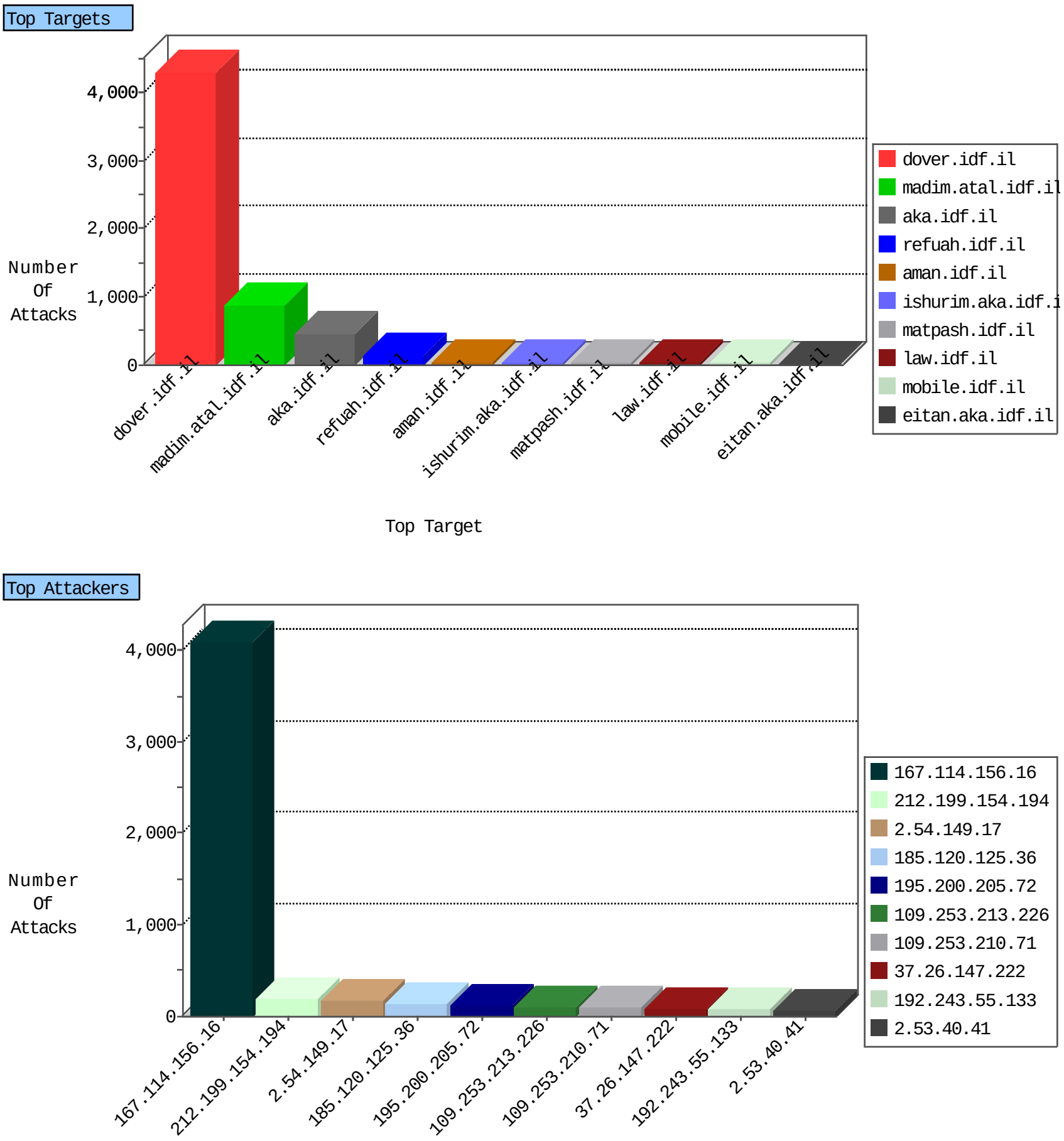
04-11-2016-12:04:00 to 04-11-2016-13:04:00

IDF Under Attack Daily Report



04-11-2016-12:04:00 to 04-11-2016-13:04:00

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	4090
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1305
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	18
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.25.121.195	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
212.25.121.195	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	2
179.43.144.50	Switzerland	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
141.150.59.46	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
74.82.47.25	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
93.215.20.252	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

04-11-2016-12:04:00 to 04-11-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
162.210.196.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
91.197.103.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.98	United States	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
192.187.114.11	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-11-2016-12:04:00 to 04-11-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.53.23.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.192.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
79.180.250.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
212.199.154.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.211.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
207.232.1.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.114.210.53	147.237.72.166	Netherlands	aka.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.76.44	Latvia	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.16.210	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
132.66.235.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.38.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.109.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.21.66.6	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.99.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.76.86	Latvia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.16.210	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.76.42	Latvia	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2016-12:04:00 to 04-11-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.200.205.72	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	63
195.200.205.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
213.55.107.217	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.253.208.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.171	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.138.75	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
62.219.239.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.210.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.23.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.197.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.164.169	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.227.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.182.90	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.136.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.215.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.182	Israel	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
213.204.93.181	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.1.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.52.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.67.174.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.137.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.27.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
213.204.93.181	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.52.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.235.108.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.52.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.147.111	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-11-2016-12:04:00 to 04-11-2016-13:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
62.0.118.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.149.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	176
185.120.125.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
109.253.213.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.253.210.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.53.40.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.55.9.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
176.13.19.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
176.13.2.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
206.190.140.158	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 206.190.140.158	Block	21
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
212.199.146.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 81.218.53.114	Block	4
212.199.146.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/7/	Block	3
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.112.23	Block	3
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.59	Block	2
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple _vti_ from 81.218.53.114	Block	2
176.13.8.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.148.133	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.78.151.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.140.58	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
109.253.146.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.146.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method [z[[#17]]Ú{þéK	Block	1
91.208.93.147	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
79.176.12.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.69.3	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/shared/clientscripts/swfobject.js	Block	1
157.55.39.13	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method =í¶¸6º7_[[#28]][[#20]]H in URL ¬[[#18]]igjÛ¸ƚˆÊÝˆ[[#0]]gÿy[[#26]]²kuÚmq{-ŕ× ½¸··v¸q2wa	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method	Block	1
31.168.23.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal URL Path Encoding ’<•₪..˜‹%Дj}¨¡xx)š½[[ץ¶#0¸e]]ɔy¨·´"¸n´¿0h¼¸tb¡•y8]]#30[[2¸¦©]]#30[[ı³ע{	Block	1
93.149.68.253	Italy	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
79.180.136.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL ¬[[#18]]igjÛ¸ƚˆÊÝˆ[[#0]]gÿy[[#26]]²kuÚmq{-ŕ× ½¸··v¸q2wa	Block	1
168.235.197.16	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.69.11	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/webresource.axd	Block	1
109.64.208.137	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1