TLS PROXIES: FRIEND OR FIEND?

Measurement via online Ad Campaign
Measurement Tool embedded in Flash ad + Google AdWords
= 2.8 million results in 2 weeks

Country Breakdown

0.41% (11,764)
of scanned connections involved a TLS proxy

Assessment of Substitute Certificates
50.8% of substitute certificates downgraded public key size
23 substitute certificates used MD5 for signing

Summary of Detected TLS Proxies

<table>
<thead>
<tr>
<th>Proxy Type</th>
<th>Connections</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Firewall</td>
<td>6,384</td>
<td>54.27%</td>
</tr>
<tr>
<td>Enterprise Firewall</td>
<td>481</td>
<td>4.30%</td>
</tr>
<tr>
<td>Personal/Enterprise</td>
<td>1,528</td>
<td>12.95%</td>
</tr>
<tr>
<td>Organization</td>
<td>1,448</td>
<td>12.31%</td>
</tr>
<tr>
<td>Malware/Spam</td>
<td>1,141</td>
<td>9.70%</td>
</tr>
<tr>
<td>Unknown</td>
<td>890</td>
<td>6.80%</td>
</tr>
</tbody>
</table>

Note: The actual amount of malware and malicious MITM may be higher since TLS proxies can provide arbitrary issue field values.

Problem
- Substitute certificate
- Encrypted traffic
- TLS Proxy
- Original certificate
- Decrypted traffic

Benevolent Uses:
- Blocking malware and viruses
- Protecting corporate secrets
- Blocking harmful websites
- Catching malicious users

Malicious Uses:
- Stealing passwords
- Identity theft
- Tracking government dissidents
- Spying (e.g., M&A surveillance)
- Censorship

Malicious Uses:
- Stealing passwords
- Identity theft
- Tracking government dissidents
- Spying (e.g., M&A surveillance)
- Censorship

What do users think about TLS proxies?

1. 72.5% of respondents believe there are acceptable uses of TLS proxies
2. 72.4% of respondents are concerned about hackers using TLS proxies

Survey Likert Results
- Disagree
- Neutral
- Agree
- Strongly Agree
- Percent

User Quotations of Note
- "Telco users should never be allowed to access via an invasion of privacy and a security risk. The potential for misuse and abuse is not worth the possible benefits."
- "I am concerned that TLS proxies could be used by my government to collect my personal information."
- "There are acceptable uses of TLS proxies in order to trust your customers that they receive legitimate traffic from malware, tracking, etc..."
- "I am concerned that the information can be used to track my information and use it for identity theft. However, I understand that it can also be used to protect my information."
- "I'm concerned that this might be used to examine my computer to detect when I'm using the computer as we should not expect privacy when we are using someone else's computer."
- "It's completely reasonable for companies to employ filtering techniques when an individual is using their computer as we should not expect privacy when we are using someone else's computer."
- "It's completely reasonable for companies to employ filtering techniques when an individual is using their computer as we should not expect privacy when we are using someone else's computer."

User Study
- 72.5% of respondents want to be notified when behind a TLS proxy
- 68.8% of respondents are concerned about government spying using TLS proxies

72.5% of respondents believe there are acceptable uses of TLS proxies

Mark O'Neill
Scott Ruoti
Daniel Zappala
Kent Seamons

1,261 survey respondents