# How I Learned to Stop Worrying and Love TLS

## Encryption, your SIEM and how it will all change.

Johannes B. Ullrich Ph.D.

Dean of Research, STI

jullrich@sans.edu

SANS Technology Institute

The best. Made better.

# About Me

- Dean of Research,
  SANS Technology Institute
- SANS Internet Storm Center
  https://isc.sans.edu
- Created DShield.org
- SANS Institute Fellow
- Past: Physicist, Web Developer
- Living in Jacksonville, FL


SANS Technology Institute

# Outline

- SIEM Data Sources affected by encryption
- How are we dealing with it today
- How is it about to change?
- What you can do about it.

SANS Technology Institute

# Network Data and SIEMs

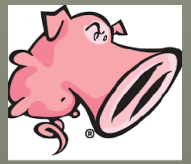
- Many SIEMs focus on host based events
- Great tools for collection them:
  - Syslog
  - Sysmon
  - File Beat…
- Lots of valuable data

# Why Bother With Network Data

- Host based data often requires agents / special configuration of host
- What about IoT, BYOD and other misc endpoints?
- Host based data may be manipulated by the attacker
- Network events are often indicative of what we worry about (e.g. data loss)
- Tends to be easy to collect (?)

# Typical Sources of Network Data

- Full packet capture
  - Can be expensive
  - But quite valuable for IR
- Network Traffic Summaries
  - Most of the value of full pcaps, but cheaper
- IDS Data
- Netflow

