
black hat®
USA 2019
AUGUST 3–8, 2019
MANDALAY BAY / LAS VEGAS
#BHUSA @BLACK HAT EVENTS

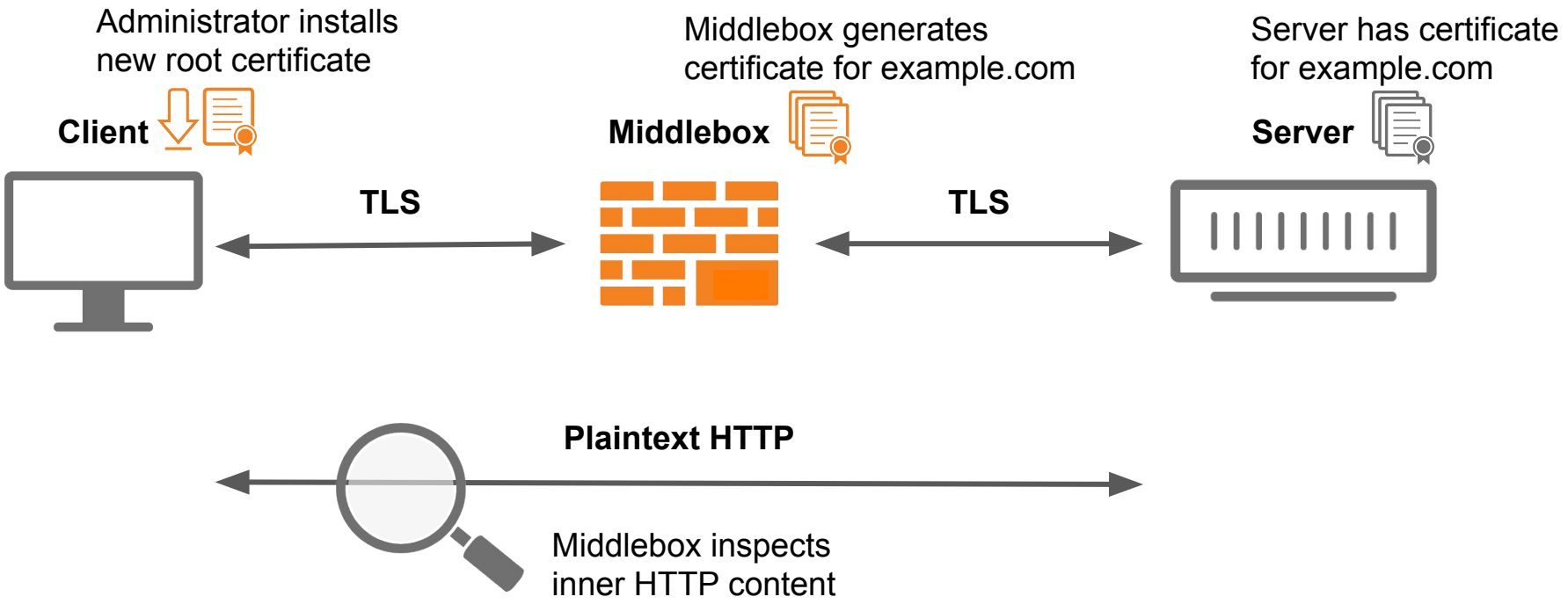
Monsters in the Middleboxes

Building Tools for Detecting HTTPS Interception

Luke Valenta
lvalenta@cloudflare.com
Twitter: @lukevalenta

Gabbi Fisher
gabbi@cloudflare.com
Twitter: @gabbifish

How HTTPS Interception Works



Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

Project Zero calls out Kaspersky AV for SSL interception practices

Using an SSL proxy that simplistically stored certificates, Kaspersky Anti-Virus left its users open to TLS certificate collisions.

By Chris Duckett | January 4, 2017 -- 01:25 GMT (17:25 PST) | Topic: Security

Blue Coat SSL Visibility Appliance contains multiple vulnerabilities

Vulnerability Note VU#498348

Original Release Date: 2015-05-29 | Last Revised: 2015-06-02

Kazakhstan government is now intercepting all HTTPS traffic

Kazakh government first wanted to intercept all HTTPS traffic way back in 2016, but they backed off after several lawsuits.

