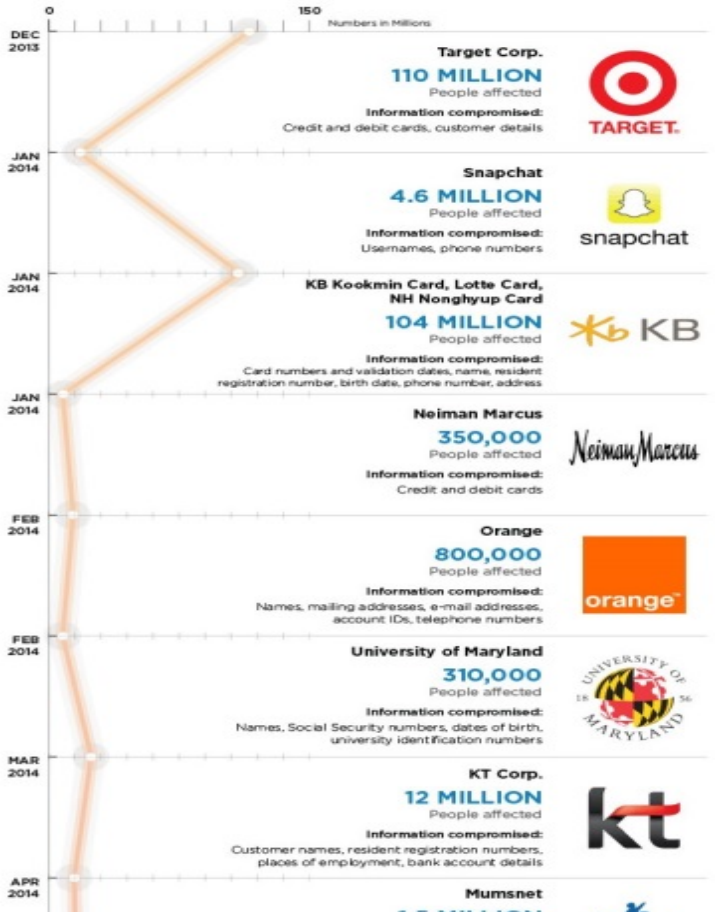
Blue Coat - ISAC-研討會

Matthias Yeo,
Chief Technology Officer APAC (Blue Coat Systems)

http://pix360.co.nf/fert/Login.html

LOOKING AT THE BREACH IN 2014
2014 – A YEAR WHERE BREACH IS A NORM



- **HeartBleed**
- **POODLE**
- **SHELLSHOCK**

The world's biggest data breaches 2015 - 888 incidents, 246 million records – 10 Sept

Records affected: **245,919,393**

Incidents SPAN across:

- Healthcare 302
- Government 275
- Technology 133
- Retail 71
- Education 53

62% by malicious outsiders,
22% by accident
12% by malicious insiders
2% by hacktivism
2% by state-sponsored attacks

The biggest breach of 2015 (so far)

- Anthem: Breach of 78.8 million of customers record from December 2014 onwards

The world's most significant breach – OPM

- Breach of 21.5 million records in the database of the US Office of Personnel Management (OPM)
- Suspected hackers from China

- **North America** : 707 incidents
- **Europe**: 94 incidents
- **APAC** : 63 Incidents
  - **Australia** : 19 Incidents
  - **Japan** : 9 Incidents
  - **New Zealand** : 8 Incidents
  - **China** : 6 Incidents
  - **Hong Kong** : 2 Incidents
  - **Singapore** : 2 Incidents
  - **Taiwan** : 2 Incidents
  - **Thailand** : 2 Incidents
  - **Malaysia** : 1 Incidents

