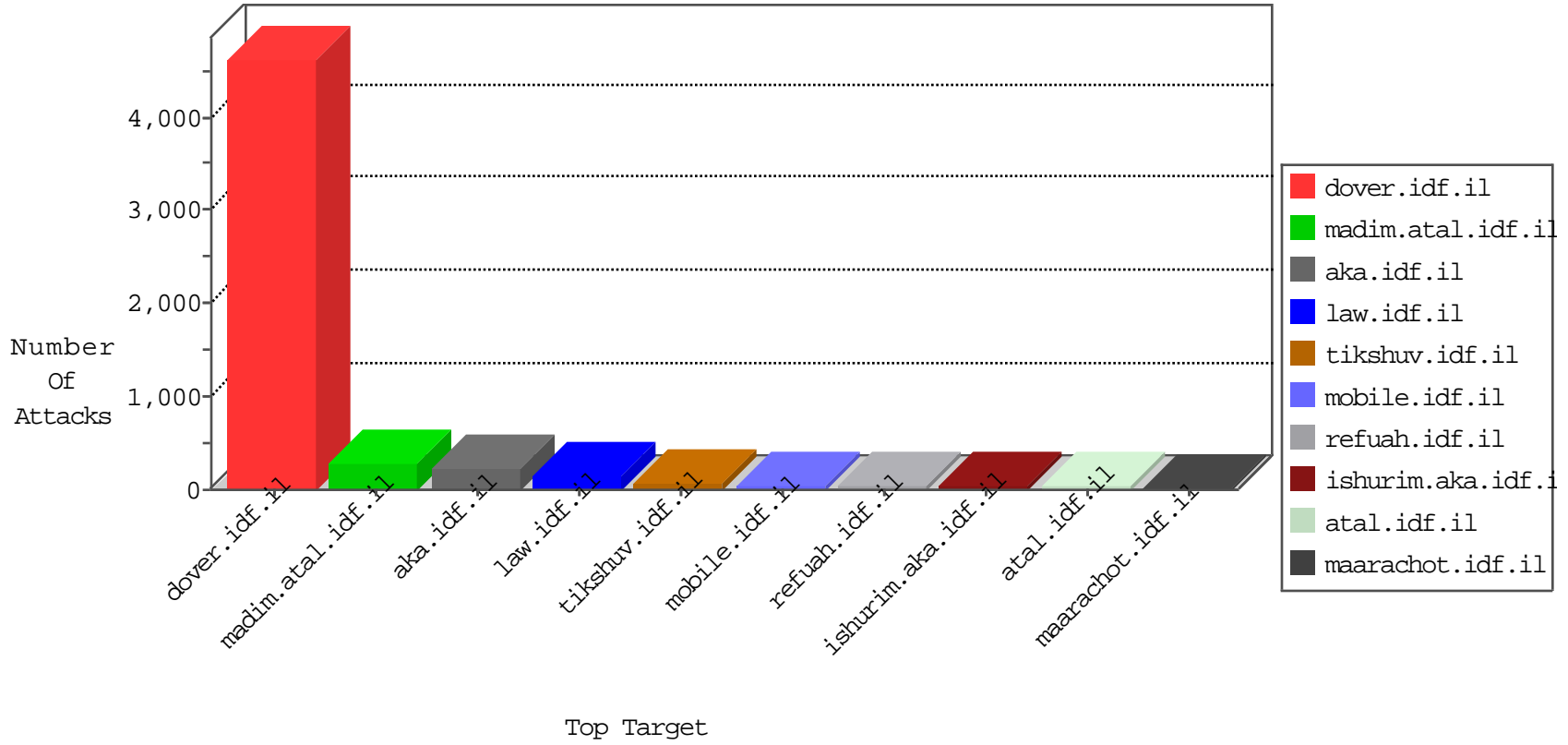


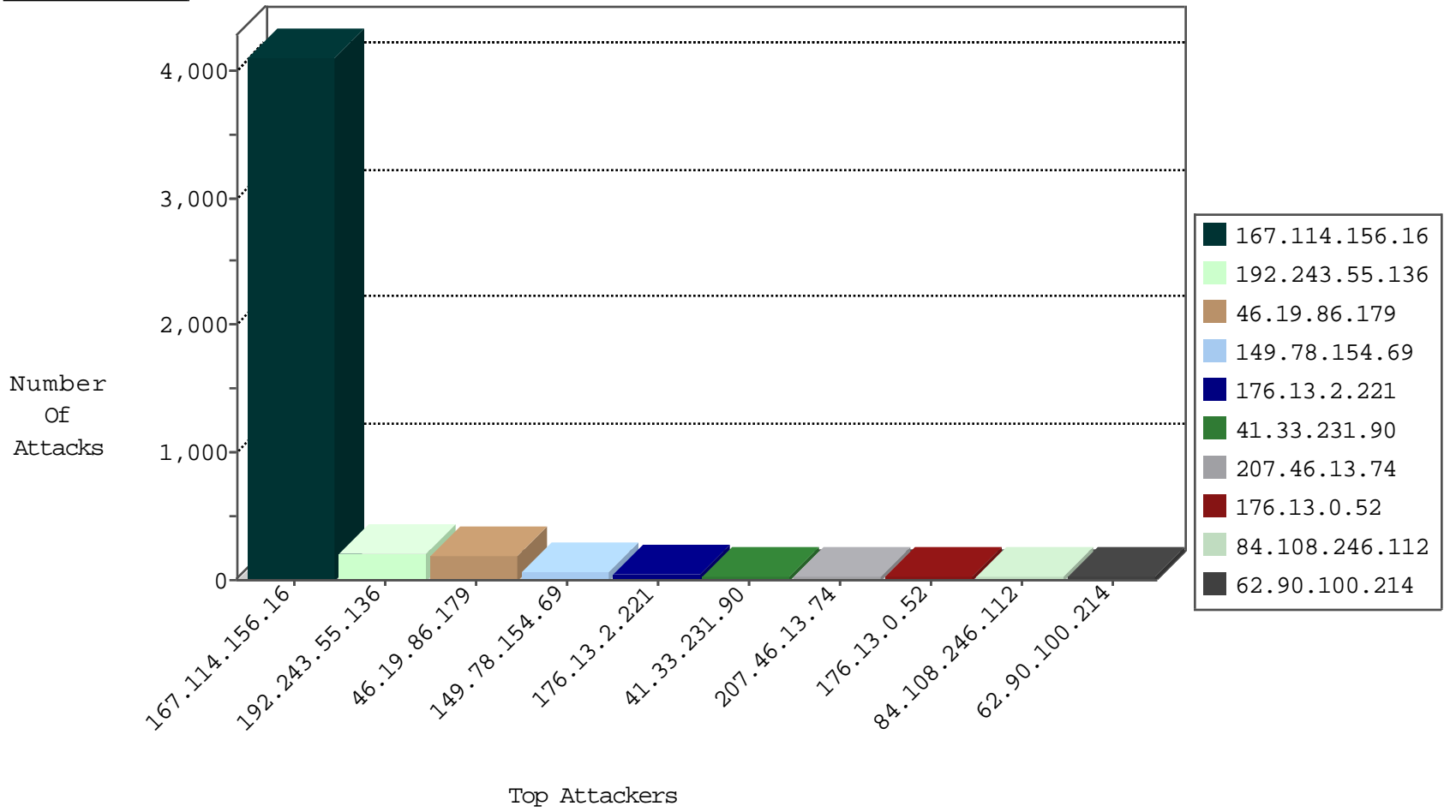
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.130.213.84	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4245
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4099
180.249.208.112	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2848
170.24.136.3	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	527
84.109.60.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	182
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
93.172.248.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.117.136.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
132.70.66.9	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
173.220.54.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
193.106.206.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.108.246.112	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
79.176.80.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
101.201.147.32	China	147.237.77.205	prisha.idf.il	block-sp-trafl	forward	2
93.201.67.3	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
82.80.86.86	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.55.3.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
124.24.247.55	Japan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
93.201.67.3	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.17	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.98	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
93.201.67.3	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
12.152.75.6	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
93.201.67.3	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
77.126.167.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.120.23	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
93.201.67.3	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
93.201.67.3	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
2.53.37.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.31.60.249	France	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.7	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.120.3.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
79.180.7.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
80.246.133.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.210.185.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.101	France	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	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
66.249.93.109	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
163.172.140.23	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.46.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.223.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.200.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
5.22.135.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
190.124.35.115	147.237.77.216	Nicaragua	dover.idf.il	ET SCAN NMAP -f -sS	1
132.73.196.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.9	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.176.120.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.210.129.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.99.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.192.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.216.176.244	147.237.77.19	Latvia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.216	Nicaragua	dover.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	28
176.13.0.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
62.90.100.214	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	18
5.22.135.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
192.243.55.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
84.108.246.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
134.191.232.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
109.253.202.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
84.94.209.7	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
176.13.3.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
192.198.151.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.139.235.138	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
