Is Network Security Monitoring Dead in the Age of Encryption?

By Dallin Warne

Follow the presentation on your device: https://bit.ly/2MEPiyo

About the Presenter

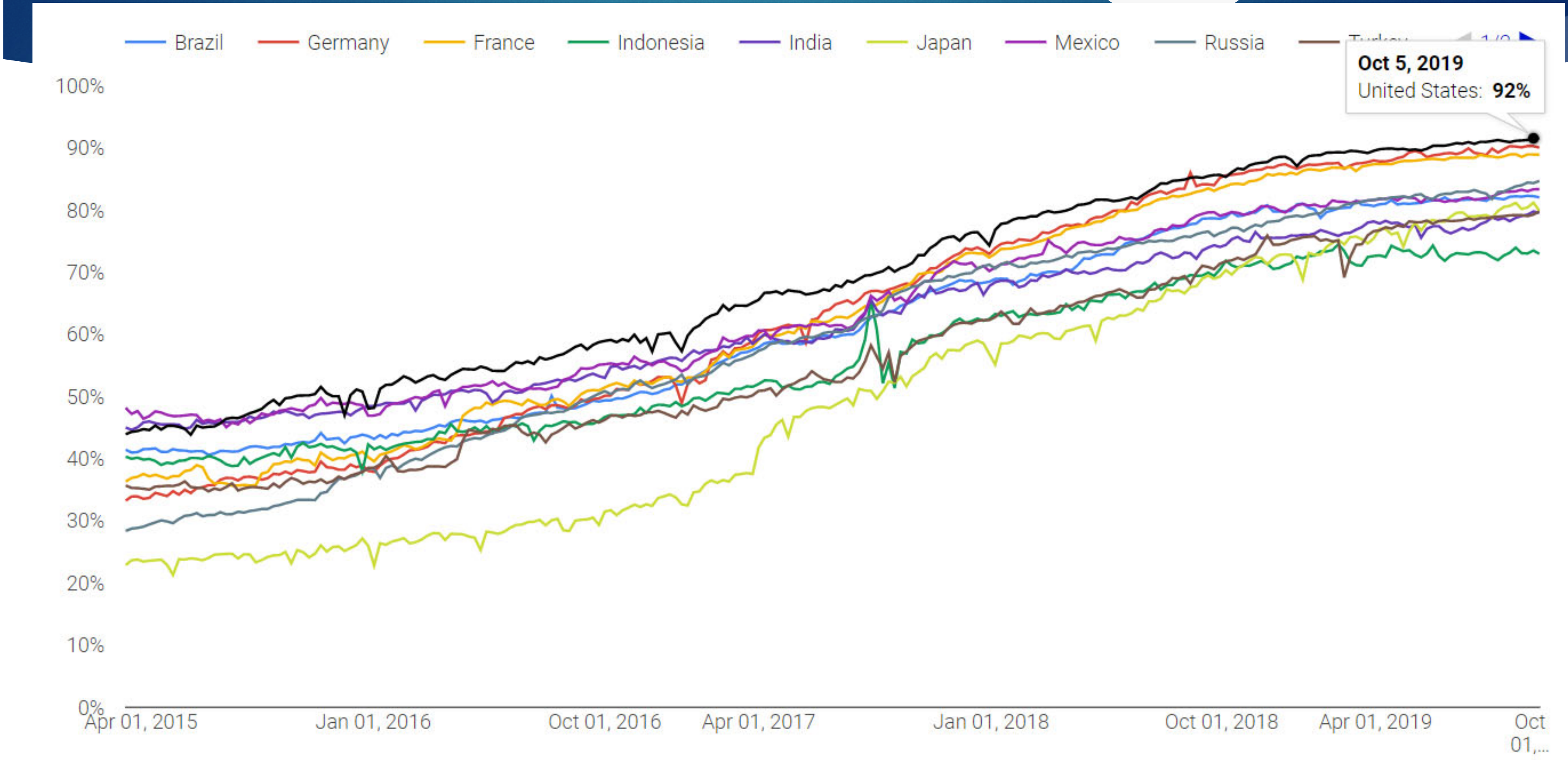
- Network operations center analyst (higher ed)
- Network Engineer (higher ed)
- Network security contractor (healthcare)
- Security engineer for multiple universities (higher ed) (present)

About the Audience

Encryption Landscape

- Encryption is prevalent, expected, and scrutinized
- Encryption costs are falling
  - Financial
  - Technical
    - Plenty of computing power
    - Becoming easier to implement

Percentage of pages loaded over HTTPS in Chrome by country



Is Network Security Monitoring Dead?

Is Network Security Monitoring Dead?

