Tranalyzer Report

test.pcap

Tranalyzer Development Team

October 23, 2018

Contents

1 Summary

- Filename: `/home/user/test.pcap`
- MD5: `56c73c0eff4074d2d37c0bbb08f2ceb9`
- File size: 1.2G
- Number of packets: 1577658 (1.58 M)
- Number of bytes: 1135805967 (1.14 G)
- First packet seen: Tue Dec 7 20:20:25 UTC 2010
- Last packet seen: Tue Dec 7 20:20:31 UTC 2010
- Capture duration: 6.51899 seconds
- Number of distinct IP addresses: 42993 (42.99 K)
  - 230 private
  - 42763 (42.76 K) public
  - 42993 (42.99 K) IPv4
  - 1169 (1.17 K) IPv6

2 Top 10 IP Addresses

SrcIP	Country	Flows
..***.***	CH	272
..***.***	CH	267
..***.***	CH	247
..***.***	CH	237
..***.***	CH	215
..***.***	CH	198
..***.***	CH	190
..***.***	CH	187
..***.***	CH	172
..***.***	CH	172

DstIP	Country	Flows
..***.***	CH	4.77 K
..***.***	CH	537
..***.***	CH	371
..***.***	CH	364
..***.***	CH	280
..***.***	CH	222
..***.***	CH	195
..***.***	CH	192
..***.***	CH	191
..***.***	CH	185

SrcIP	Country	Packets
..***.***	CH	9.68 K
..***.***	CH	8.24 K
..***.***	SI	7.15 K
..***.***	CH	7.09 K
..***.***	CH	7.06 K
..***.***	DE	5.88 K
..***.***	CH	5.86 K
..***.***	CH	5.69 K
..***.***	CH	5.18 K
..***.***	CH	4.87 K

DstIP	Country	Packets
..***.***	US	27.06 K
..***.***	CH	17.82 K
..***.***	US	13.73 K
..***.***	KG	10.45 K
..***.***	CH	9.59 K
..***.***	CH	9.27 K
..***.***	CH	8.91 K
..***.***	DE	8.52 K
..***.***	US	8.47 K
..***.***	EU	7.49 K

SrcIP	Country	Bytes
..***.***	SI	9.77 M
..***.***	DE	8.37 M
..***.***	CH	7.55 M
..***.***	CH	5.28 M
..***.***	CH	5.27 M
..***.***	CH	5.26 M
..***.***	CH	5.18 M
..***.***	CH	5.12 M
..***.***	CH	5.11 M
..***.***	CH	4.91 M

DstIP	Country	Bytes
..***.***	US	39.33 M
..***.***	CH	25.99 M
..***.***	US	20.05 M
..***.***	KG	15.11 M
..***.***	CH	13.59 M
..***.***	CH	13.15 M
..***.***	CH	12.90 M
..***.***	DE	12.38 M
..***.***	US	12.37 M
..***.***	CH	10.48 M

3 Top 10 Countries

Src Country	Flows
CH	55.91 K
US	2.82 K
DE	1.80 K
—	1.57 K
IT	901
GB	840
FR	807
CA	663
RU	640
ES	537

Src Country	Packets
CH	863.05 K
DE	52.07 K
US	38.46 K
GB	36.21 K
NL	19.80 K
FR	13.32 K
SI	10.63 K
IT	10.60 K
IE	8.15 K
CA	6.63 K

Src Country	Bytes
CH	231.04 M
US	33.50 M
GB	29.80 M
DE	29.17 M
NL	18.04 M
SI	14.11 M
FR	7.70 M
IT	7.24 M
SE	6.38 M
RO	5.81 M

