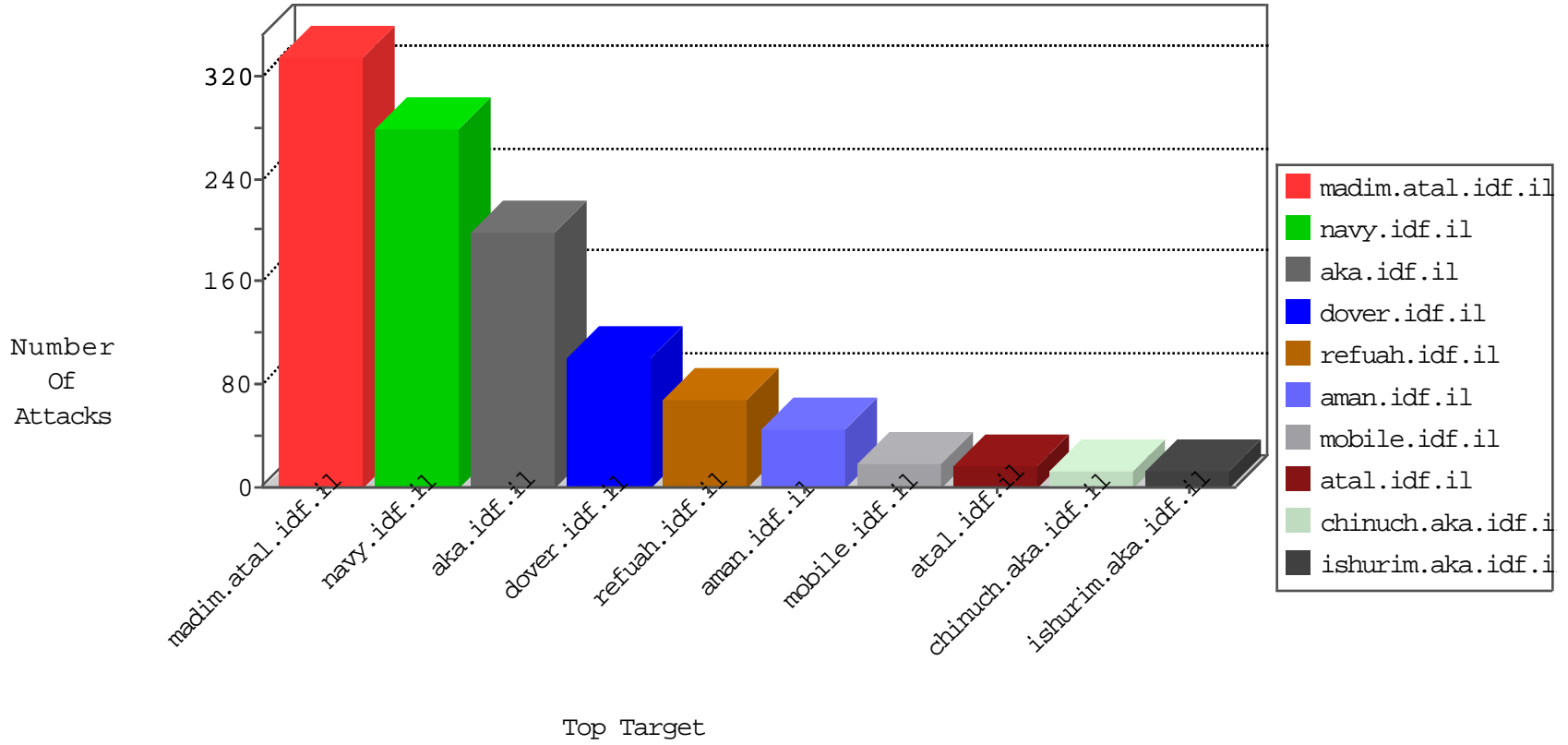


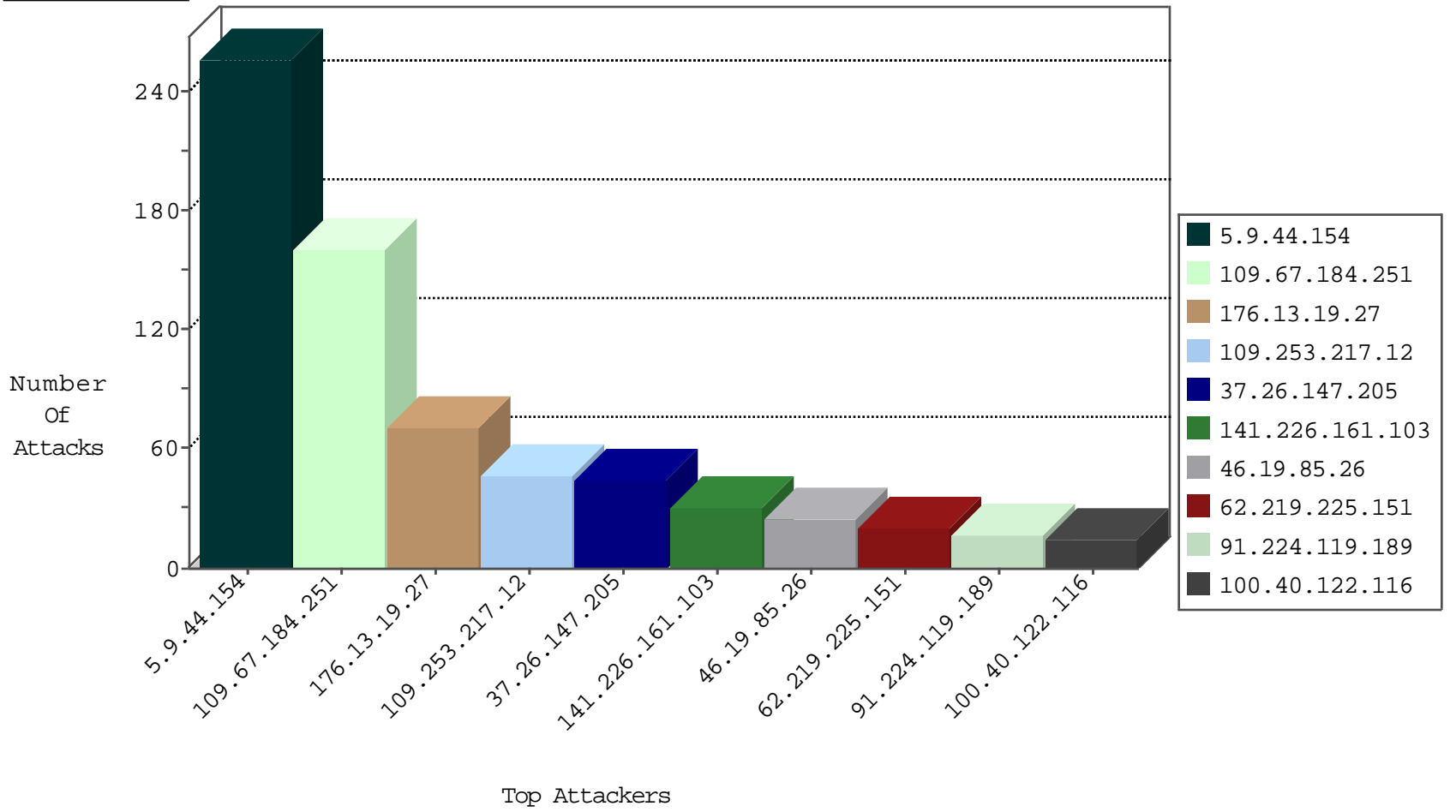
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
2.53.27.80	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
62.219.164.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	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
160.80.221.39	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.167	ishurim.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
120.76.190.112	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
123.59.59.52	China	147.237.76.30	himush.idf.il	block-sp-trafl	forward	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.177.24.40	Russian Federation	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.54.18.219	Saudi Arabia	147.237.76.147	chinuch.aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
123.126.68.115	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
105.98.69.228	Algeria	147.237.76.42	refuah.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
105.98.69.228	Algeria	147.237.77.170	maarachot.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.177.24.40	147.237.77.233	Russian Federation	atal.idf.il	SQL Injection - Select From	8
105.98.69.228	147.237.76.42	Algeria	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
105.98.69.228	147.237.77.170	Algeria	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.79.103.178	147.237.77.176	United States	matpash.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	1
113.240.250.154	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
216.81.230.167	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.150.38.110	147.237.0.35	Mexico	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
172.245.173.142	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.162.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.242.237	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
211.141.78.56	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.245.183.109	147.237.0.200	Indonesia	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
201.150.38.110	147.237.0.35	Mexico	akaws.idf.il	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.14	United Kingdom	e.orchot.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
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack		monitor	151
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	101
141.226.161.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
62.219.225.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
141.226.161.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
185.32.179.207	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
84.229.37.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
213.8.204.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
141.226.161.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.196.19	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	7
91.224.119.189	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.178.126.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.224.119.189	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
91.224.119.189	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.55.147.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.219.225.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
46.19.86.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
80.178.189.54	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.12	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.114.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
199.30.16.163	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.69.114.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
77.139.102.82	France	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.37	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
73.133.199.209	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.116.95.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.65	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.23.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.145	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
