THE IMPORTANCE OF ENCRYPTED TRAFFIC MANAGEMENT

PRESENTED BY
David Leung
Senior Systems Engineer
AIRPORT SECURITY CHECK
CLOUD SERVICES DRIVING INCREASE IN SSL/TLS ENCRYPTED TRAFFIC

encrypted traffic  <->  unencrypted traffic

YOUR ENTERPRISE

Firewall / IDS / IPS
Malware Analysis
Data Leak Prevention
HOW ENCRYPTED TRAFFIC WORKS?

SSL/TLS
NSS Research shows that **25% - 35%**
Of enterprise traffic is SSL

Gartner estimates a **20%** Rate of Annual INCREASE
In encrypted traffic

YOUR ENTERPRISE

encrypted traffic ↔ ↔ ↔
unencrypted traffic ↔ ↔ ↔
SSL Connections: 11.9%
SSL Volume: 65.6%
Gartner believes that, in 2017, more than half of network attacks will use encrypted traffic to bypass controls.

CYBERCRIMINALS USING SSL/TLS TO HIDE ATTACKS FROM DETECTION

ZEUS
GameOver
Cridex
ShyLock
SpyEye
Gartner estimates that Enabling traffic decryption or re-encryption on a firewall, SWG, or IPS will reduce the overall performance of the appliance by more than **80%**.

**LESS THAN 20%** of organizations with an IPS or UTM appliance decrypt inbound or outbound SSL traffic... and more.
NSS Research shows that 25% - 35% of enterprise traffic is SSL.

Gartner estimates that enabling traffic decryption or re-encryption on a firewall, SWG, or IPS will reduce the overall performance of the appliance by more than 80%.

1 Million

200 K

… and more
Complex sets of laws regulations on privacy, along with a high risk of conflict with employees, kill most security leaders’ outbound Web traffic decryption projects.
A NEW APPROACH: ENCRYPTED TRAFFIC MANAGEMENT

Policy Driven

Support ALL SSL/TLS

SSL Visibility to Security Controls

Web Gateway
Firewall / IDS / IPS
Email Gateways
Malware Analysis
Network Forensics
Security Analytics
Data Leak Prevention
... and more
BLUE COAT SSL VISIBILITY APPLIANCE

Host Cat.

SSL / TLS 70+

Decrypt Once Feed Many
NSS Research shows that 25% - 35% of enterprise traffic is SSL.

Gartner believes that, in 2017, more than half of network attacks will use encrypted traffic to bypass controls.

Less than 20% of organizations with an IPS or UTM appliance decrypt inbound or outbound SSL traffic...

And more...
RECOMMENDATIONS

Take Inventory of Internet traffic mix

Evaluate risk of un-inspected traffic

Enhance network security with Encrypted Traffic Management

Monitor, refine and enforce
Demo Webcast: Learn to Mitigate the Threats Hidden in Encrypted Traffic

It is evident today that the majority of Advanced Persistent Threats (APTs) use SSL as a transport. Current security appliances are blind to SSL traffic & can’t mitigate these hidden threats. Join our live demo and learn to protect your data against malware hidden in SSL encrypted traffic.

During this 30-minute demo you will learn how to:

- Identify and inspect SSL traffic in real-time without hindering business critical application performance.
- Empower multiple traditional security applications simultaneously such as NGFW, NGIPS, SIEM & DLP with visibility into encrypted traffic. ‘Decrypt Once — Feed Many’

All attendees will receive a free copy of the "Enterprise Traffic Management for Dummies" e-book.

Register Now

Select a Date: -- Please Select a Session --
WEB’S SHADIEST NEIGHBORHOOD

Blue Coat Research Maps the Web’s Shadiest Neighborhoods

September 2015
TOP 10 TLDS WITH SHADY SITES

In 2013-2014, over 600 new TLDs were approved.

Lax Policies for Purchasing TLDs Breeds Danger

The Web's Top 10 TLDS with Shady Sites*

<table>
<thead>
<tr>
<th>Rank</th>
<th>Top-Level Domain Name</th>
<th>Percentage of Shady Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>.zip</td>
<td>100.00%</td>
</tr>
<tr>
<td>2</td>
<td>.review</td>
<td>100.00%</td>
</tr>
<tr>
<td>3</td>
<td>.country</td>
<td>99.97%</td>
</tr>
<tr>
<td>4</td>
<td>.kim</td>
<td>99.74%</td>
</tr>
<tr>
<td>5</td>
<td>.cricket</td>
<td>99.57%</td>
</tr>
<tr>
<td>6</td>
<td>.science</td>
<td>99.35%</td>
</tr>
<tr>
<td>7</td>
<td>.work</td>
<td>98.20%</td>
</tr>
<tr>
<td>8</td>
<td>.party</td>
<td>98.07%</td>
</tr>
<tr>
<td>9</td>
<td>.gq (Equatorial Guinea)</td>
<td>97.68%</td>
</tr>
<tr>
<td>10</td>
<td>.link</td>
<td>96.98%</td>
</tr>
</tbody>
</table>

Most Common
- Spam
- Scam
- Suspicious
- Potentially Unwanted Software (PUS)

Less Common
- Malware
- Botnet
- Phishing
MINIMIZE THE RISK FOR BUSINESS AND CONSUMERS

### The Web’s “Safest” Neighborhoods

<table>
<thead>
<tr>
<th>Rank</th>
<th>Top-Level Domain Name</th>
<th>Percentage of Shady Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>.jp (Japan)</td>
<td>1.95%</td>
</tr>
<tr>
<td>9</td>
<td>.london</td>
<td>1.85%</td>
</tr>
<tr>
<td>8</td>
<td>.kw (Kuwait)</td>
<td>1.61%</td>
</tr>
<tr>
<td>7</td>
<td>.tel</td>
<td>1.60%</td>
</tr>
<tr>
<td>6</td>
<td>.gi (Gibraltar)</td>
<td>1.26%</td>
</tr>
<tr>
<td>5</td>
<td>.gov</td>
<td>0.96%</td>
</tr>
<tr>
<td>4</td>
<td>.church</td>
<td>0.84%</td>
</tr>
<tr>
<td>3</td>
<td>.ck (Cook Islands)</td>
<td>0.52%</td>
</tr>
<tr>
<td>2</td>
<td>.jobs</td>
<td>0.36%</td>
</tr>
<tr>
<td>1</td>
<td>.mil</td>
<td>0.24%</td>
</tr>
</tbody>
</table>

### How to Minimize the Risk for Businesses and Consumers

In summary, everyone, whether a business user or consumer, should be aware and vigilant about the online neighborhoods they visit. Even the “safest” TLDs are not without risk of threats from nefarious players, and it remains as critical as ever to have strong digital security protection and policies in place.

- **Businesses** should consider **blocking traffic that leads to the riskiest TLDs**. For example, Blue Coat has previously recommended that businesses consider blocking traffic to .work, .gq, .science, .kim and .country. The remaining five TLDs in the Top 10 Shadiest TLDs list deserve similar consideration.

- **Users** should use **caution to click on any links that have these TLDs** in them if they encounter them in search results, e-mail, or social network environments.

- **If unsure about the source**, hover the mouse over a link to verify that it leads to the address displayed in the text of the link.

- **Remember** that you can "press and hold" a link on a mobile device (not just click) to verify it leads to where it says it does.
THANK YOU