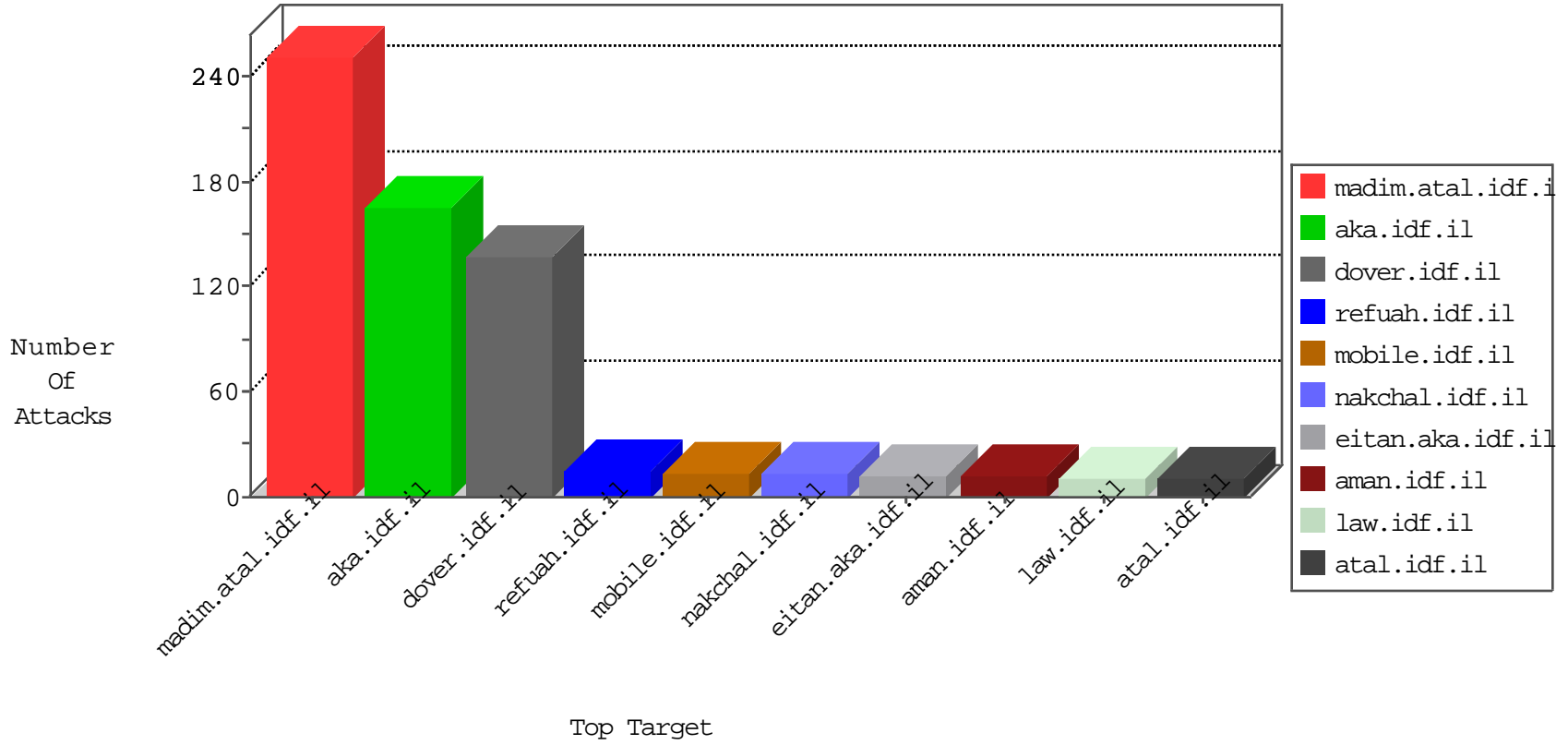


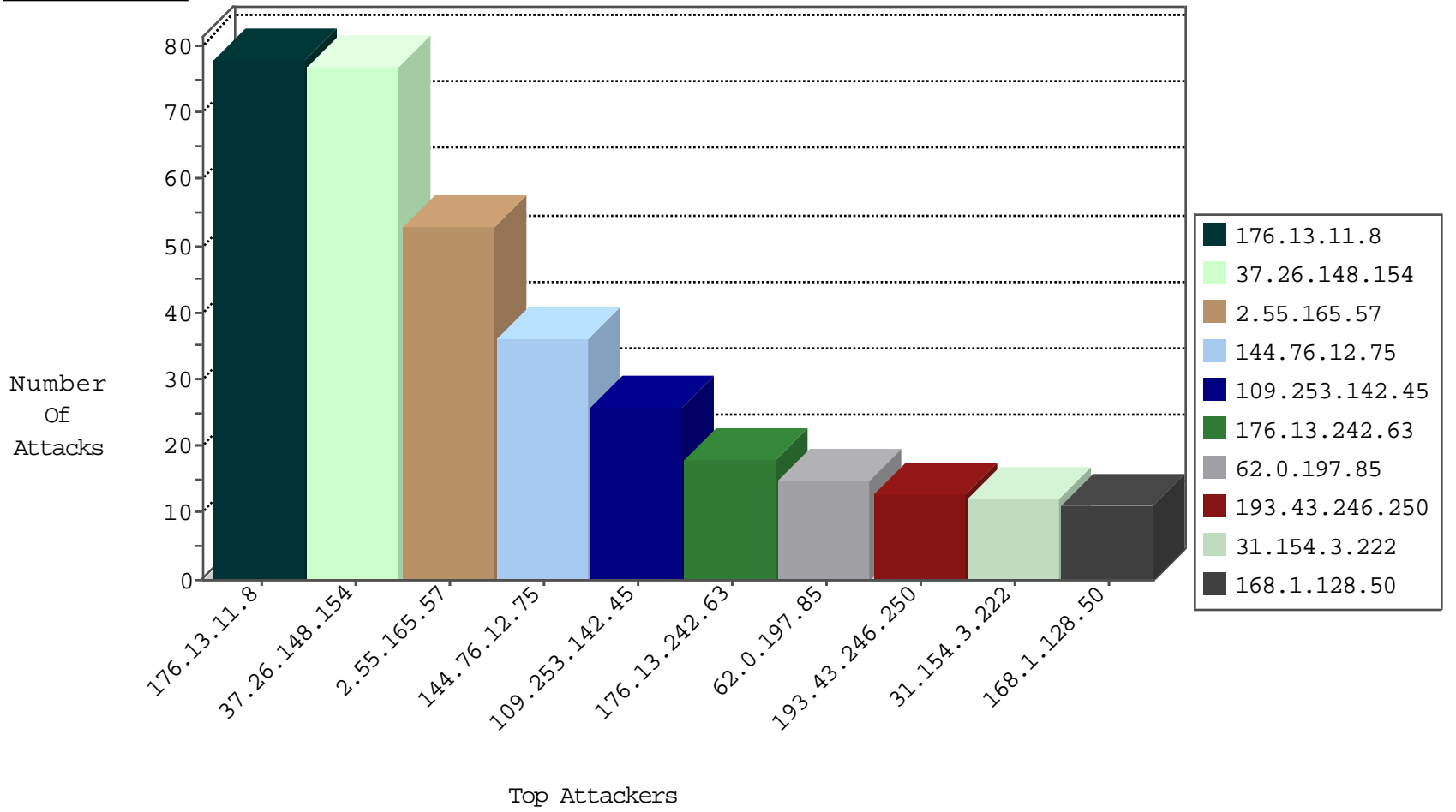
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.113	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	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
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.217	e.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
130.217.77.4	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
192.243.55.138	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
37.26.149.211	Israel	147.237.72.166	aka.idf.il	Invalid I4 Header Length	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
185.40.4.185	Russian Federation	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	36
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.120.188.149	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.123.204.57	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.152.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.50	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.65.110.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
79.177.221.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.50	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
65.60.36.203	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.1.128.50	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.173.50.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.50	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
52.166.249.197	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.50	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.116.158.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.111.107.58	147.237.8.46	Chile	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.218.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
190.67.192.63	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
132.74.14.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.222.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.13.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.136.27.66	147.237.77.178	Bangladesh	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.246.130.168	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
168.1.128.50	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
109.253.201.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
79.178.95.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.50	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.87.109.253	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
77.124.19.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.1.128.50	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
103.244.59.205	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.50	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	1
62.128.40.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
218.87.109.253	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
168.1.128.50	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
46.254.9.91	147.237.76.30	Sweden	himush.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.105.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
109.253.142.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
31.154.3.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.133.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.65.6.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.208.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.241.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.130.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.253.142.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.253.142.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
