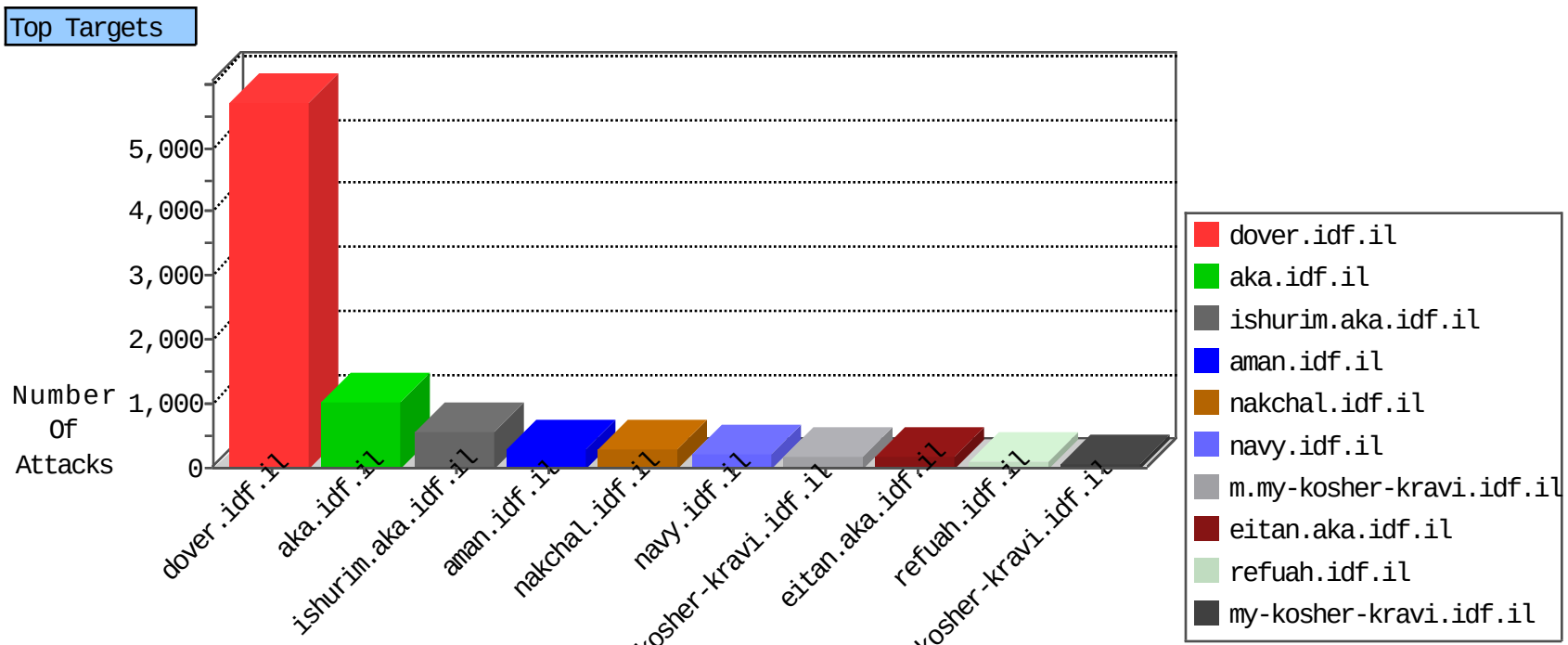
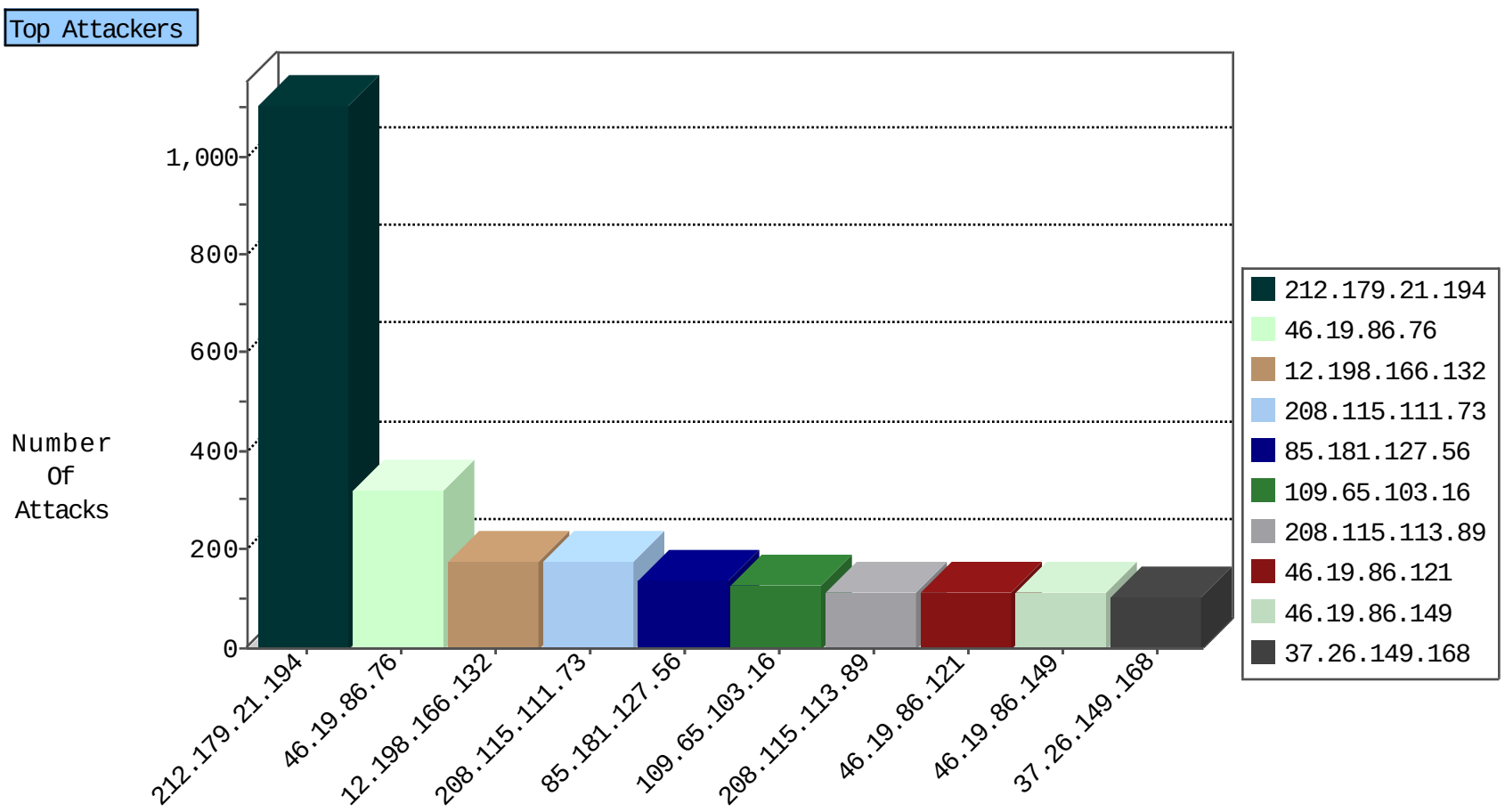
10-22-2015-16:04:03 to 10-22-2015-17:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-22-2015-16:04:03 to 10-22-2015-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	298
2.52.7.118	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	117
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
212.199.63.46	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	74
79.176.22.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	56
79.180.55.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
46.19.85.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
46.121.110.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	29
46.19.86.62	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
62.219.62.202	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
77.125.110.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
79.179.200.191	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
5.29.183.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
93.173.8.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.12.150.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.246.136.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.175.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
77.126.253.189	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.179.58.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.181.62.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
80.12.35.33	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
212.117.128.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
80.179.184.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.54.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
185.112.232.105		147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.160.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.180.190.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
94.199.238.15	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
64.233.172.170	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.66.158.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.121.211.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
199.203.196.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.214.239	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.108.82.13	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
5.29.71.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
174.119.6.32	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.66.49.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
192.116.166.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.9.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.26.147.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.78.49.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.139.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.148.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.181.107.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.3.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

10-22-2015-16:04:03 to 10-22-2015-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.150.187	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
31.154.25.122	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-22-2015-16:04:03 to 10-22-2015-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