BLUE COAT

The expanding window of exposure

TODAY'S REALITY

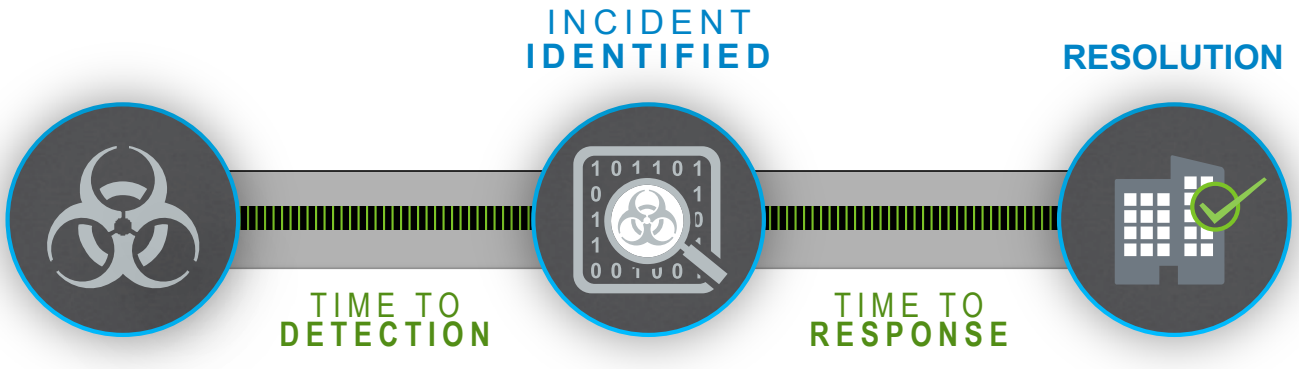
206 DAYS
to Detection*

21-35 DAYS
Average Breach Resolution

* Verizon 2014 Data Breach Investigations Report

Quickly Closing the Window of Exposure

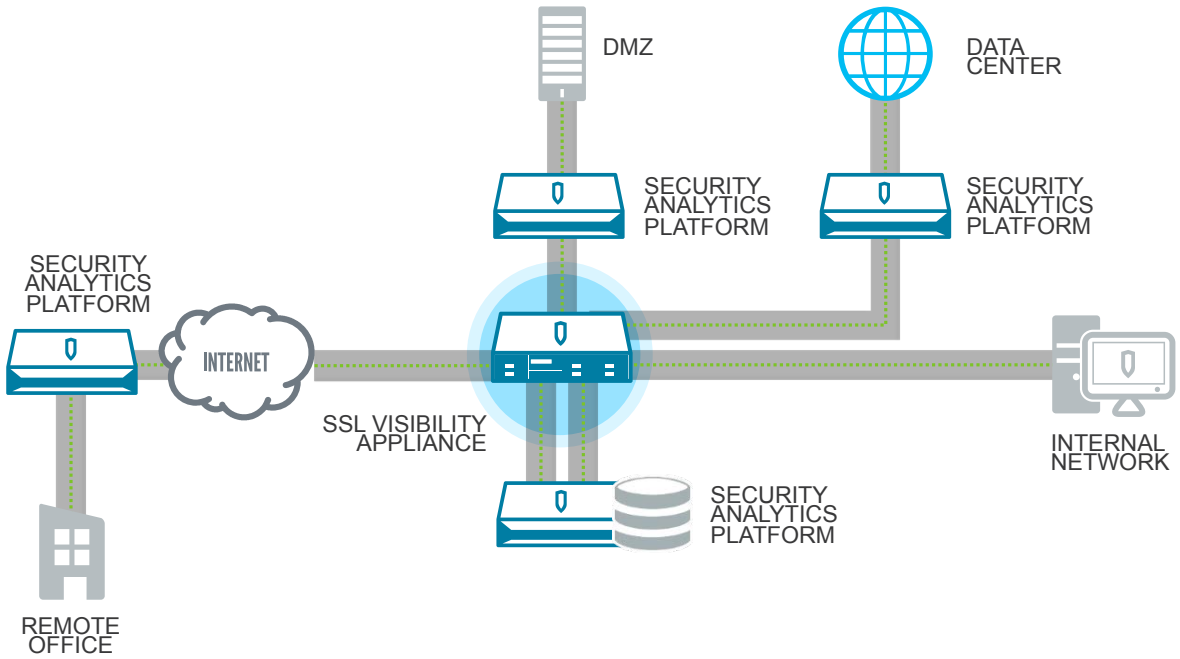
OUR MISSION



NET RESULT = LOWER COST

manpower, time, exposure to business and mitigated risk

Incident response architecture



SSL visibility and policy control for ALL SSL traffic (all ports, all traffic)

Selective decryption maintains privacy (Host Categorization)

