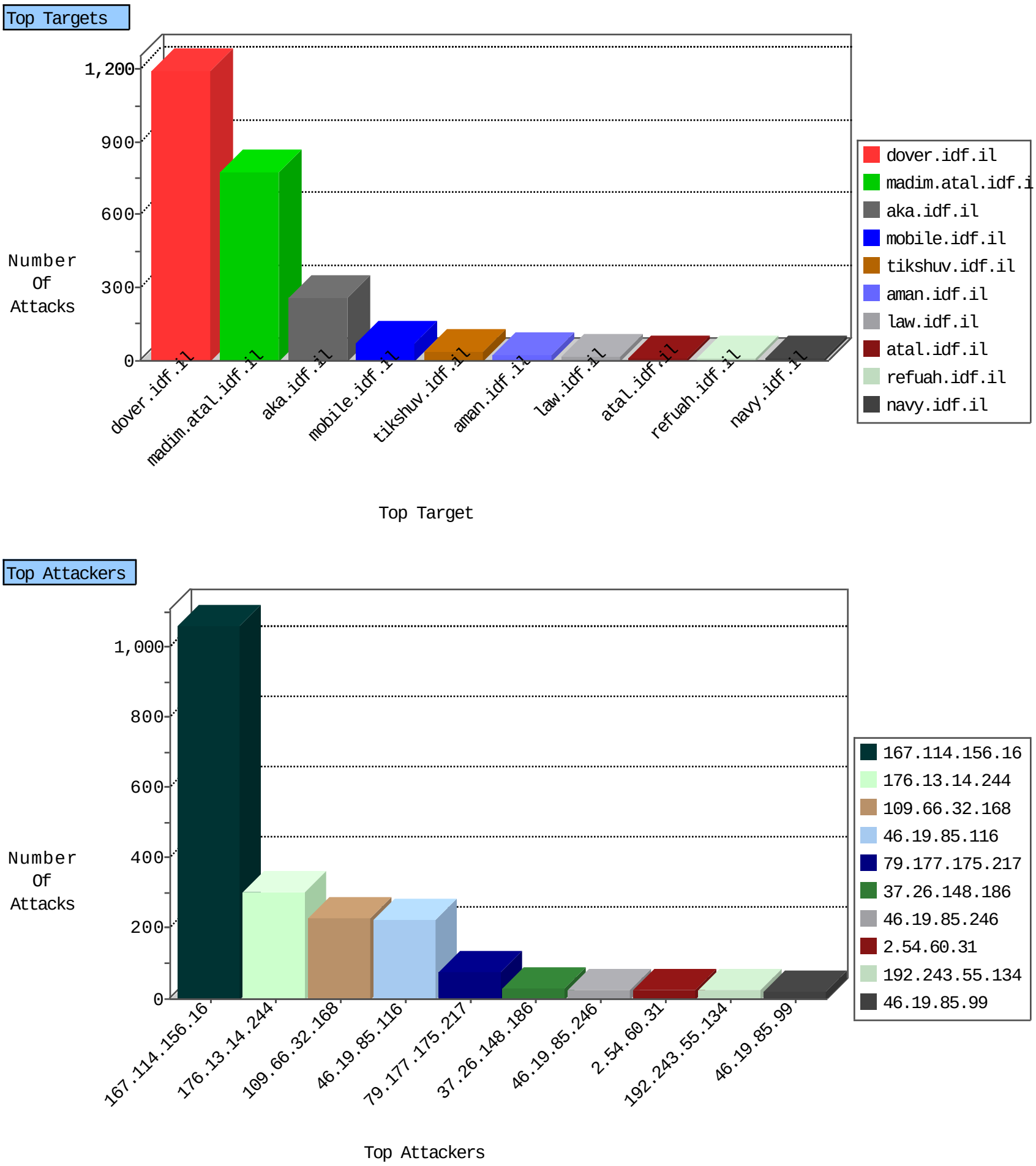
03-11-2016-16:04:07 to 03-11-2016-17:04:07

IDF Under Attack
Daily Report



03-11-2016-16:04:07 to 03-11-2016-17:04:07

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	DOS-Tool-SwitchbladG	dest-reset	4000
79.177.175.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.50	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.50	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.17	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.50	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.50	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.50	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-11-2016-16:04:07 to 03-11-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.144.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.181.218.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.86.115	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
89.138.176.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.11.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.65.23.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.66.16.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.14	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-11-2016-16:04:07 to 03-11-2016-17:04:07

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	4
199.101.186.245	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
122.116.206.72	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.44.133.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
218.57.11.7	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
104.44.133.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.57.11.7	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.57.11.7	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

03-11-2016-16:04:07 to 03-11-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	150
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	alert	75
79.177.175.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
79.177.175.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
2.54.185.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.60.31	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.183.8.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.183.202.47	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	9
77.125.4.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.115.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.51.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.167.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.154.146.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.20.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
84.108.98.134	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.32.179.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.32.179.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.54.143.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.32.179.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.143.136	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.38.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.121.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.0.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.203.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.124.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.250.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.60.31	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.60.31	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
151.34.248.224	Italy	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.199	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.177.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.73.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.15.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.64.235	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.32.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	232
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	225
176.13.14.244	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	81
79.183.229.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.19.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.146.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
2.54.185.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.73.23	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
85.56.108.38	Spain	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.72.211	Israel	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
84.109.51.135	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71095.pdf	Block	1
40.77.167.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.2.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.38.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/shaca	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
46.120.72.211	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/admin	Block	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
84.111.232.111	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.153	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/links/links.aspx	Block	1
40.77.167.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
54.166.81.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
31.154.146.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.229.32.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl63 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx	Block	1
41.238.190.85	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.9.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files	Block	1
94.230.93.52	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
37.8.82.124	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
131.253.25.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.251.91.165	Finland	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
66.249.64.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.64.59.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.82.65.82	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he/shared/usercontrols/headerupper/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/booklets.aspx	Block	1
37.26.146.196	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1