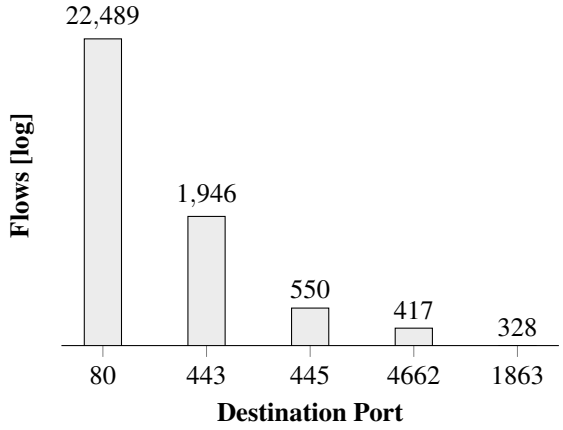
Dst Country	Flows
CH	32.79 K
US	12.88 K
DE	4.40 K
EU	2.49 K
GB	1.93 K
—	1.78 K
NL	1.50 K
IT	1.34 K
FR	1.24 K
CA	1.16 K

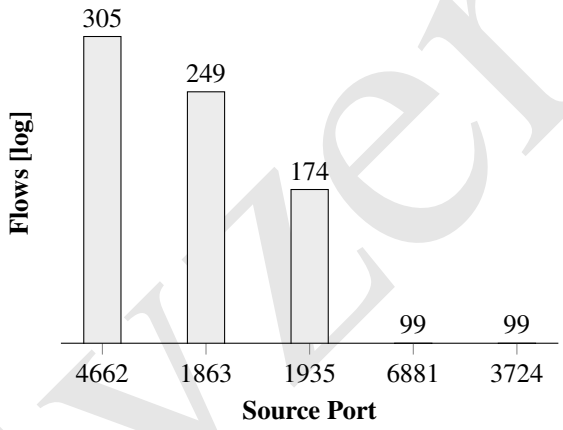
Dst Country	Packets
CH	417.54 K
US	207.33 K
DE	85.34 K
EU	67.36 K
NL	51.18 K
GB	32.17 K
N/A	15.58 K
IT	15.27 K
KG	15.15 K
FR	10.76 K

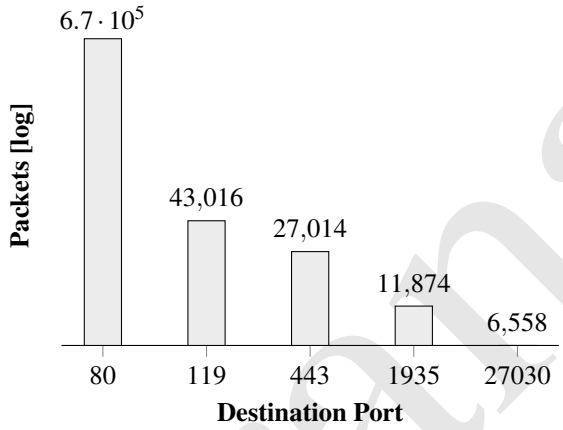
Dst Country	Bytes
CH	421.19 M
US	258.04 M
DE	97.01 M
EU	90.77 M
NL	69.81 M
GB	35.82 M
KG	21.90 M
N/A	18.31 M
IT	16.01 M
FR	8.55 M

