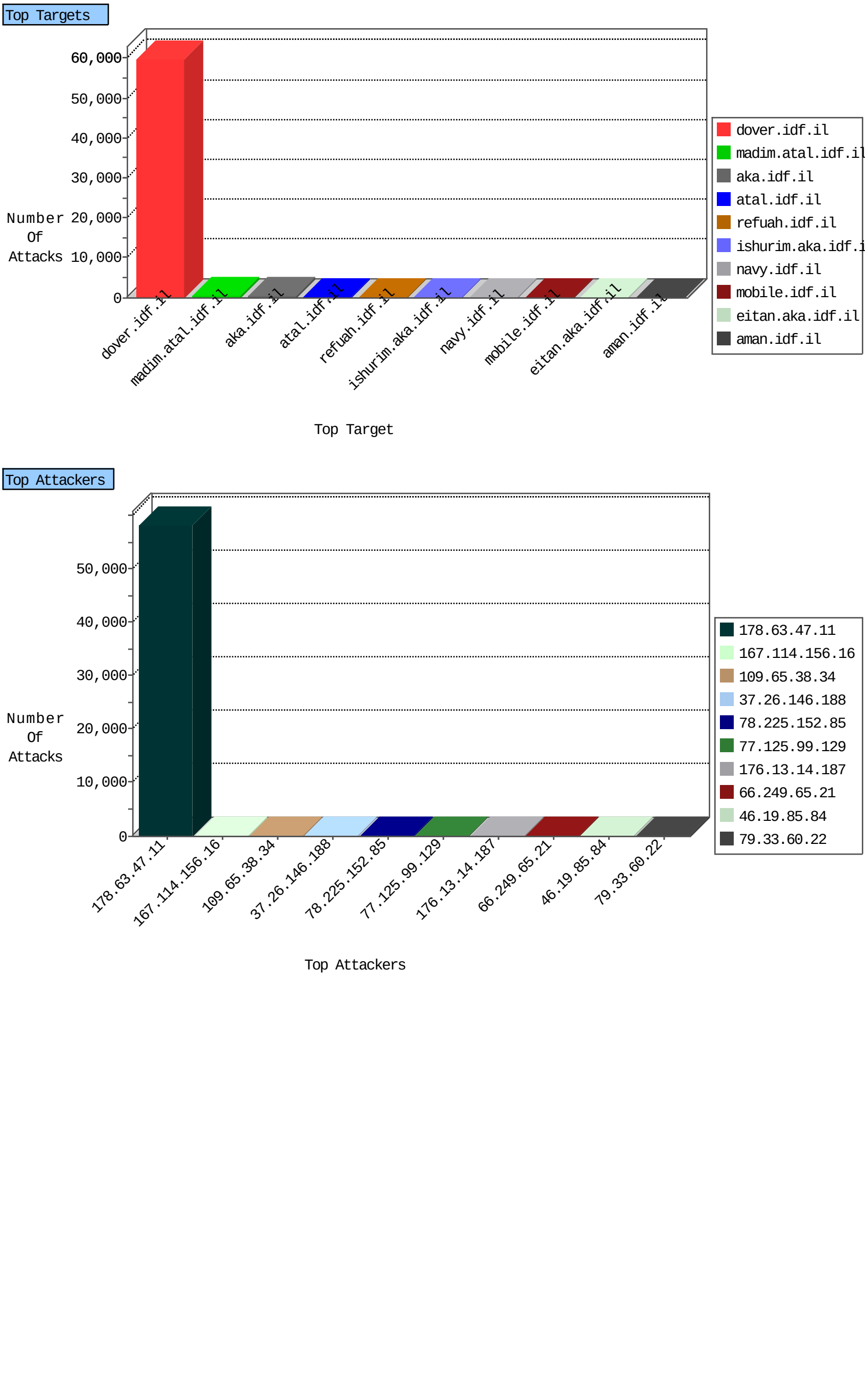
05-03-2016-22:04:08 to 05-03-2016-23:04:08

IDF Under Attack
Daily Report



05-03-2016-22:04:08 to 05-03-2016-23:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	9256
178.63.47.11	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2504
95.61.84.42	Spain	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1521
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1101
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1036
37.26.148.162	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	660
141.105.80.2	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	627
176.13.14.187	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	37
72.22.182.162	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8
89.138.122.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
79.183.33.137	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
107.150.32.62	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
107.150.46.34	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
79.33.60.22	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
164.132.145.27	Italy	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
89.216.220.16		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
107.150.46.36	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
134.35.238.14	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

05-03-2016-22:04:08 to 05-03-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-22:04:08 to 05-03-2016-23:04:08

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
66.249.64.163	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.3.147.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.176	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
84.228.142.31	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
45.62.254.174	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.93.46	147.237.77.176	India	matpash.idf.il	ET SCAN Potential SSH Scan	1
40.76.60.52	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
1.187.252.153	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.22.40.140	147.237.76.201	India	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
198.20.69.74	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1
5.22.135.241	147.237.77.216	Israel	dover.idf.il	SERVER-WEBAPP admin.php access	1

05-03-2016-22:04:08 to 05-03-2016-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
178.63.47.11	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58097
109.65.38.34	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	200
37.26.146.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	191
78.225.152.85	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
66.249.65.21	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
79.33.60.22	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.26.146.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
89.139.9.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
85.130.218.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
125.88.204.115	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.71.203.75	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.255.152.16	Netherlands	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.217.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
154.0.184.79	Gabon	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
176.13.17.58	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.130.218.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.46.41.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.179.170.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.105.80.1	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
50.87.144.145	United States	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	7
84.228.142.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.228.142.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.105.80.2	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.92.226	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.72.103.229	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

05-03-2016-22:04:08 to 05-03-2016-23:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.99.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.13.14.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
46.19.86.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.13.6.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.55.13.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
194.90.105.112	Israel	147.237.72.167	ishurim.aka.idf.i	Automated Vulnerability Scanning V1	Block	11
80.178.137.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
80.246.130.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
213.8.204.41	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1564	Block	3
77.126.61.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.109.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
79.177.114.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.181.108.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.39.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
201.15.189.247	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 201.15.189.247	Block	2
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	2
144.76.195.74	Germany	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 144.76.195.74	Block	2
81.218.183.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.109.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/	Block	2
87.68.32.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.135.241	Israel	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
185.3.147.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
132.66.236.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3384.jpg	Block	1
107.150.32.62	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.defences1.com/	Block	1
84.108.77.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.153.233.130	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
201.15.189.247	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/home/pniot.aspx	Block	1
66.249.84.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.252.114.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1810-he	Block	1
109.253.200.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
66.249.65.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.70.18.220	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
37.142.64.97	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.64.97	Block	1
5.22.135.241	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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/9/size100x0/3369.jpg	Block	1
132.66.236.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
109.65.38.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
5.254.243.253	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
37.142.64.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
87.71.99.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.22.135.241	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/admin.php	Block	1
80.178.137.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/4/	Block	1
66.249.79.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1806-21852-he/dover.aspx	Block	1

05-03-2016-22:04:08 to 05-03-2016-23:04:08