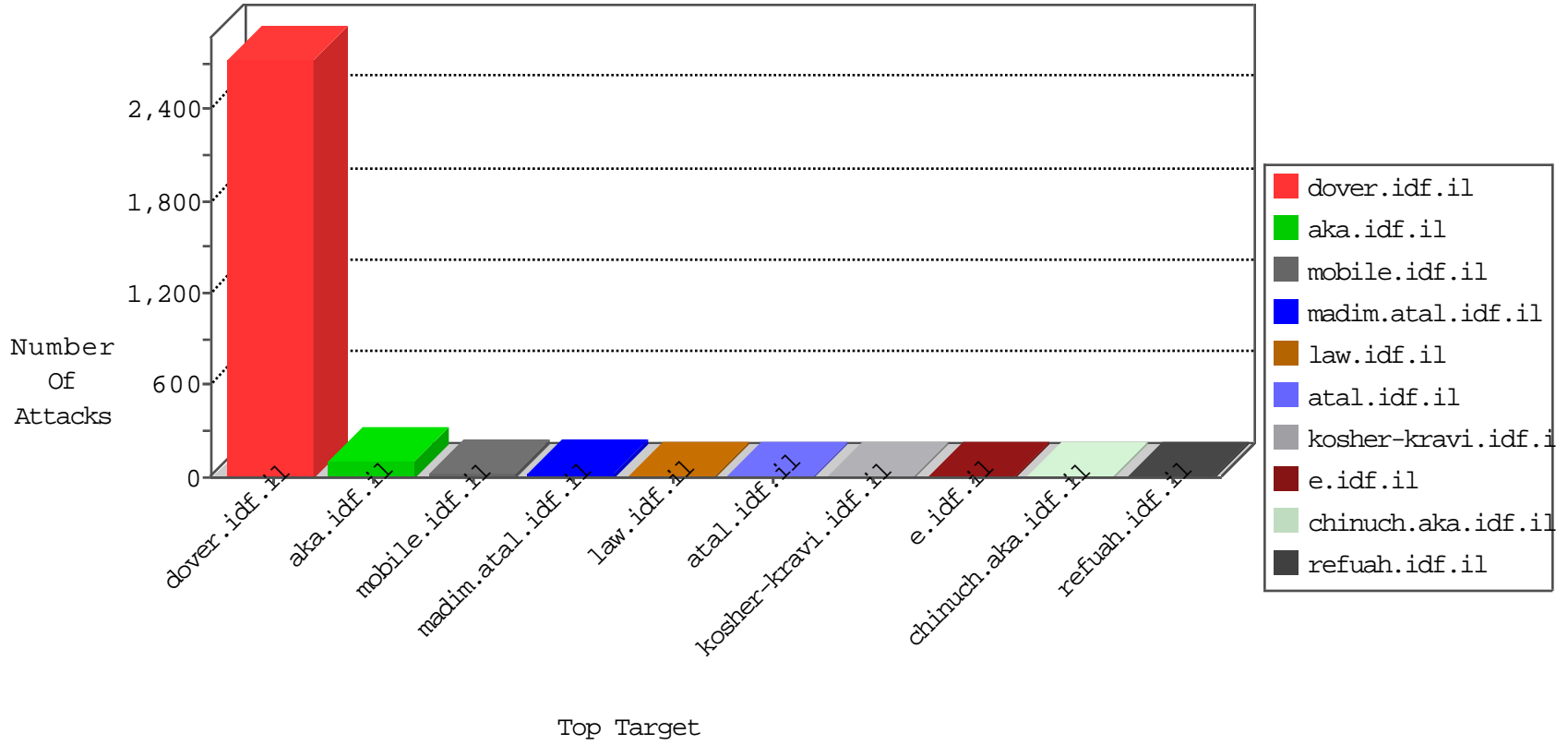


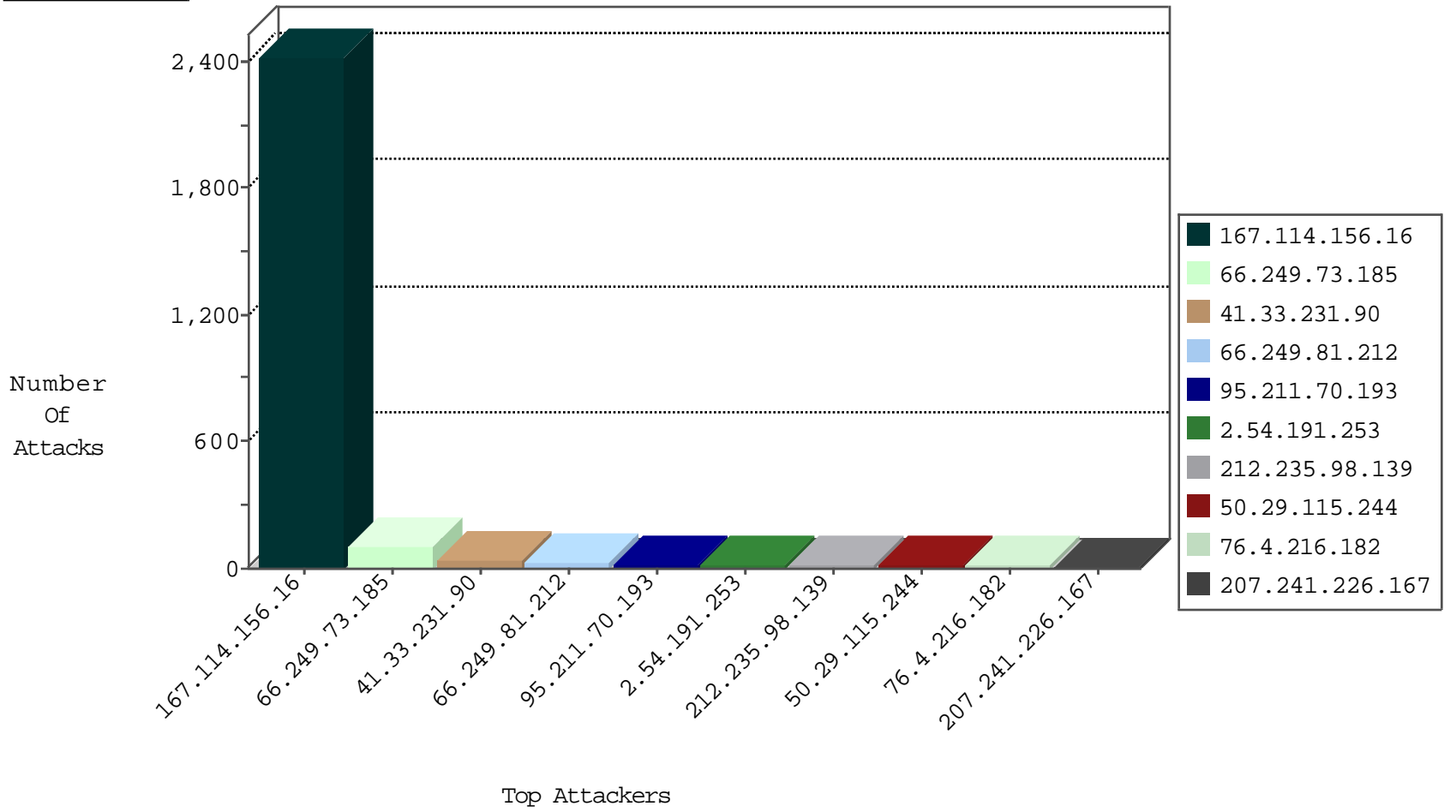
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3304
37.26.147.225	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.211.70.193	Netherlands	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.211.70.193	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
162.216.19.183	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
162.216.19.183	147.237.77.216	United States	dover.idf.il	GPL WEB_SERVER TRACE attempt	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
115.47.52.157	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 3072	1
51.254.44.137	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.43.236.38	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
222.73.119.253	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.226.212.78	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.0.15	Cote D'Ivoire	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.0.15	Cote D'Ivoire	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
162.216.19.183	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.0.35	India	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
104.43.236.38	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.196	United States	e.sviva.idf.il	ET DROP Dshield Block Listed Source	1
61.182.170.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.0.15	Cote D'Ivoire	kosher-kravi.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
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.54.191.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
76.4.216.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.241.226.167	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	10
84.109.65.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.29.115.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.99	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
203.171.41.47	New Zealand	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
188.120.148.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
50.29.115.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
99.103.119.108	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.113.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.57.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.101.61.176	Ireland	147.237.77.74	law.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	2
37.26.149.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.113	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.76.111.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.149.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.241.237.211	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
50.29.115.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.112	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.149.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
85.65.52.28	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.73	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
74.82.47.59	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.64	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.111	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.113	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.123	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.80	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.181.188.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
180.153.206.36	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.115	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.111	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.124	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.10.63	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	5
176.12.144.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.76.111.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.25	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
40.77.167.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
173.252.80.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.242.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.175.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
162.216.19.183	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.216.19.183	Block	1
31.13.110.106	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.55.189.122	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.49	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.49	Block	1
66.249.78.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
173.252.121.118	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.13.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.137.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.226.90	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
162.216.19.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/404testpage4525d2fdc	Block	1
31.13.110.111	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.4.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
173.252.121.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.29.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17558.jpg	Block	1
66.249.73.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20594-he/dover.aspx	Block	1
168.235.205.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shl_idfspokeperson	Block	1
31.154.21.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ufi/reaction/	Block	1
2.54.191.253	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
208.115.111.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
146.185.234.48	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	1
221.231.6.195	China	147.237.76.39	mobile.meitav.idf.il	Unauthorized HTTP Method	Block	1
84.110.40.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1