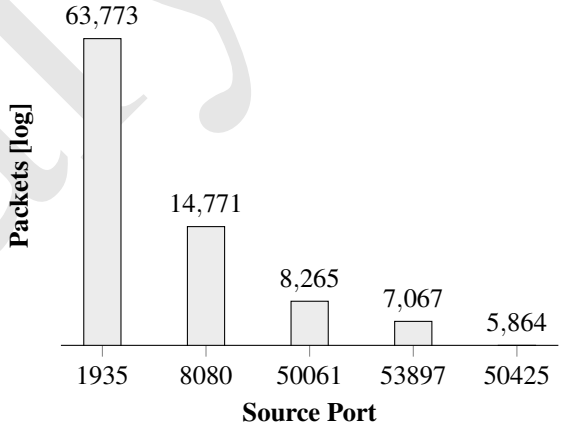
4 Top 5 Ports

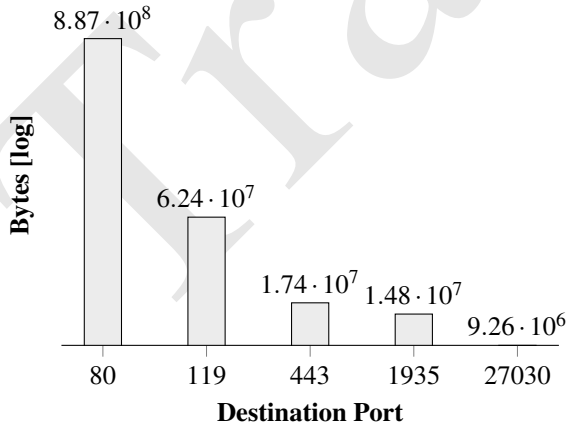
4.1 Top 5 TCP Ports

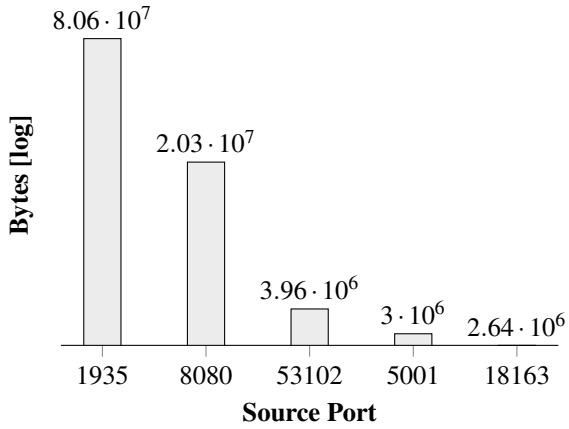




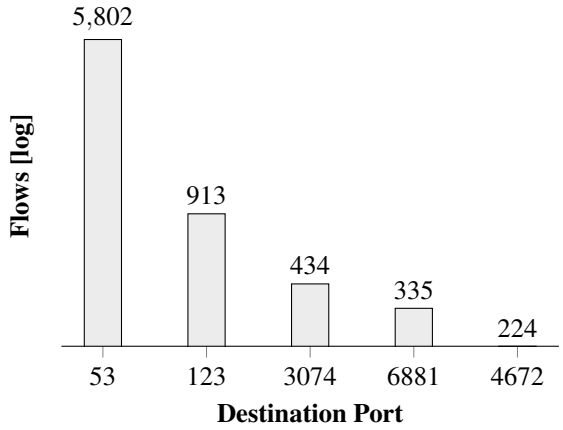


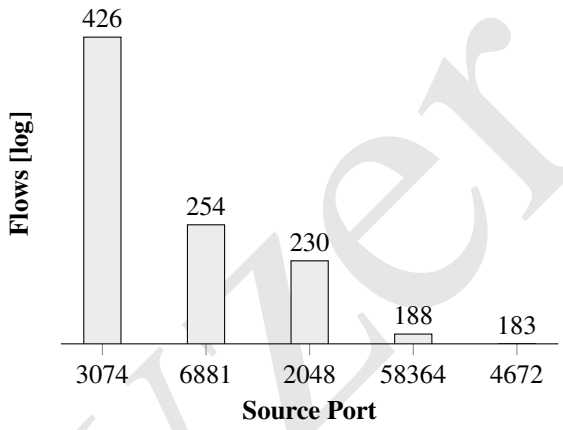


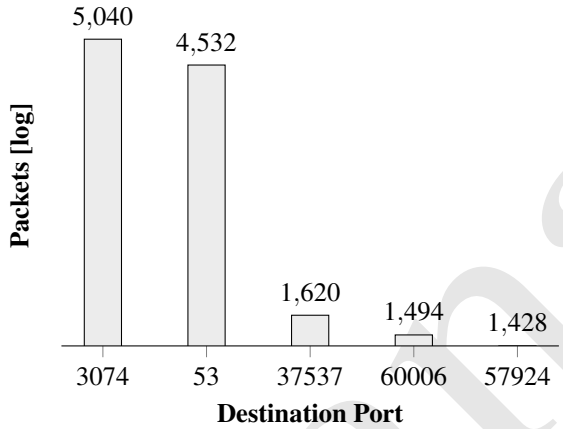


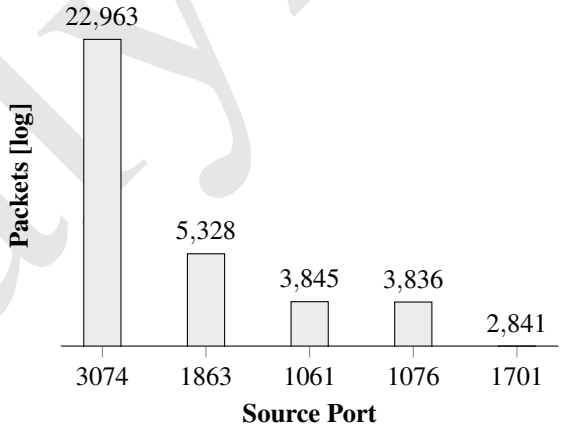


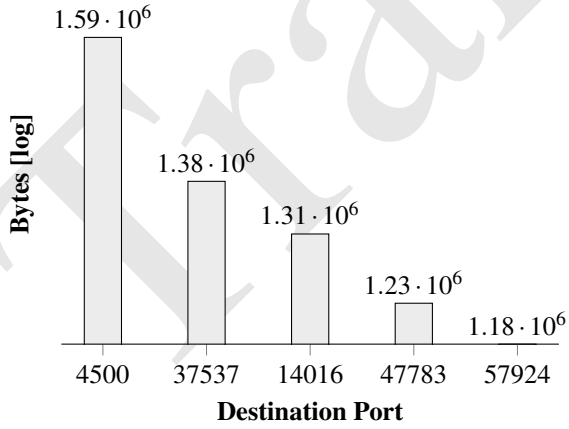
4.2 Top 5 UDP Ports

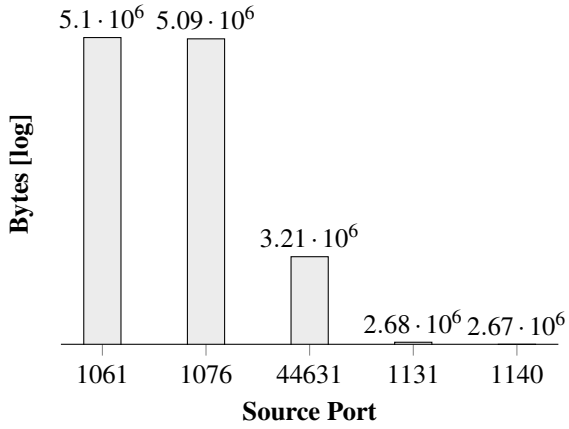




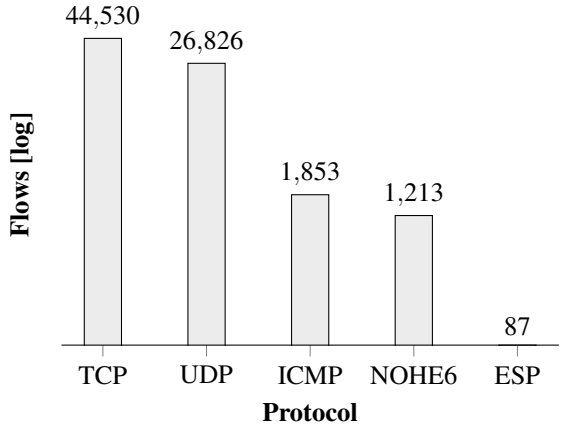


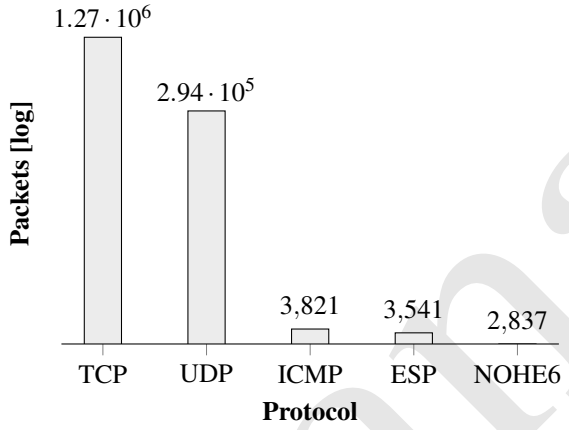


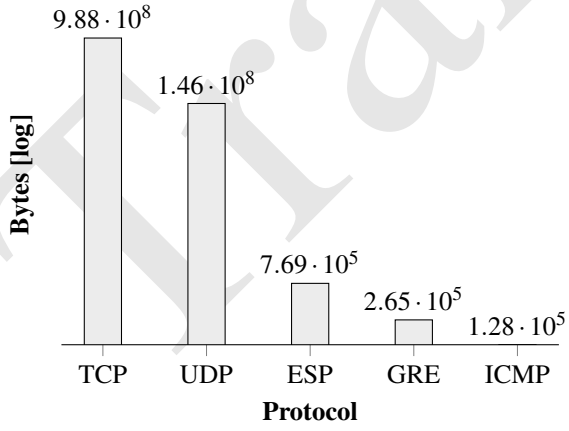




5 Top Protocols and Applications







Application	Flows
Unknown	30.19 K
HTTP	18.25 K
BitTorrent	7.00 K
DNS	5.80 K
SSL	3.65 K
ICMP	1.85 K
Skype	1.85 K
NTP	915
SMB	477
Viber	466

Application	Packets
Unknown	881.57 K
HTTP	376.24 K
RTMP	85.87 K
RTP	70.35 K
SSL	46.11 K
BitTorrent	30.50 K
HTTP_Proxy	22.14 K
IPsec	7.42 K
DNS	6.68 K
FTP_DATA	5.37 K