Encryption Effects

- Encryption reduces but does not eliminate network visibility
- Encryption changes an organization’s approach to network security monitoring

Reasons NSM Lives On

- Reason #1: Not everything is encrypted
- Reason #2: Network itself needs protecting
- Reason #3: Inventory and profiling
- Reason #4: NSM is device and application agnostic
- Reason #5: Auditing and forensics

Reason #1: Not everything is encrypted

- …Or will be in the near future
- And what’s unencrypted still has security value

Why?: Shadow, & Legacy, non-standard IT

Older protocols, older mindsets.

Poor IoT Security.

Expensive enterprise applications and hardware are hard to decommission.

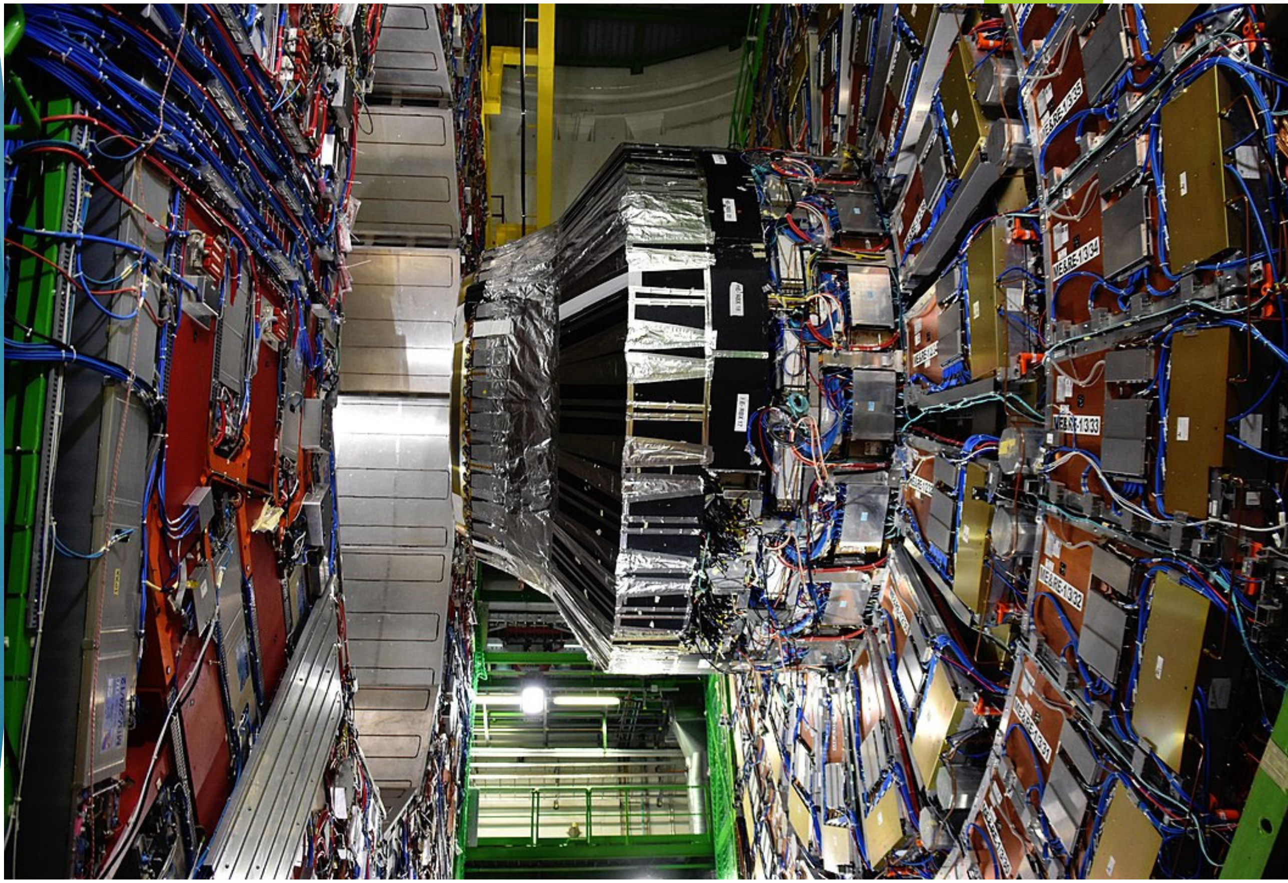


Photo credit: SimonWaldherr

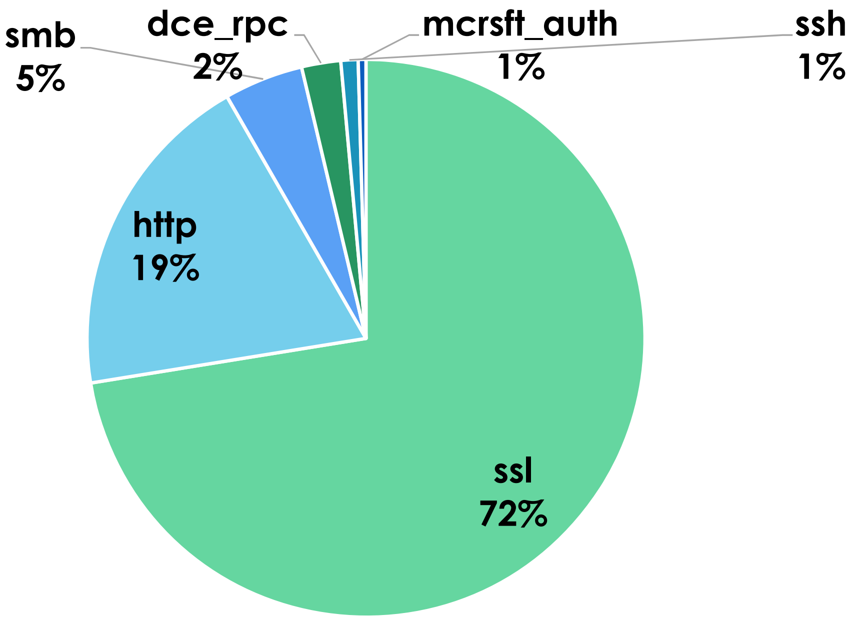
Why? (Cont): Encryption Barriers to Entry

- Still often hard to implement correctly
  - SMB, SNMP, syslog, internal apps/devices
- Low return on investment
  - Backend services (e.g. database connections)
- Performance hits
  - Tor
- Security not prioritized

State of Network Encryption

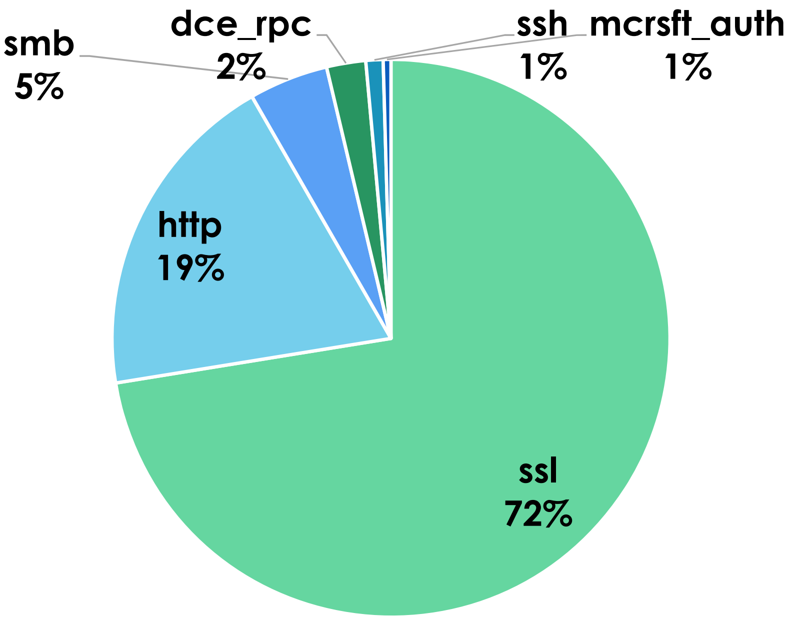
- 92% US web traffic is encrypted —Google
- 8% HTTP traffic is still *a lot* when looking at shear volume of web traffic
- Is web traffic all we care about?
  - Telnet, SNMP, SMB, DNS, SQL, FTP, DHCP, syslog, SMTP, TLS handshake…
  - TCP/UDP/ICMP headers, MAC addresses

