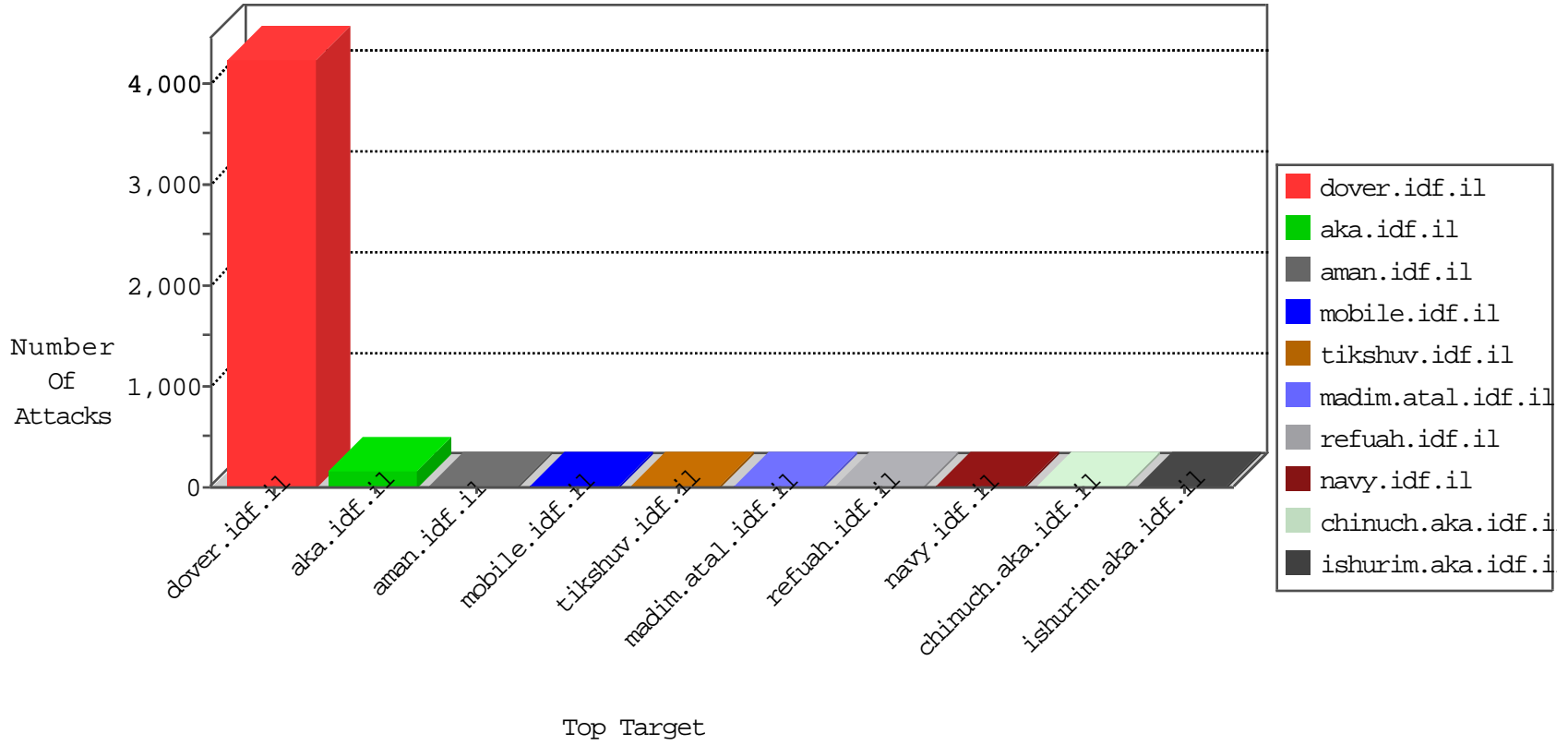




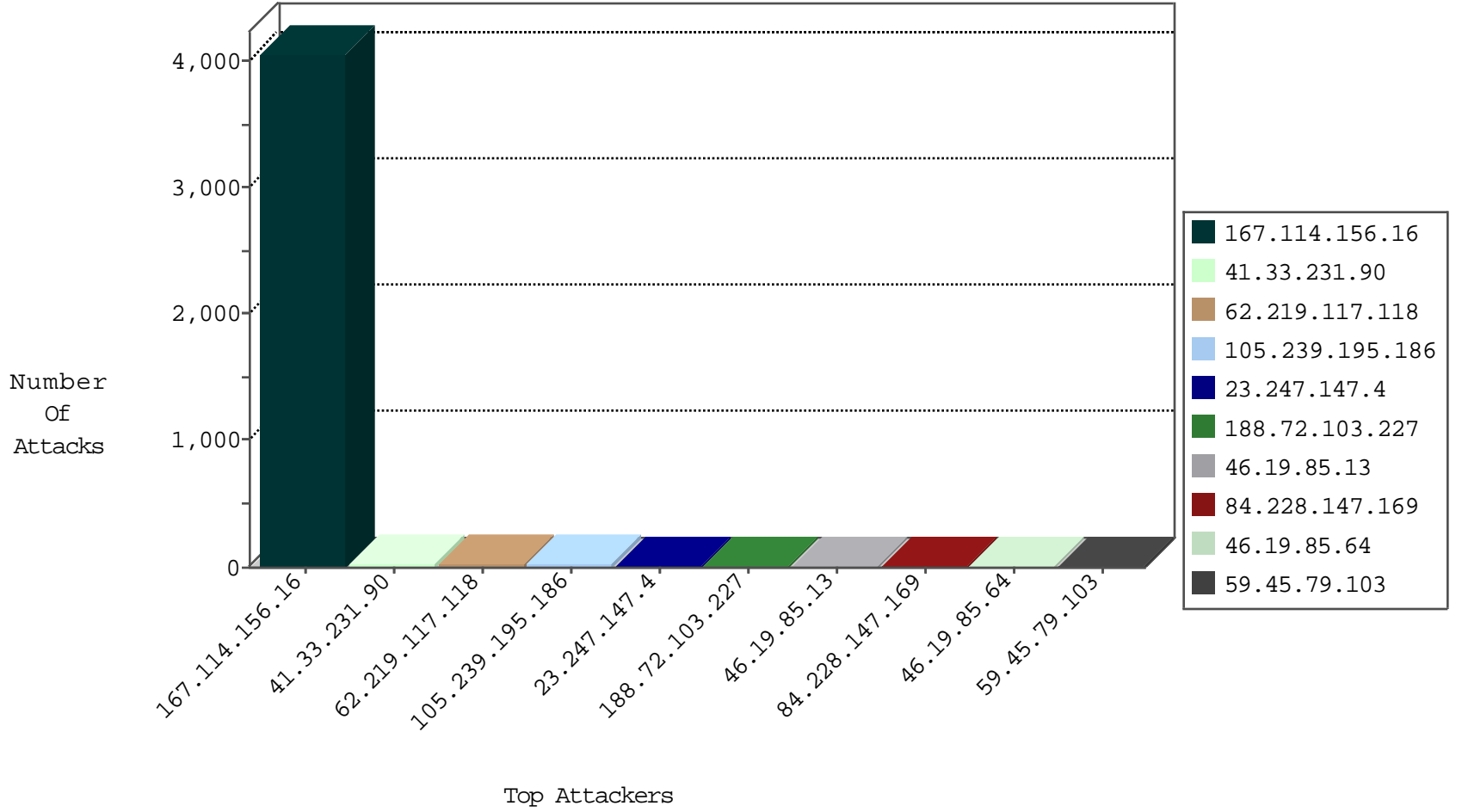
# IDF Under Attack Daily Report



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_Ip_Web_In	drop	4046
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
179.43.141.194	Switzerland	147.237.8.24	e.lifestyle.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
179.43.141.194	Switzerland	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.163.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.106	China	147.237.76.42	refuah.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
106.120.188.165	China	147.237.77.216	dover.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

## 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
59.45.79.103	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.151.147.34	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.76.148	Germany	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
101.200.82.129	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.103	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
1.54.106.90	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.103	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
210.15.242.7	147.237.77.178	Australia	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
192.151.147.34	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.4.79.76	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
115.28.218.77	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.219.117.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
188.72.103.227	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
84.228.147.169	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
62.219.162.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.179.15.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.13	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.219.117.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.92.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.176	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.199.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.243.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.220.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
65.55.210.100	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.120.148.154	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.70.27.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.150	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.130.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.59.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.38.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.134.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.19.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.64.87.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.53.42.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.138.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.190.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.72.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.233.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.37.57	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
185.3.144.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-16-2016-19:04:01 to 04-16-2016-20:04:01

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.50.193	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.13	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.50.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.11.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
31.154.254.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 31.154.254.160	Block	4
46.117.199.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.38.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.70.38.62	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21100-	Block	1
81.111.195.163	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
23.247.147.4	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/	Block	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.182.20.12	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/163-7173-he/patzar.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
204.79.180.251	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.209	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3467.jpg	Block	1
204.79.180.33	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
27.159.234.88	China	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
108.26.186.192	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	1
81.111.195.163	United Kingdom	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.111.195.163	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2297.jpg	Block	1
204.79.180.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/	Block	1
2.53.37.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
93.172.229.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/horaot	Block	1
204.79.180.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.21.55	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.111.195.163	United Kingdom	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/13.asp	Block	1
157.55.39.172	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
2.53.135.13	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
93.172.229.16	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
204.79.180.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.111.195.163	United Kingdom	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.210	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.210	Block	1
23.247.147.4	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
106.186.113.132	Japan	147.237.77.233	atal.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.117.199.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.79.180.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1