By Catalin Cimpanu for Zero Day | July 18, 2019 -- 19:38 GMT (12:38 PDT) | Topic: Security

Types of HTTPS Interception

Antivirus/Corporate/Government

Mac malware intercepts encrypted web traffic for ad injection

Posted: October 24, 2018 by Thomas Reed
Last updated: October 25, 2018

SEARCHAWESOME

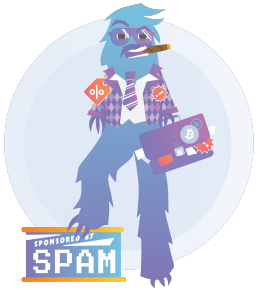
- Censorship

Alert (TA15-051A)

Lenovo Superfish Adware Vulnerable to HTTPS Spoofing

Original release date: February 20, 2015 | Last revised: September 30, 2016

Malware



- Inject ads
- Steal private data

Types of HTTPS Interception

Antivirus/Corporate/Government

- Detect malware
- Detect C&C traffic
- Detect exfiltration
- Anti-terrorism
- Censorship

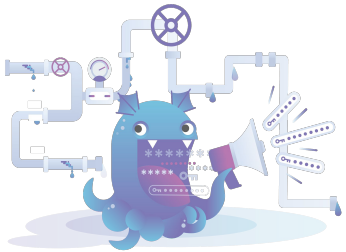
Vulnerability Report – CVE-2018-17612

Certificate Management Vulnerability in Sennheiser HeadSetup

Hans-Joachim Knobloch, André Domnick
Secorvo Security Consulting GmbH

Version 1.2
Date October 31, 2018

Leaky Proxies



- Product features
- Convenience

Types of HTTPS Interception

Antivirus/Corporate/Government

Incident report on memory leak caused by Cloudflare parser bug

23 Feb 2017 by John Graham-Cumming.

CLOUDTEST VULNERABILITY (CVE-2019-11011)

By Akamai InfoSec June 17, 2019 10:00 AM

0 Comments

Ticketbleed (CVE-2016-9244)

Ticketbleed is a software vulnerability in the TLS/SSL stack of F5 BIG-IP appliances allowing a remote attacker to extract up to 31 bytes of uninitialized memory at a time.

