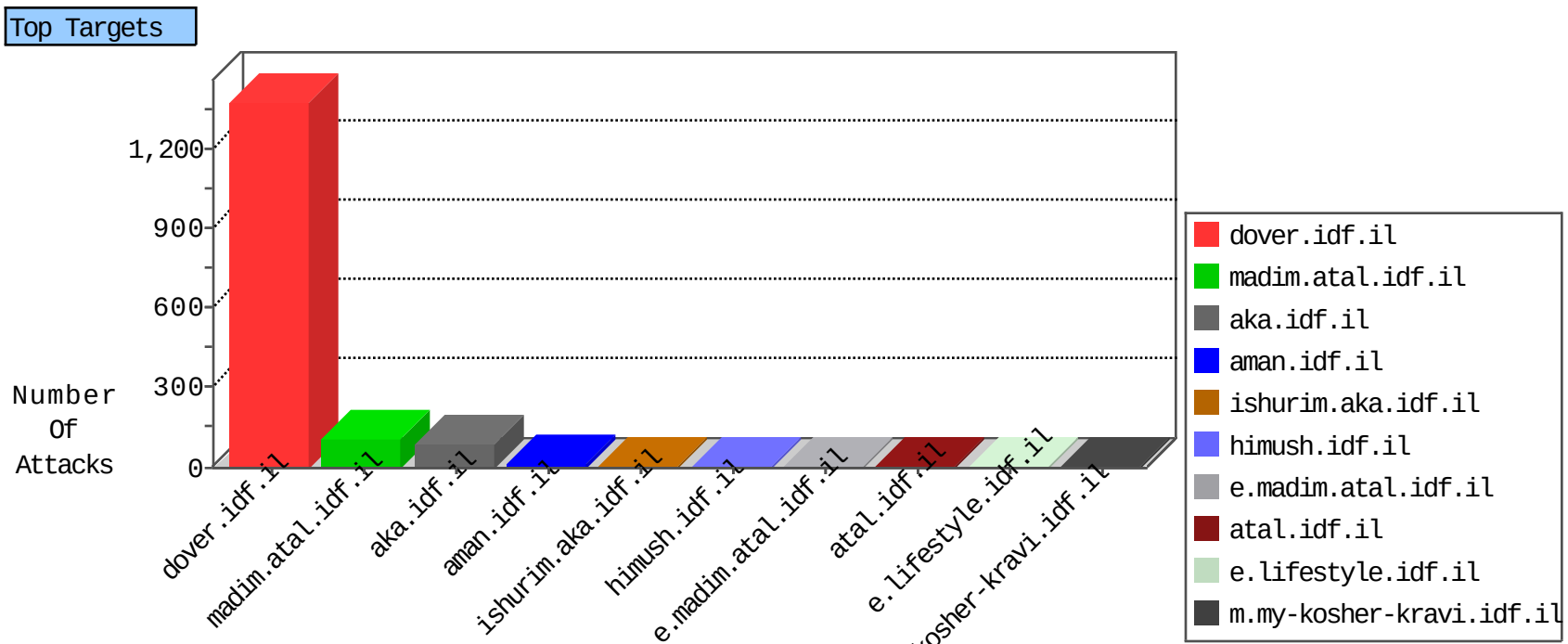
11-09-2015-07:04:00 to 11-09-2015-08:04:00