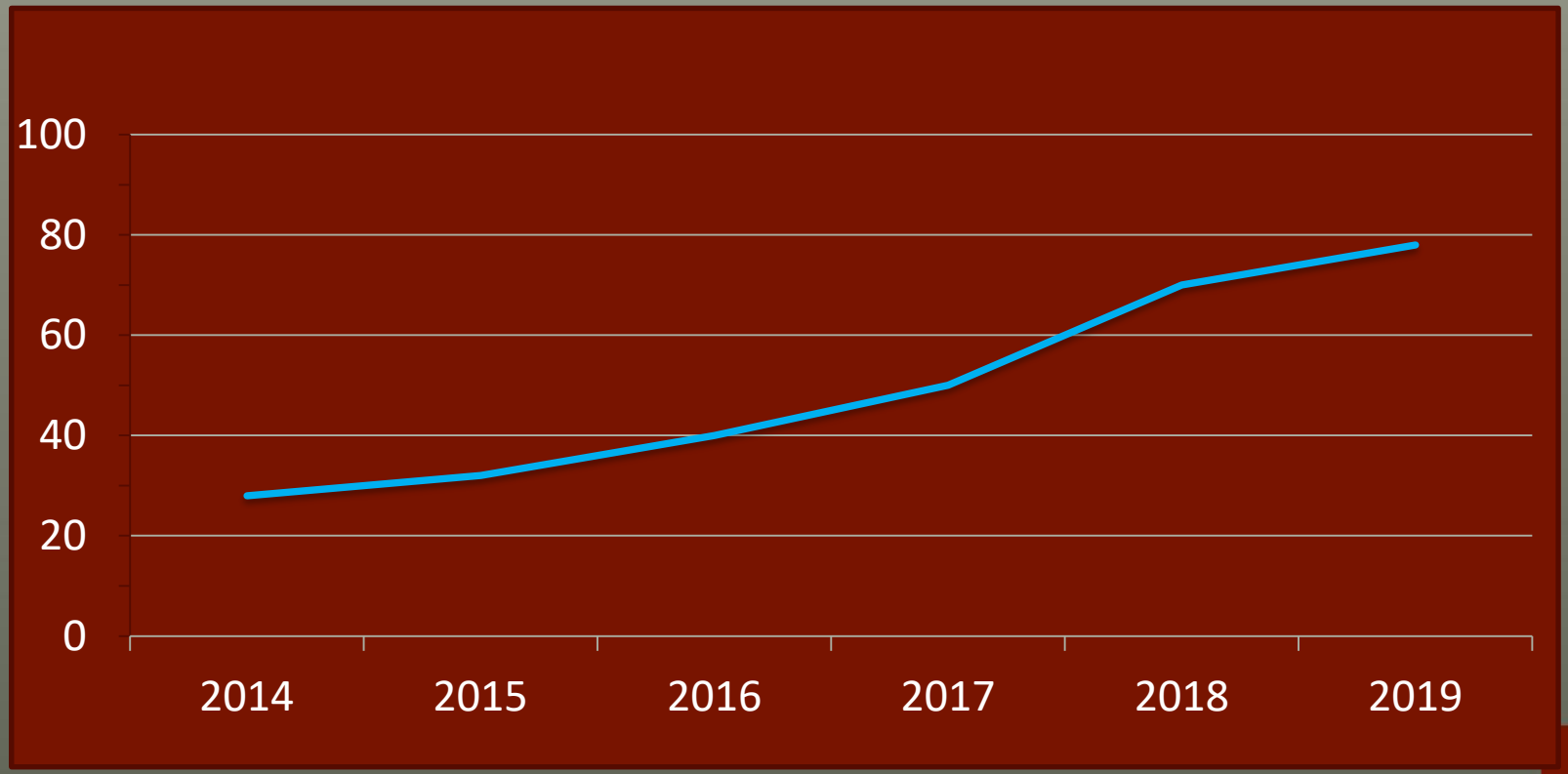



# What's the Problem with Network Data?

- One chance to collect it. Packet loss is common
- Encryption!
- NAT / DHCP. IP Address may not relate to physical system
- Cost of collecting full PCAPs:

| Network Speed | Data / Day |
|---|---|
| 1 Gbit | 1-10 TBytes |

# TLS Everywhere




Data: Firefox Telemetry

SANS Technology Institute

# How to “crack” Encryption

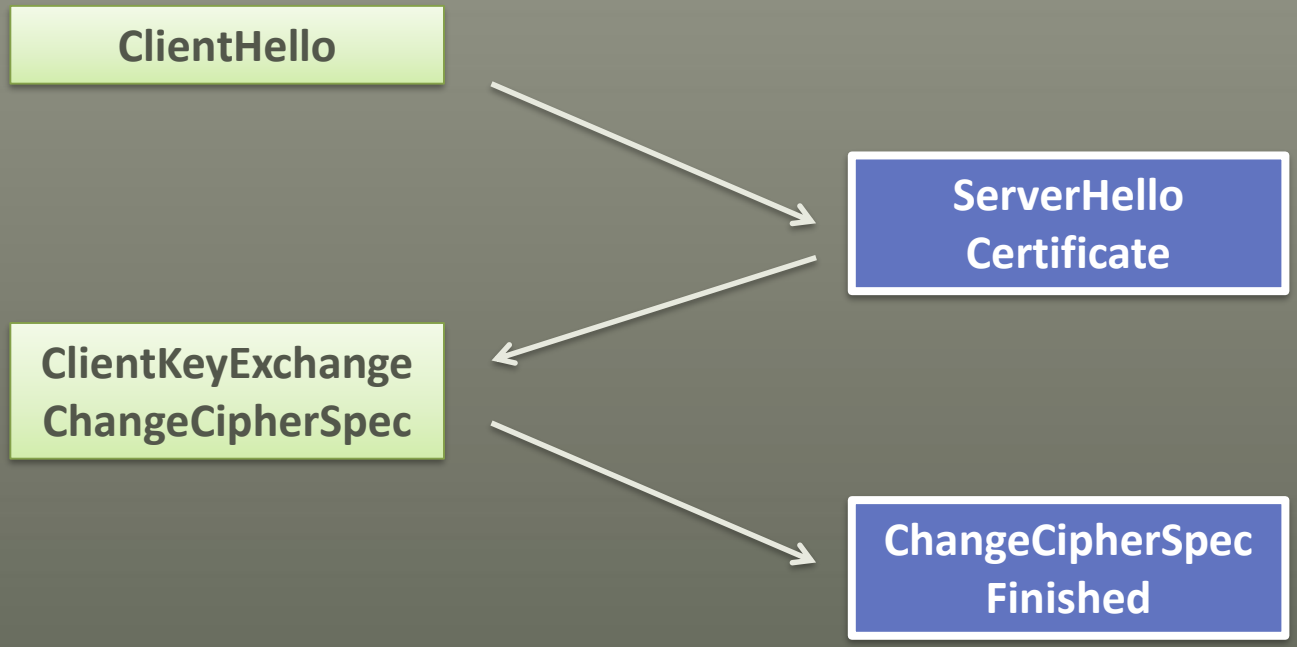
- TLS Primer
- Passive decryption appliances
- Proxies
- End Point Solutions
- Don’t …