31.168.149.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.53.184.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.152	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.242.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.8	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.246.133.191	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.8	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.127.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.203.179.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
93.173.50.107	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.171	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.9.5.17	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.246.138.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
91.197.61.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.142.45	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	2
62.0.225.254	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.155.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
100.92.2.20		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.57.36.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.40	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.108.92.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.74.105.107	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
109.253.246.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
200.111.107.58	Chile	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.5.100.215	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.36.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.11.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
2.55.165.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
176.13.242.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.130.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.231.84	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
212.179.238.58	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
176.13.17.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.146.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.193.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.19.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.74.118.200	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.138.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.162.220	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
79.180.220.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1
46.116.82.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
109.65.6.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.137.158	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/gyus/general.aspx	Block	1
84.229.80.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
80.246.137.158	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method .1 in URL www.aka.idf.il	Block	1
212.179.238.58	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.179.238.58	Block	1
66.249.66.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
114.97.198.63	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-he/idfg.aspx/trackback/	Block	1
85.64.96.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.130.39	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
176.13.248.123	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.133.50	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.138.35	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
212.179.238.58	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	1
77.139.186.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
85.115.52.201	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
80.246.130.245	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
185.120.124.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct117 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.53.149.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.220.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.220.150	Block	1
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
80.246.137.158	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus/kadatz	Block	1
83.56.37.203	Spain	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1