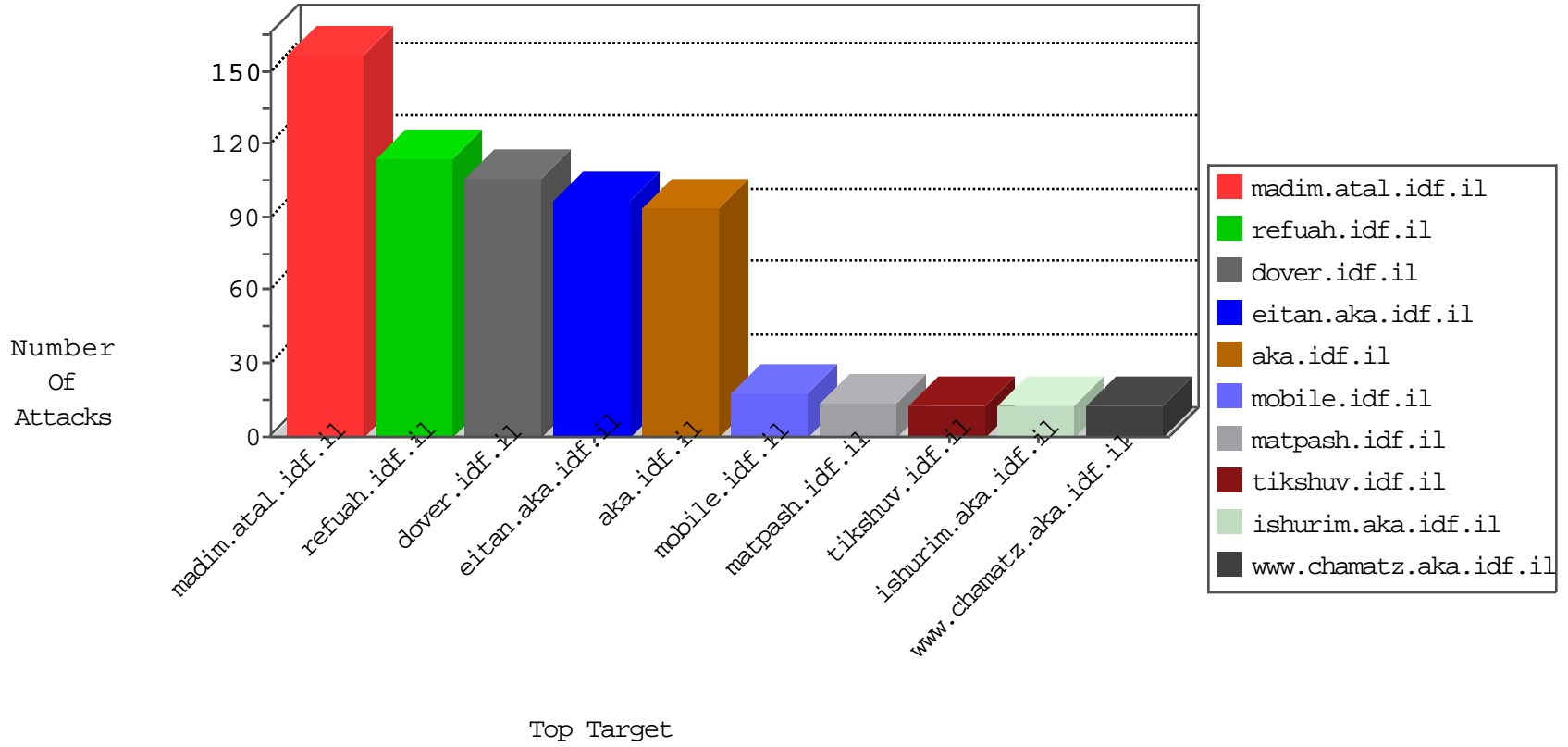


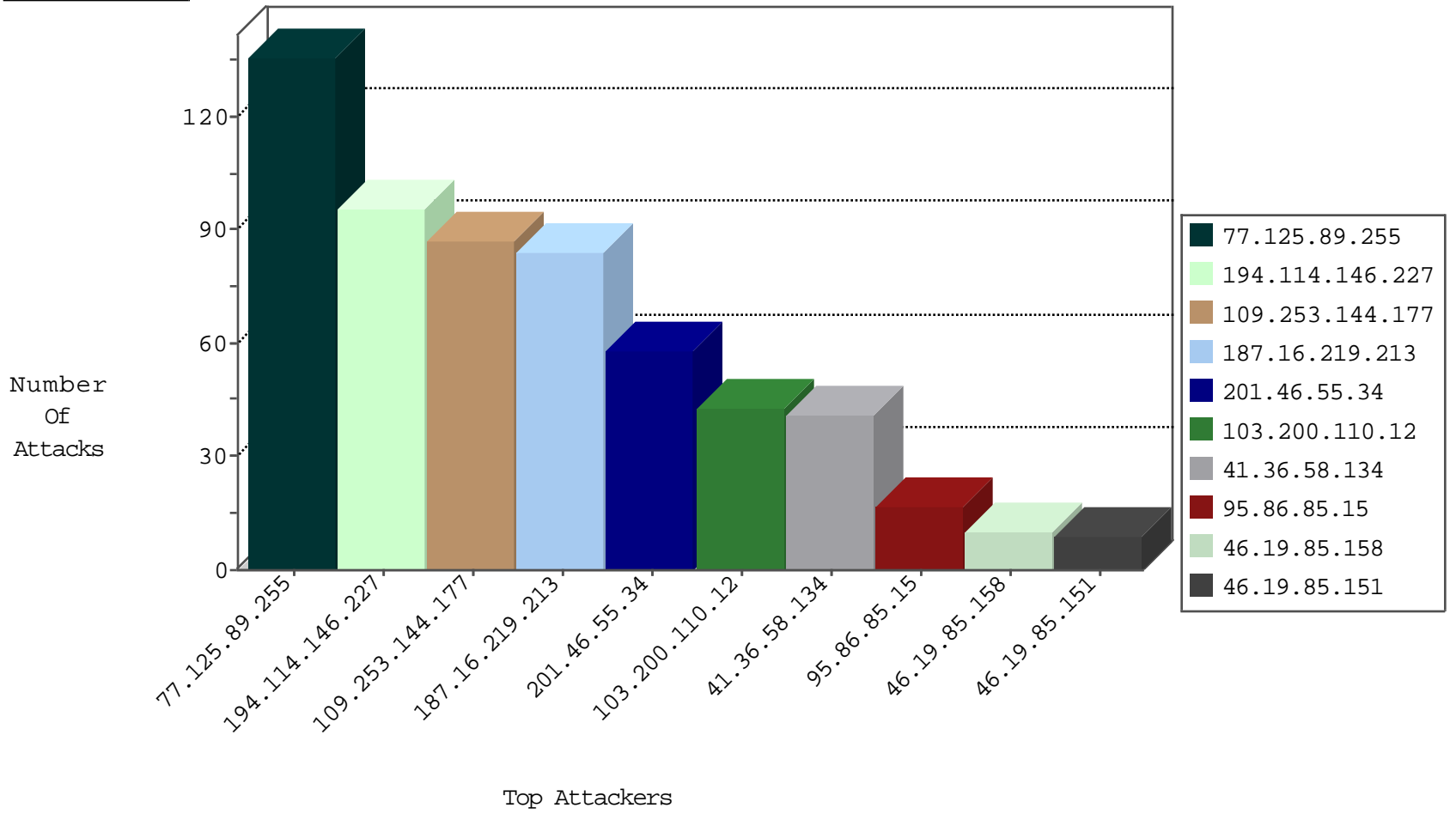
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
58.60.229.34	China	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.129.221.101	China	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	1
103.16.199.144	Indonesia	147.237.76.30	himush.idf.il	Invalid L4 Header Length	drop	1
58.60.229.34	China	147.237.0.15	kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
58.60.229.34	China	147.237.77.121	e.navy.idf.il	Invalid L4 Header Length	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.196.233.188	China	147.237.8.28	e.mobile-ks.idf.il	Invalid TCP Flags	drop	1
120.27.196.178	China	147.237.76.31	nakchal.idf.il	Invalid TCP Flags	drop	1
58.60.229.34	China	147.237.0.16	my-kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
219.141.189.72	China	147.237.8.14	e.orchot.idf.il	Invalid L4 Header Length	drop	1
91.210.104.87	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Invalid TCP Flags	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
58.60.229.34	China	147.237.8.14	e.orchot.idf.il	Invalid L4 Header Length	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
137.132.80.110	Singapore	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
101.201.68.21	China	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	CI000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.114.146.227	147.237.76.42	Israel	refuah.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	10
31.168.172.136	147.237.72.14	Israel	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	2
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
31.168.172.136	147.237.72.14	Israel	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.171.205	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.158	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.21	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.0.253	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
104.167.6.84	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.149	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -f -sS	1
52.166.130.115	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.76.199	Switzerland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.21	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.155.174	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
94.102.52.71	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.149	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.144.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	87
41.36.58.134	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	41
109.253.142.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
187.16.219.213	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
187.16.219.213	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
187.16.219.213	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
187.16.219.213	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
187.16.219.213	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.253.84.35	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
187.16.219.213	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
187.16.219.213	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
77.126.83.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.242.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
187.16.219.213	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.23.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
187.16.219.213	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
187.16.219.213	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
201.46.55.34	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
187.16.219.213	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
187.16.219.213	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
84.109.230.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
187.16.219.213	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.46.41.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
187.16.219.213	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.89.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	48
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	35
95.86.85.15	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.85.15	Block	17
176.13.244.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/4/	Block	3
176.13.23.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
82.8.187.169	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluum/templates/inner.asp	Block	1
207.46.13.168	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
212.252.80.163	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	1
180.76.15.155	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storaguent_meanings_entreat.yan	Block	1
173.63.167.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
212.252.80.163	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=65428	Block	1
77.138.204.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
198.161.119.4	Canada	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589- en/dover.aspx	Block	1
192.243.55.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.asp	Block	1
78.46.84.199	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
199.185.67.14	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx english	Block	1
176.13.227.131	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.89	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1