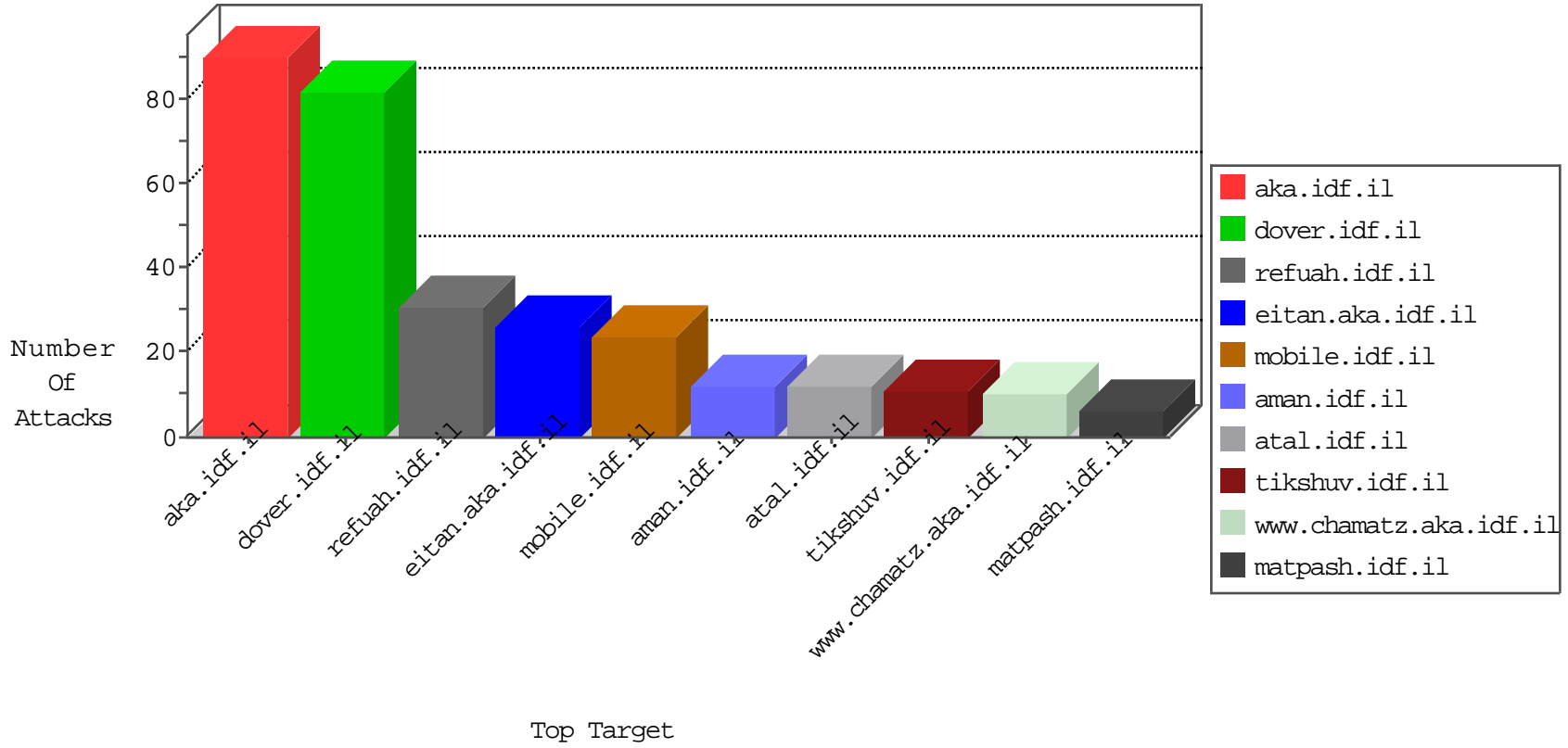


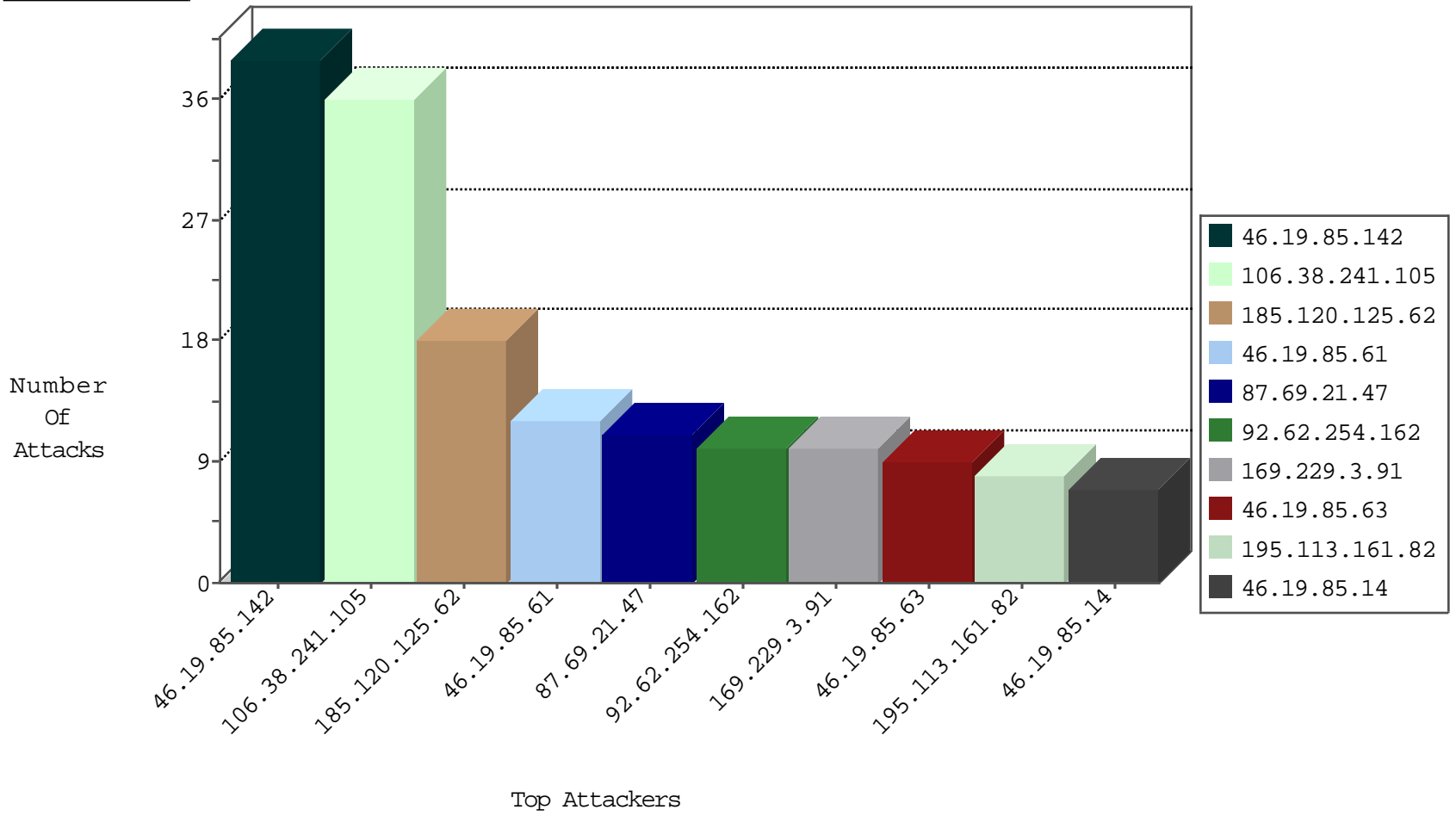
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	8
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	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
129.22.150.78	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.117.226.180	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
188.204.118.102	Netherlands	147.237.77.234	halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
188.204.118.102	Netherlands	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
188.204.118.102	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.156	aman.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	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	22
106.38.241.105	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	7
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	6
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
191.96.249.34	147.237.0.15	Chile	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
162.243.218.193	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.0.35	Japan	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
85.113.108.179	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	1
66.212.179.106	147.237.77.233	Canada	atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.212.179.106	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.18.162	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
192.81.216.190	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.34	147.237.0.200	Chile	m4u.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
187.38.27.35	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.242.4.52	147.237.77.121	Japan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
101.178.206.92	147.237.76.147	Australia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
66.212.179.106	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.57.162.182	147.237.0.34	Thailand	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.34	147.237.77.216	Chile	dover.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.212	Netherlands	e.dover.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
185.120.125.62	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
92.62.254.162	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.43.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.14	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.238.199.127	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.3.124	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
73.106.79.3	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.64.13.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
179.159.167.224	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.242.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.142.5.255	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.126.39.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.253.25.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
196.206.22.6	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
93.238.199.127	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.153.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.14	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
216.145.11.94	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
141.212.122.29	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.81.216.190	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.169	Japan	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.104	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.138.41.10	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.88	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
196.206.22.6	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.21	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.22.211.69	China	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.30	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.21.47	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.69.21.47	Block	9
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.21.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	2
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	2
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
77.237.146.28	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
104.131.160.127	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1627-he/refuah.aspx	Block	1
195.90.103.48	Poland	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 195.90.103.48 (Open Mode)	None	1
80.246.130.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
66.249.76.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
195.90.103.48	Poland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.56	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
157.55.39.67	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
40.77.167.57	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
176.113.126.237	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1
104.131.160.127	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.131.160.127	Block	1
66.249.66.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1