Protocols by Bytes

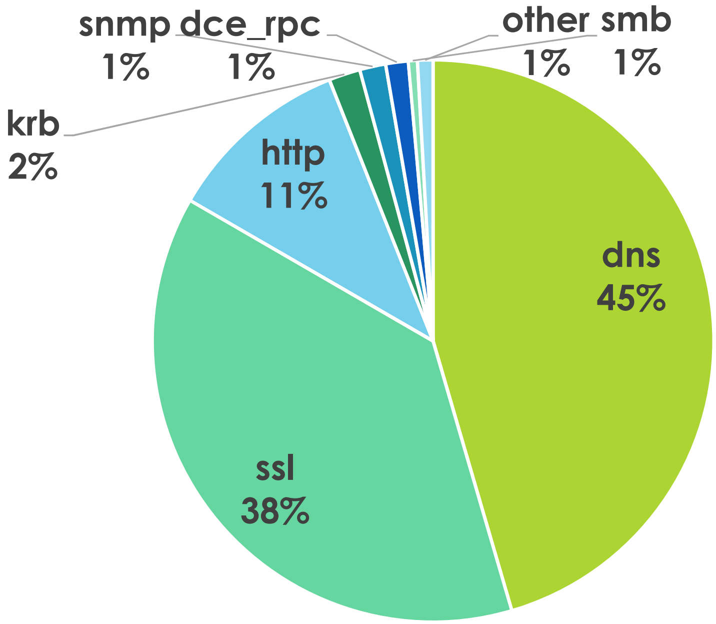


Protocol by Bytes

Protocols by Bytes & Session Count



Protocol by Bytes

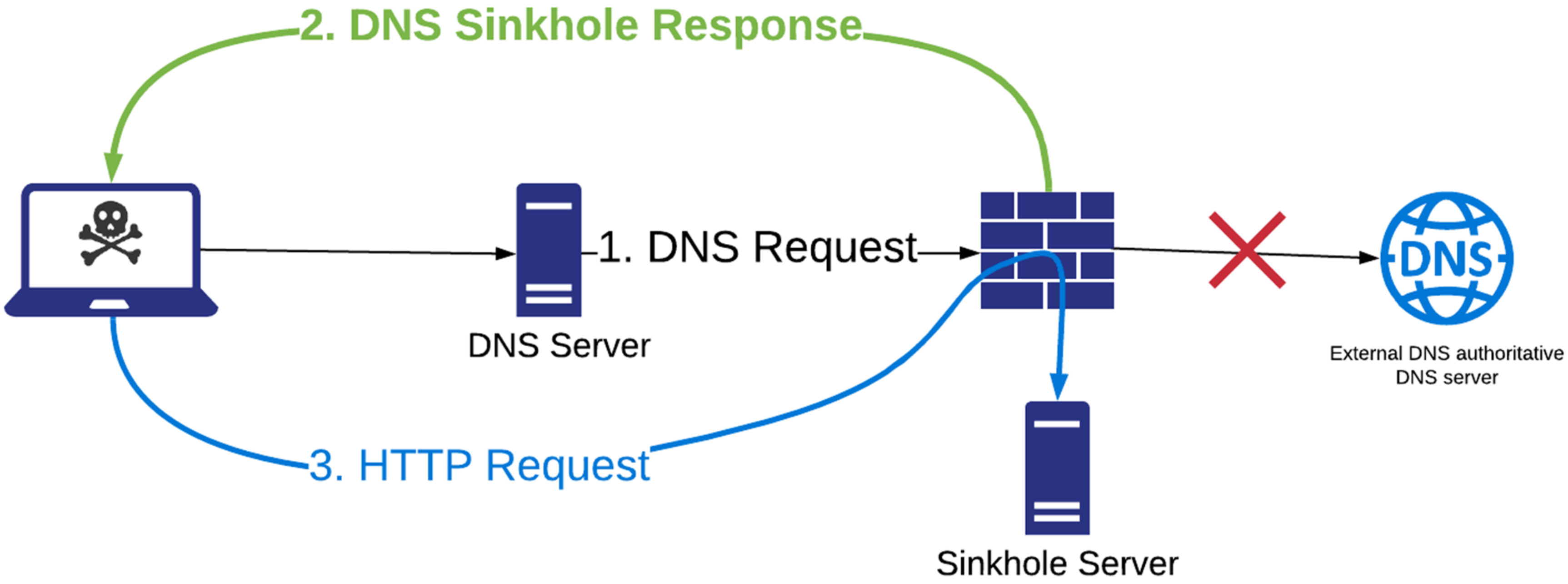


Protocol by Session Count

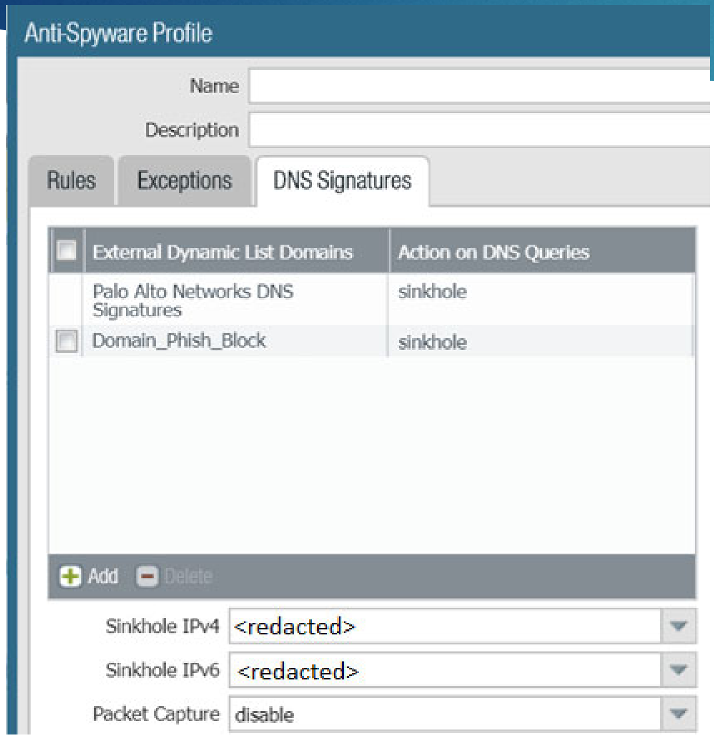
DNS

- Statistics & performance monitoring
- Detect machines bypassing approved DNS
- Identify new, malicious, or phishing domains
- Dynamically generated algorithm (DGA) domains
- Sinkhole bad domains
- DNS tunneling

