

SSLammed, SSLayed and SSLapped Around - Why Hackers Love SSL



Grant Asplund

Director of Evangelism
Blue Coat Systems
@gasplund



Today's SSL Landscape

2017 U.S. Retail

e-Commerce Sales



34.2B^S Success On Demand



webex



Secure Sockets Layer (SSL) or Transport Layer Security (TLS)

Top 10 Most Visited Web Sites



In Our Labs

- ◆ Annual
 - ◆ +246.25 Billion Requests – HTTP – Down 3% to 83%
 - ◆ +39 Billion Requests – HTTPS – Up 5% to 14%
- ◆ Daily
 - ◆ Up to 750M Domain or IP Address rating requests - HTTP
 - ◆ Up to 110M Domain or IP Address ratings requests – HTTPS
 - ◆ 30K Unique/Unknown Executable Applications Contained - HTTPS

In Our Labs – Typical Seven Days...

- ◆ Top 50 Sites Visited - 69% HTTPS
- ◆ Top 10 Most Visited Sites – 100% HTTPS
- ◆ 1.1M Sites Classified - Potentially Unwanted Software
 - ◆ 24% - Enterprise Users 76% - Consumer Users
 - ◆ Most Use Port 443 - Legitimately Purchased SSL Certificates
- ◆ +40,000 Requests - Newly-Classified Malicious HTTPS Sites
- ◆ 100,000 Requests to Command and Control HTTPS Sites
 - ◆ Typically Already Infected – 35% from Enterprise Users



- ◆ Delivery of Malicious Code
- ◆ Command and Control
- ◆ Exfiltration
- ◆ C&C Often Use Port 9001
(75% during period analyzed)

Over a seven-day period, the ten most commonly used port numbers for SSL traffic to servers classified as “botnet command and control”



Port	Percentage
9001	74.66%
443	5.45%
80	2.51%
9201	1.97%
8443	1.73%
8080	1.68%
9090	1.06%
110	0.99%
1337	0.98%
9101	0.98%

Bogus Dyre “Google” SSL certificate (used in July, 2014) #RSAC

Certificate

General Details Certification Path

Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	root@google.com, 94.23.236....
Valid from	Thursday, July 24, 2014 9:53:....
Valid to	Friday, July 24, 2015 9:53:38 ...
Subject	root@google.com, 94.23.236....
Public key	RSA (1024 Bits)
Thumbprint algorithm	sha1
Thumbprint	h2 ca f5 a1 82 79 c1 ch 10 da

E = root@google.com
CN = 94.23.236.54
OU = google
O = Google
L = miami
S = FL
C = US

Edit Properties... Copy to File...

Learn more about [certificate details](#)

Fake

Certificate

General Details Certification Path

Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Google Internet Authority G2, ...
Valid from	Wednesday, June 04, 2014 2:...
Valid to	Monday, September 01, 2014 ...
Subject	www.google.com, Google Inc,...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1.3.6....)
Subject Alternative Name	DNS Name = www.google.com

CN = www.google.com
O = Google Inc
L = Mountain View
S = California
C = US

Edit Properties... Copy to File...

Learn more about [certificate details](#)

Real

Recent Dyre C&C SSL certificates with 360-day validity, 1024 bit RSA keys, and key-mash details

Certificate

General Details Certification Path

Show: <All>

Field	Value
Issuer	asdgdgs, sdfhdsga, asdgd... Wednesday, December 10, 20...
Valid from	Saturday, December 05, 2015...
Valid to	asdgfdgs, sdfhdsga, asdgd...
Subject	RSA (1024 Bits)
Public key	sha1
Thumbprint algorithm	c5 94 bc 20 27 8f 47 5b 77 2d ...
Thumbprint	

**CN = asgdgdgs
OU = sdfhdsga
O = asdgdftdf
L = sdfhsdfghdf
S = sdfghshfsd
C = AU**

Edit Properties... Copy to File...

Learn more about [certificate details](#)

Certificate

General Details Certification Path

Show: <All>

Field	Value
Issuer	aswqervcx, iukjfghj, dfshsdhr... Monday, December 15, 2014 ...
Valid from	Thursday, December 10, 2015...
Valid to	aswqervcx, iukjfghj, dfshsdhr...
Subject	RSA (1024 Bits)
Public key	sha1
Thumbprint algorithm	55 7b 84 3e 06 5f c6 0a 16 5d ...
Thumbprint	

**CN = aswqervcx
OU = iukjfghj
O = dfshsdhrey
L = wf dagfh
S = sdfhvbnnsfd
C = AU**

Edit Properties... Copy to File...