SANS Technology Institute

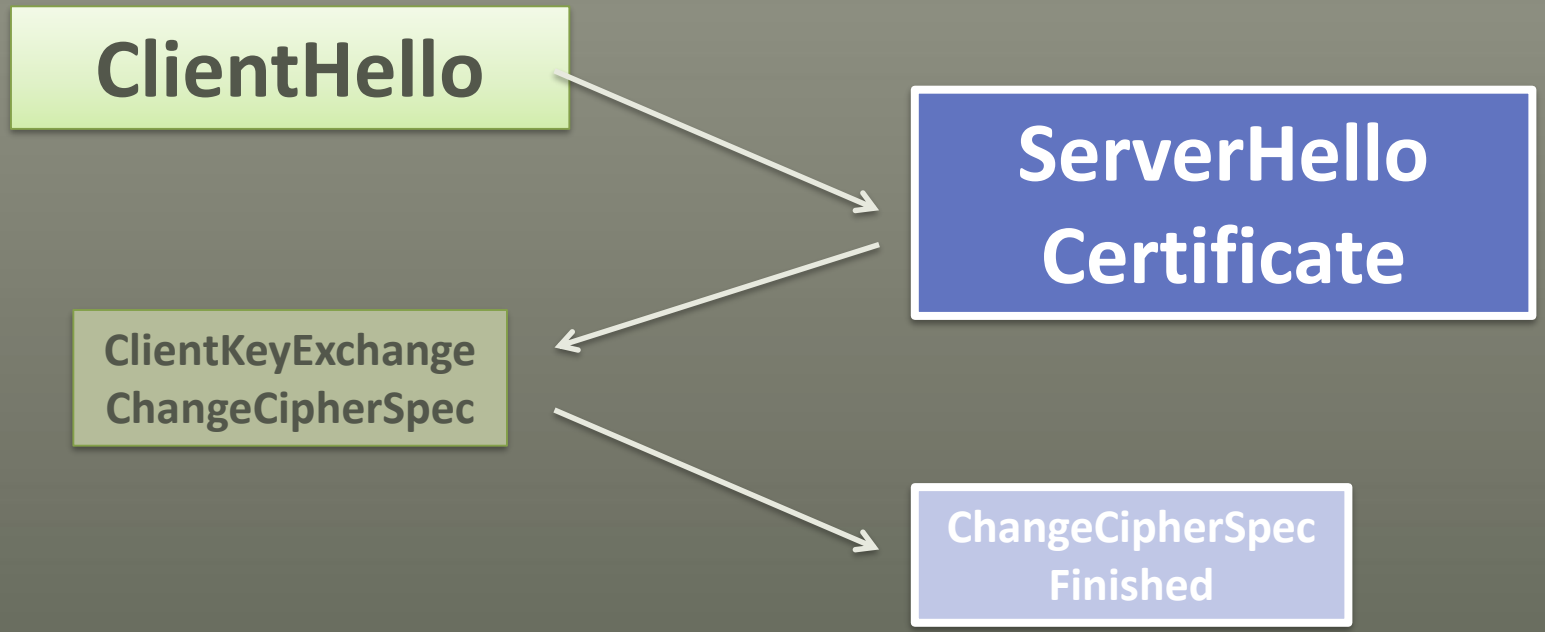
# TLS Primer

- SSL/TLS combines the scalability of public/private keys with the efficiency of symmetric encryption standards
- Very flexible to adjust to different requirements
- Can authenticate, encrypt and protect integrity
- Wide support
- But… easy to mess up