95.186.153.38	147.237.77.216	Saudi Arabia	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.208.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.159	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.148.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.12.144.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.48.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.61.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.25.210.25	147.237.77.170	China	maarachot.idf.il	SQL Injection - Select From	1
109.67.112.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.51.96	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
219.74.38.242	147.237.77.216	Singapore	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.132.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.162.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.77.170	Russian Federation	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.19.86.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
149.78.178.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
120.25.210.25	147.237.77.170	China	maarachot.idf.il	ET WEB_SERVER Poison Null Byte	1

10-22-2015-16:04:03 to 10-22-2015-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1036
46.19.86.76	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	318
12.198.166.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	176
85.181.127.56	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
46.19.86.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
46.19.86.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
89.187.220.66	Lebanon	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	87
89.187.220.90	Lebanon	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	68
37.26.148.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
95.86.99.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
46.19.86.180	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
79.179.189.69	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
100.100.49.246		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	58
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
172.56.31.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
85.250.211.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
77.125.123.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.85.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
94.199.238.15	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
2.54.175.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.115.207		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
62.201.214.221	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
79.181.107.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
84.109.242.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.52.7.118	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.176.22.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
197.248.52.234	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
82.102.169.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.34	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
80.178.210.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.112.232.5		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23

10-22-2015-16:04:03 to 10-22-2015-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.168	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	103
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	84
109.65.103.16	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	70
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	56