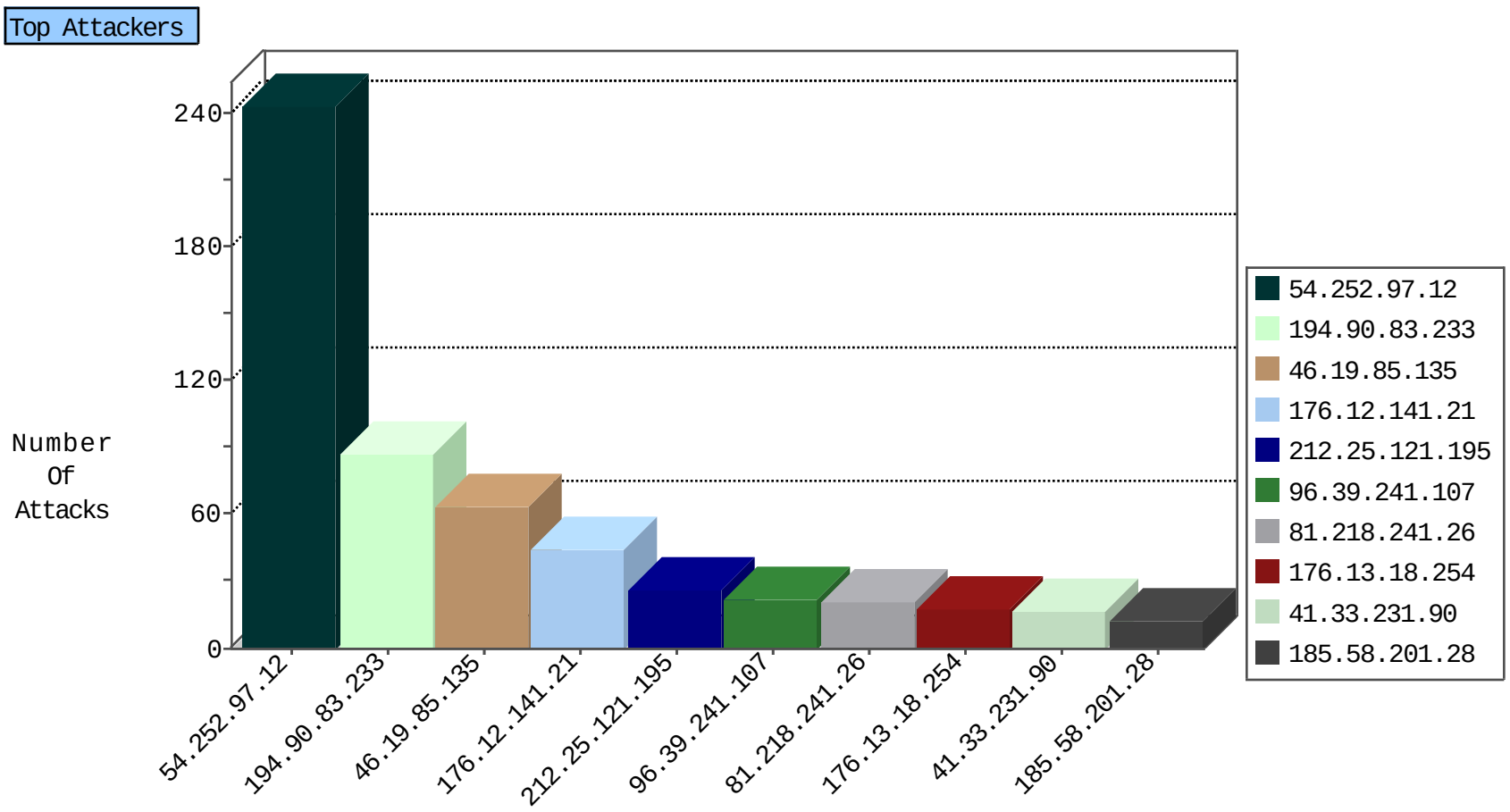
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-09-2015-07:04:00 to 11-09-2015-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.252.97.12	Australia	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	769
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	124
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	26
89.42.53.2	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	7
199.185.225.14	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
140.117.78.4	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
218.38.14.4	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
193.34.70.8	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
158.75.3.19	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
132.248.238.127	Mexico	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
83.166.223.6	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
89.33.88.126	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
142.151.128.65	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
147.83.138.59	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
89.33.88.114	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
188.240.45.15	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
128.197.238.99	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
168.122.23.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
147.83.138.60	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
89.19.0.107	Turkey	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
83.150.81.28	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
121.154.105.108	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
188.240.45.13	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
147.83.138.61	Spain	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
200.145.150.16	Brazil	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
140.113.20.125	Taiwan	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	4
122.0.28.23	Malaysia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
96.47.192.10	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
158.75.18.13	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
185.35.160.123	Russian Federation	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.30.14	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
203.234.49.6	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
200.71.112.3	Venezuela	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
160.216.102.5	Czech Republic	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
83.241.138.74	Sweden	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.35.12	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
81.209.34.43	Finland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.28.13	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
128.39.106.18	Norway	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
141.32.222.110	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
12.107.60.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
74.84.80.50	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
158.75.18.14	Poland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
85.121.159.125	Romania	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
168.122.47.13	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
142.151.128.67	Canada	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
158.108.249.30	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
165.246.154.3	Korea, Republic of	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3

11-09-2015-07:04:00 to 11-09-2015-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-09-2015-07:04:00 to 11-09-2015-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.252.97.12	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 2048	13
54.252.97.12	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -f -sS	13
54.252.97.12	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 1024	13
54.252.97.12	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 4096	12
54.252.97.12	147.237.77.216	Australia	dover.idf.il	ET SCAN NMAP -sS window 3072	12
185.58.201.28	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	3
84.21.203.130	147.237.8.46	Bulgaria	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.165.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.197.120	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.197.120	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
84.21.203.130	147.237.76.44	Bulgaria	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.67.237	147.237.0.34	United States	tikshuv.idf.il	SERVER-IIS asp-dot attempt	1
46.19.86.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.100.84.253	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.62.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.36	147.237.76.176	China	test.ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
172.98.197.120	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
123.173.90.229	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-09-2015-07:04:00 to 11-09-2015-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	87
96.39.241.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
176.13.18.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
80.246.133.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.102.254.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
92.48.11.112	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
94.159.177.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
193.188.136.30	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.228.176.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
93.207.25.181	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.235.143.108	Lebanon	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
80.246.130.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.88.20.65	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.32	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.29.126.99	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.120.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
108.21.68.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.130.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.11.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
220.130.250.82	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
14.139.220.116	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.238.6.174	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	4
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.147.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.238.6.174	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
81.218.189.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.123.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.180.217.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.117.180.21	Luxembourg	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.165.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.238.6.174	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
77.126.97.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.178.202.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.3.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.104.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.129.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.149.17.31	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

11-09-2015-07:04:00 to 11-09-2015-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
176.12.141.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.135	Block	7
176.12.142.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.12.143.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.143.109	None	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.67.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1111-7643-he/nakhal.aspx	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9703-he/refuah.aspx	Block	1
2.54.190.230	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.169.225	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.12.143.109	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.197.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.81.18	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
107.150.43.206	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
66.249.67.217	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
46.19.86.38	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.188.184	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.81.18	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.8.81.18	Block	1
118.33.90.68	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.67.237	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/general.asp...669&docid=72592	Block	1
54.252.97.12	Australia	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.3.242	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.169.10.185	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
66.249.67.48	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/robots.txt	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
61.78.69.113	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.156.59	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.74	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
85.65.83.96	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1

11-09-2015-07:04:00 to 11-09-2015-08:04:00