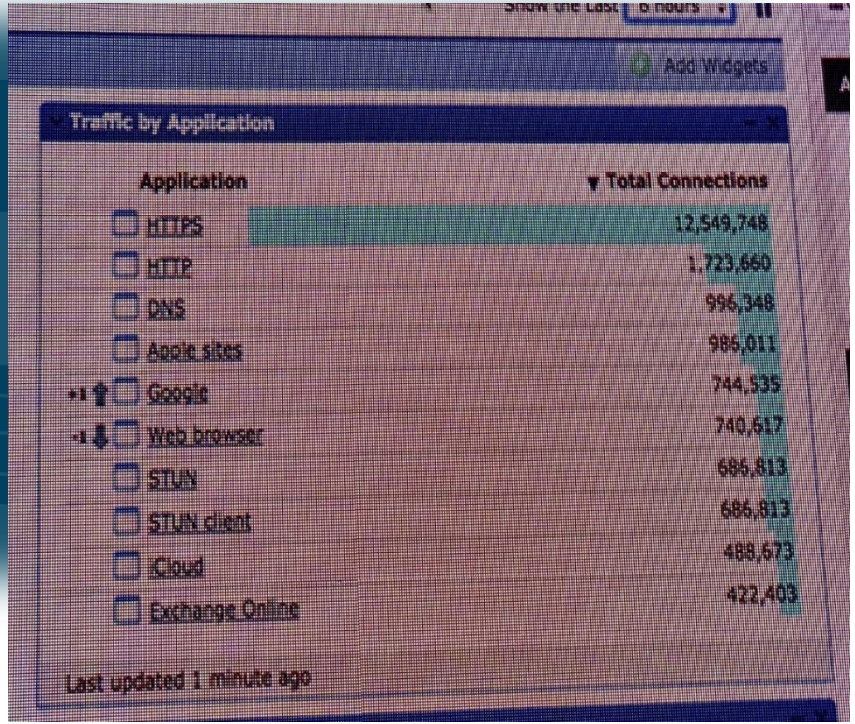
Using Artificial Intelligence to detect threats without Decryption

Encrypted Traffic Analytics

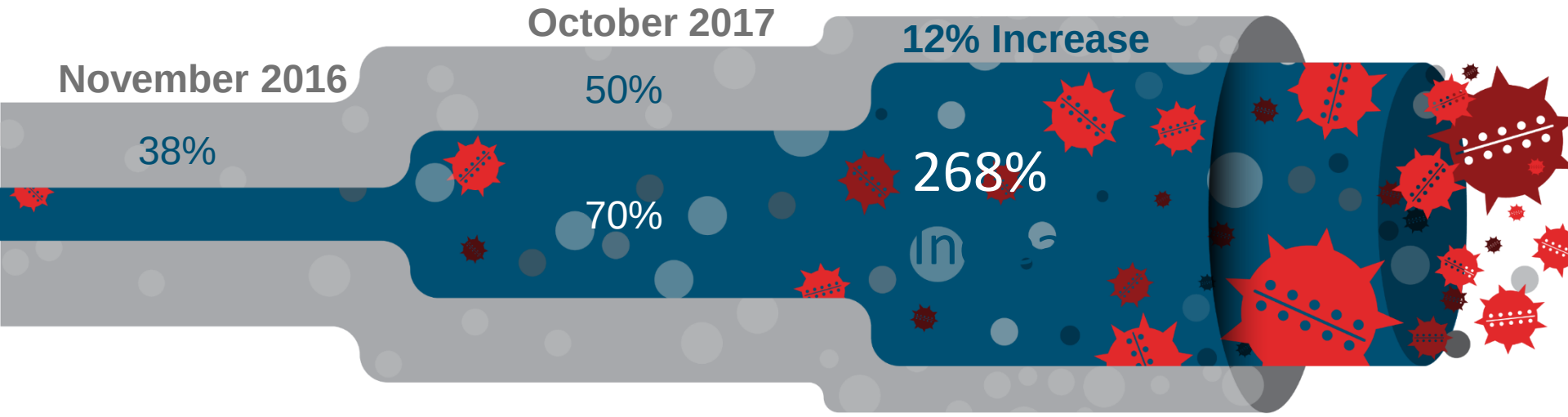
Daniel Tulen, Enablement Lead Stealthwatch EMEAR
Cisco, Advanced Threat Solutions

Networks are becoming less and less transparent!

