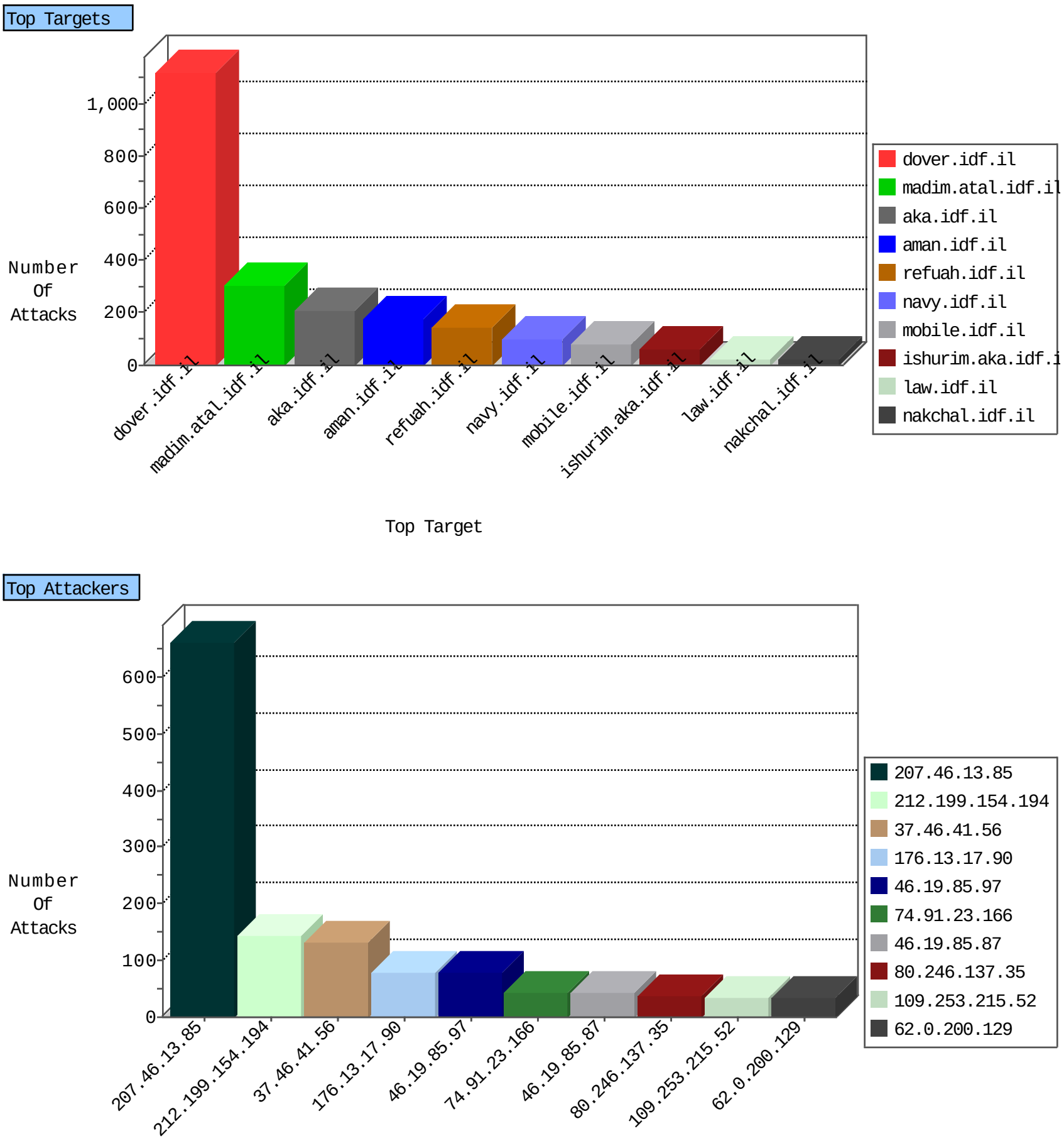
10-05-2016-09:04:00 to 10-05-2016-10:04:00

IDF Under Attack Daily Report



10-05-2016-09:04:00 to 10-05-2016-10:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.154.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	781
77.125.7.89	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
82.221.105.6	Iceland	147.237.76.176	test.ncore.idf.il	Black List	drop	1
176.13.8.25	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
80.179.90.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-05-2016-09:04:00 to 10-05-2016-10:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
62.210.250.212	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-05-2016-09:04:00 to 10-05-2016-10:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.118.197.230	147.237.76.38	Romania	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
89.248.163.3	147.237.0.33	Netherlands	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.3.147.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.146.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.150.177.188	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
217.23.6.58	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.135	147.237.0.34	Europe	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
217.23.6.58	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
46.229.223.8	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.251.250	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
217.23.6.58	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.207.145.105	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.93.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.25.107.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.121.147.218	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
194.120.84.9	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.28.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.70.189.124	147.237.72.156	China	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.246.136.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.228.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.230.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.218.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.213.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.90.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.23.6.58	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.207.145.105	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.196.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.24.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.149.222.5	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

10-05-2016-09:04:00 to 10-05-2016-10:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	660
212.199.154.194	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	71
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
2.53.146.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	31
2.53.128.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.57.138.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
62.0.200.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
62.0.207.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
109.253.201.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
148.177.168.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
158.169.40.7	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
80.246.138.125	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.117.17.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
118.173.132.113	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.65	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.53.24.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
194.90.66.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
109.253.215.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
31.146.114.66	Georgia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
62.219.173.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.215.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
109.253.215.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
62.0.200.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.179.104.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.167	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.158.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.152.9.215	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.117.141.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.35	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.222.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.46.41.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
176.13.17.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
80.246.137.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
79.182.41.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
112.111.161.170	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.111.161.170	Block	17
132.68.89.196	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	7
176.13.8.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.28.165.164	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
112.111.161.170	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
80.246.140.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.201.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	3
46.19.85.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.224.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.20.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.72.86.150	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.22.134.110	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.53.23.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.235.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
132.68.89.196	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 132.68.89.196	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
80.246.139.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
200.78.168.54	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
80.246.140.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.24.168	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.64.60	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
112.111.161.170	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
84.109.112.123	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.55.182.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.242.12	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.116	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmsendmessage.aspx	Block	1
109.67.203.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
46.19.86.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
212.150.133.226	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.53.32.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
77.138.26.16	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
115.28.206.23	China	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
85.64.127.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
178.154.189.201	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/351-	Block	1
148.177.168.117	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
66.249.76.117	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
46.117.17.158	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	Block	1