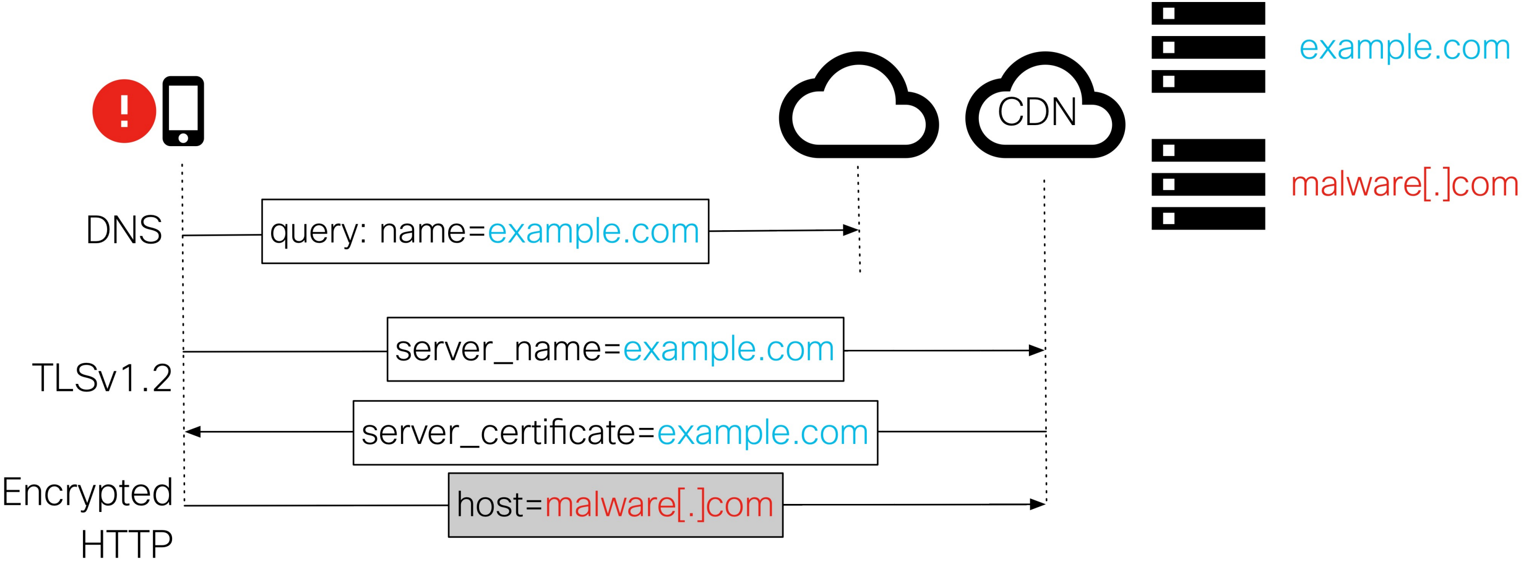
response: cname=seobundlekit.com

TLSv1.2

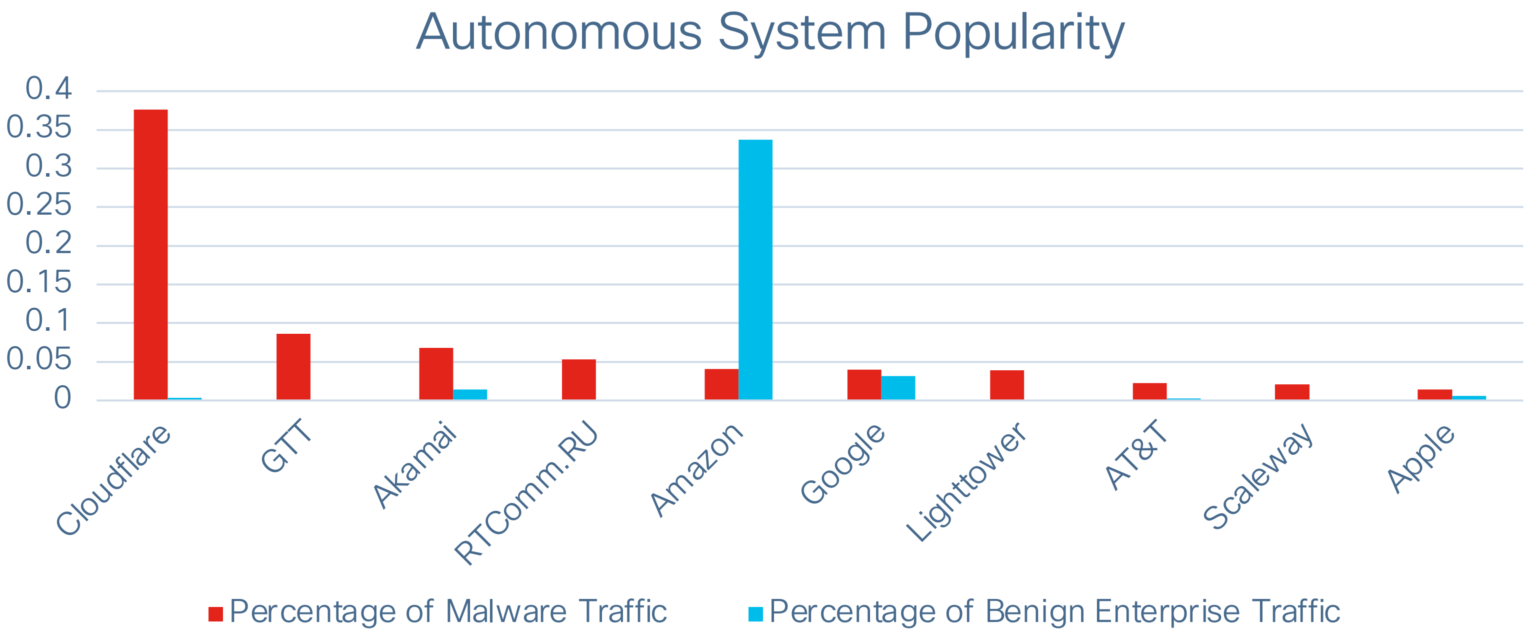
server_name=seobundlekit.com