# TLS Handshake



# TLS Handshake



# JA3: TLS Fingerprinting

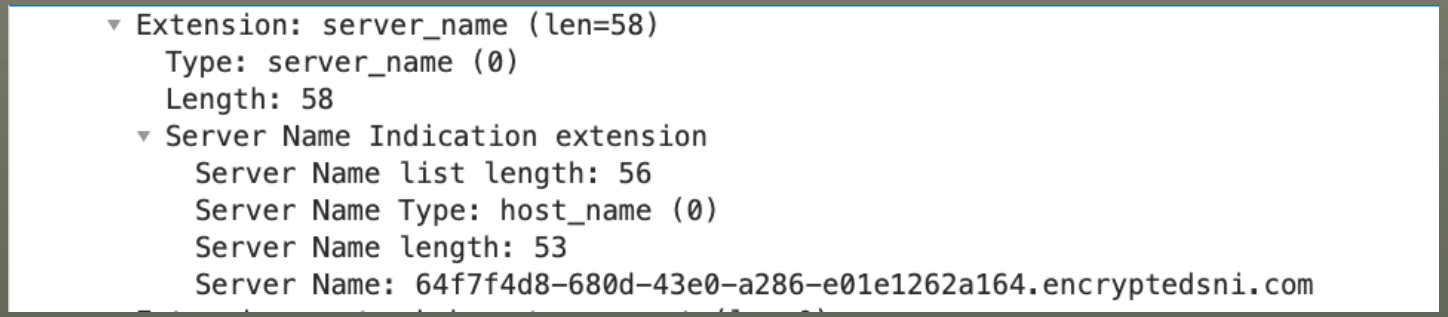
- Created by Salesforce (2017)
- Open Source. Python library, Zeek module
- BroSysmon to automate hash mapping
- Distinguishes two Fingerprint hashes
  - Client (JA3): md5(TLS Version, Ciphers, Extensions, EllipticCurves, EllipticCurvePointFormats)
  - Server (JA3S): md5(TLS Version, Cipher, Extension)

# Client Hello

- Supported TLS Versions
- Ciphers supported by client
- Various encryption parameters supported
- ”Client Random”
- Server Name Indication
- Application Layer Protocol Negotiation

# Server Hello

- Selected TLS Version
- Selected Cipher
- ”Server Random”
- Certificate



# Passive Decryption Appliances

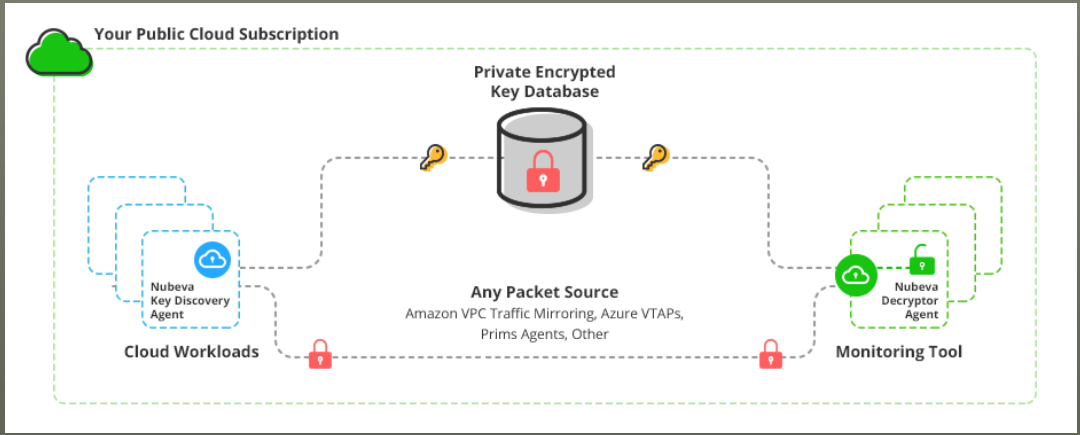
- Passive decryption no longer works with modern / well configured TLS
- Diffie Hellman Keyexchanges are now universally used and decrypting the key exchange will no longer reveal the “premaster secret”
- Only way to make them work is to collect premaster secrets from end points: Requires agent.

# Proxies

- Proxies essentially launch a MiTM attack against TLS
- Works well. But requires that end points trust the proxies certificate authority: Special endpoint configuration required
- Can add substantial (> 100ms) latency / break some modern web applications
- But proxies are a great source of logs for your SIEM

# End Point Solutions

- Proxies on end point intercepting requests
- Browser plugins
- End point configuration options
- And more…



# But what if we just don't bother?

- We can still get some data for our SIEM:
  - SNI host names
  - Client Hello / Server Hello Fingerprints
  - Certificates (including issuers)

SANS Technology Institute

# What can we learn from SNI?

- Hostname user is about to connect to
- Can be used to compare to block lists / IoC feeds
- DOES NOT HAVE TO BE RIGHT (domain fronting)
- Should also show up in DNS queries