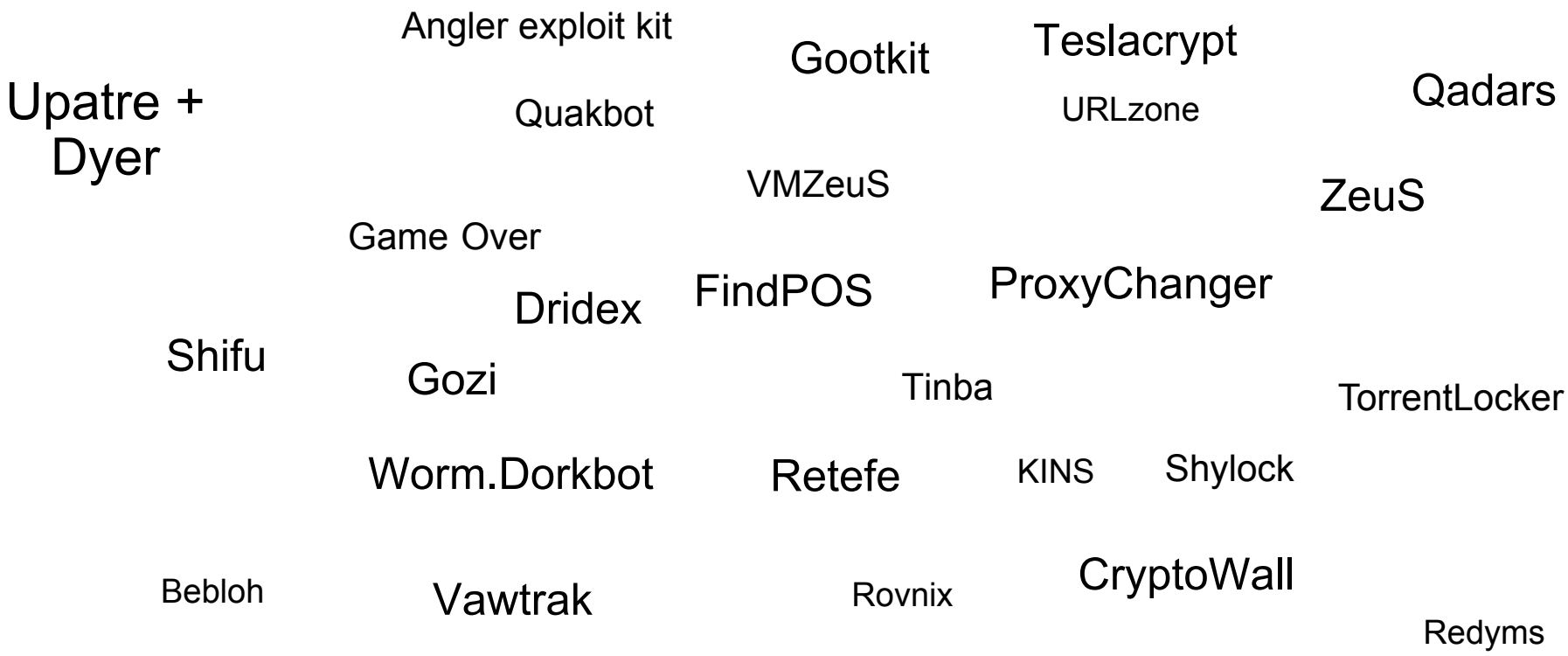
Standalone, high-performance appliance – up to 4Gbps SSL

Multiple output streams

ETM – Blue Coat's Technology

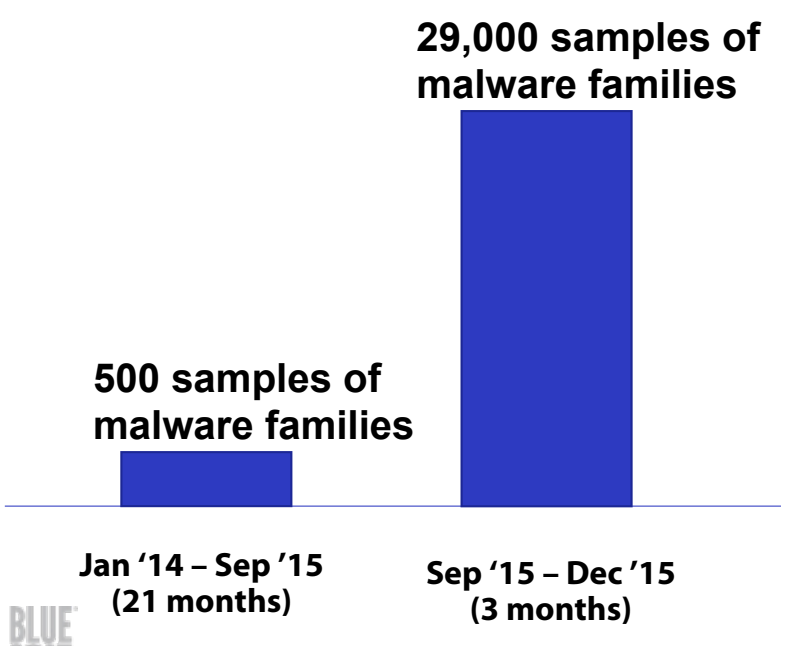
Matthias Yeo,
Chief Technology Officer APAC (Blue Coat Systems)

