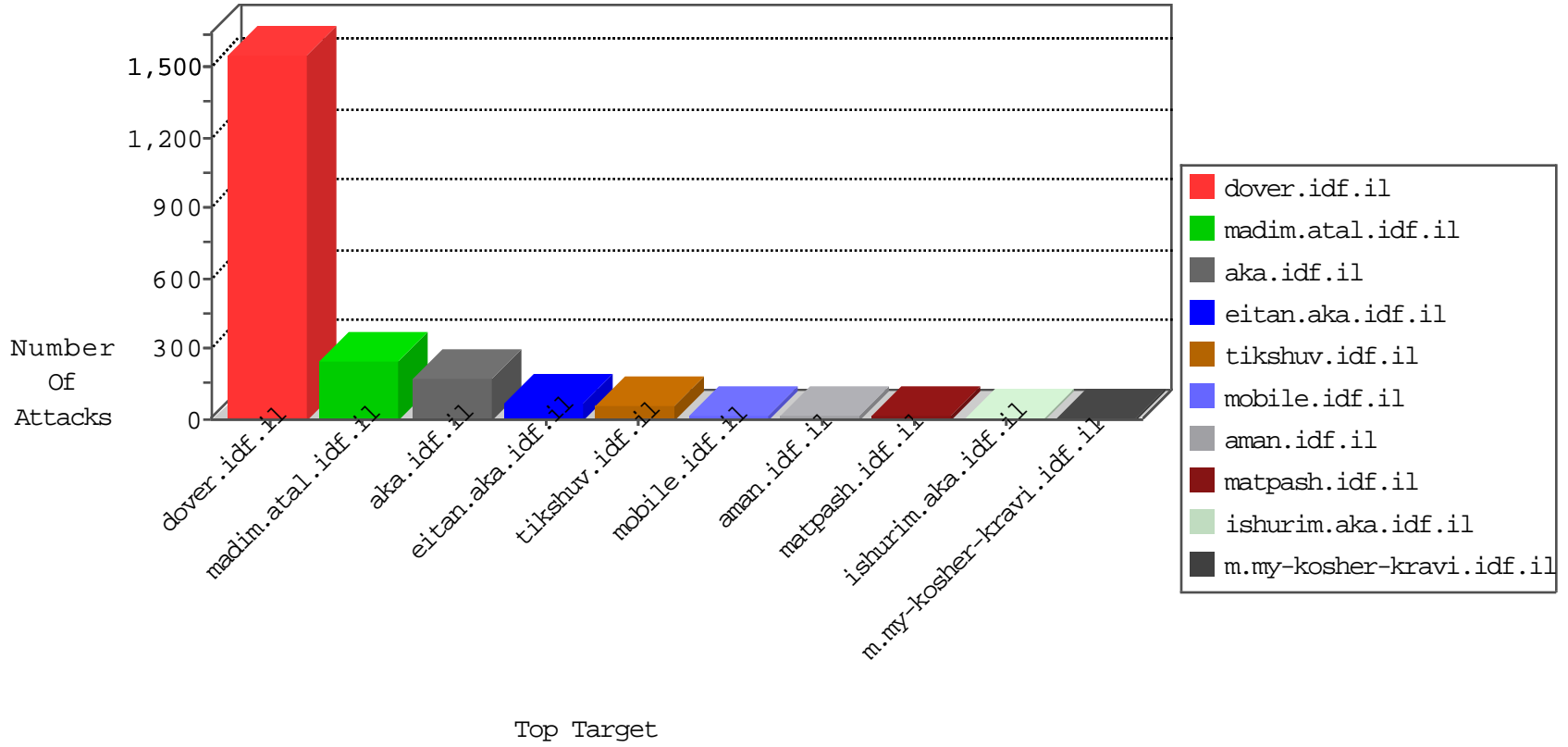


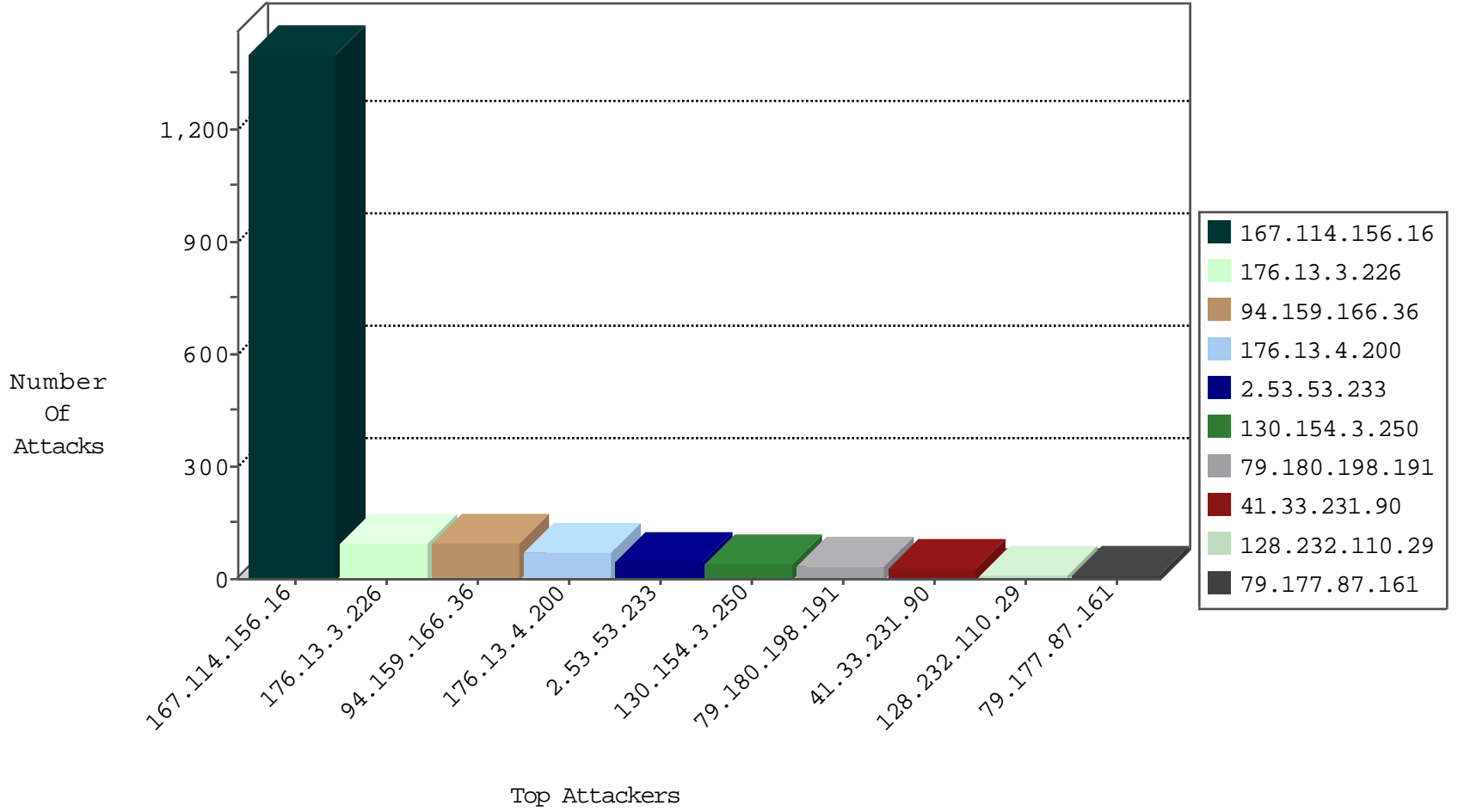
IDF Under Attack Daily Report



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	1403
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
79.178.205.207	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.198.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	31
77.126.24.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
77.126.96.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
94.23.19.178	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.129.87	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
94.23.19.178	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.131.242	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
94.23.19.178	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.131.242	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.129.87	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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
79.176.74.203	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
177.223.52.167	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
106.184.2.29	147.237.76.31	Japan	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
89.216.119.94	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 2048	1
185.103.252.98	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.161	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
106.186.113.132	147.237.0.34	Japan	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
94.53.1.4	147.237.76.30	Romania	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.112	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
220.231.195.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
188.127.231.115	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.243	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
180.97.106.161	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.4.200	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
130.154.3.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.3.226	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
176.13.3.226	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
94.230.86.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.177.87.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
176.13.9.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.87.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.27.105.185	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.6.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.225.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.42	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.250.131.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.177.6.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.203.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.78	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.94.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.63.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.140.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.68.17.88	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.207.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.216.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.12.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.13.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.196.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.74.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.66.51.14	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.76.