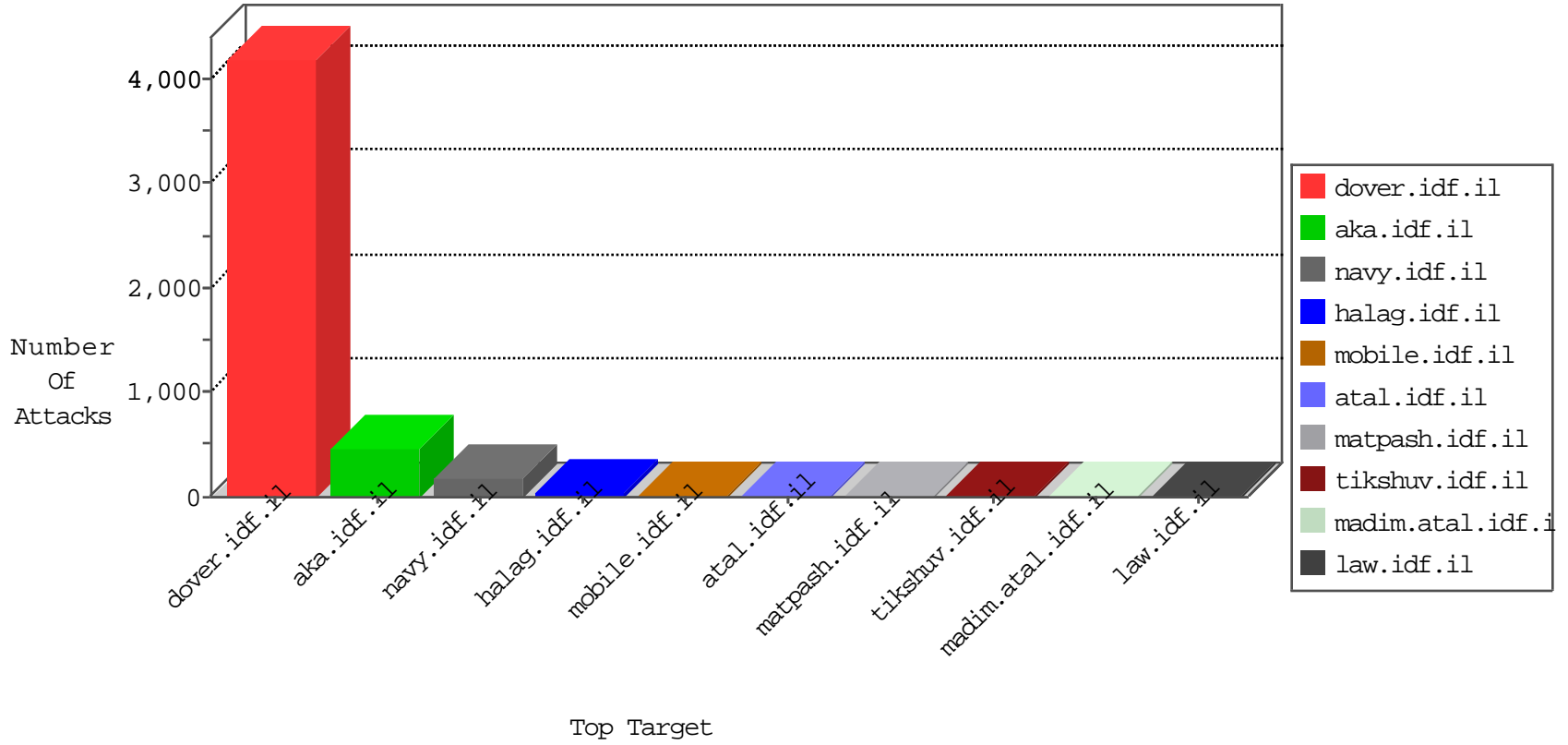




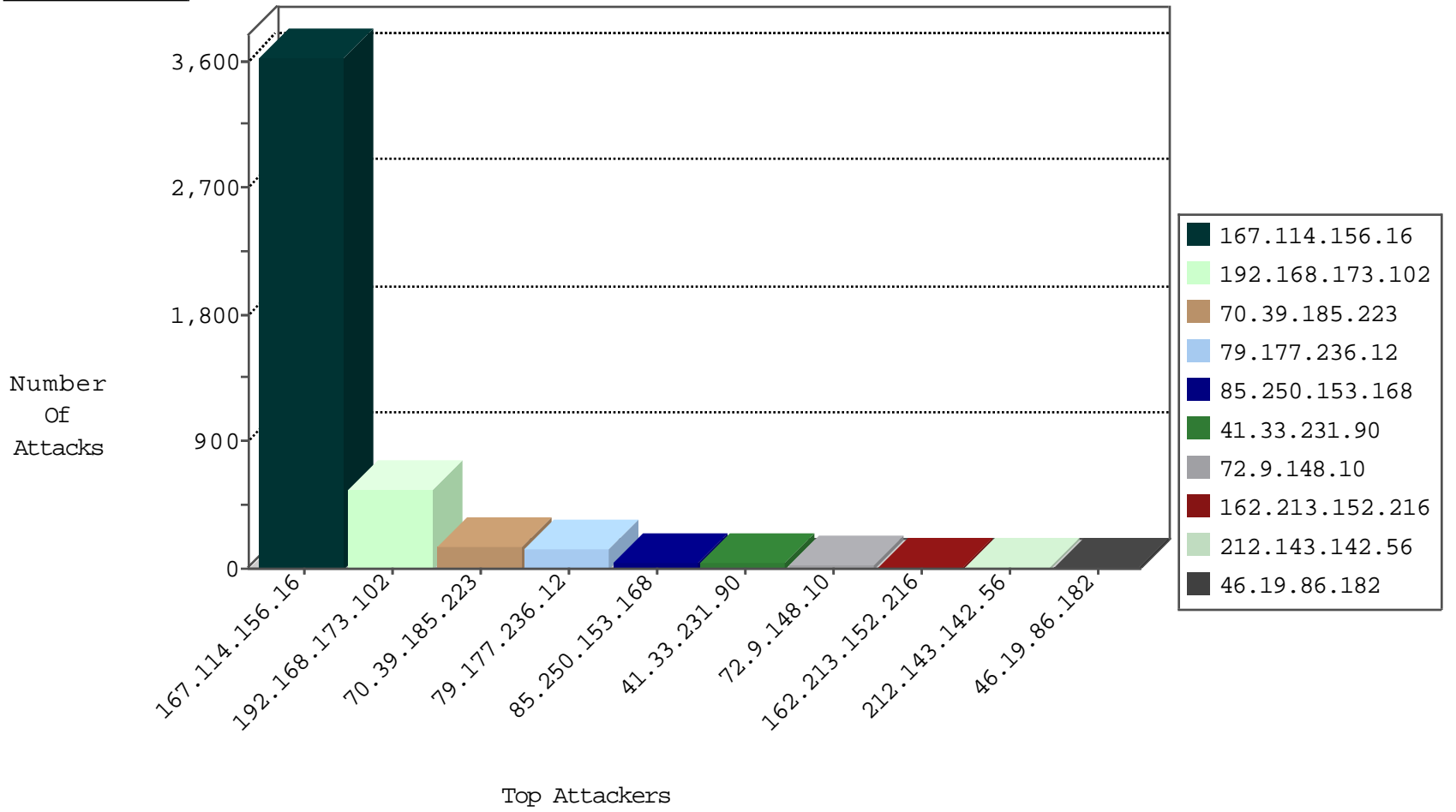
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	3631
79.177.236.12	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	135
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
70.39.185.223	United States	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
70.39.185.223	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
5.22.131.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.146.229	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
79.183.149.64	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
162.213.152.216	United States	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
162.213.152.216	United States	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
199.30.16.167	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
162.213.152.216	United States	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
79.183.149.64	Israel	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	1
149.78.44.255	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.213.152.216	United States	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.68.136	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
88.204.187.90	147.237.77.61	Kazakstan	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
79.178.218.180	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
64.13.147.226	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.77.178	Latvia	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.248.108	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.54.169	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.76.170.207	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
162.213.152.216	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
104.128.144.131	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.77.61	Kazakstan	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.248.108	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.248.108	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
162.213.152.216	147.237.0.19	United States	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
151.250.218.11	147.237.8.27	Turkey	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.204.187.90	147.237.77.61	Kazakstan	e.cogat.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
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	358
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	195
70.39.185.223	United States	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	98
70.39.185.223	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
85.250.153.168	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.250.153.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.182	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
207.241.229.248	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
79.194.71.235	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
5.22.135.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.51.220.166	Iraq	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
2.52.176.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.111.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.68	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
2.53.5.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.216	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	5
73.204.20.9	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.78.44.255	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.117.182.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