Google Chrome marks all HTTP sites as not secure since July 2018



Malicious Activity within Encrypted Traffic



Global Encrypted Web Traffic

Malicious Sandbox Binaries with Encryption

Now Available: Cisco Encrypted Traffic Analytics

Industry's first network with the ability to find threats in encrypted traffic **without decryption**

Avoid, stop, or mitigate threats faster then ever before | Real-time flow analysis for better visibility

Privacy AND Security

Machine learning techniques

- **Supervised**:
  - We know the input and the output. The algorithms learn to predict the output from the input data. We're looking for the expected result.
- **Unsupervised**:
  - We know the input and the algorithms learn to inherent structure from this input data. The result is unknown upfront
- **Semi-supervised**:
  - Some input data is known but most of it is unknown and a mixture of supervised and unsupervised techniques can be used

Conclusion:

You need Multi-Layer Machine Learning to get a high fidelity outcome

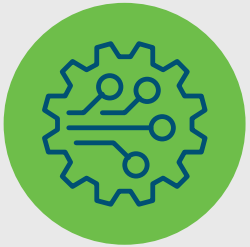
Public Disclosure of Research in 2016

Cisco Research

Known
Malware Traffic

Known
Benign Traffic

Extract Observable
Features in the Data



Employ Machine
Learning techniques to
build detectors

Known Malware
sessions detected
in encrypted traffic
with high accuracy

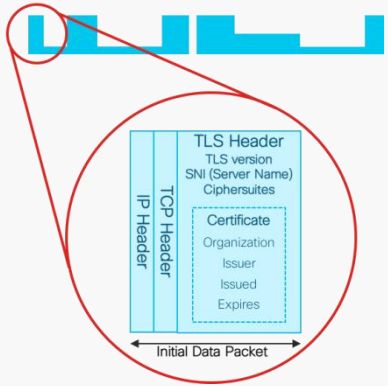
"Identifying Encrypted Malware Traffic with Contextual Flow Data"

AISec '16 | Blake Anderson, David McGrew (Cisco Fellow)

How can we inspect encrypted traffic?