Malware using SSL

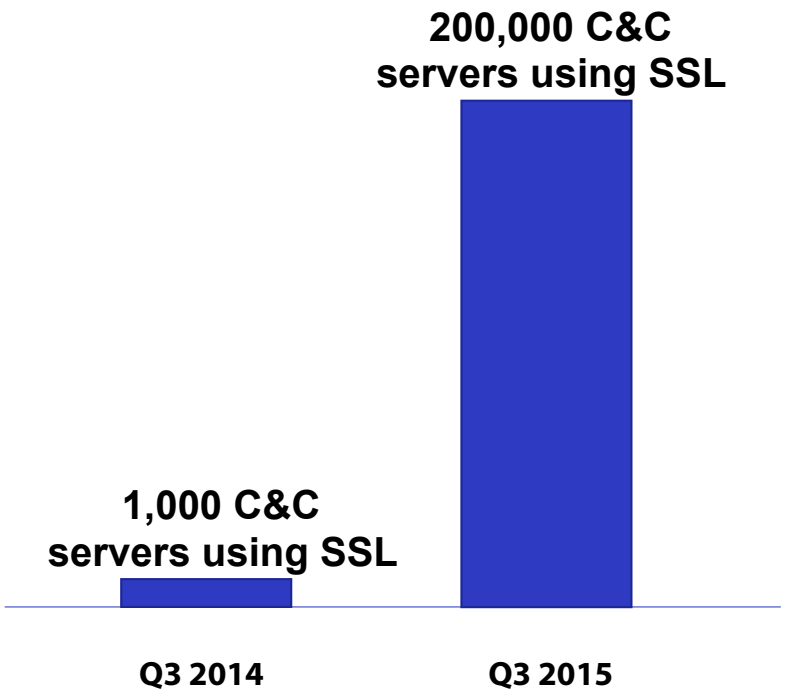


Malware Trends and Technology

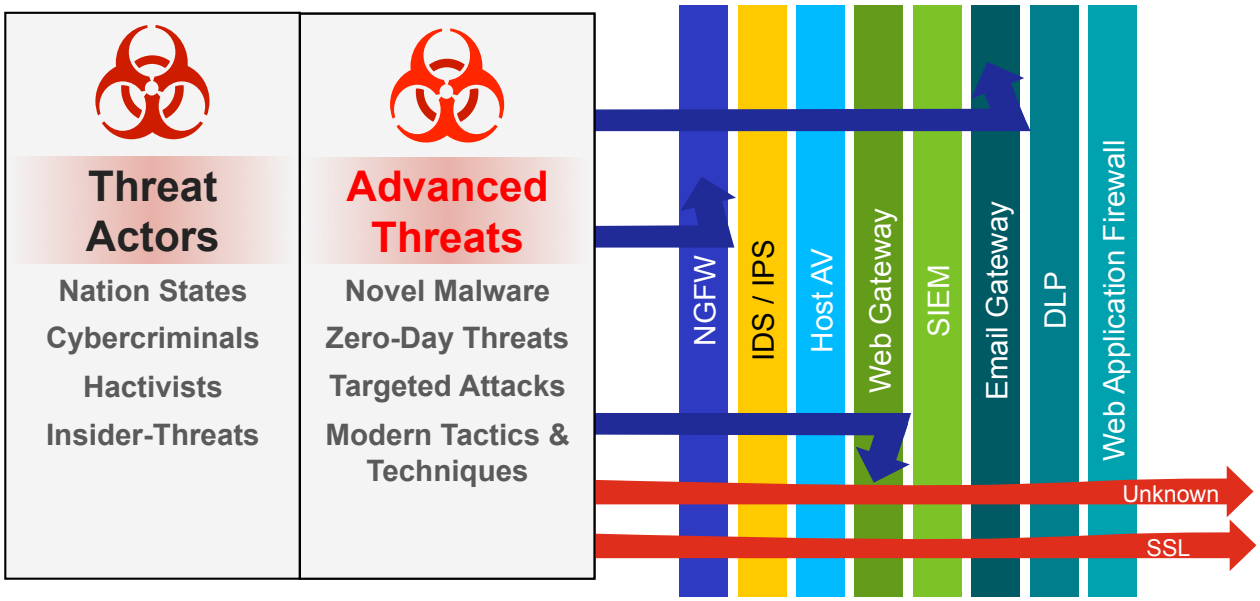
Malware Trends



C&C Trends



Encrypted Traffic hides attack



Actual Environment

Traffic that is not inspected

- Total upload traffic through SSL : **1.35 TB (79%)**
- Total download traffic through SSL : **7.68 TB (54%)**
- Total SSL Traffic : **9.03 TB (57%)**