5.102.242.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.16.162	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.185.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
151.236.18.84	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
157.55.2.146	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
103.251.132.70	Palau	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
66.249.83.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.19.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.112.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.210.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.102.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.146.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.130.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.137.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.193.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.81.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.130.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.144.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.162.39.92	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.130.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.125.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
17.138.56.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
193.169.52.208	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
109.160.175.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.8.129.157	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.129.157	Block	2
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-	Block	1
197.118.224.70	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
131.253.25.137	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.aspx/getjs	Block	1
77.237.146.28	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 3931161.1.1423931161.1423931161.; in URL asp.net_sessionid=buc15a55v5qdy345nkox2o55	Block	1
213.8.129.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationsservice.aspx/getauthuser	Block	1
95.219.48.31	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.75.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
200.39.26.169	Mexico	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
141.212.122.209	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.178.218.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.117.57.21	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
213.8.129.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/en	Block	1
190.210.186.137	Argentina	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
105.107.28.17	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
207.46.13.29	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
141.255.155.246	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.179.116.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
219.74.38.129	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=0%7C10%2C0%7C11%2C0%7C12%2C0%7C13%2C1%7C14; __atuvs=5707f7f906a5c566000	Block	1
212.199.151.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationsservice.aspx/getauthuser	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
85.250.153.168	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
197.15.245.65	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.15.245.65	Block	1
2.52.176.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.6.53.181	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Malformed URL asp.net_sessionid=buc15a55v5qdy345nkox2o55;	Block	1