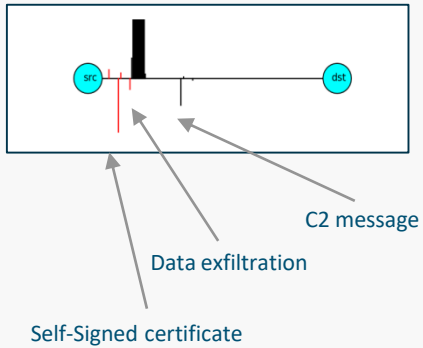
Initial data packet

Make the most of the unencrypted fields



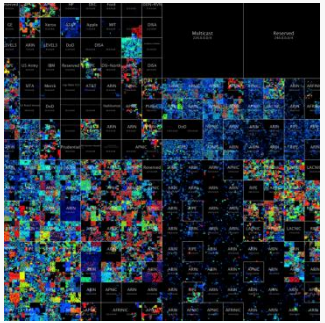
Sequence of packet lengths and times

Identify the content type through the size and timing of packets



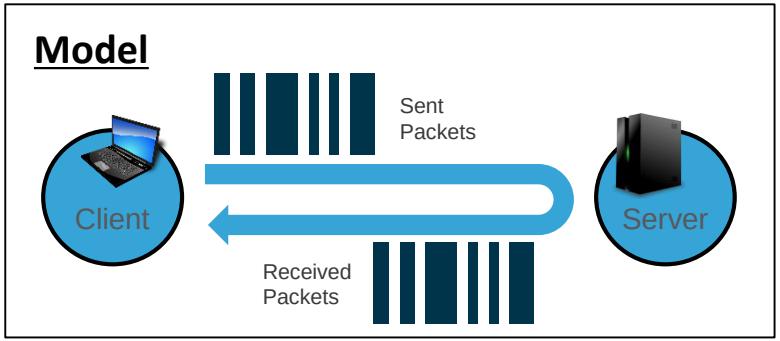
Global Risk Map

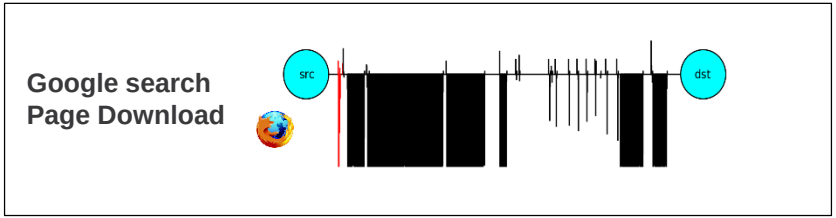
Who's who of the Internet's dark side

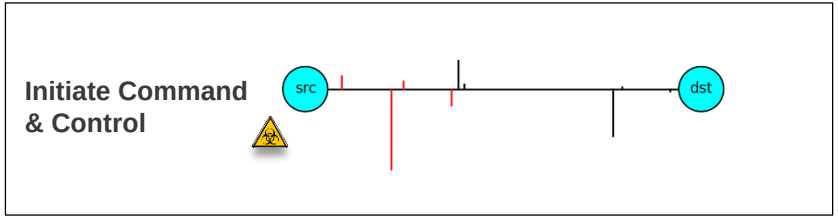


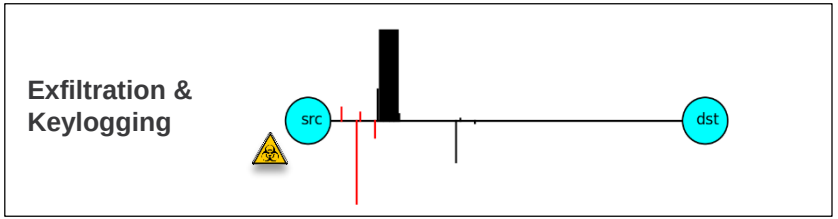
Broad behavioral information about the servers on the Internet.

SPLT shows TLS Metadata differences









Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic.