Application	Bytes
Unknown	720.66 M
HTTP	208.24 M
RTP	68.46 M
RTMP	63.11 M
BitTorrent	21.97 M
HTTP_Proxy	18.94 M
SSL	10.48 M
FTP_DATA	4.65 M
Direct_Download_Link	3.51 M
IPsec	2.49 M

6 Protocols over Non-Standard Ports

Detected	Expected	Bytes	Packets	Flows
rtp	ndmp (10000)	58.55 M	44.14 K	23
rtmp	macromedia-fcs (1935)	7.71 M	31.53 K	142
ssl	http (80)	6.80 M	33.11 K	2.60 K
direct_download_link	http (80)	3.51 M	4.05 K	59
rtp	msnp (1863)	1.93 M	3.62 K	24
ftp_data	http (80)	1.35 M	957	4
edonkey	http (80)	1.32 M	1.42 K	2
mssql-tds	ms-wbt-server (3389)	1.07 M	2.01 K	71
oscar	http (80)	950.31 K	675	4
rtmp	bnetfile (1120)	624.34 K	430	1

7 Cleartext Passwords

Client	Server	Proto	Username	Password	Flows
..***.***	***.***.***.***	FTP	********	********	3
..***.***	***.***.***.***	FTP	********	********	2
..***.***	***.***.***.***	HTTP Basic	********	********	2
..***.***	***.***.***.***	HTTP Basic	********	********	2
