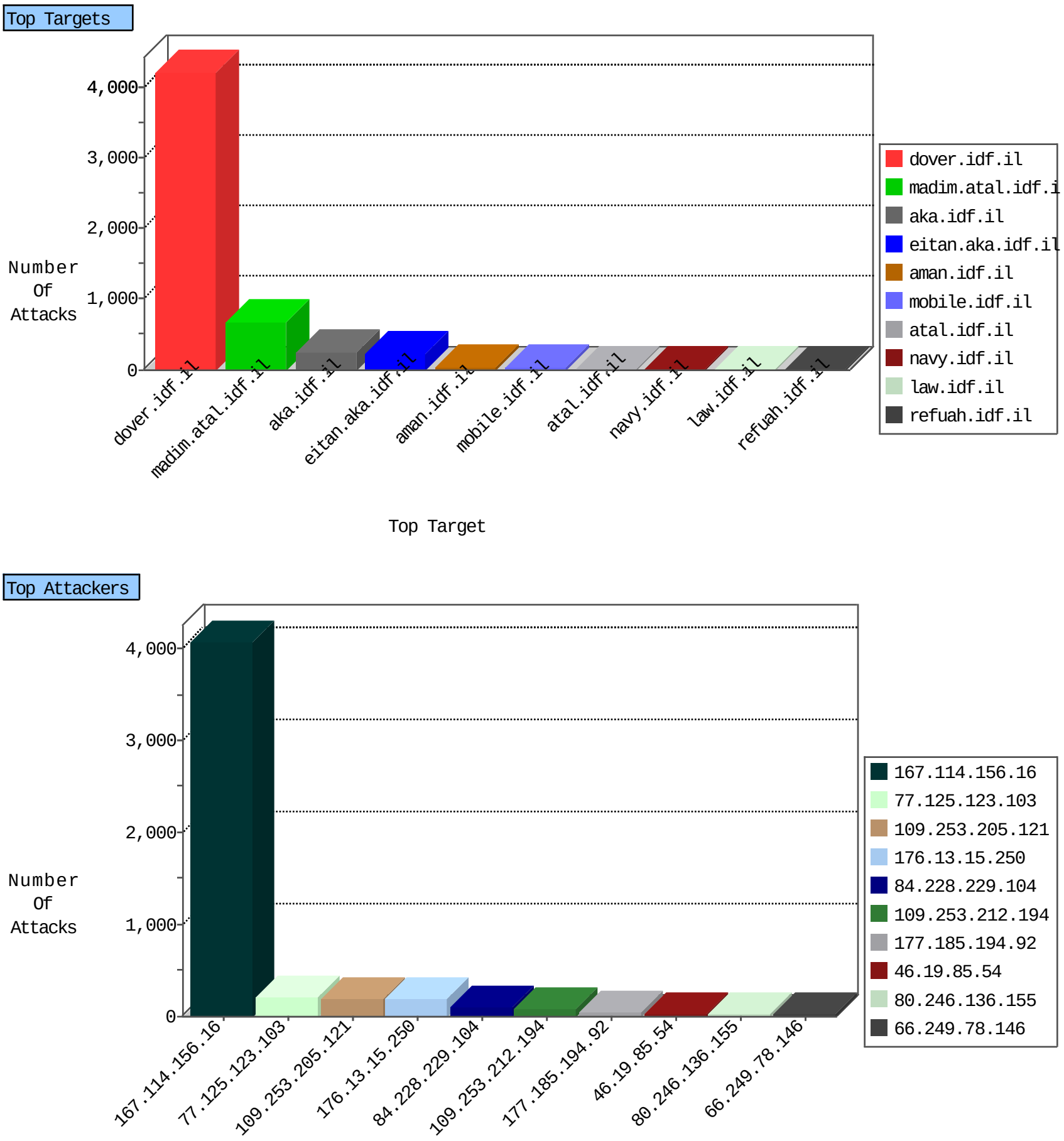
04-19-2016-19:04:03 to 04-19-2016-20:04:03

IDF Under Attack Daily Report



04-19-2016-19:04:03 to 04-19-2016-20:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4081
79.178.196.121	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
94.102.49.116	Netherlands	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
172.82.174.52	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
123.30.183.145	Vietnam	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
209.126.110.228	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
82.145.220.186	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
158.69.115.207	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-19-2016-19:04:03 to 04-19-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.194.92	Brazil	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
177.185.194.92	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
62.210.225.135	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	5056: HTTP: Cross Site Scripting (Javascript in HTTP request)	Block	1

04-19-2016-19:04:03 to 04-19-2016-20:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.194.92	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	37
62.210.225.135	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.93.182	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
62.128.48.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.217.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.220.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.10.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.74.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.95.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.142.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.150.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.109.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

04-19-2016-19:04:03 to 04-19-2016-20:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.123.103	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
87.71.84.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.55.137.36	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.211.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.131.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.175.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.21.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.71.55.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
80.178.190.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.194.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.106.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.15.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.132.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.132.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.244.198	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.253.143.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.54.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
79.176.54.228	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.95.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.54.228	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.67.168.149	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.242.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.19.102	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.91.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.145.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.95.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.59.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.152.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.64.25.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.124.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.107.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.199.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
140.32.69.29	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.23.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.214.232.10	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.64.56.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-19:04:03 to 04-19-2016-20:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.65.131.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.19.102	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
140.32.69.29	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.6.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.8.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.130.181.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	188
176.13.15.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
84.228.229.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
109.253.212.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
80.246.136.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
109.253.221.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.156.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.8.20.109	Block	5
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 95.8.20.109	Block	3
89.139.166.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.102.6.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.55.52.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.115.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.70.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
24.114.223.254	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
37.26.149.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.242	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
105.157.193.229	Morocco	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
87.69.78.78	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.19	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/1056-he.patzar.aspx	Block	1
37.60.150.58	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
141.212.122.161	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8911-he/refuah.aspx	Block	1
5.29.120.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
71.165.244.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
208.80.155.214	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
157.55.39.152	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.109.163.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20451-he/dover.aspx	Block	1
24.114.223.254	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
91.223.89.51	Ukraine	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
80.178.190.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/home	Block	1
217.132.130.255	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx′½„¿„¯„′½„¿„¯„′•′½„¿„¯„′£	Block	1
46.19.85.54	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
197.116.10.100	Algeria	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
95.8.20.109	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
157.55.39.180	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
105.157.193.229	Morocco	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
2.53.181.165	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
199.207.253.101	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.45	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
82.205.127.183	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1