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.128.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.74.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.28.154.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.16.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.7.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.204.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.70.51.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.50.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.225.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.140.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.237.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.102.195.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.159.166.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
176.13.3.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.53.53.233	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	41
108.56.67.236	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 108.56.67.236	Block	8
2.53.53.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.53.130.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.140.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.2.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.186.1.182	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.178.97.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx	Block	2
200.79.13.211	Mexico	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	2
80.246.139.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.161.9.6	Block	2
109.64.252.244	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.64.252.244	Block	2
69.58.178.58	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
46.19.86.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.65.145.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx	Block	1
199.30.24.50	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.25.229	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.4	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.116.222.137	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.116.222.137	Block	1
91.104.0.50	Hungary	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/populations/tzav_rishon.jpg	Block	1
5.22.135.195	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
149.78.157.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/templates/inner.asp	Block	1
130.154.3.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.16.177	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
203.33.121.38	Australia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
37.187.114.171	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to /irj/portal	Block	1
149.78.180.92	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
108.56.67.236	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	1
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$txtSearch in www.idf.il/1283-en/dover.aspx	Block	1
130.154.3.250	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
96.90.121.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/69687.pdf	Block	1
217.69.136.209	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
149.88.175.64	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.228.79.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
176.13.9.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.161.9.6	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
131.253.25.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
106.186.113.132	Japan	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1