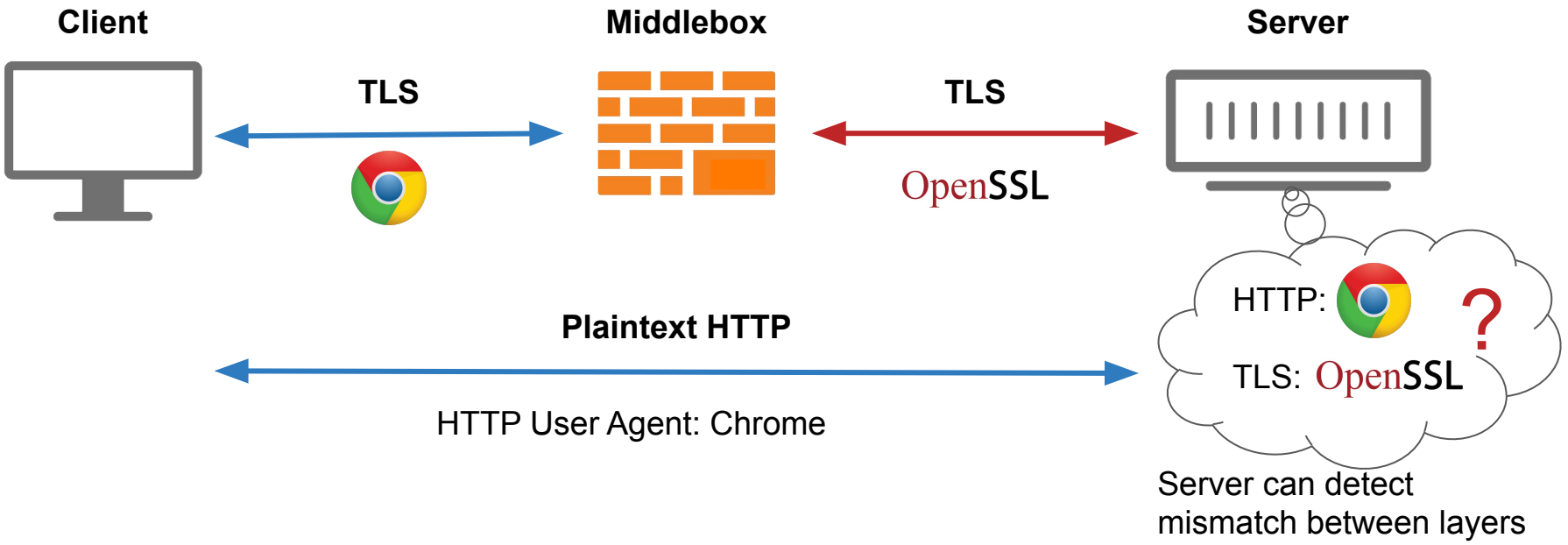
Malware

- Inject ads
- Steal private data

Reverse Proxies

- Security
- Performance
- Reliability

Detecting HTTPS Interception [Durumeric et al., 2017]



Identifying HTTP and TLS Clients

HTTP

Parse User Agent Header

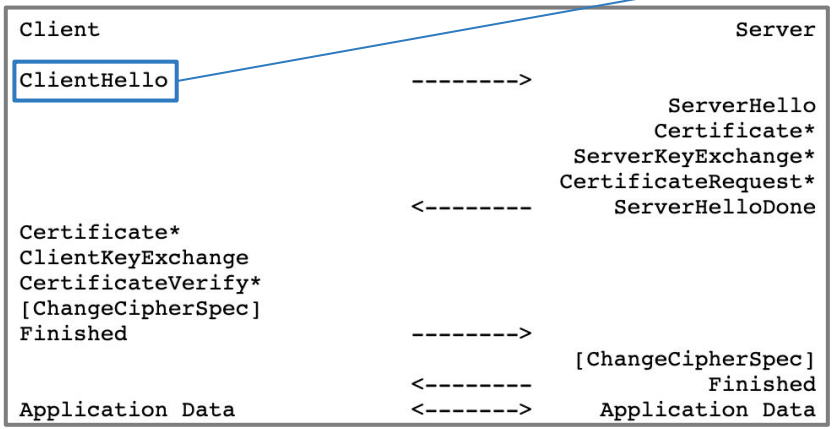
```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.100 Safari/537.36
```

TLS

No identifying field is present in the protocol. Instead, use known techniques for fingerprinting browsers based on TLS Client Hello.

1. [Ristić; 2009]
2. [Majkowski; 2012]
3. [Brotherston; 2015]
4. [Anderson, McGrew; 2016]
5. [Durumeric et al.; 2017]
6. [Althouse & Atkinson, Atkins; 2017]
7. [Frolov, Wustrow; 2019]
8. [...and others]

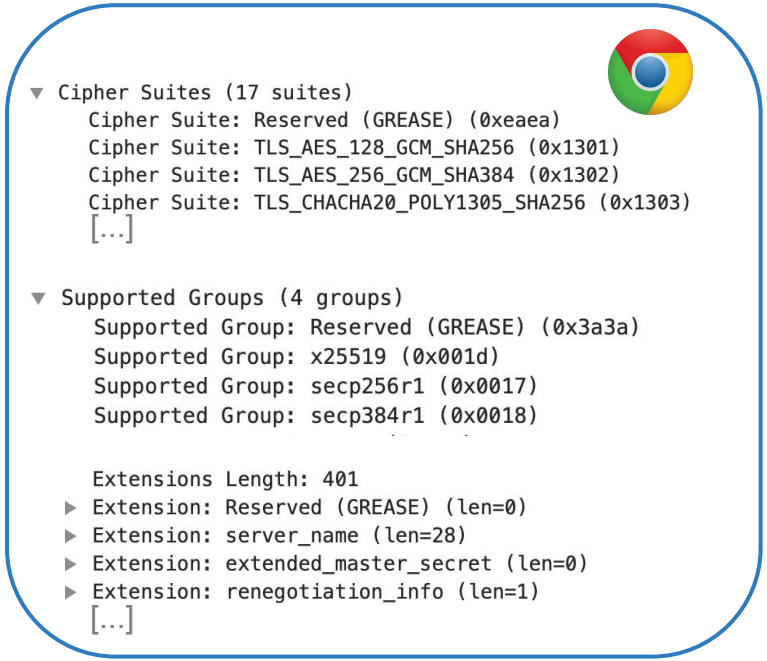
TLS Handshake (RFC 5246)

