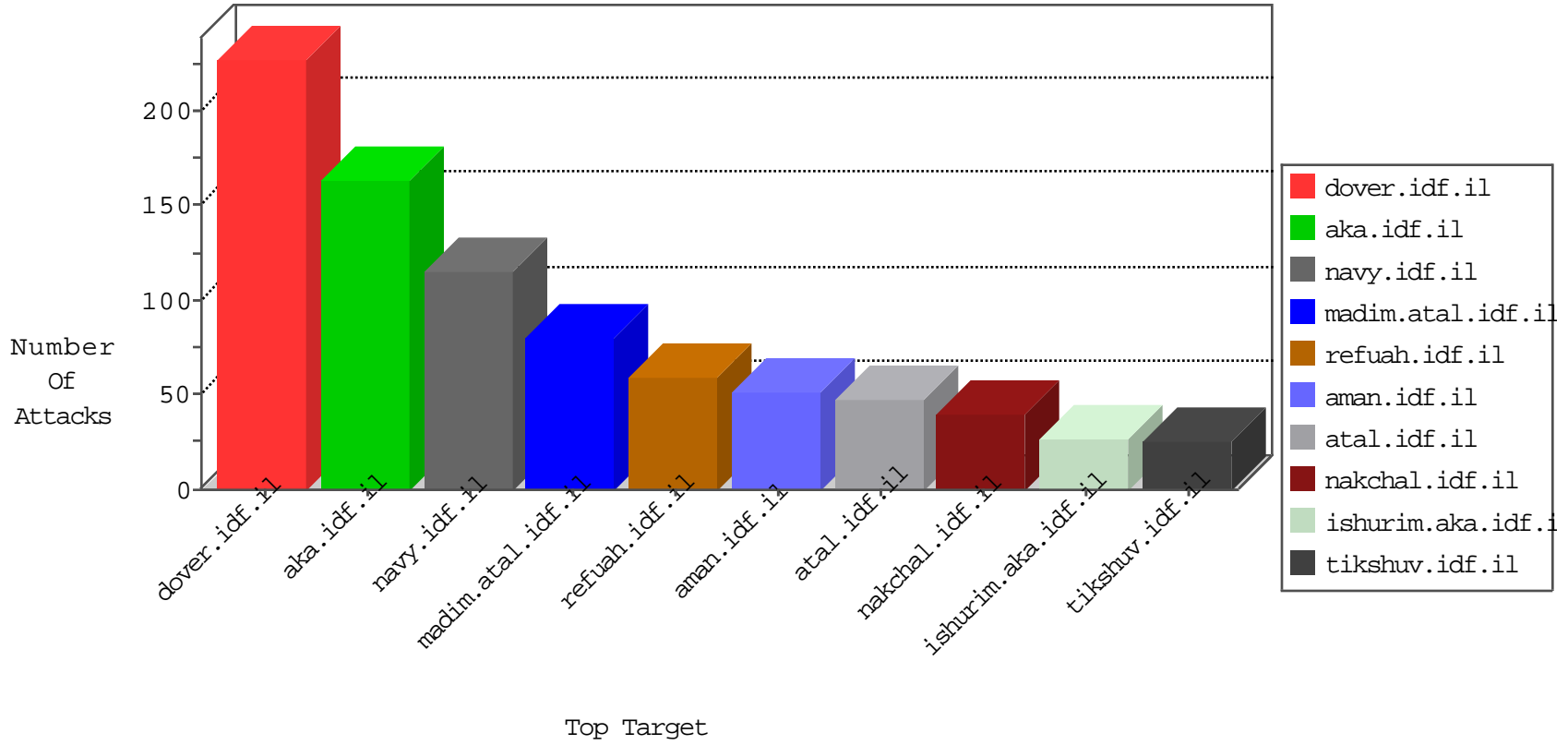


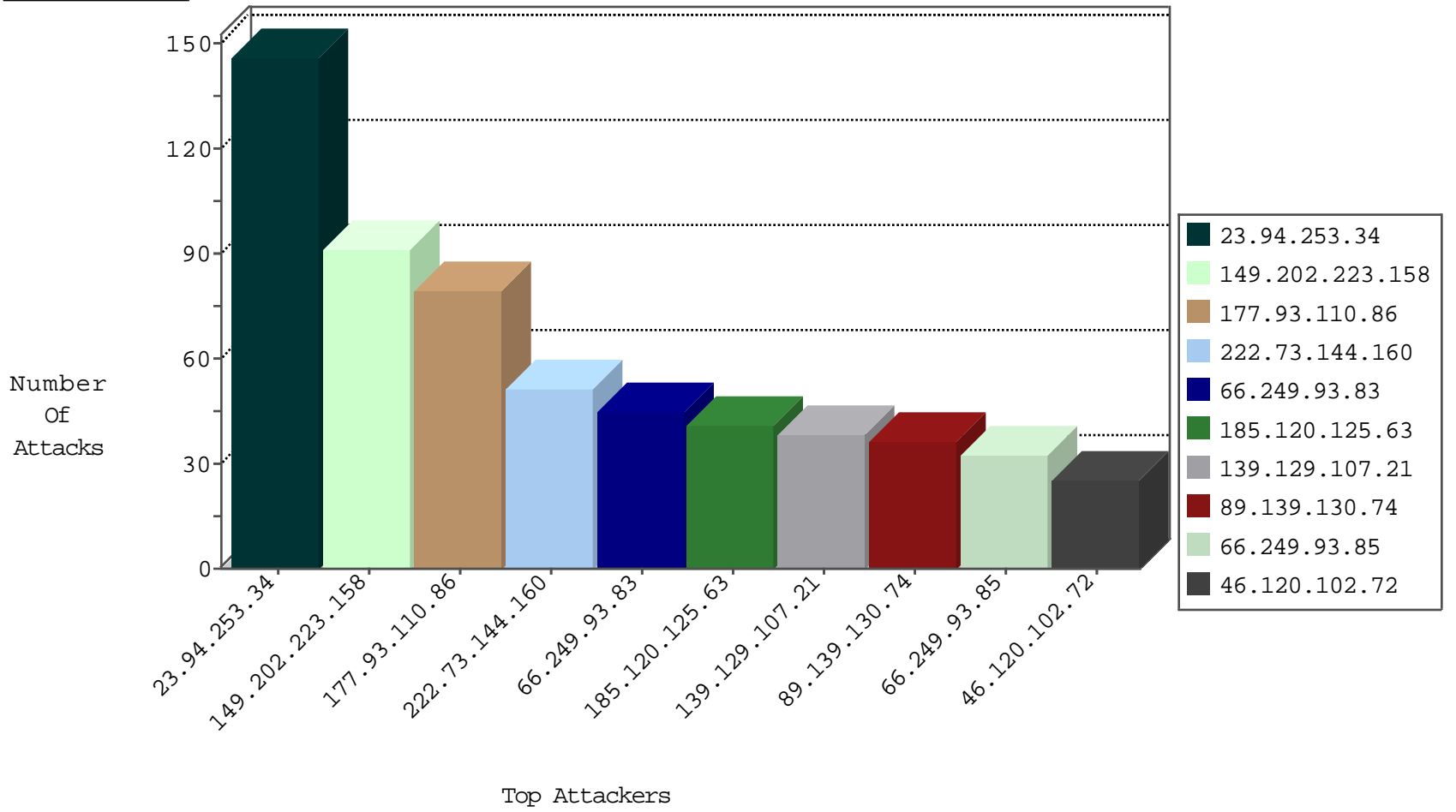
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.239.167	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14322
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11532
166.137.126.35	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
68.180.229.190	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1
141.226.151.233	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
120.132.50.135	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

09-10-2016-18:04:10 to 09-10-2016-19:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
91.241.236.19	Ukraine	147.237.77.176	matpash.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
200.58.214.138	147.237.77.205	Colombia	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.12.175.233	147.237.72.14	Singapore	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
116.12.175.233	147.237.72.14	Singapore	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
106.186.20.183	147.237.77.216	Japan	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.197.232.10	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
212.7.199.208	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
200.58.214.138	147.237.77.205	Colombia	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.72.14	Singapore	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
23.239.31.132	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.241.236.19	147.237.77.176	Ukraine	matpash.idf.il	SQL Injection - Select From	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.130.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.120.102.72	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop		drop	17
222.73.144.160	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop		drop	15
66.249.93.83	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	13
66.249.93.83	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	13
2.53.154.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop		drop	12
85.64.75.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.116.13.254	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.61.159	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
222.73.144.160	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
222.73.144.160	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.177.246.182	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
222.73.144.160	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
23.94.253.34	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
139.129.107.21	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
139.129.107.21	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
23.94.253.34	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
139.129.107.21	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
23.94.253.34	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
23.94.253.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
23.94.253.34	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
149.202.223.158	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
23.94.253.34	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
23.94.253.34	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
149.202.223.158	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
23.94.253.34	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
149.202.223.158	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
23.94.253.34	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