170.24.136.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.176.80.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.235.98.139	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	10
173.220.54.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.136.194	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.138.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.126.226	Israel	147.237.0.35	akaws.idf.il	drop		drop	8
46.19.85.6	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.133.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.95.217.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
192.243.55.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.70.31.78	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.55.159.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.118	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.168.89.106	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
109.253.131.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.37	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.12.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.217.170	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
185.27.105.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
176.13.2.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.53.17.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.25.84.200	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
80.246.136.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.25.84.200	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
46.19.86.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.198	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.50.34.198	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
65.55.210.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.224	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.252	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.65.4.30	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationservice.aspx/getauthuser	Block	2
79.180.162.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.34.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
54.200.120.218	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
212.66.41.147	Ukraine	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
46.19.85.123	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.43	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.43	Block	1
88.12.171.219	Spain	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in ww.idf.il/1065-en/dover.aspx	Block	1
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
72.55.25.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/skira/default.asp	Block	1
212.117.137.146	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
150.70.173.42	Japan	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.15/	Block	1
212.66.41.147	Ukraine	147.237.76.42	refuah.idf.il	Parameter Type Violation SortDir in www.refua.atal.idf.il/1226-he/refuah.aspx	Block	1
109.160.204.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.39.222.159	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kiosk/	Block	1
130.185.155.10	Sweden	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
62.90.147.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.66.41.147	Ukraine	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
212.25.84.200	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 212.25.84.200	Block	1
89.139.34.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.139.34.41	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
74.82.47.4	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.64.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/70517.pdf	Block	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
110.53.183.62	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
46.29.255.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
212.66.41.147	Ukraine	147.237.76.42	refuah.idf.il	Parameter Type Violation lang in www.refua.atal.idf.il/1226-he/refuah.aspx	Block	1
82.166.240.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.44	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1