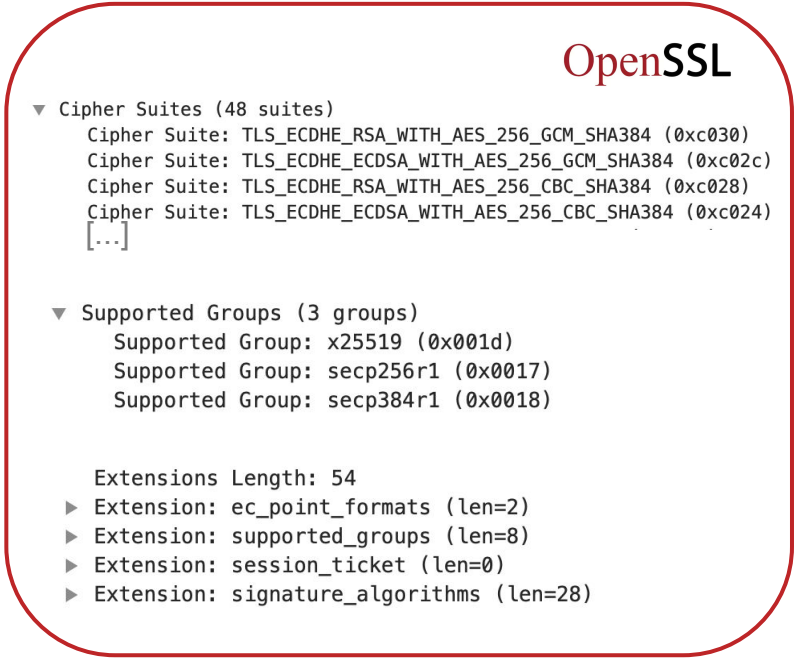



```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

TLS libraries tend to keep these fields the same!

TLS Fingerprinting based on Client Hello

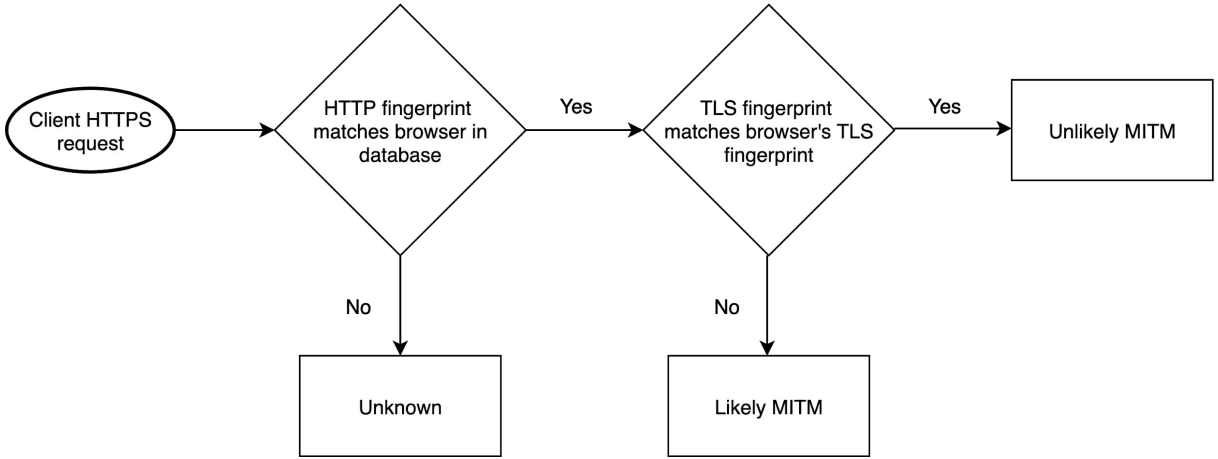




HTTPS Interception Detection Process

1. Build database of HTTP and TLS browser fingerprints

2. Check HTTP and TLS fingerprints of incoming requests against database



MITMEngine: HTTPS Interception Detection Library

Open sourced at https://github.com/cloudflare/mitmengine. PRs welcome!

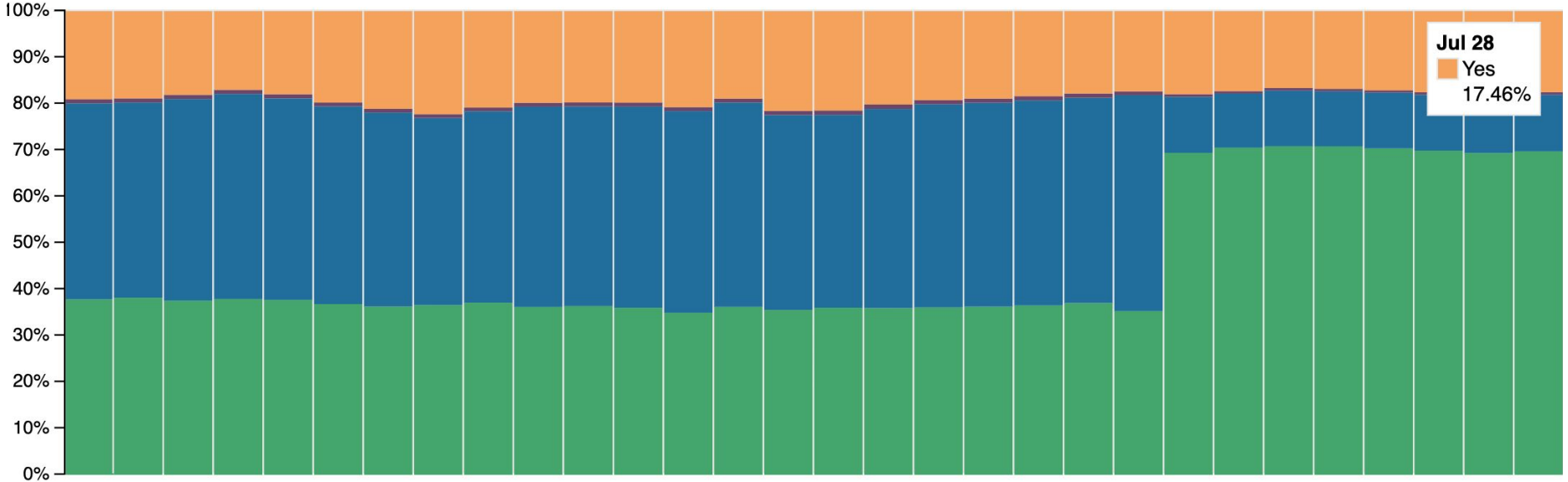
- Goal #1: Maintainability
  - Fingerprints quickly go stale with browser updates
  - Time-consuming to generate new fingerprints manually
  - Goal is to automatically generate ground truth fingerprints from Cloudflare's network
- Goal #2: Flexibility
  - Currently support a flexible fingerprint format to model a variety of browser behavior
  - Plan to add support for other TLS fingerprint formats (JA3, tlsfingerprint.io)
- Goal #3: Performance
  - The system should be fast enough to deploy at scale
  - Currently deployed on a sample of Cloudflare traffic

MALCOLM: HTTPS Interception on Cloudflare's Network