Learn more about [certificate details](#)

Seeing and Apprehending Upatre



	Time	Source(s)	Type	Method
	16:14:19	dl.dropboxusercontent.com/content_link/KrlTzo0Y9hNtkaYgHDBFh3HWa...	application/zip	GET
	16:15:04	dl.dropboxusercontent.com/content_link/RhkVNAq871IjkMuhw8nIEegRch...	application/zip	GET
<p><i>Screenshot of malicious downloads delivered from Dropbox, decrypted by the SSL Visibility Appliance, and extracted by Security Analytics</i></p> <p>Presented: application/zip Selected: application/zip Source Port: 63827 Destination Port: 443 Extension: zip MD5: 4eadf7d091610e892729fd9373ee8b1a SHA1: 2c27fb791f6741261848c511e72873d267ab2e1d Fuzzy Hash: 1536:QP4QWjsYgXS7aNMQUXaBDfkDAPHW5F9q2E92yAHvMO:QwQWj/EAUDAYH+D6998N Original URL: dl.dropboxusercontent.com/content_link/RhkVNAq871IjkMuhw8nIEegRchHeqUtVTejUfGt6UgoPZIIPDVmtkB6aJvWdLNl3 File Name: RhkVNAq871IjkMuhw8nIEegRchHeqUtVTejUfGt6UgoPZIIPDVmtkB6aJvWdLNl3 URI Host: dl.dropboxusercontent.com Referrer: www.dropbox.com/s/4zyk914w8whtgkq/Or%C3%A7amento.pdf.zip</p>				
Actions Preview Download Analyze PCAP Explore Root Cause Reputation				
	10:51:07	dl.dropboxusercontent.com/content_link/0mXPoQ56Yrf9zvipesxRzLfLOh1...	application/zip	GET
	10:51:27	dl.dropboxusercontent.com/content_link/3OBpg04pRyj3BctFw8XjnPBCN...	application/zip	GET
	10:51:33	dl.dropboxusercontent.com/content_link/BN4FqSyjhob4NOnsbEZm3KGa...	application/zip	GET
	10:52:03	dl.dropboxusercontent.com/content_link/Hq7DTTG1ZiAVLaYK89EboLk5...	application/zip	GET

Artifact Preview

Text Hex HTTP Headers Strings File Info

GET /2807uk2/[REDACTED]_W512600.C[REDACTED]/[REDACTED]/5/publickey/[REDACTED][REDACTED] / HTTP/1.1
User-Agent: Opera/9.80
Host: 94.23.236.54:15000

Malware version Machine name OS version Unique identifier string Command Public IP address

HTTP/1.1 200 OK

Server: Stalin

Content-Length: 400

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/5/publickey/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/0/Win_XP_32bit/1037/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/5/rplc/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/1/nfpnQXNKVMkBQIFyRNIGDQmTfHdsMiV/17