DNS Sinkhole



Sinkhole Example

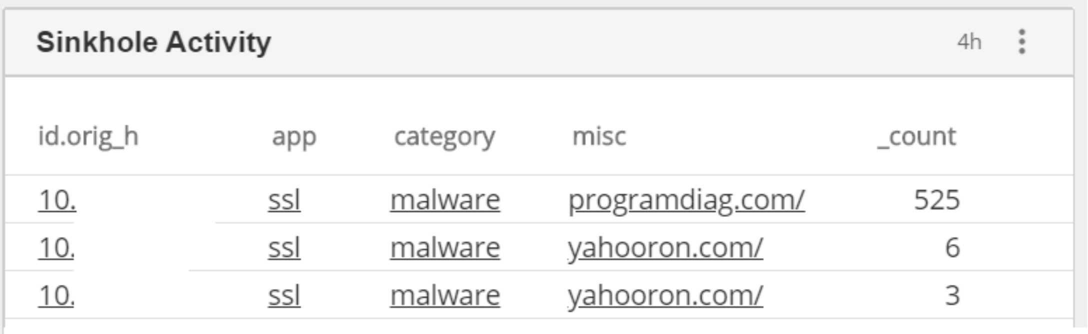


Anti-Spyware Profile

Name	
Description	

	External Dynamic List Domains	Action on DNS Queries
	Palo Alto Networks DNS Signatures	sinkhole
□	Domain_Phish_Block	sinkhole

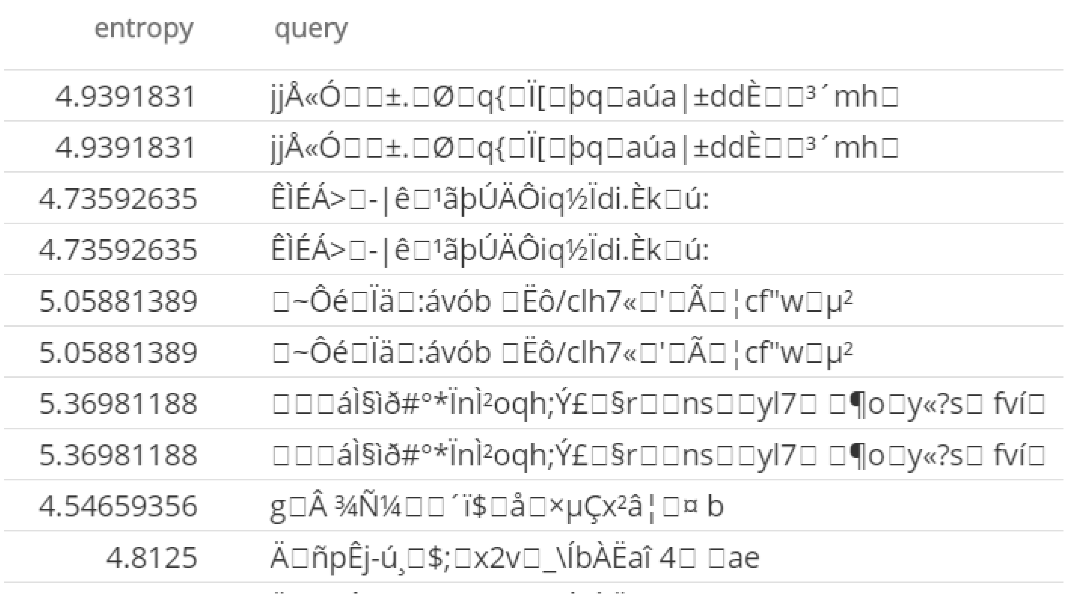
Sinkhole IPv4	<redacted>
Sinkhole IPv6	<redacted>
Packet Capture	disable



Sinkhole Activity

id.orig_h	app	category	misc	_count
10.	ssl	malware	programdiag.com/	525
10.	ssl	malware	yahooron.com/	6
10.	ssl	malware	yahooron.com/	3