..***.***	***.***.***.***	POP3	********	********	1
..***.***	***.***.***.***	POP3	********	********	1
..***.***	***.***.***.***	SMTP	********	********	1
..***.***	***.***.***.***	POP3	********	********	1
..***.***	***.***.***.***	POP3	********	********	1
..***.***	***.***.***.***	POP3	********	********	1

8 DNS

8.1 Top 10 DNS Queries

DNS Query	Count
www.facebook.com	108
static.ak.fbcdn.net	68
profile.ak.fbcdn.net	56
ntp.ruckuswireless.com	56
www.google.com	51
db._dns-sd._udp.0.1.168.192.in-addr.arpa	46
b._dns-sd._udp.0.1.168.192.in-addr.arpa	46
www.google-analytics.com	45
lb._dns-sd._udp.0.1.168.192.in-addr.arpa	41
r._dns-sd._udp.0.1.168.192.in-addr.arpa	38

8.2 Top 10 DNS Answers

DNS Answer	Count
netgnome.ch	134
www.google.com	77
a749.g.akamai.net	61
www.l.google.com	59
www.facebook.com	58
static.ak.facebook.com.edgesuite.net	54
l.google.com	44
a1725.l.akamai.net	39
static.ak.fbcdn.net	33
clients.l.google.com	32