# SNI Related Queries

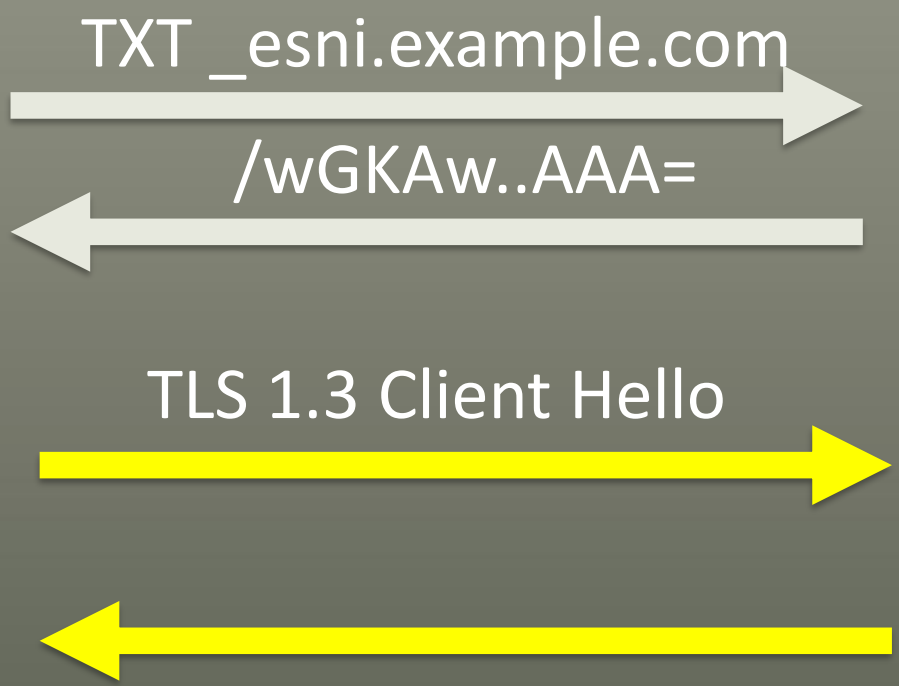
- “top new host names” (similar to DNS query)
- “unusual host name” (length, entropy)
- SNI is one of the more useful TLS Client Hello options
- But…

SANS Technology Institute

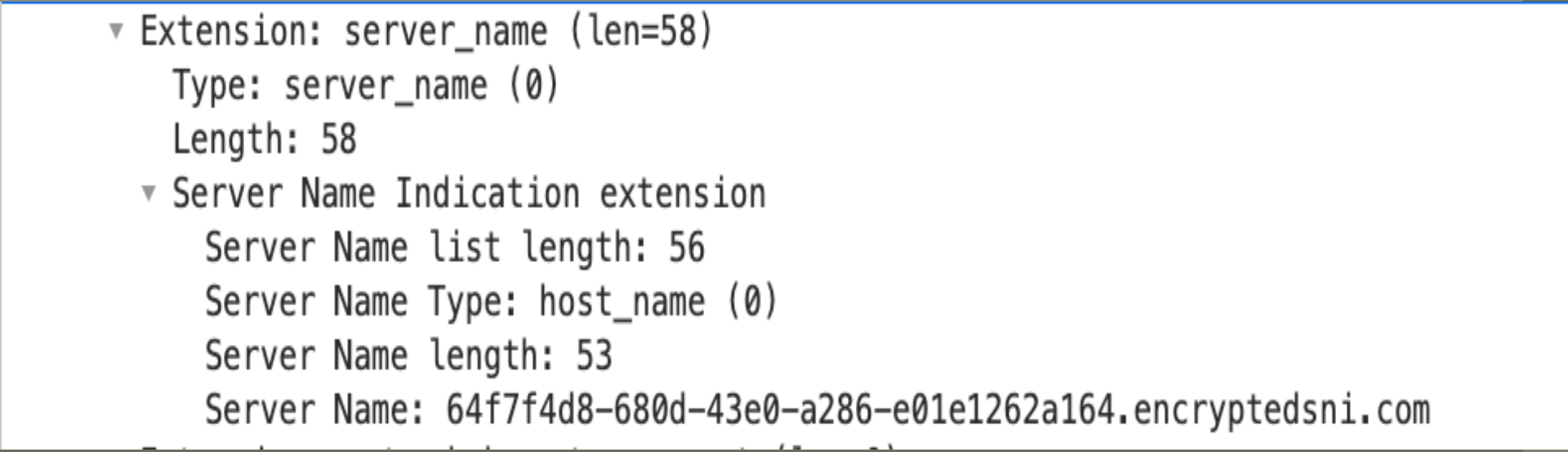
# TLS 1.3

- Perfect Forward Secrecy (PFS) now the default.
- Sharing server keys will no longer work (hasn't worked well without TLS)
- Encrypted Certificate. No longer easy to verify that SNI matches Certificate
- Key_share extension re-uses keys negotiated in prior connection. Can be negotiated out-of band (unlikely)
- Server Random indicates TLS 1.3 support even if TLS 1.1/2 is used.

