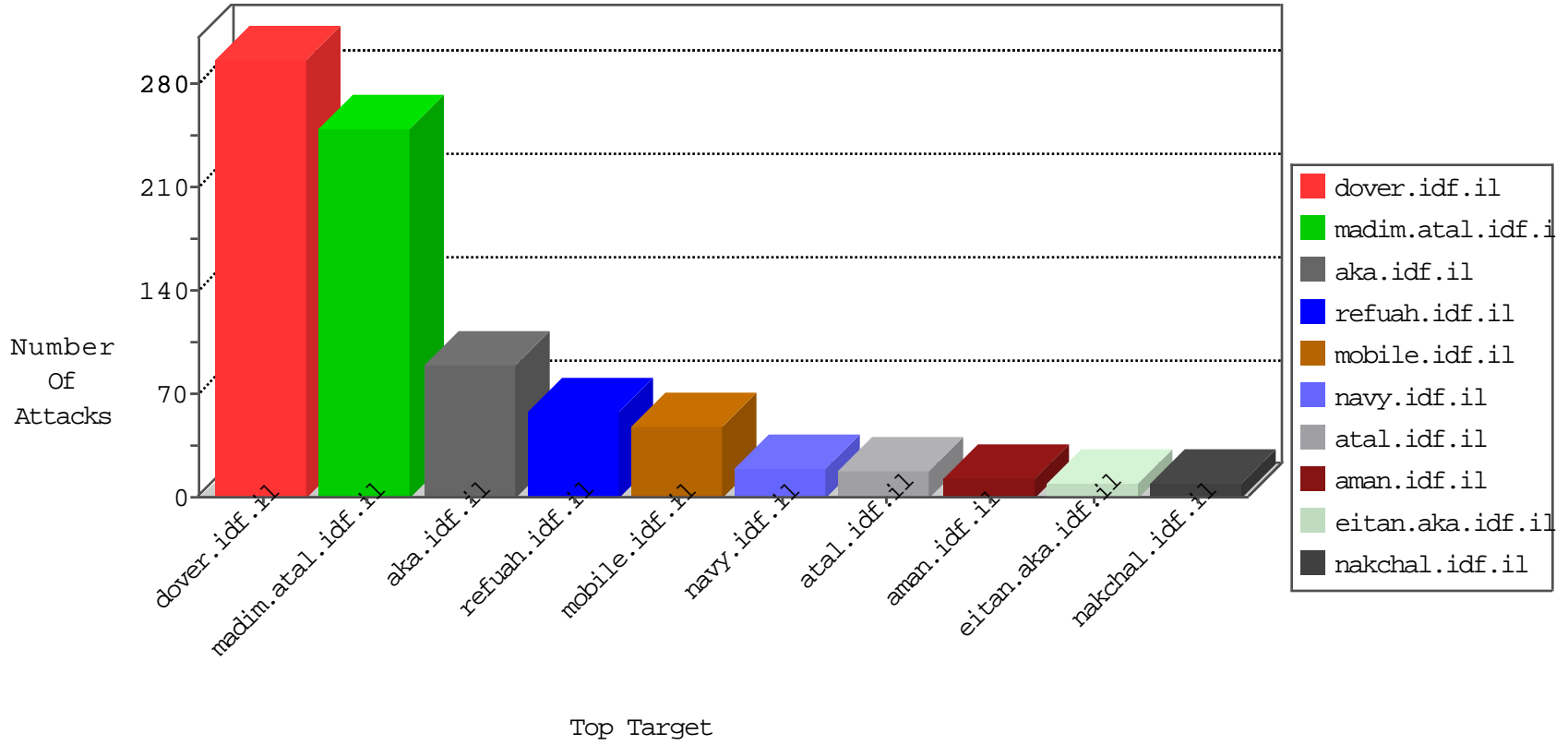


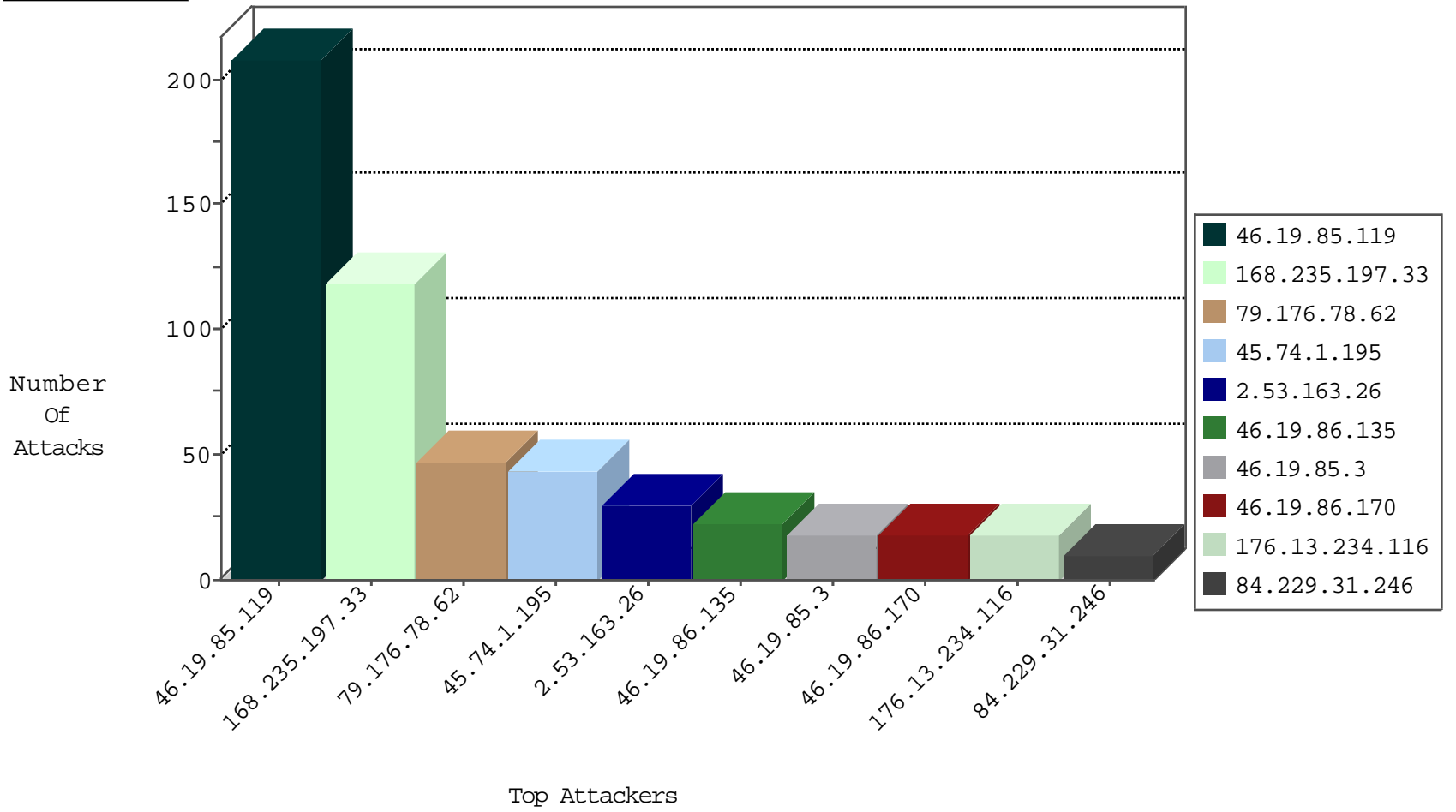
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.147.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
168.235.197.33	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.82.160.238	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.193.159	France	147.237.77.216	dover.idf.i	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	1
78.183.208.206	Turkey	147.237.77.216	dover.idf.i	5141: HTTP: Sqlmap HTTP Request	Block	1
91.121.193.159	France	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.238.237.157	147.237.77.234	Germany	halag.idf.il	ET SCAN Potential SSH Scan	1
178.238.237.157	147.237.76.197	Germany	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
178.238.237.157	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
163.172.177.160	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
128.232.110.28	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.121.193.159	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP backup access	1
61.240.144.65	147.237.77.233	China	atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
222.186.56.179	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.4.120.149	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.61	United States	e.cogat.idf.il	ET DROP Dshield Block Listed Source	1
5.255.90.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
178.238.237.157	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
178.238.237.157	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
178.238.237.157	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.177.160	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.54.157	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
78.183.208.206	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
222.186.56.179	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.235	Netherlands	sviva.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
168.235.197.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
79.176.78.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
45.74.1.195	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	43
2.53.163.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.229.31.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.170	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.146.114.66	Georgia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
109.253.207.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.185.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.206.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.135	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.135	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.155	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.250.174.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.155	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.155.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.158.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.138	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.164.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.240	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.3	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.122.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.32.179.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.10.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.111.76.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.149.186	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.10.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.242.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
68.180.229.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.22.134.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.124	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.94.115.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.124	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.72.47.174	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.185.15	Israel	147.237.77.234	halag.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.216.182.82	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.14.17	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
176.13.234.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.253.215.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
84.111.233.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.111.233.17	Block	3
46.116.114.188	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.158.49.179	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
195.154.41.132	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
31.154.81.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
91.121.193.159	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.138.65.252	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.111.233.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/login.aspx	Block	1
66.249.64.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
195.154.41.132	France	147.237.77.235	sviva.idf.il	Distributed Unauthorized Method for Known URL on 147.237.77.235/	Block	1
46.19.85.74	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
91.121.193.159	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/plugins/cherry-plugin/admin/import-export/upload.php	Block	1
77.139.161.239	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
85.250.174.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/35/	Block	1
95.86.102.180	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
78.46.42.235	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.102.9.8	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
31.154.81.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
185.3.147.78	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.24.60	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
79.176.78.62	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
31.154.81.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
91.121.193.159	France	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-22231-he/dover.aspx	Block	1
109.253.207.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1