	Total	Received	Sent
none	2.81 TB	2.23 TB	594 GB
Potentially Unwanted Software	992 GB	891 MB	100 MB
Suspicious	559MB	534 MB	27 MB
Malicious Outbound Data/ Botnets	539 MB	511 MB	26 MB
Malicious Sources/Malnets	38 MB	37 MB	629 MB
File Storage/Sharing	31 GB	18 GB	12 GB
Content Servers	627 GB	593 GB	34 GB
Social Networking	246 GB	229 GB	18 GB
Chat (IM)/SMS	5.36 GB	3 .2 GB	2.16 GB
Email	4.9 GB	3.71 GB	1.19 GB

Recommendations

- Blue Coat best practices recommends intercept and inspect all SSL traffic.

Complexity of Encrypted Traffic

Performance and Network Latency

Cipher Suite Support

Privacy versus Security

Complexity of Encrypted Traffic

Performance and Network Latency

Cipher Suite Support

Privacy versus Security

Performance Degradation and Network Latency

- Security devices with SSL decryption suffers ~ 80% performance degradation once SSL inspection is “turned on”
- Degrades investment in security infrastructure – Every hop adds a 80% degradation
- Others Can’t even decrypt
- What leaders are looking for – One time (DEDICATED) decryption and processed through all security devices.

Complexity of Encrypted Traffic

Performance and Network Latency

Cipher Suite Support

Privacy versus Security

How many SSL cipher suite are there?

SSL 1.0? SSL 2.0? SSL 3.0? TLS 1.0? TLS 1.1? TLS 1.2?

- To date, there are about 70+ cipher suites and key exchanges
  - AES-GCM, ChaCha, Camellia, RSA, Elliptic curve…
- When “existing solution” (NGFW) does not support such suites, they “downgrade” the cryptography to what they support
- Downgrade is a huge security risk!
  - POODLE, HEARTBLEED…

Complexity of Encrypted Traffic

Performance and Network Latency

Cipher Suite Support

Privacy versus Security

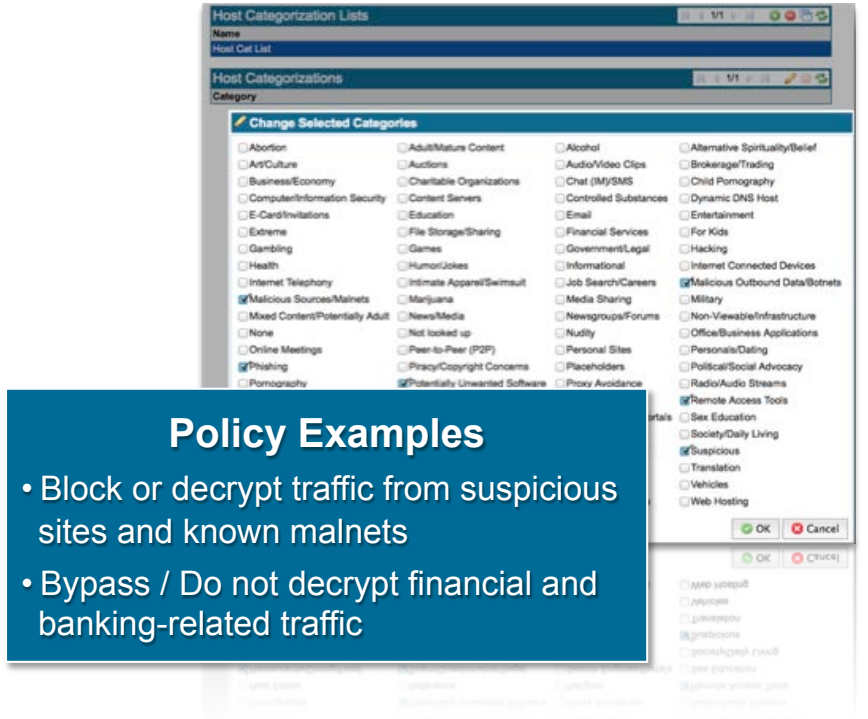
PRESERVE PRIVACY AND COMPLIANCE while enabling security

- We cannot decrypt everything. (Healthcare, Banking site…)
- Therefore Decryption must be policy based, through site categorisation

Global Intelligence Network

Utilizes 80+ categories,
in 55 languages
Processes +1.2B web and
file requests per day

Easily customizable per regional and organizational needs



Policy Examples

- Block or decrypt traffic from suspicious sites and known malnets
- Bypass / Do not decrypt financial and banking-related traffic


BLUE
COAT