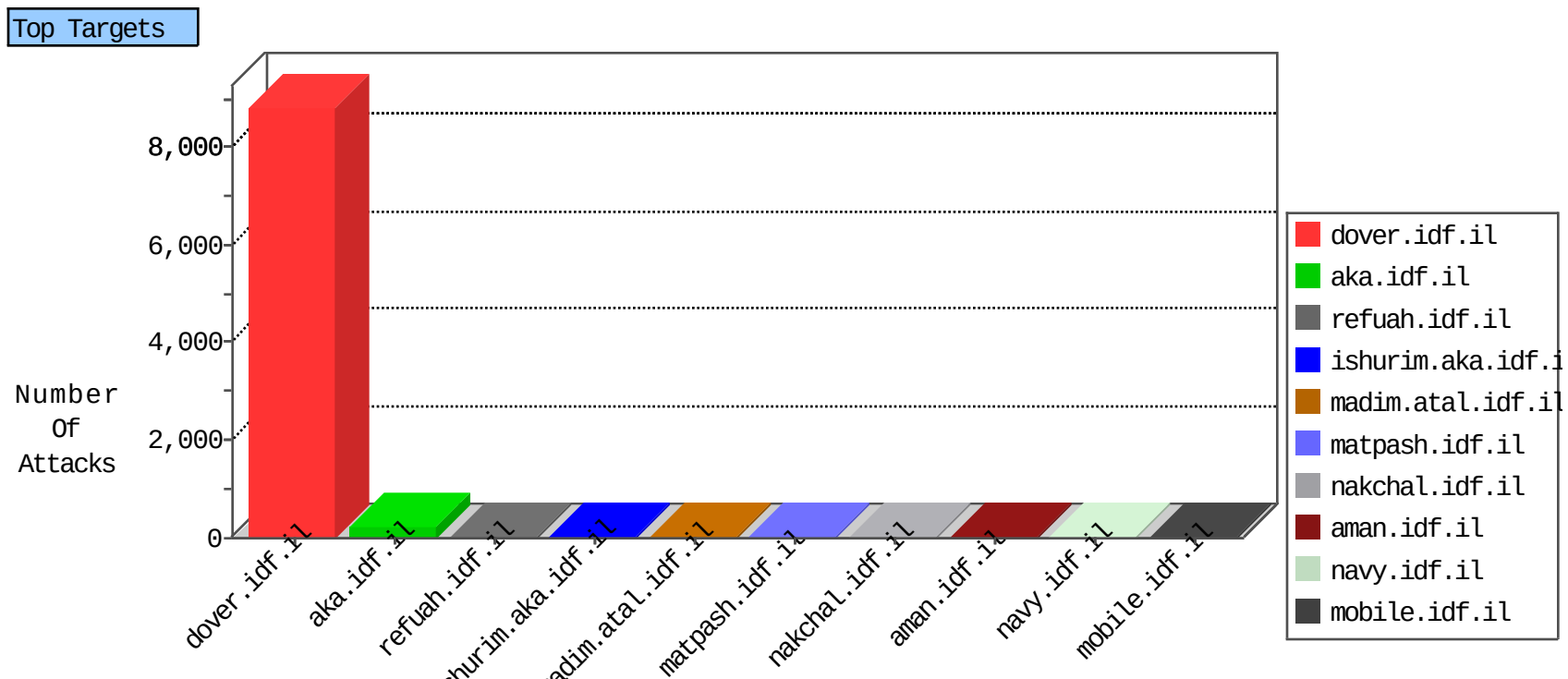
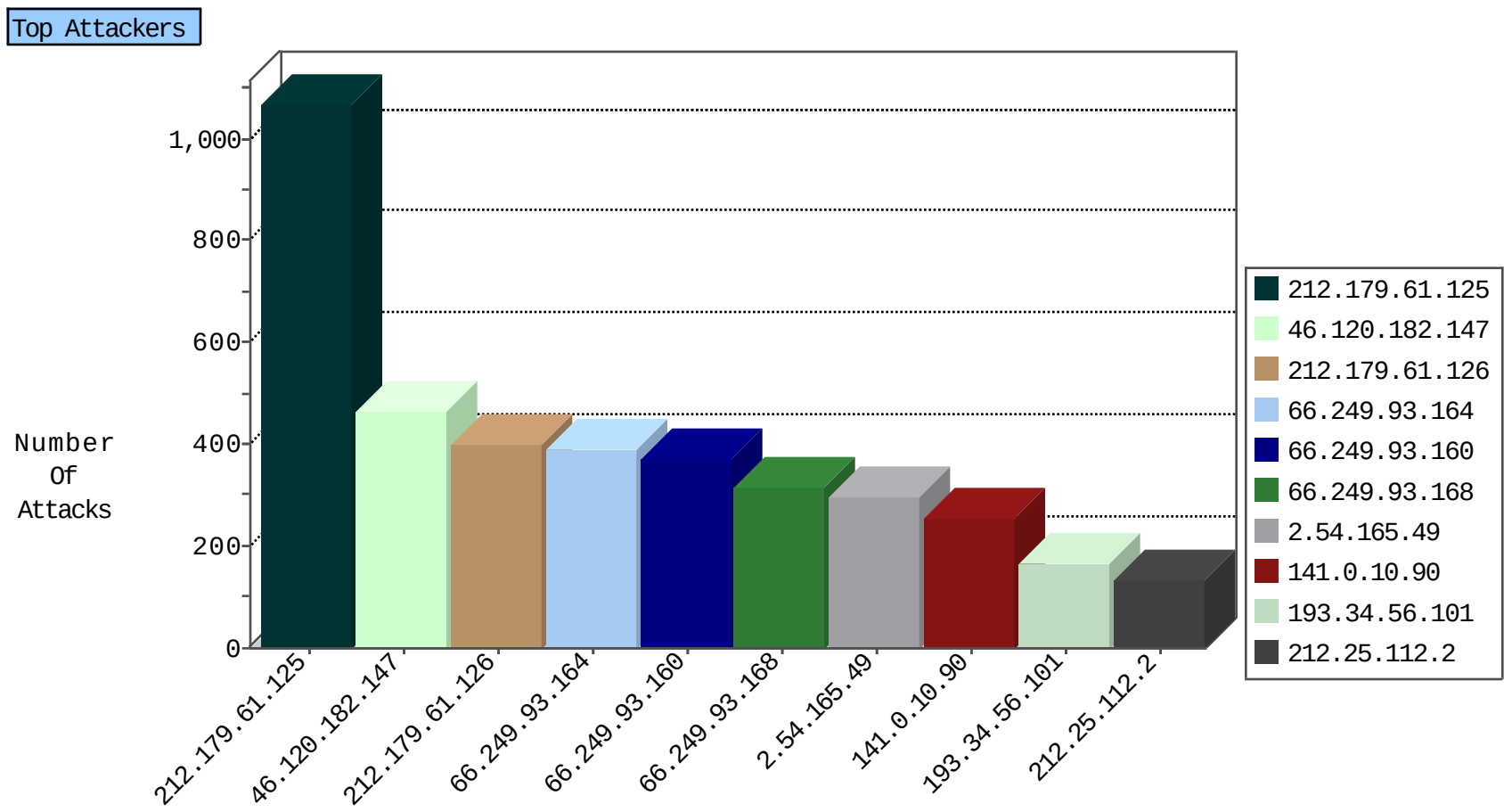
04-20-2015-09:03:04 to 04-20-2015-10:03:04

