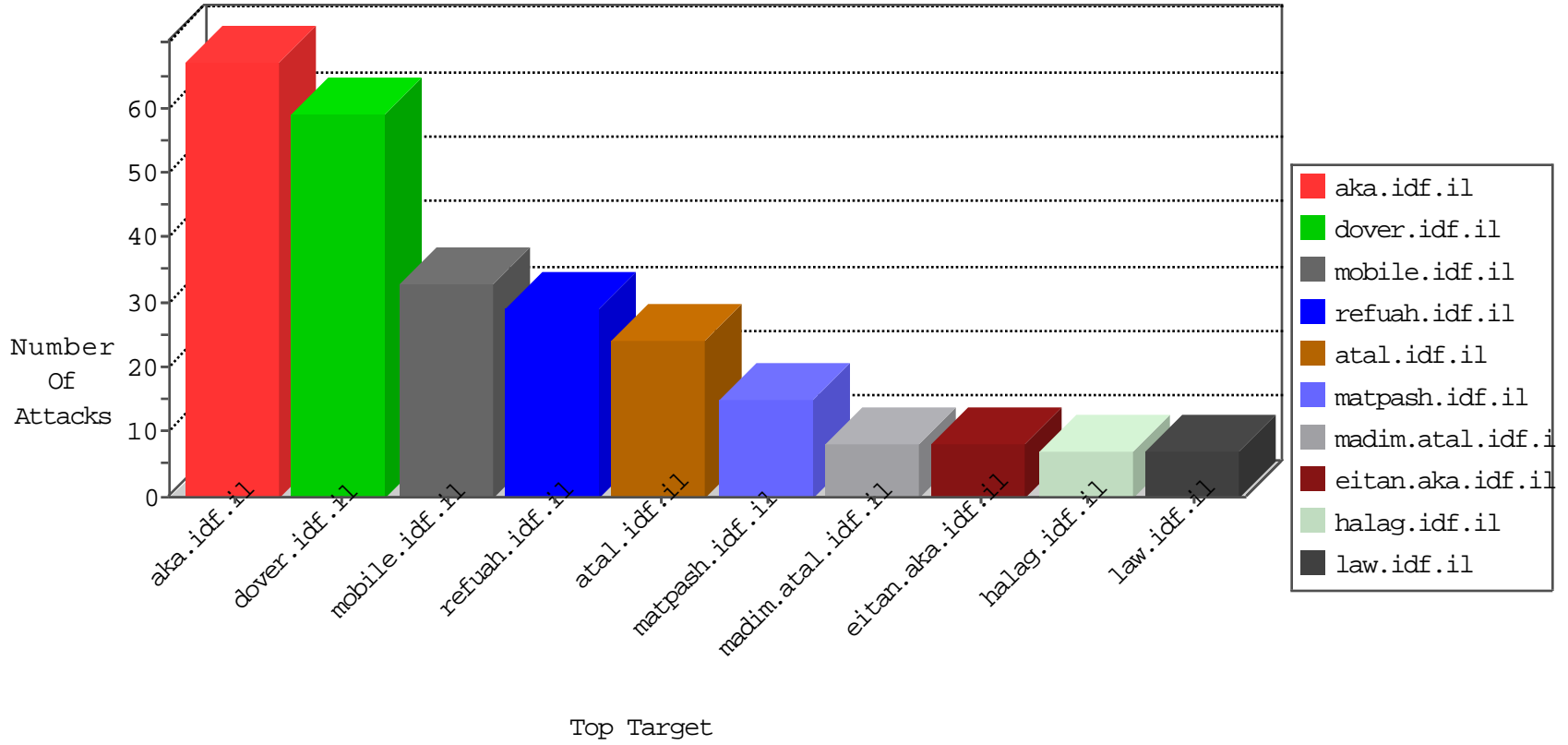


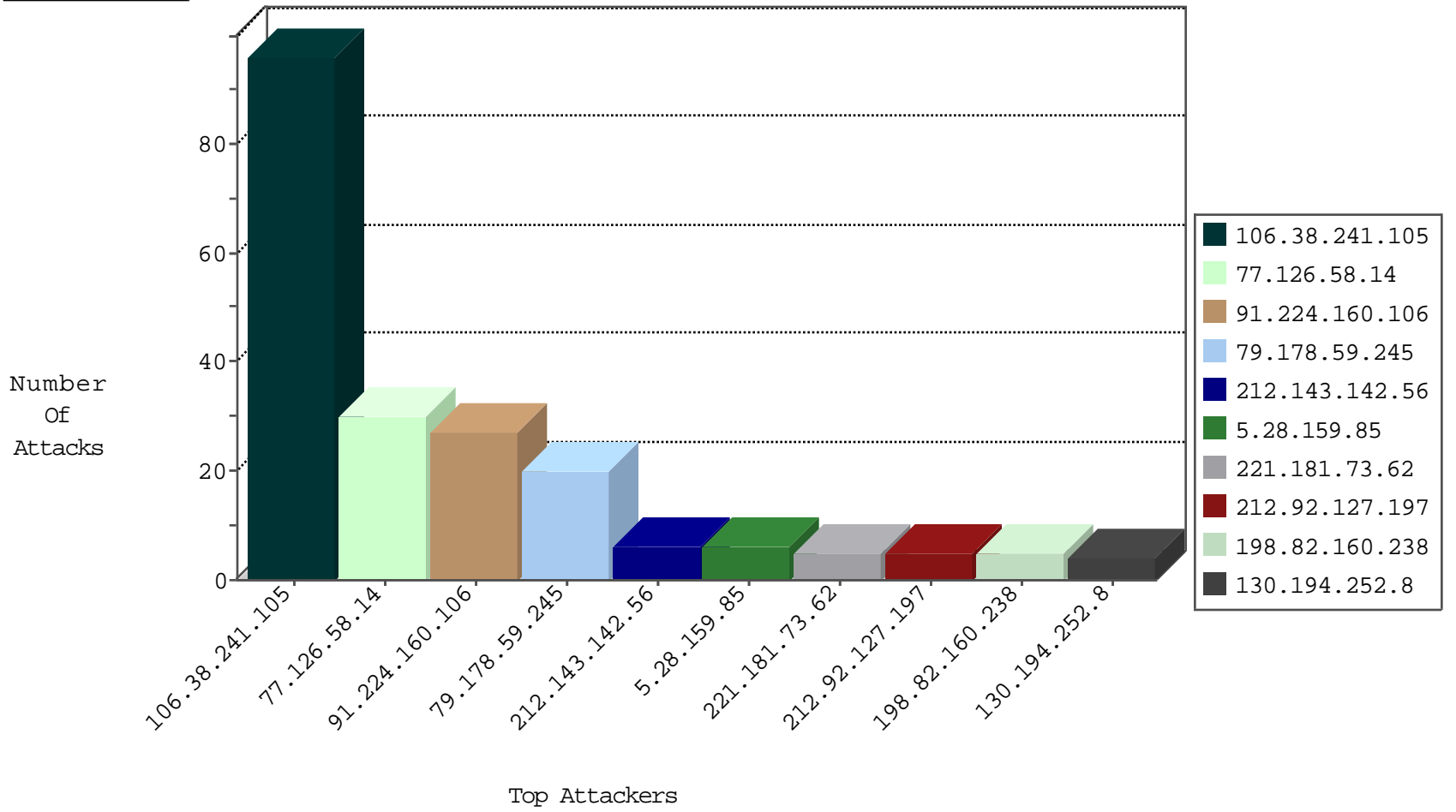
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
130.194.252.8	Australia	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
156.56.250.227	United States	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
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	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	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	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	1
131.179.150.72	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
112.78.13.73	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	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
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
112.78.13.78	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
112.78.13.74	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
122.114.117.82	China	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.82.160.221	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
112.78.13.75	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
112.78.13.76	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	31
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	24
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	17
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	14
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
78.46.50.246	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
106.38.241.105	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.77.234	halag.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
212.92.127.197	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
212.92.127.197	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.92.127.197	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.77.74	Japan	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.176	Japan	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.176	Netherlands	test.noore.idf.il	ET SCAN Potential SSH Scan	1
121.188.170.61	147.237.72.166	Korea, Republic of	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
212.92.127.197	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.92.127.197	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
201.38.68.132	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.198	Netherlands	e.ychalan.idf.il	ET SCAN Potential SSH Scan	1
14.18.232.118	147.237.77.234	China	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.242.4.52	147.237.8.27	Japan	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.177	Netherlands	noore.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
121.224.165.227	147.237.8.14	China	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.178.59.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.28.159.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.252	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
217.132.154.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
185.3.147.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.16	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.171.186.205	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
221.181.73.62	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
2.55.165.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.218.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.210.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.91.20.60	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
221.181.73.62	China	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
185.89.85.26	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.17	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
95.90.238.232	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.2.212.154	Romania	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.179.192.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
172.58.136.202	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.210.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.181.73.62	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
186.61.37.93	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.24	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
95.90.238.232	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
212.179.192.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.208.187.102	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
78.133.219.163	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.181.73.62	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
141.212.122.25	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
104.45.18.178	Netherlands	147.237.0.34	tikshuv.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
46.19.86.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.179.192.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.15.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.147	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
221.181.73.62	China	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
141.226.218.119	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.186.113.169	Japan	147.237.0.33	idf.il	drop		drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.63.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.63.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.1.235	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.53.1.235	Block	1
77.139.241.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
104.144.148.125	United States	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
66.102.9.30	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
79.178.59.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
104.144.148.125	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to ww.logistics.atal.idf.il/wp-login.php	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
157.55.39.122	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
216.244.66.241	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.139.93.25	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
80.246.130.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1