DNS Detection Tunneling Example



entropy	query
4.9391831	jjÅ«Ó□□±.□Ø□q{□Ï[□þq□aúa|±ddÈ□□³´mh□
4.9391831	jjÅ«Ó□□±.□Ø□q{□Ï[□þq□aúa|±ddÈ□□³´mh□
4.73592635	ÊÌÉÁ>□-|ê□¹ãþÚÄÔiq½Ïdi.Èk□ú:
4.73592635	ÊÌÉÁ>□-|ê□¹ãþÚÄÔiq½Ïdi.Èk□ú:
5.05881389	□~Ôé□Ïä□:ávób □Ëô/clh7«□'□Ã□¦cf"w□µ²
5.05881389	□~Ôé□Ïä□:ávób □Ëô/clh7«□'□Ã□¦cf"w□µ²
5.36981188	□□□áÌ§ìð#°*ÏnÌ²oqh;Ý£□§r□□ns□□yl7□ □¶o□y«?s□ fví□
5.36981188	□□□áÌ§ìð#°*ÏnÌ²oqh;Ý£□§r□□ns□□yl7□ □¶o□y«?s□ fví□
4.54659356	g□Â ¾Ñ¼□□´ï$□å□×µÇx²â¦□¤ b
4.8125	Ä□ñpÊj-ú¸□$;□x2v□_\ÍbÀËaî 4□ □ae

Tool Analysis

Palo Alto Networks Firewall

- Anti-spyware DNS sinkholing
- DNS security (DGA, tunneling)
- IPS vulnerability protections

Zeek (formerly Bro)

- DNS.log
- DNS metrics and analytics
- DGA detection
- Tunneling detection

Honorable Mention: Pi-Hole

DNS-Over-HTTPS (DoH)

- Some controversy
- Can still maintain DNS visibility
- Attend “DNS and TLS Privacy and Security - Content Security Today and Tomorrow” session on Friday for more in-depth discussion

SSL/TLS

- Often clients try HTTP first
- Metadata analysis
- Server Name Indicator (SNI)
  - TLS 1.3 can encrypt SNI
    - Watch the adoption rate
  - Force downgrade
  - Block in DNS
- Certificate information
  - Common Name
  - Subject Alternative Names (SAN) from certificate
- JA3 hashes
- Encrypted Traffic Analytics

Palo Alto Botnet Example

Confidence	Source address	Description
4	10.0.0.20	Repeatedly visited (169) the same malicious URL webarteronline.com/
4	192.168.1.5	Repeatedly visited (48) the same malicious URL dprince.org/
4	192.168.0.9	Repeatedly visited (94) the same malicious URL connect360bd.com

Zeek SSL Log Example

cert_chain_fuids[0]	FrwPxxxxxxxxxxxxx
cert_chain_fuids[1]	F8HPyyyyyyyyyyyyy
cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
established	true
id.orig_h	192.168.1.5
id.orig_p	32450
id.resp_h	216.58.193.194
id.resp_p	443
issuer	CN=GTS CA 1O1,O=Google Trust Services,C=US
ja3	ebf5e0e525258d7a8dcb54aa1564ecbd
ja3s	cd5a8d2e276eabf0839bf1a25acc479e
next_protocol	h2
resumed	false
server_name	connectivitycheck.gstatic.com
subject	CN=*.google.com,O=Google LLC,L=Mountain View,ST=California,C=US
validation_status	ok
version	TLSv12

Tool Analysis

Palo Alto

- Vulnerability protection
  - e.g. Heartbleed
- URL log w/ site category
- Correlated events
- Botnet report

Zeek

- SSL.log, X509.log
  - Server names
  - JA3
- Certificate information

Value from Encrypted Sessions

- MAC Address
  - Vendor & Device profiling
- VLAN
- IP addresses
  - Threat intelligence
  - Geolocation
- Ports
  - Port scanners
- Protocols
- Bytes sent/received
- Time-based patterns
- IP-based patterns
- Metadata