8.3 Top DNS IPv4/6 Addresses

DNS IPv4 Address	Count
..***.***	80
..***.***	80
..***.***	80
..***.***	80
..***.***	80
..***.***	73
..***.***	71
..***.***	65
..***.***	60
..***.***	60

DNS IPv6 Address	Count
****:****:****:****:****:****::****	2
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1
****:****:****:****:****:****::****	1

8.4 Top-Level Domains (TLD) and Second-Level Domains (SLD)

TLD	Count
com	2.90 K
net	1.07 K
ch	998
arpa	401
org	240
de	208
tv	79
invalid	60
biz	51
uk	28

SLD	Count
fbcdn.net	413
in-addr.arpa	401
facebook.com	277
netgnome.ch	259
google.com	252
akamai.net	192
apple.com	179
bluewin.ch	120
youtube.com	105
google.ch	99

9 HTTP

9.1 Top 10 HTTP User-Agents

User-Agent	Count
Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12	381
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_5; de-de) AppleWebKit/533.19.4 (KHTML, like Gecko) Version/5.0.3 Safari/533.19.4	255
Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12 (.NET CLR 3.5.30729)	149
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12	142
Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10	141
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; de-de) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5	131
Mozilla/5.0 (Windows; U; Windows NT 6.0; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12 (.NET CLR 3.5.30729)	111
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/534.10 (KHTML, like Gecko) Chrome/8.0.552.215 Safari/534.10	104
Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12	103
Mozilla/5.0 (Windows; U; Windows NT 6.0; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12 (.NET CLR 3.5.30729; .NET4.0C)	89

9.2 Top 10 HTTP Hosts and Servers

HTTP Host	Count
www.facebook.com	369
profile.ak.fbcdn.net	253
gartenhof.live1-f.akamaihd.net	136
www.google-analytics.com	132
static.ak.fbcdn.net	97
www.google.ch	67
www.dekoria.de	58
creative.ak.fbcdn.net	57
b.static.ak.fbcdn.net	54
www.youtube.com	53

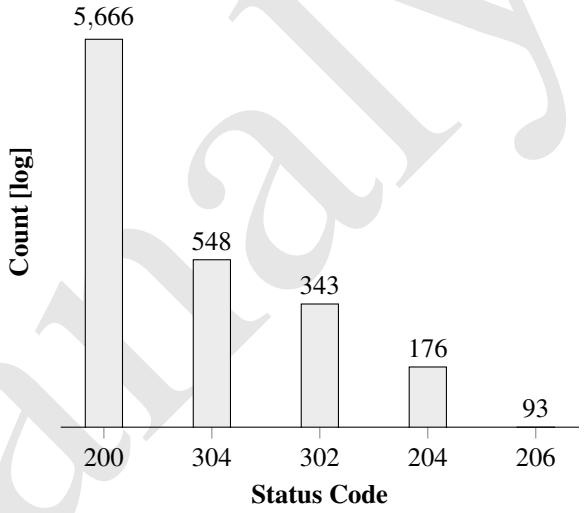
HTTP Server	Count
Apache	1016
Microsoft-IIS/6.0	275
nginx	173
Golfe	164
video_thumbnail_server	143
Microsoft-IIS/7.5	131
AkamaiGHost	126
Apache-Coyote/1.1	123
Apache/2.2.3 (CentOS)	105
GFE/2.0	88

9.3 Top 10 Content-Types

HTTP Content-Type	Count
text	3.34 K
image	3.06 K
application	1.80 K
video	128
multipart	33
audio	9
message	1

HTTP Content-Subtypes	Count
text/html	1.68 K
image/jpeg	1.64 K
image/gif	884
text/plain	623
application/x-javascript	621
image/png	500
application/x-www-form-urlencoded	407
text/xml	354
text/css	267
text/javascript	202