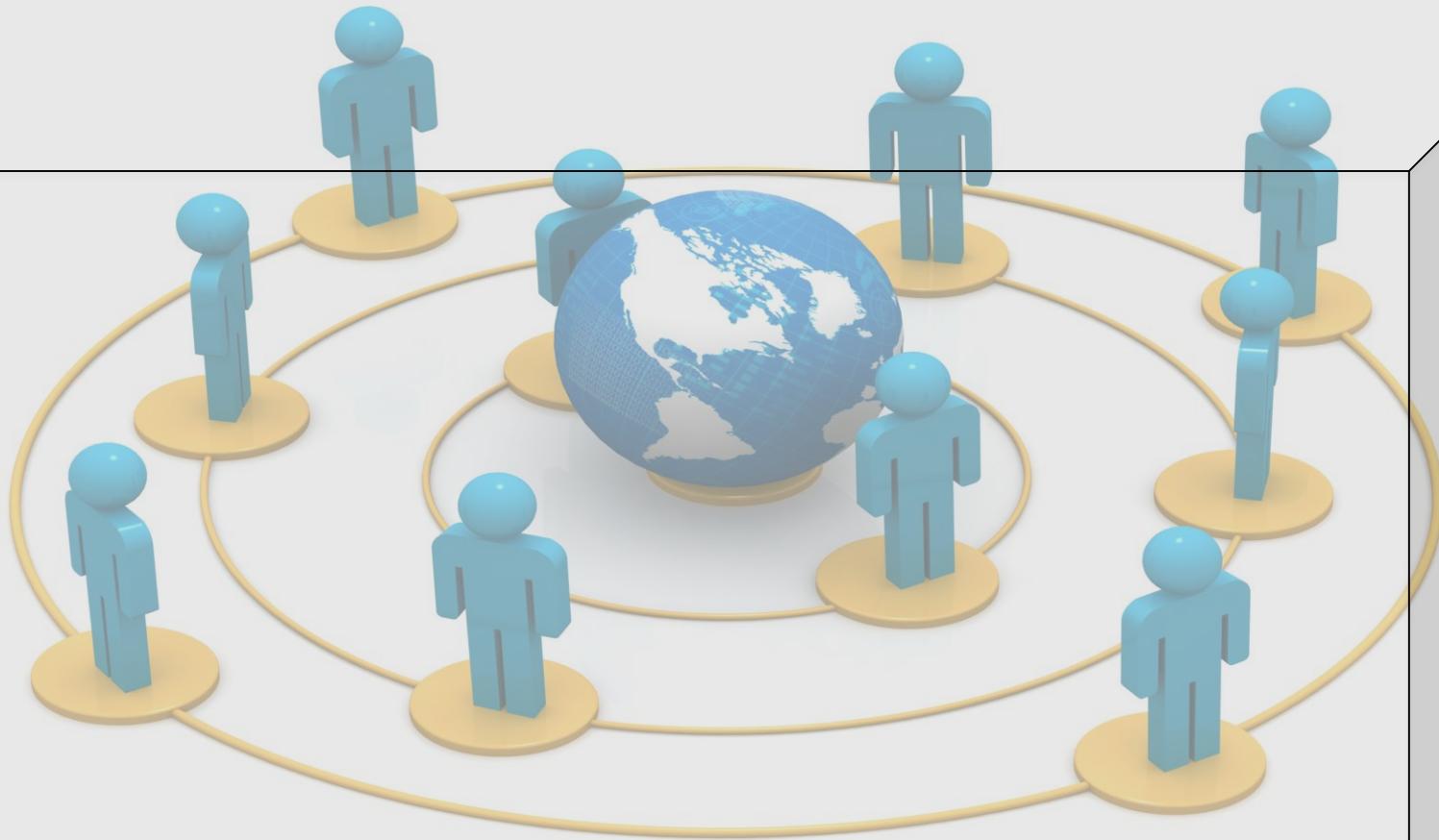
/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/14/NAT/Symmetric%20NAT/0/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/14/user/not_support/0/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/63/browsnapshot/174.29.12.29/

/0309us1/D620_W512600.1228F774285096F5DEC1D42C7C85E2D6/63/browsnapshot/174.29.12.29/





Private and Confidential

[Projects](#)[Blog](#)[About](#)[Join](#)[Media](#)

Building Together a Trustworthy Internet

one project at a time

SSL Pulse



Survey of the SSL Implementation of the Most Popular Web Sites

Summary

Published Date: **February 07, 2015**

Comparisons are made against the previous month's data.

[◀ Previous](#)[Next ▶](#)

SSL Security Summary



Total sites surveyed

148,486

- 0.4 %

Inadequate security

124,105

- 2.5 %

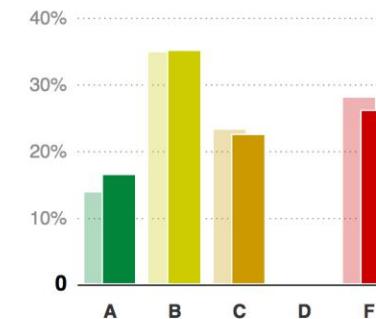
Secure sites

■ A+ ■ A- ■ A

24,381

+ 2.5 %

SSL Labs Grade Distribution



SSL Server Test

Enter domain name for testing:

[Submit](#)

About This Project

Title: **SSL Pulse**
Created by: **SSL Labs**
Date Published: **April 25, 2012**

Details:

“White organic id acti crypt fix in honited ito
“GInentvloe pericrypt arose impact of
deas. It is as if you were to see the fruits of
dead sonies you will be back for you have
selected and the other is the keep
extra extra extra extra extra extra extra extra
dead from the tree seems no longer
After a week you can easily identify
as seen this is the basis of the one, only being
moderately to each of the encrypted file's
priorities and the others is super kahante
the decryption is very, please do not
how can the encryption on the
network as seen at a place, C.
capture in a forensics
security encrypted data 80%.”





VIRUS

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Thank You!

Grant Asplund
Director of Evangelism
grant.asplund@bluecoat.com
[@gasplund](https://twitter.com/gasplund)