Tool Analysis

Palo Alto

- Traffic log
- Resource & DoS protection
- Reconnaissance protection

Zeek

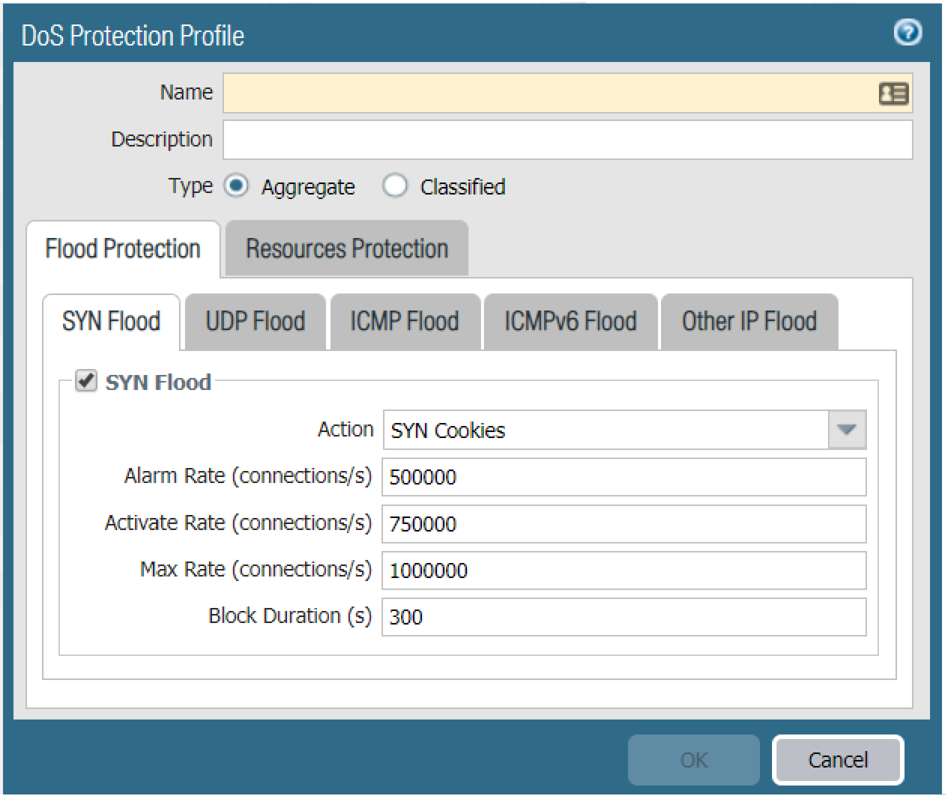
- Conn.log
- Weird.log
- Intel.log
- Protocol Anomaly log (DPD.log)
- Ssh.log

Reasons NSM Lives On

- Reason #1: Not everything is encrypted
- Reason #2: Network itself needs protecting
- Reason #3: Inventory and profiling
- Reason #4: NSM is device and application agnostic
- Reason #5: Auditing and forensics

Reason #2: Network Itself Needs Protecting

- Lower-layer protections
- Firewalling & proper network segmentation
- DoS & resource protection
- User/Device Authentication
- Don’t end up on blacklists



Name

Description

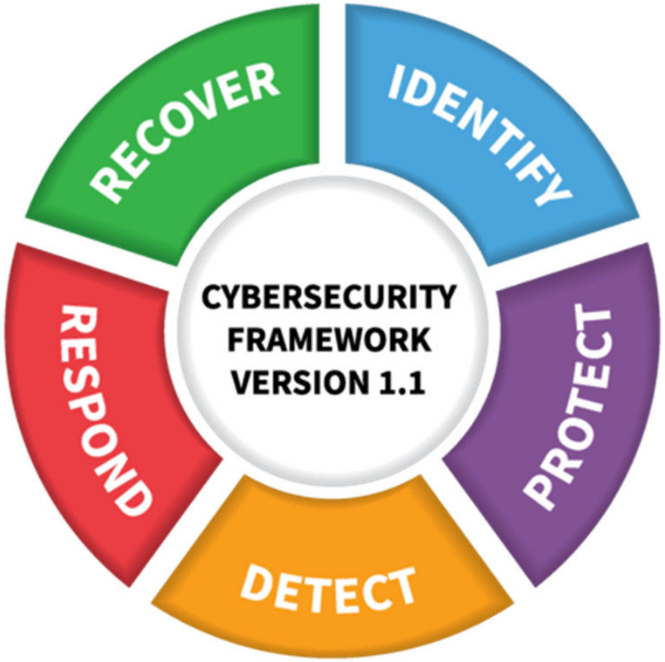
Type ● Aggregate ○ Classified

☑ SYN Flood

Action	SYN Cookies
Alarm Rate (connections/s)	500000
Activate Rate (connections/s)	750000
Max Rate (connections/s)	1000000
Block Duration (s)	300

Reason #3: Inventory and Profiling

- Cybersecurity Frameworks first step is inventory
  - External attack surface inventoried already by OSINT services and attackers
  - Perform reconnaissance on yourself
- You can't adequately protect what you don't know
- Frameworks have network recommendations



Reason #4: Device & Application Agnostic

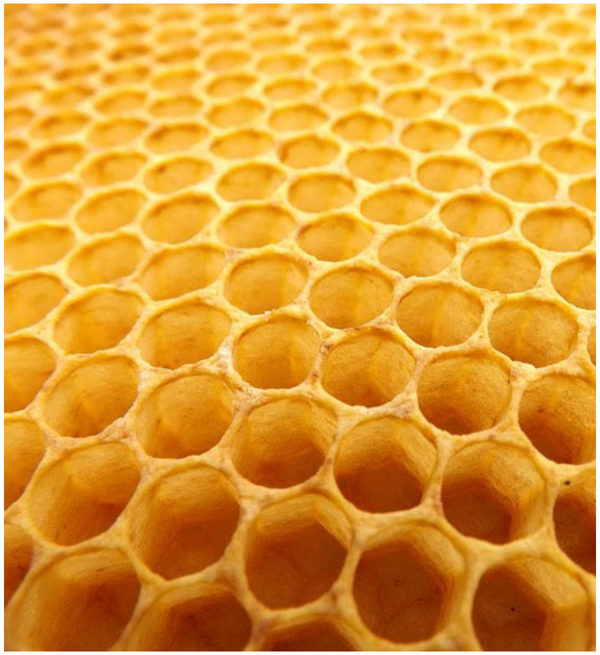
- Network protections are the same
  - It doesn’t matter if the login form is on your SSO page or a webcam login
- Normalize events
  - Minimal configuration in logging system
- Perhaps the closest you can get to protecting assets you don’t have visibility into
  - Shadow IT, decentralized IT, IoT, guests, network reputation