Public dashboard located at https://malcolm.cloudflare.com.

- Provides insight into HTTPS Interception observed by Cloudflare
- Powered by MITMEngine
- Allows for filtering by OS, browser, HTTPS interception tool, etc.

MALCOLM: Overall HTTPS Interception Rates

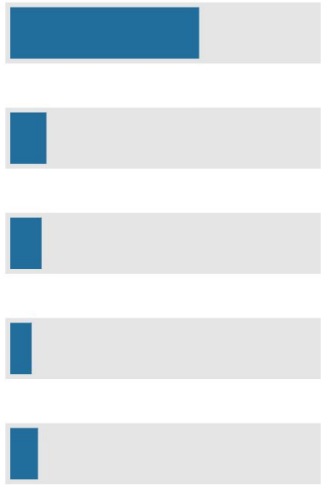


MALCOLM: HTTPS Interception by Browser/OS

BROWSER / USER AGENT

The following table displays recognized browsers.

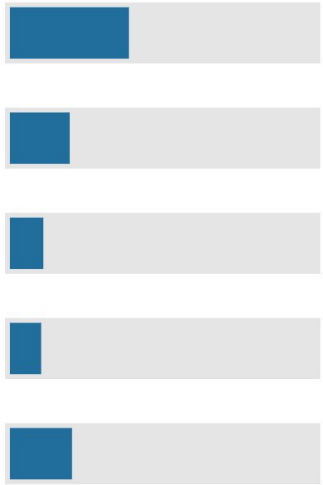
Chrome	61.81%
Safari	11.84%
IE	10.26%
Firefox	7.01%
Other	9.08%



OPERATING SYSTEM

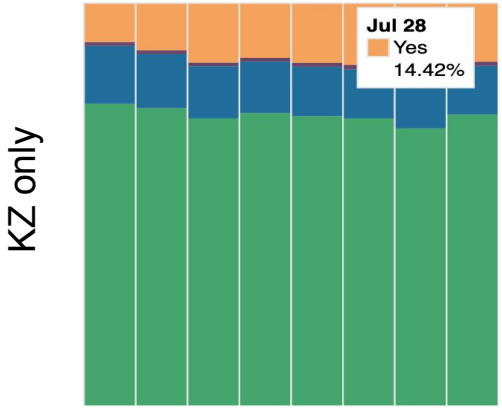
The following table displays recognized operating systems.

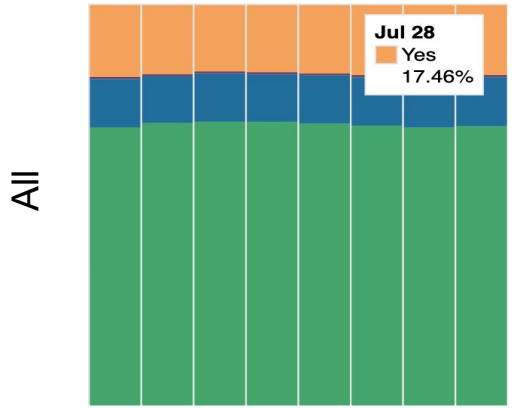
Android	38.95%
Windows 10	19.58%
iOS	10.93%
Windows 7	10.23%
Other	20.31%



Case Study: Kazakhstan

- Summary of incident w/ live results at https://censoredplanet.org/kazakhstan
- KZ chooses which domains to MITM based on SNI (server name indication)
- Encrypted SNI (eSNI) is on the horizon -- makes selective interception harder
- New MALCOLM feature (soon): filter MITM results by country





Black Hat Sound Bytes

TLS-terminating middleboxes pose serious threats to network security