109.65.103.16	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 109.65.103.16	Block	56
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	56
109.66.15.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.66.15.185	Block	42
2.54.52.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×?×™×©×•×¨×™×?	Block	42
82.80.17.163	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	42
212.179.28.34	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$fat in my-kosher-kravi.idf.il/ajax/reserveschedule/trainingformiframe.aspx	Block	39
94.153.10.149	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 94.153.10.149	Block	28
83.130.1.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
80.230.98.94	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	28
95.35.186.247	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
82.80.150.187	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	28
46.120.74.200	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	28
176.12.151.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
76.182.201.212	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method G[[#0]][[#0]][[#0]]JÂ¢[[#15]]Â’Â?Ã?lÃ‰Â [[#26]][[#5]]Â¤}ÃŽ-Ã¿[[#4]]Ã…[[#26]]Â^C[[#25]]$ÂŽ	Block	14
142.54.172.99	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to dns.cloud.ph/	Block	14
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.120.74.200	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.120.74.200	Block	14
77.125.165.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.1.154	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Unknown Parameter modul.GoTo in www.aka.idf.il/main/giyus/default.aspx	None	14
64.79.144.10	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 64.79.144.10	None	14
46.19.85.87	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
79.180.164.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
142.54.172.99	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to dns.cloud.ph/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
94.153.10.149	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	14
82.80.150.187	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 82.80.150.187	Block	14
46.120.74.200	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	14
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
79.178.35.37	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1085-he/nakhal.aspx	Block	14
132.71.108.4	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
66.102.9.10	United States	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../images/newsarrow.gif	Block	14
84.108.233.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20537-he/	Block	14
46.19.85.87	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
213.57.227.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
149.88.28.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	14
54.67.16.167	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	14
31.168.142.42	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
207.46.13.65	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/sitemap.aspx	Block	14
79.178.58.184	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
141.212.122.96	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /x	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17754	Block	14
84.228.168.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyusmain/home/default.aspx	Block	14
80.246.140.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14

10-22-2015-16:04:03 to 10-22-2015-17:04:03