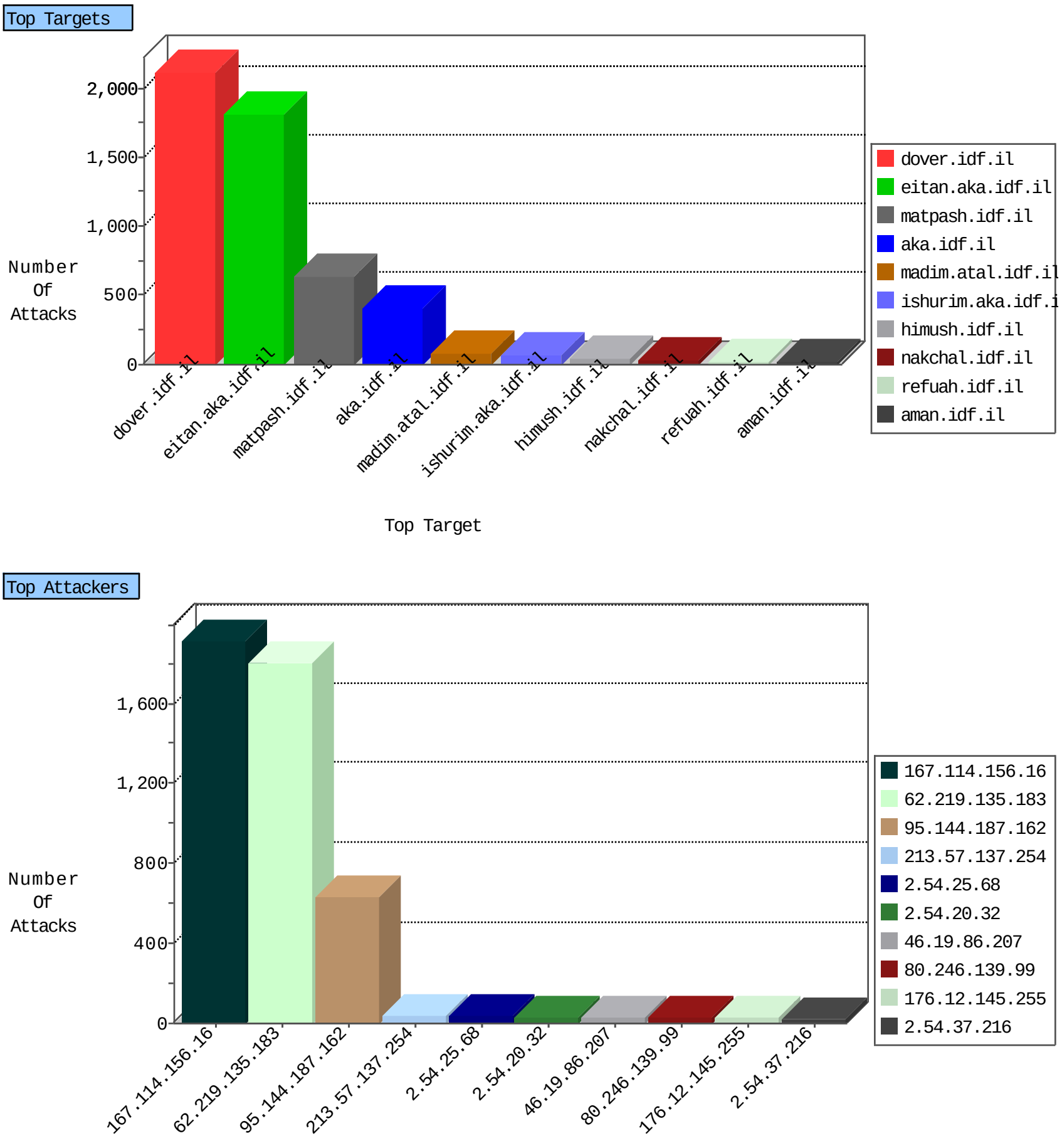
12-16-2015-08:04:01 to 12-16-2015-09:04:01

IDF Under Attack Daily Report



12-16-2015-08:04:01 to 12-16-2015-09:04:01

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	3281
80.246.136.202	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
2.52.164.154	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
210.215.149.197	Australia	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

12-16-2015-08:04:01 to 12-16-2015-09:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.108.59	Netherlands	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	8
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.75	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-16-2015-08:04:01 to 12-16-2015-09:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
198.20.108.59	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	12
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
198.20.108.59	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
188.120.148.155	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
188.120.148.155	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
66.249.93.107	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
175.44.218.6	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
175.44.218.6	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
108.184.162.6	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
186.103.142.170	147.237.76.30	Chile	himush.idf.il	ET SCAN NMAP -sS window 1024	1
108.184.162.6	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
86.235.170.145	147.237.0.35	France	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.44.218.6	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
175.44.218.6	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
31.168.67.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
175.44.218.6	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
108.184.162.6	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
108.184.162.6	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
182.86.228.89	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.184.162.6	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
175.44.218.6	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
62.219.135.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
175.44.218.6	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

12-16-2015-08:04:01 to 12-16-2015-09:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.219.135.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1716
95.144.187.162	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	637
2.54.37.216	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.57.137.254	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
207.241.229.104	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	18
46.19.86.85	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
213.57.137.254	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
199.30.24.36	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.136.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
217.194.197.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
82.80.153.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
2.54.172.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.132.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.164.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.135.14	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
113.106.101.75	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
62.219.135.183	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
217.25.48.17	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.25.48.17	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.219.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.61.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.7.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.254.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.161.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.80.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.66.107	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
79.183.190.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.171	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
2.52.12.180	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.81	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
62.219.135.183	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 62.219.135.183	Block	79
2.54.25.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.25.68	Block	34
2.54.20.32	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.20.32	Block	30
80.246.139.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.207	Block	28
176.12.145.255	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.12.145.255	Block	28
46.19.86.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.6.239	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.6.239	Block	21
2.54.174.185	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	12
185.24.207.15	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.24.207.15	Block	9
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	7
149.78.158.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.66.83	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.246.137.46	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.137.46	Block	5
66.249.66.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.12.151.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.199.57.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.32.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
176.13.15.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.45	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.138.45	Block	3
66.249.66.87	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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	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
176.13.13.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.202.35	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
212.179.177.148	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.219.161.153	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
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	1
84.111.160.81	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
80.246.137.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/dist/fonts/opensanshebrew/opensanshebrew-bold.ttf	Block	1
68.180.228.49	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
2.54.165.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.1.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.112.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
60.214.152.78	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/jeecms.do	Block	1
185.32.179.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.201.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.33.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
113.106.101.75	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-14255-en/dover.aspx	Block	1