Finding malicious activity in encrypted traffic

Telemetry Exporter*

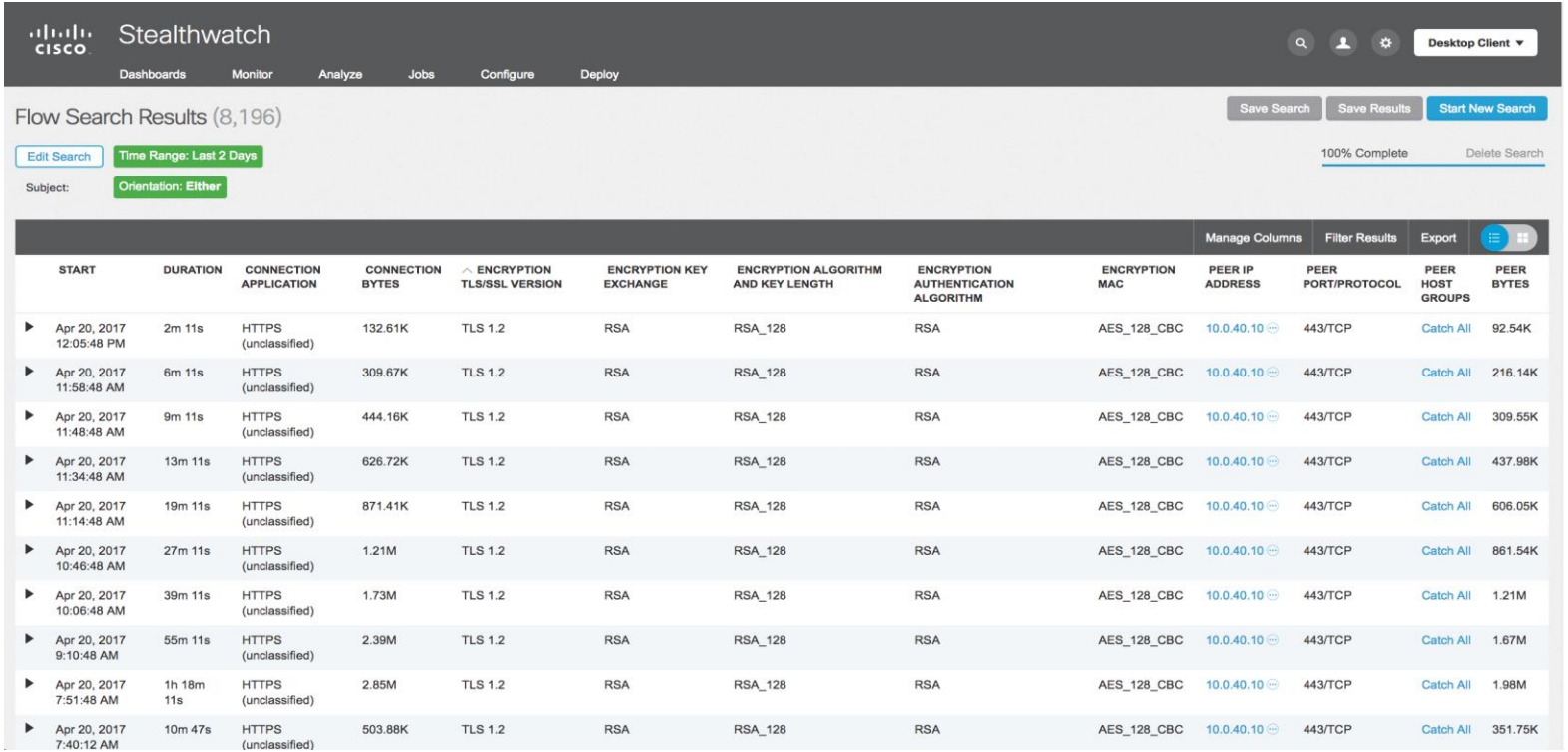
Cisco Stealthwatch®

* Catalyst, ISR, ASR, CSR are supported

Leveraged network	Faster investigation	Higher precision	Stronger protection
Enhanced NetFlow from Cisco's newest switches and routers	Enhanced analytics and machine learning	Global-to-local knowledge correlation	Continuous Enterprise-wide compliance

How much of your business is in the clear versus encrypted?

Encryption details on all network flows



START	DURATION	CONNECTION APPLICATION	CONNECTION BYTES	ENCRYPTION TLS/SSL VERSION	ENCRYPTION KEY EXCHANGE	ENCRYPTION ALGORITHM AND KEY LENGTH	ENCRYPTION AUTHENTICATION ALGORITHM	ENCRYPTION MAC	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
Apr 20, 2017 12:05:48 PM	2m 11s	HTTPS (unclassified)	132.61K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	92.54K
Apr 20, 2017 11:58:48 AM	6m 11s	HTTPS (unclassified)	309.67K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	216.14K
Apr 20, 2017 11:48:48 AM	9m 11s	HTTPS (unclassified)	444.16K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	309.55K
Apr 20, 2017 11:34:48 AM	13m 11s	HTTPS (unclassified)	626.72K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	437.98K
Apr 20, 2017 11:14:48 AM	19m 11s	HTTPS (unclassified)	871.41K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	606.05K
Apr 20, 2017 10:46:48 AM	27m 11s	HTTPS (unclassified)	1.21M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	861.54K
Apr 20, 2017 10:06:48 AM	39m 11s	HTTPS (unclassified)	1.73M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.21M
Apr 20, 2017 9:10:48 AM	55m 11s	HTTPS (unclassified)	2.39M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.67M
Apr 20, 2017 7:51:48 AM	1h 18m 11s	HTTPS (unclassified)	2.85M	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	1.98M
Apr 20, 2017 7:40:12 AM	10m 47s	HTTPS (unclassified)	503.88K	TLS 1.2	RSA	RSA_128	RSA	AES_128_CBC	10.0.40.10	443/TCP	Catch All	351.75K

Next Steps

Learn more about ETA

http://www.cisco.com/go/eta


CISCO