# Encrypted SNI (eSNI)



# Normal Client SNI



# Encrypted Client SNI

```
▼ Extension: encrypted_server_name (len=366)
    Type: encrypted_server_name (65486)
    Length: 366
    Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  ▼ Key Share Entry: Group: x25519, Key Exchange length: 32
      Group: x25519 (29)
      Key Exchange Length: 32
      Key Exchange: 4906f76bdb96ed7f26b4e1b4649f4463190d7cd5067a3a27…
    Record Digest Length: 32
    Record Digest: 5e8afa4d04a05fa3b685ba29766ec81e0e872892ef7ac53d…
    Encrypted SNI Length: 292
    Encrypted SNI: 9f9d2b127889cf23f1069e5ddf9c5dcaeedd385d82694744…
```

# DNS?

- _esni.* TXT requests can be recorded / blocked
- These requests would still be visible
- But browsers may not use ESNI unless “TRR” (Trusted Recursive Resolver) is configured
- TRR = DNS over HTTPS

# Recent Attack: “Reductor” (Kaspersky)

- Patches Chrome/Firefox
- Adds ”userid” field to client random
- Attacker uses this to identify victims during TLS handshake
- Malware also has ability to install certificates

```
struct client_hello_system_fingerprint {
DWORD initial_xor_key; // First four bytes generated by original system PRNG function
DWORD predefined_const; // Set to 0x45F2837D
DWORD cert_hash; // Reductor's digital certificates hash
DWORD hwid_hash // Target's hardware hash
};
```

# How to detect “Reductor”

- Profile client random
- Look for fixed static strings
- Calculate entropy

# DoH Botnets: Godlua

- Linux DDoS Botnet July 2019
- First uses “regular” DNS query to lookup C2 domain: d.heheda.tk
- Uses Github/Pastebin for C2
- Uses DoH queries to retrieve TXT records that contain ciphertext

SANS Technology Institute

# GodLua DoH Query (QiHoo 360)

```
GET /dns-query?name=t.cloudappconfig.com&type=TXT
Host: cloudflare-dns.com
Accept: application/dns-json
```


{”Status”: 0,
“TC”: false …
“Question”: [{“name”: “t.cloudappconfig.com”, “type”: 16}],
“Answer”: [{
“name”:”t.cloudappconfig.com.”, “type”: 16, ”TTL”: 214,
“data”: “[ciphertext]”}
]}

# How to detect GodLua?

- DoH uses “odd” mime-type
- Requires TLS interception
- Usually, DoH uses “application/dns-message”
- Response in binary
- GodLua uses “application/dns-json”
- Response in JSON. More for debugging

# PsiXBot

- Identified August/September 2019 (Proofpoint)
- Earlier versions back to 2017
- FastFlux DNS Infrastructure
- RC4 encryption with hard coded static key
- Source of some sextortion emails and malspam
- Distributed via Spelevo EK

# PsiXBot DNS Query

```
GET /resolve?name=fnoetwotb4nwob524o.hk&type=A
Host: dns.google.com
Accept: application/dns-json
```

```
{"Status": 0,
 "TC": false …
 "Question": [{"name": "fnoetwotb4nwob524o.hk", "type": 6}],
 "Authority": [{
    "name":"fnoetwotb4nwob524o.hk.", "type": 6, "TTL": 599,
    "data": "a.dnspod.com. domainadmin…."}
]}
```

SANS Technology Institute

# How to Deal with DoH?

- TLS interception will still work
- Currently: bots use JSON format while normal DoH does not
- Block DoH
  - Deploy “use-application-dns.net” NXDOMAIN response.
  - Block DoH IPs/Hostnames
  - Enforce client configuration

# Or… just let it happen

- TLS interception will still provide data
- Parse responses and treat them like DNS logs
- Lots of other indicators for the activity
- Blocking it may just push it to a different channel (e.g. custom DoH)

# Thank You!

## Questions?

jullrich@sans.edu

http://isc.sans.edu

Daily Podcasts * Daily ”Diary” Posts * Data Feeds

Twitter: @johullrich / @sans_isc

SANS Technology Institute