server_certificate=seobundlekit.com

Malware Hiding in Domain Fronting

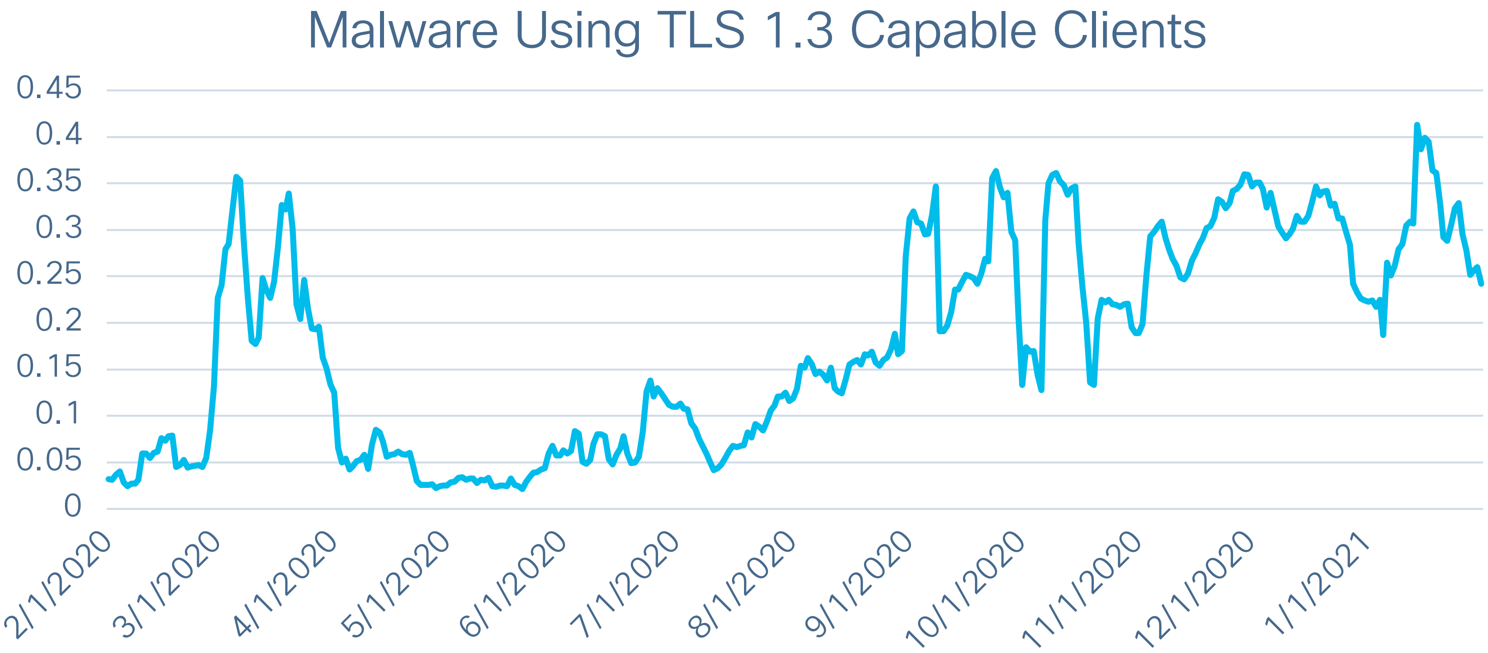


Malware Hosting Providers