Heuristics based on HTTP and TLS fingerprints can be effective at detecting HTTPS interception

Our new open source tool and public dashboard provide new insights into the state of HTTPS interception on the Internet

References

- [Ristić; 2009] HTTP client fingerprinting using SSL handshake analysis. https://blog.ivanristic.com/2009/06/http-client-fingerprinting-using-ssl-handshake-analysis.html
- [Majkowski; 2012] SSL fingerprinting for p0f. https://idea.popcount.org/2012-06-17-ssl-fingerprinting-for-p0f
- [Brotherston; 2015] TLS Fingerprinting: Smarter Defending & Stealthier Attacking. https://blog.squarelemon.com/tls-fingerprinting/
- [Anderson, McGrew; 2016]. TLS Fingerprinting in the Real World. https://blogs.cisco.com/security/tls-fingerprinting-in-the-real-world
- [Durumeric et al.; 2017] The Security Impact of HTTPS Interception. https://jhalderm.com/pub/papers/interception-ndss17.pdf
- [Althouse, Atkinson, Atkins; 2017]. TLS Fingerprinting with JA3 and JA3S. https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967
- [Frolov, Wustrow; 2019]. Tlsfingerprint.io
- [Raman et al.; 2019] Kazakhstan's HTTPS Interception. https://censoredplanet.org/kazakhstan