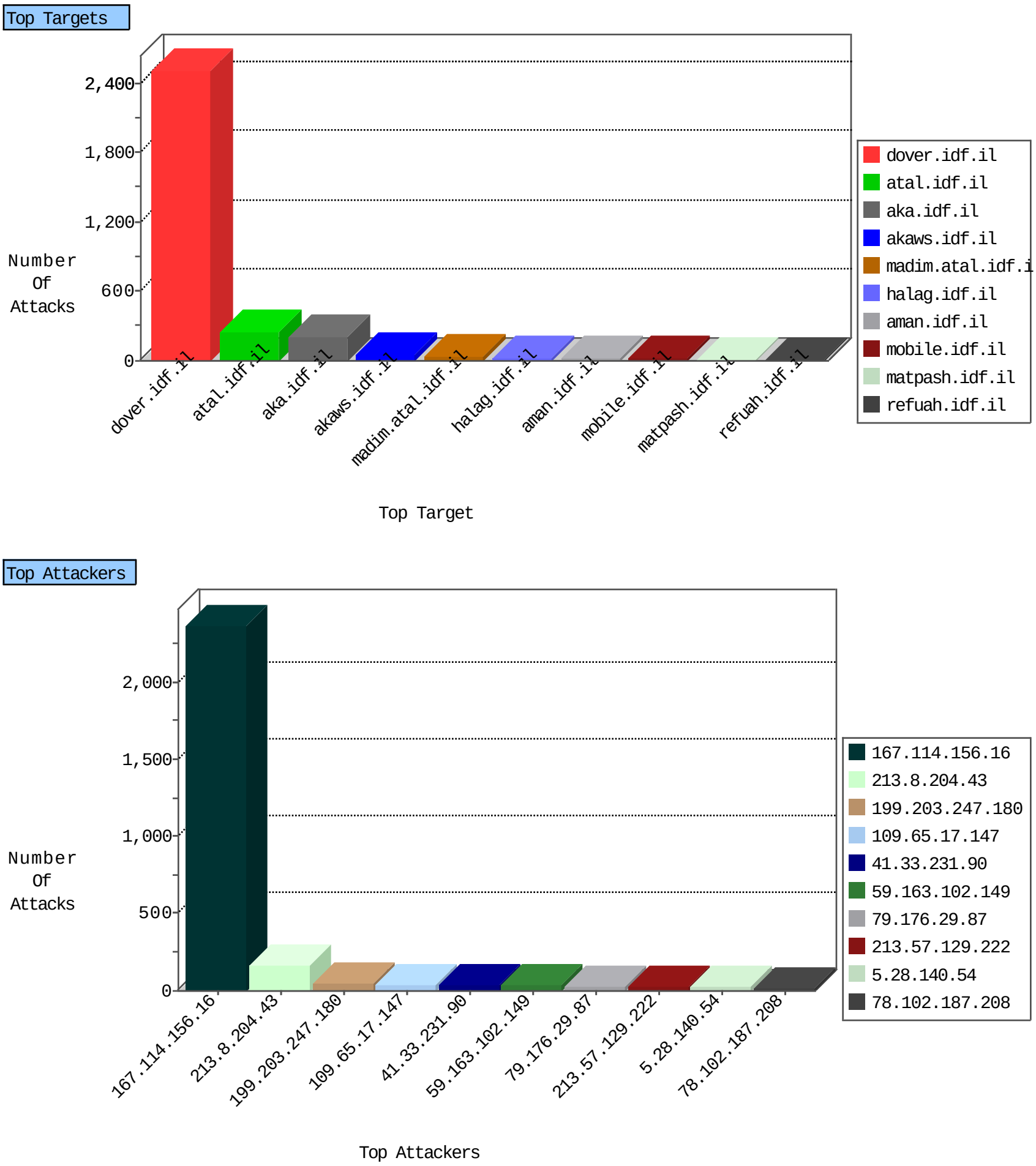
12-18-2015-17:04:03 to 12-18-2015-18:04:03

IDF Under Attack Daily Report



12-18-2015-17:04:03 to 12-18-2015-18:04:03

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	DOS-Tool-SwitchbladG	dest-reset	3386
146.185.57.7	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
59.163.102.149	India	147.237.77.227	e.hamaz.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
208.67.1.66	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

12-18-2015-17:04:03 to 12-18-2015-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-18-2015-17:04:03 to 12-18-2015-18:04:03

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	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.163.102.149	147.237.77.243	India	mobile.idf.il	ET SCAN Potential SSH Scan	2
59.163.102.149	147.237.77.233	India	atal.idf.il	ET SCAN Potential SSH Scan	2
59.163.102.149	147.237.77.170	India	maarachot.idf.il	ET SCAN Potential SSH Scan	1
219.153.15.122	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.72.156	India	aman.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.19	India	law-forum.idf.il	ET SCAN Potential SSH Scan	1
219.153.15.122	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.8.46	India	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.201	India	e.atal.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.8.14	India	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
219.153.15.122	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.176	India	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
59.163.102.149	147.237.76.44	India	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.234	India	halag.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.38	India	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.30	India	himush.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.72.166	India	aka.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.74	India	law.idf.il	ET SCAN Potential SSH Scan	1
219.153.15.122	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.72.14	India	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.202	India	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.8.27	India	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
219.153.15.122	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.199	India	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.0.19	India	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.223	147.237.0.34	United States	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	1
59.163.102.149	147.237.76.196	India	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
78.193.2.8	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.163.102.149	147.237.76.86	India	navy.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
59.163.102.149	147.237.76.39	India	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.76.34	India	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.77.216	India	dover.idf.il	ET SCAN Potential SSH Scan	1
59.163.102.149	147.237.72.217	India	e.idf.il	ET SCAN Potential SSH Scan	1

12-18-2015-17:04:03 to 12-18-2015-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.8.204.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	168
199.203.247.180	Israel	147.237.0.35	akaws.idf.il	drop		drop	49
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.65.17.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
78.102.187.208	Czech Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
109.65.17.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.54.167.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.176.29.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
176.12.141.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
213.57.129.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
197.49.116.118	Egypt	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.57.164.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
5.28.140.54	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.171.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.132.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.28.140.54	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.176.29.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
62.28.244.1	Portugal	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
117.103.185.20	Japan	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
213.57.129.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
130.207.203.56	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
2.54.42.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.192.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.29.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.250.5.155	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.240.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
157.55.2.129	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.179.52.149	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.52		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.130.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.46.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.232.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
213.57.42.29	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.136.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
31.210.183.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
109.65.164.134	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.249.12.51	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.12.136.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.8.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.178.8.177	Block	14
109.67.32.228	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.32.228	Block	12
176.12.140.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.20.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.186.184.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.94.49.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.97.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
62.28.244.1	Portugal	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.28.244.1	Block	2
31.168.120.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
37.142.64.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.53.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.10.163	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation SearchText in www.logistics.atal.idf.il/938-he/halag.aspx	Block	1
213.57.164.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.228.69.92	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.176.107.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.164.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.116.218.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.28.140.54	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
93.172.43.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/12836.jpg	Block	1
79.183.5.148	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.69.26	Block	1
159.203.121.163	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
109.64.142.149	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
40.77.167.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.60.23	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
213.57.164.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.146.117	Block	1
79.178.160.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.153.32.246	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
109.65.17.147	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
40.77.167.42	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.65.117.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.215.175	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
79.182.113.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.32.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/67701.pd	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.230.69.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/home/def...78&catid=38978	Block	1
176.12.141.151	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.198.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
45.55.42.154		147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
85.250.214.43	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1