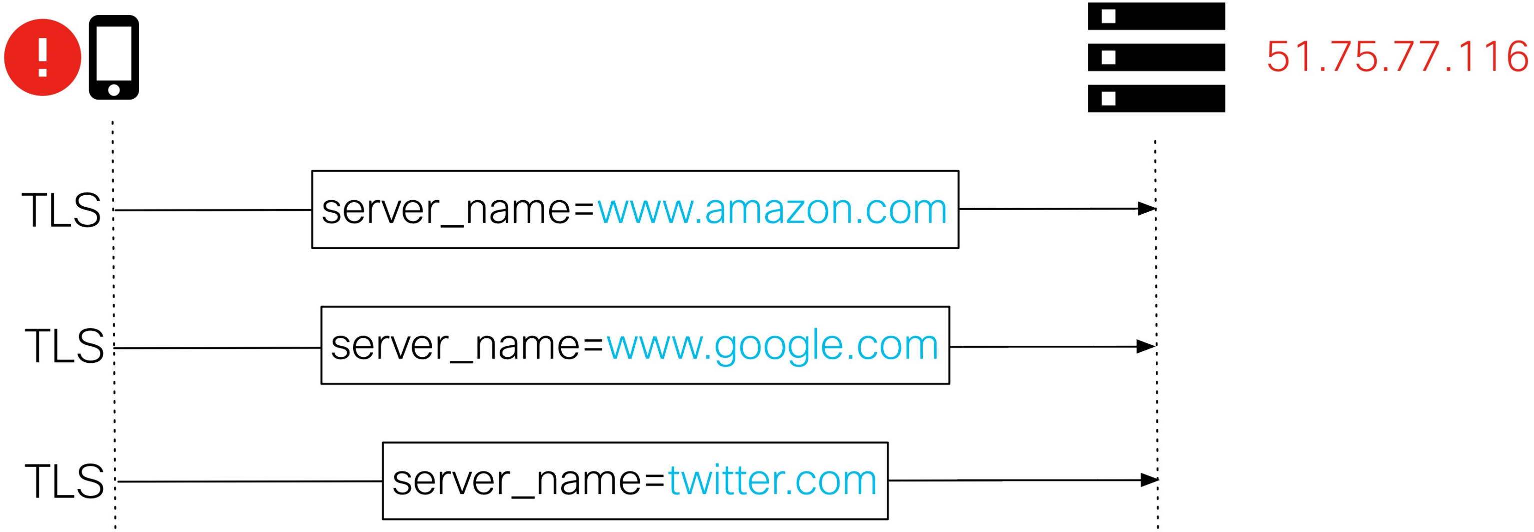


Malware's Continuing Shift to TLS

Source: Cisco Secure Malware Analytics (Threat Grid)