149.202.223.158	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
139.129.107.21	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
23.94.253.34	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
222.73.144.160	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
23.94.253.34	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
87.70.30.37	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
23.94.253.34	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.125.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.55.185.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.213	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.65.196.133	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-q/dover.aspx	Block	2
212.36.30.186	Bulgaria	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
189.217.175.232	Mexico	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.116.13.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
95.65.196.133	Turkey	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 95.65.196.133 (Open Mode)	None	1
77.138.61.47	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112075.pdf	Block	1
66.102.9.3	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
37.26.149.203	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
157.55.39.20	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
2.53.34.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.52.46	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
77.124.22.96	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.117.61.159	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
204.79.180.216	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
95.65.196.133	Turkey	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.146.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.211.230	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.16.163.130	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.237.74.105	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.125.85.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
210.162.15.6	Japan	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.102.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.148.224	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.0.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
40.77.167.78	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
5.102.242.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
93.162.186.174	Denmark	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
77.127.5.23	Israel	147.237.72.156	aman.idf.il	Illegal Parameter Encoding ct100\$ct100\$cphMain\$CPHMainContent\$ct17082 in www.aman.idf.il/modiin/questionnaires.aspx	None	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
109.64.99.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/faq.aspx	Block	1
37.26.148.224	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.227.79	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.73	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
93.172.252.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.127.5.23	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/cityofficers/	Block	1
109.67.207.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.148.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.17.123	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	1
79.181.207.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.33	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1