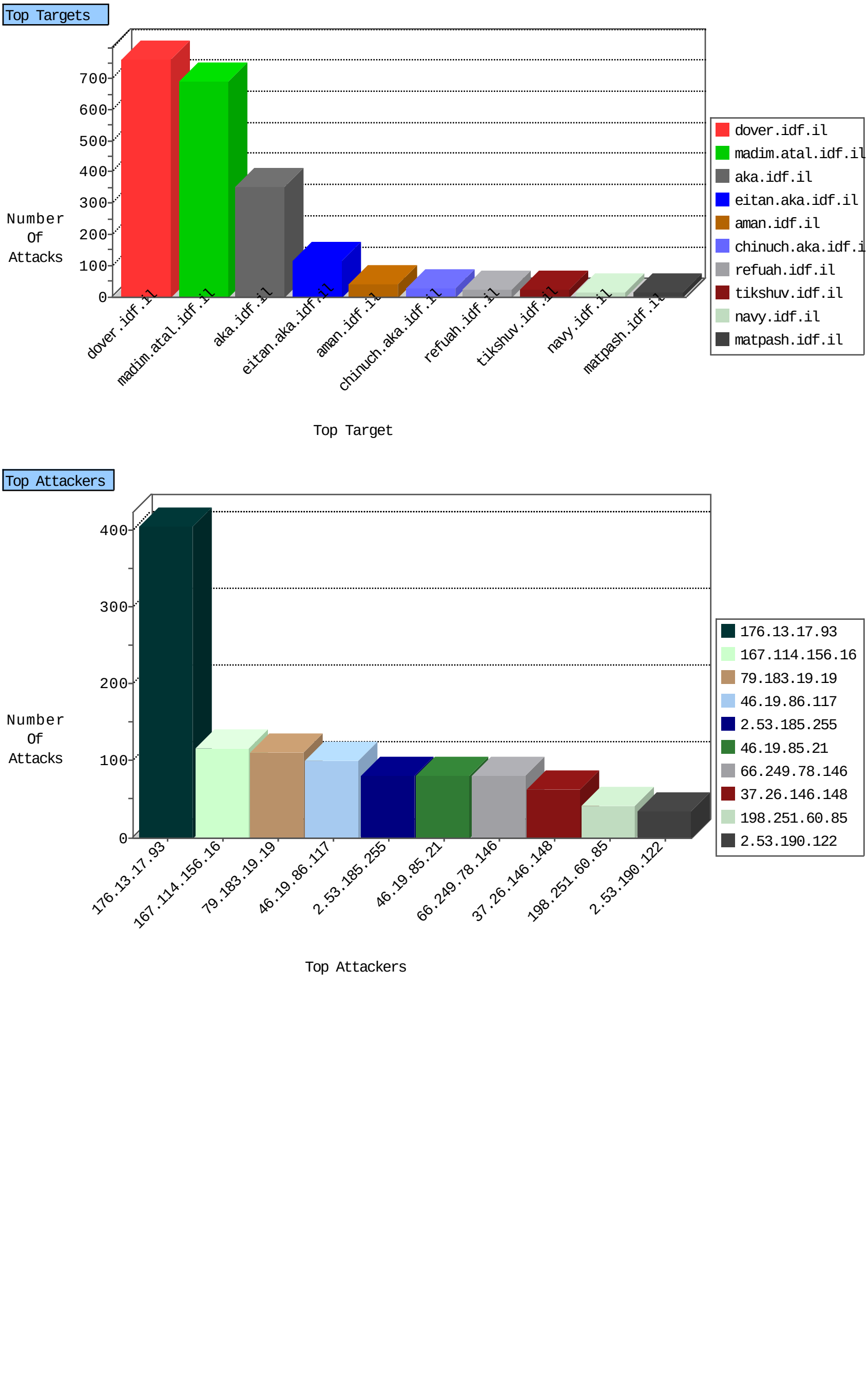
05-04-2016-19:04:09 to 05-04-2016-20:04:09

IDF Under Attack
Daily Report



05-04-2016-19:04:09 to 05-04-2016-20:04:09

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	5058
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	601
66.249.73.192	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	312
5.29.89.23	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	6
109.64.234.31	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	4
212.143.254.66	Israel	147.237.76.200	eitan.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
88.168.145.185	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.146.185	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
31.13.110.117	Ireland	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
191.96.249.50	Chile	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
71.6.146.185	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

05-04-2016-19:04:09 to 05-04-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-04-2016-19:04:09 to 05-04-2016-20:04:09

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
13.82.25.17	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.86.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.60.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.251.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.51.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.75.215.87	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
115.182.17.13	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
79.182.111.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.149.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.234	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
104.214.34.99	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.3.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.31.213.119	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.14.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.152.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.255.21.58	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
89.138.177.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.20.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.14.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.185.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.182.17.13	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
79.183.114.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.215.150.44	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.13.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.214.34.99	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
46.121.12.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.141.36.54	147.237.77.170	Italy	maarachot.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.19.86.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.96	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

05-04-2016-19:04:09 to 05-04-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.17.93	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	187
79.183.19.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
176.13.17.93	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	93
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
37.26.146.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
198.251.60.85	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
204.102.229.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
89.138.123.36	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
113.210.57.0	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.53.190.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
79.179.115.117	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
191.115.43.115	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
131.137.245.209	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.204.249.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.71.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.135.190.253	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
86.25.228.187	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.167.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.86.84.66	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.187.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.22.129.116	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.232	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.145.95.43	United Kingdom	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.20.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.180	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.190.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.253.210.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.190.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.121.106.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
2.53.185.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
66.220.145.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
131.253.25.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
131.253.25.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
80.246.136.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.38.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.64.178.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.14.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.86.154	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
87.69.219.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.69.219.76	Block	2
131.253.25.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.0.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.138.123.36	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
31.154.3.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.60.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.233.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/fiyus	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/4/2764.jpg	Block	1
46.117.63.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
71.244.112.136	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.73.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1154-en/dover.aspx	Block	1
89.204.138.185	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2392.jpg	Block	1
142.4.216.172	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
62.90.211.122	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/mobile	Block	1
87.69.195.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1074-he/אגף הטכנולוגיה והל וג'סטיקה.aspx	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/9/949.pdf).	Block	1
84.108.49.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch.	Block	1
2.55.22.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.167.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
180.180.126.98	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.55.15	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/rights/asp/info.asp	Block	1
149.88.195.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
5.29.70.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
87.69.219.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
79.180.28.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71700.pdf	Block	1
85.64.55.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1