Malware Domain Faking



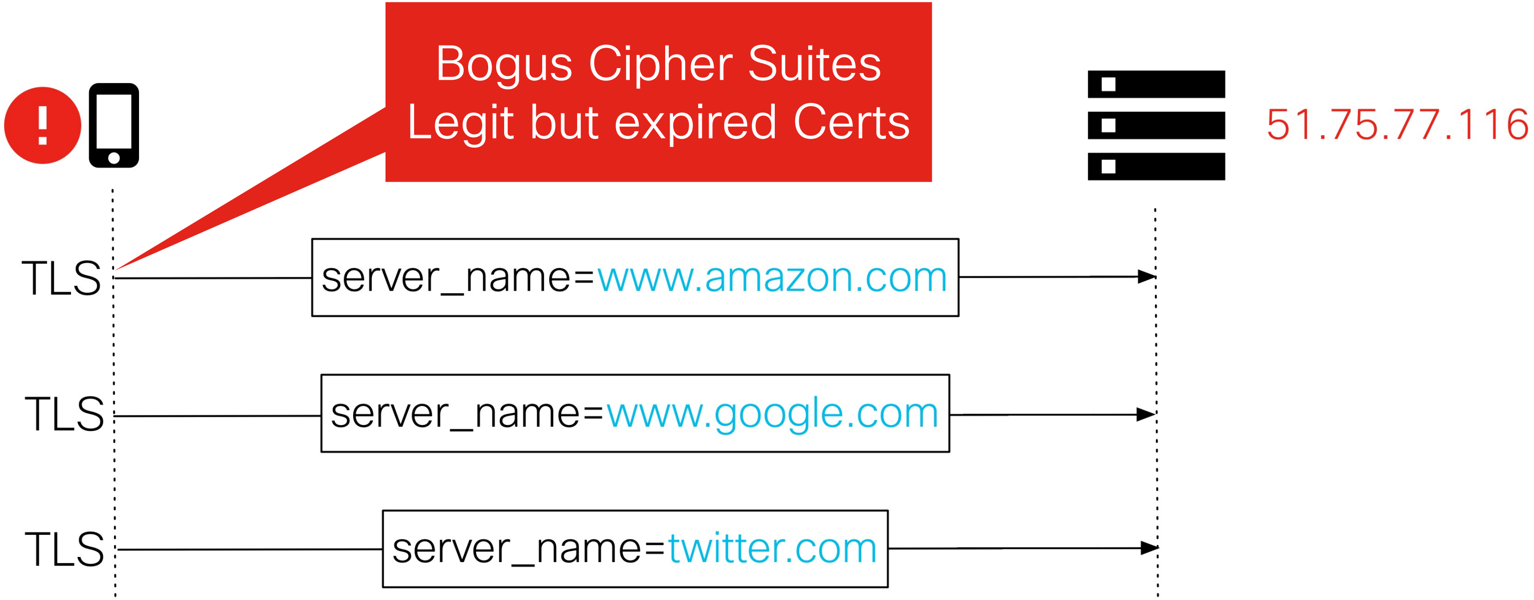
51.75.77.116

TLS server_name=www.amazon.com

TLS server_name=www.google.com

TLS server_name=twitter.com

Malware Domain Faking



Bogus Cipher Suites
Legit but expired Certs

51.75.77.116

TLS server_name=www.amazon.com

TLS server_name=www.google.com

TLS server_name=twitter.com

TLS Fingerprinting

Cisco TLS Fingerprinting with Destination Context

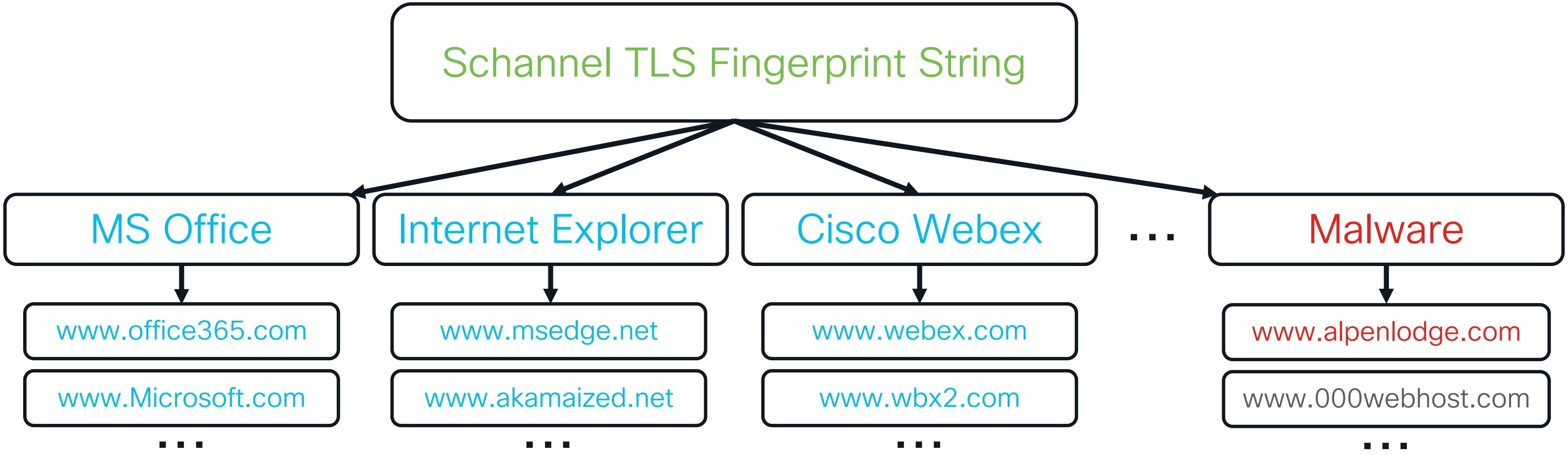
Inputs

- Fingerprint string from packet
- Destination Context
  - IP Address
  - Port
  - Server Name

Outputs

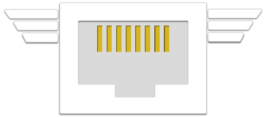
- Client process name
- Malware detection
- Operating System name

Destination Context Matters



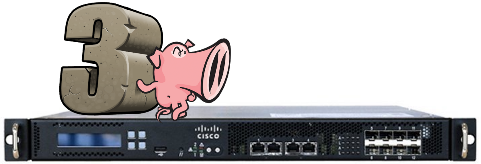
Conclusions

Cisco TLS Fingerprinting with Destination Context



https://github.com/cisco/mercury

Today



Firepower 7.1 Beta

Fall 2021

Conclusions

- More Encryption
  - TLSv1.3, QUIC, and DoH will see continued adoption
- More Privacy
  - Privacy benefits against ISPs and Governments (but not against malware, CDNs, advertisers, web trackers, etc.)
- More Malware
  - IoCs can be found in TLS Server Names and Server Certificates
  - Domain Fronting can hide IoCs
  - TLS Fingerprinting regains can identify malware, processes, and OSes

Continue your education

- Demos in the Cisco campus
- Meet the engineer 1:1 meetings
- Walk-in labs
- Related sessions

The bridge to possible

Thank you

cisco Live!

#CiscoLive