176.13.11.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
80.246.136.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
87.70.30.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.59.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.232.162	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
87.70.30.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.1.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.61	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.30.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
100.40.122.116	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.184.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
176.13.19.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
37.26.147.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.217.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
77.138.240.101	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/gyus/leshakot/	Block	6
85.64.60.117	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
84.108.3.202	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	5
84.108.3.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/	Block	5
46.19.85.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.41.166	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.242.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
75.40.152.196	United States	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/14-he/patzar.aspx	Block	2
77.138.70.242	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
77.138.71.214	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.202.107.10	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
77.139.226.119	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
77.138.139.81	France	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
90.41.166.166	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
84.108.193.245	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
31.154.81.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
77.139.81.145	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
77.138.41.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash/sheelon.aspx	Block	1
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/163-7353-en/patzar.aspx	Block	1
87.69.215.183	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.165.162.202	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.138.150.159	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
176.13.250.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.94.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.109.113.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.139.81.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
157.55.39.59	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.117.8.32	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.117.8.32	Block	1
87.70.25.29	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.77.47.181	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.152.161	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
176.228.164.15	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	1
95.86.96.101	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.125.37.2	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.229.37.158	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	1
77.139.102.82	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.111	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
62.219.225.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
87.73.121.61	Denmark	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
183.89.25.101	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.49.17	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.229.37.221	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.139.102.82	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1