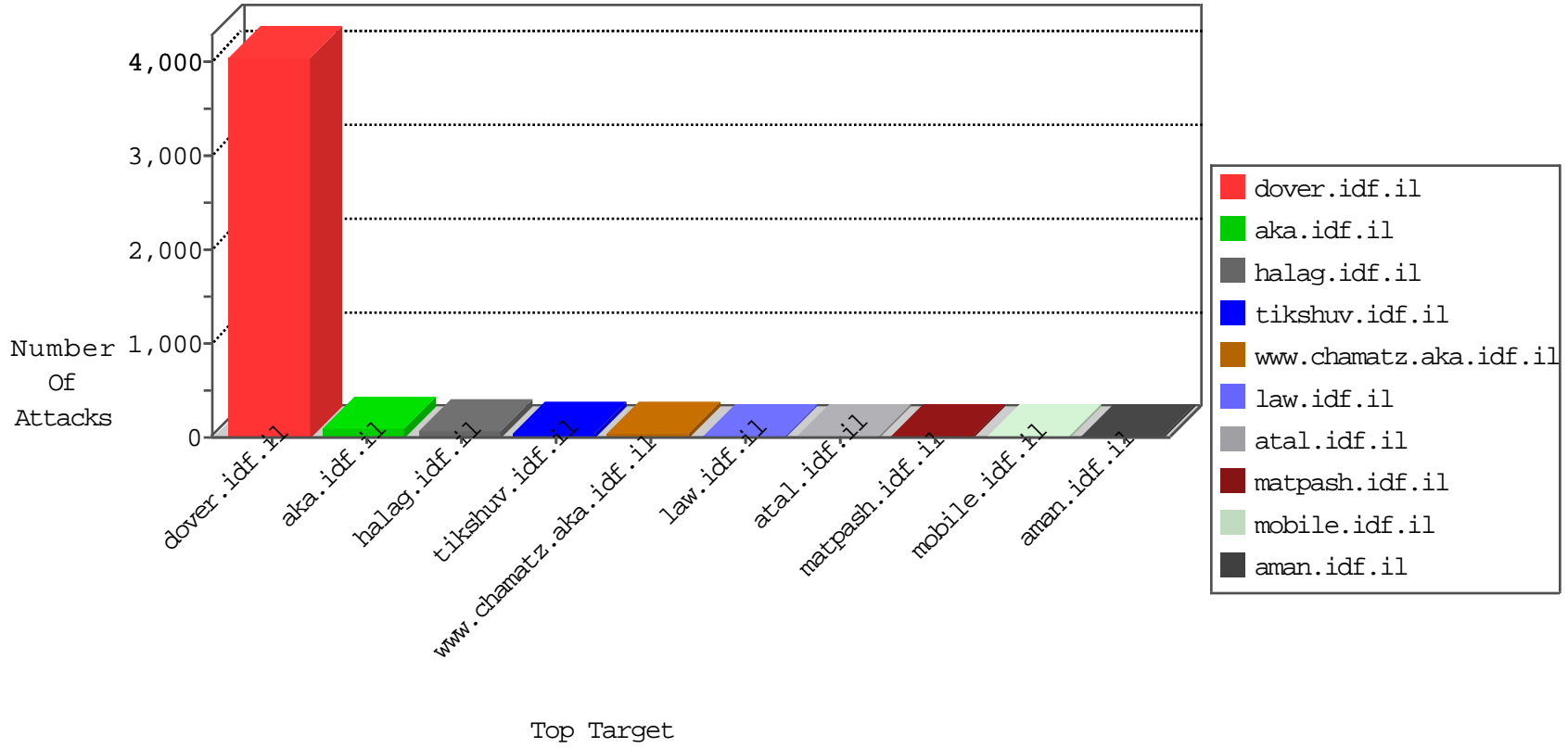


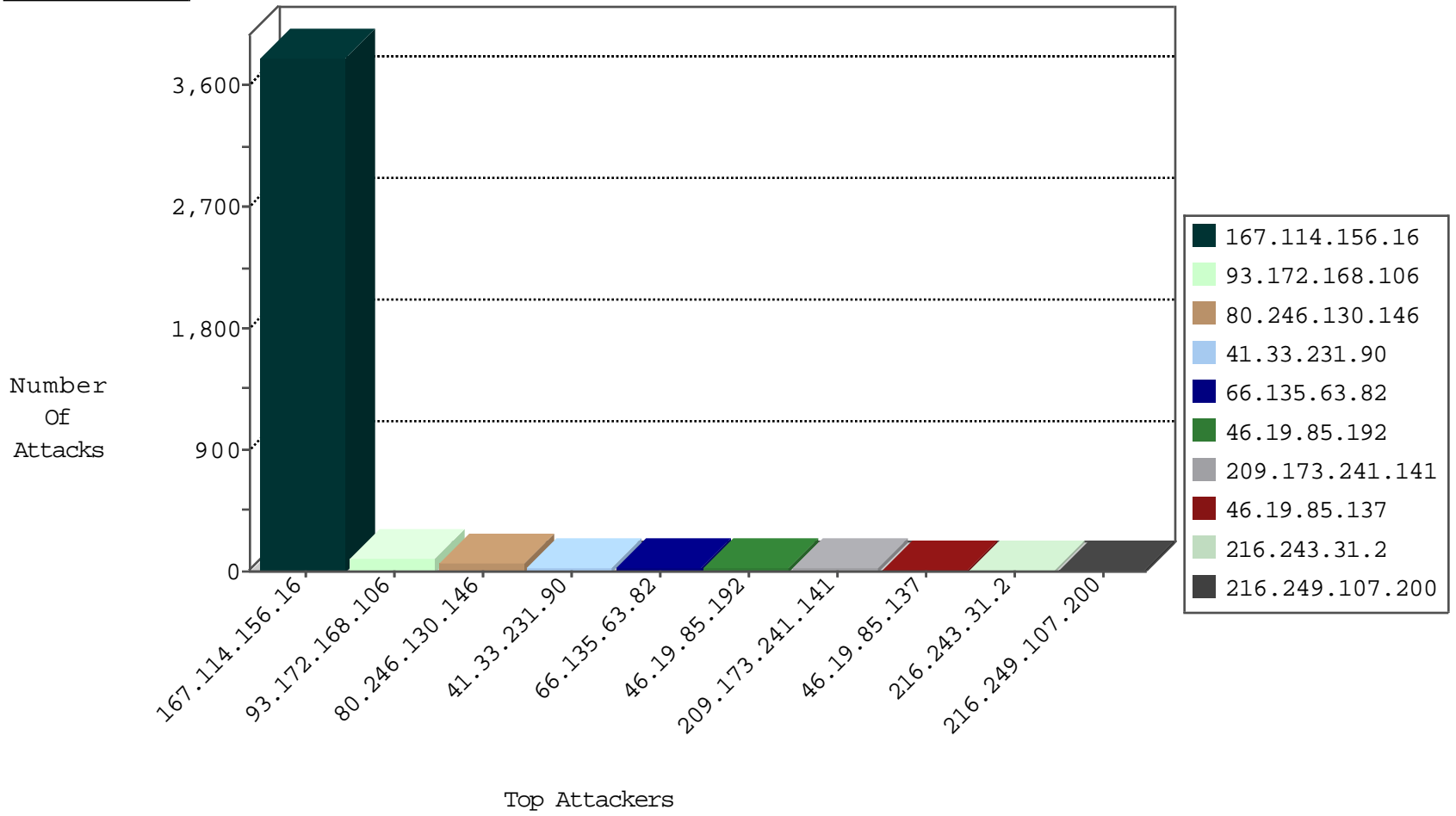
IDF Under Attack Daily Report



Top Targets



Top Attackers



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_Tp_Web_In	drop	3816
79.177.39.89	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
79.177.39.89	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.108.152.18	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
79.182.36.215	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
125.127.86.131	China	147.237.77.227	e.haraz.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
216.249.107.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
134.147.203.115	Germany	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	2
120.132.50.135	China	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.135.63.82	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
149.88.88.119	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
195.234.228.90	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
67.228.38.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
62.210.115.133	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
209.173.241.141	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
209.173.241.141	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
216.249.107.200	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.73.150.148	Turkey	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
94.73.150.148	Turkey	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
94.73.150.148	Turkey	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.135.63.82	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	14
209.173.241.141	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	10
94.73.150.148	147.237.76.42	Turkey	refuah.idf.il	SQL Injection - Select From	6
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
216.249.107.200	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	4
195.234.228.90	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	4
79.177.202.69	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
37.97.143.205	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
162.144.41.122	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
120.150.96.54	147.237.72.14	Australia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.76.34	Kazakstan	ychalan.idf.il	ET SCAN NMAP -f -sS	1
37.97.143.205	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.54.169	147.237.8.28	France	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
186.112.18.220	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.144.41.122	147.237.76.34	United States	ychalan.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.34	Kazakstan	ychalan.idf.il	ET SCAN NMAP -sS window 2048	1
82.166.184.187	147.237.72.14	Israel	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
61.216.10.236	147.237.8.46	Taiwan	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.77.234	Latvia	halag.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.168.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
80.246.130.146	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.27.75	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.213.138	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.125.75.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.141.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
216.249.107.200	United States	147.237.77.216	dover.idf.il	IP Fragments	Failed to generate IP packet from fragments	drop	4
89.139.231.151	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.29.216.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.137	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.137	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.9.240.226	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.182.48.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.187.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.26.148.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.146.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.7.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.104.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.120.125.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.116.4.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.20.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.141.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.65.21.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.46.38.151	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.3.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
40.78.146.128	United States	147.237.76.30	himush.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	2
104.209.188.207	United States	147.237.76.30	himush.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	2
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.47.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.214.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.214.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.148.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
169.229.3.91	United States	147.237.76.148	ggcenter.aka.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.230.86.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.93	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
79.176.138.150	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 79.176.138.150	Block	6
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.207.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
79.176.138.150	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	2
2.53.52.248	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.191	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.85.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.36.161	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
38.125.121.5	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
176.13.17.210	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
69.171.228.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.150.168.95	Germany	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
79.182.60.214	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.148.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
149.88.190.212	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
77.75.77.36	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
80.246.130.146	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.63	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
37.26.149.219	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.50	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.125.159.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
89.139.231.81	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1