IDF Under Attack
04-20-2015-09:03:04

Top Targets



Top Attackers



04-20-2015-09:03:04 to 04-20-2015-10:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
185.32.177.54	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
212.179.228.162	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.177.5.94	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	3
79.178.5.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.111.216.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
192.116.142.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
5.28.146.100	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
192.168.1.102		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.61.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
185.32.179.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
210.61.217.43	Taiwan	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.65.148.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.66.124.89	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.166.65.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
62.219.117.40	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
209.88.157.240	Israel	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-20-2015-09:03:04 to 04-20-2015-10:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
10.3.0.107		147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
31.154.17.106	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
77.125.153.239	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
95.35.45.129	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
212.117.140.194	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
82.80.196.44	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
104.232.1.100		147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
84.108.164.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
185.32.178.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
199.203.68.10	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-20-2015-09:03:04 to 04-20-2015-10:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.28.163.195	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
117.135.163.104	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
109.253.159.240	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.29.223	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.27.245	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.36.23	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.143.65	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.76	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.69	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
119.97.231.102	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
112.101.64.5	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.245.99.48		147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.104.89	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	1
147.236.238.22	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
119.97.231.102	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
37.26.146.148	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
117.135.163.104	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1

04-20-2015-09:03:04 to 04-20-2015-10:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1067
46.120.182.147	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	464
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	397
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	382
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	354
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	301
2.54.165.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	296
141.0.10.90	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	255
193.34.56.101	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	168
212.25.112.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	131
212.143.58.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	107
81.218.251.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
46.19.85.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
46.19.85.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	77
46.116.211.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
46.19.86.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	57
166.137.136.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
2.54.0.4	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
217.194.199.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
109.253.133.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
2.54.178.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
194.90.117.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
193.47.165.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
109.160.198.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
79.177.5.94	Israel	147.237.72.166	aka.idf.il	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	40
109.253.159.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
46.19.86.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
31.168.206.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
62.128.35.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.86.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
109.253.139.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
62.0.111.228	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
62.219.86.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
2.54.190.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.19.85.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
212.199.71.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
109.253.129.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
46.116.210.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
83.130.116.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
81.218.188.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
109.253.141.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.151.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
199.203.89.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
212.150.95.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.19.86.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
147.236.238.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.68.208.55	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 87.68.208.55	Block	28
77.127.127.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
95.86.103.113	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
109.67.146.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
149.78.176.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
81.218.97.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.97.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/scripts/css3pie.htc	Block	2
2.54.130.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	2
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	2
193.156.156.90	Norway	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
46.121.29.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.12	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8687-he/refuah.aspx	Block	1
37.8.27.99	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
79.176.195.11	Israel	147.237.0.16	my-kosher-kravi.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/webresource.axd	None	1
66.249.64.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in aka.idf.il/yohalan/home/home.asp	None	1
176.12.150.64	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
109.253.145.201	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
46.19.86.126	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
2.54.34.18	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
213.244.123.98	Palestinian Territory Occupied	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
194.114.146.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1397-he/atal.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
62.210.132.6	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
157.55.39.49	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/info.asp	Block	1
37.16.72.139	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
89.138.226.233	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
80.178.212.121	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.179.61.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.65.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
109.253.145.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
46.116.168.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
2.54.35.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.203.68.10	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
62.210.132.6	France	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
157.55.39.88	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	Block	1
37.26.146.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
80.179.202.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
212.179.132.204	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.138.17.205	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.65.15	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
125.209.235.170	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.117.206.215	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
81.218.135.212	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.22	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1