Reason #5: Auditing and Forensics

- Auditing:
  - Find misconfigurations or poor performance
  - Confirm you don’t have SMB open to the internet
  - Find all web servers serving content over HTTP instead of HTTPS
- Forensics
  - You will want any data to help paint a picture of what happened
  - Once a machine is popped, the trust in any endpoint reporting and logs drops significantly

Modern NSM Strategies

- Proper segmentation
  - Not just VLANs and ACLs, but firewalls, IPS, IDS
- East-west traffic monitoring
  - Idea of a trusted networks will persist
- Tap/span behind SSL termination
- Decrypt & inspect traffic



Strategy: Centralize & Consolidate

Fort Knox. Photo Credit: Michael Vadon on Flickr

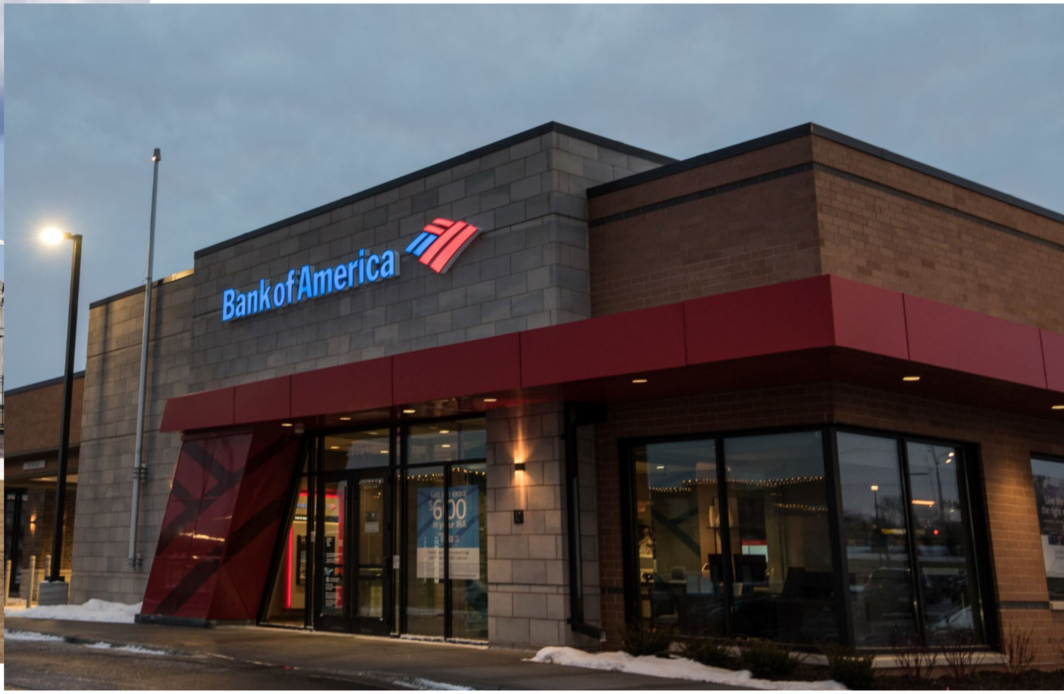


Photo Credit: Tony Webster on Flickr

Decryption

- Really need app-level data for full security visibility
- Decryption options often limited to SSL/TLS
- Certificates managed by operating system
  - Phone apps and web browsers also managing certificates

Decryption (Continued)

- Not trivial
  - Trial and error
  - Figure out certificate management for full coverage
  - Re-exposing sensitive data
- Forward to other NSM tools
- Don’t expect 100% decryption

Trends

- Risk offload
  - Isolate uncontrolled or unmanaged assets
  - SaaS or 3rd party management

Trends

- Integrating security data
  - SIEM or logging solutions
  - Vendors offering network, endpoint, cloud, application tools integrated together
  - Big data security analytics—Cortex XDR, Chronicle Backstory, user-behavior analytics, etc.
- Move from high confidence investigations to highly suspicious/abnormal approach

NSM: One Puzzle Piece

- NSM is just one piece of a well-rounded security program
- Consider a holistic security program

The End is just The Beginning

@forewarnedyou

https://dallinwarne.com

https://linkedin.com/in/dallinwarne/