9.4 Top 5 HTTP Status Codes



10 HTTPS

10.1 Top 10 HTTPS Server Name Indication (SNI) and Certificate Common Name (CN)

HTTPS SNI	Count
urs.microsoft.com	23
mail.google.com	16
e-finance.postfinance.ch	15
mac-services.apple.com	10
ebanking1.ubs.com	9
s.yimg.com	8
login.yahoo.com	7
info.tam.ch	6
esta.cbp.dhs.gov	6
courier.push.apple.com.	6

HTTPS Cert. CN	Count
∗.itunes.apple.com	8
courier.push.apple.com	8
∗.systemmonitor.eu.com	6
www.yallo.ch	4
www.google.com	4
client.akamai.com	4
∗.wlxrs.com	3
secure.wlxrs.com	3
pop.gmx.net	3
epass.migros.net	3

10.2 Top 10 Known HTTPS JA3 Signatures

JA3 Hash	Description	Count
2201d8e006f8f005a6b415f61e677532	MSIE 10.0 Trident/6.0, Malware Test FP: blackhole-ek-traffic, sweet-orange-ek-post-infection-traffic, sweet-orange-ek-traffic, styx-ek-traffic	47
2baf01616e930d378df97576e2686df3	MSIE 8.0 & 9.0 Trident/5.0	19
de350869b8c85de67a350c8d186f11e6	Mozilla/4.0 (compatible; MSIE 6.0 or MSIE 7.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022), Malware Test FP: angler-ek-malware-payload-sandbox-analysis-winxp, smoke-loader-post-infection-traffic	15
b9103d9d134e0c59cafbe4ae0a8299a8	Malware: Unknown traffic associated with Dridex	11
96eba628dcb2b47607192ba74a3b55ba	Malware Test FP: angler-ek-traffic-01	3
1d095e68489d3c535297cd8dffb06cb9	Non-Specific Microsoft Socket, Malware Test FP: brazil-malspam-pushes-banload, dhl-malspam-traffic, post-infection-traffic-from-terror-ek-payload, contract-malspam-traffic, cryptowall-traffic, fake-font-update-for-chrome, phishing-malware-run-on-vm, fiesta-ek-post-infection-and-click-fraud-traffic, phishing-malware-sandbox-analysis, angler-ek-traffic, goon-ek-traffic, magnitude-ek-traffic, brazil-malspam-solicitacao-de-orcamento-traffic-example, cryptowall-infection-on-vm, nuclear-ek-traffic, zeus-panda-ba	3
b237ac4bcc16c142168df03a871677bd	Opera/9.80 Presto/2.10.289 Version/12.00	1

11 Warnings

11.1 EXE Downloads

SrcIP4	DstIP4	Advertised Mime	Filename	Size	MD5
..***.***	***.***.***.***	application/octet-stream	_msdownload_update_software_defu_-2010_12_mpas-d_bd1_-0f0fd010a8a0e9c9987b4be882db	8.0K	a8bbf79dedeb2523b92f27c8995efbf4

11.2 ARP Spoofing

ARP spoofing detected for:

- 192.168.47.1
  - 00:0c:29:1d:b3:b1
  - 00:50:56:c0:00:08
- 192.168.47.2
  - 00:0c:29:1d:b3:b1
  - 00:50:56:fd:2f:16
- 192.168.47.254
  - 00:0c:29:1d:b3:b1
  - 00:50:56:f9:f5:54

11.3 DNS Zone Transfer

Time	Client	Server	Query
2010-01-31 22:16:21.261079Z	172.16.16.164	172.16.16.139	contoso.local

11.4 SSH Connections

DateFirstSeen	Duration	srcIP	dstIP	SPkts	SBytes	sshVersion
2010-12-07 20:20:25Z	0.904072	***.***.***.***	***.***.***.***	7	15	SSH-2.0–1.0
2010-12-07 20:20:25Z	0.872386	***.***.***.***	***.***.***.***	5	669	SSH-2.0-OpenSSH_5.6
2010-12-07 20:20:28Z	3.507468	***.***.***.***	***.***.***.***	11	520	SSH-2.0-libssh-0.1
2010-12-07 20:20:28Z	3.507857	***.***.***.***	***.***.***.***	14	1.66 K	SSH-2.0-OpenSSH_5.2