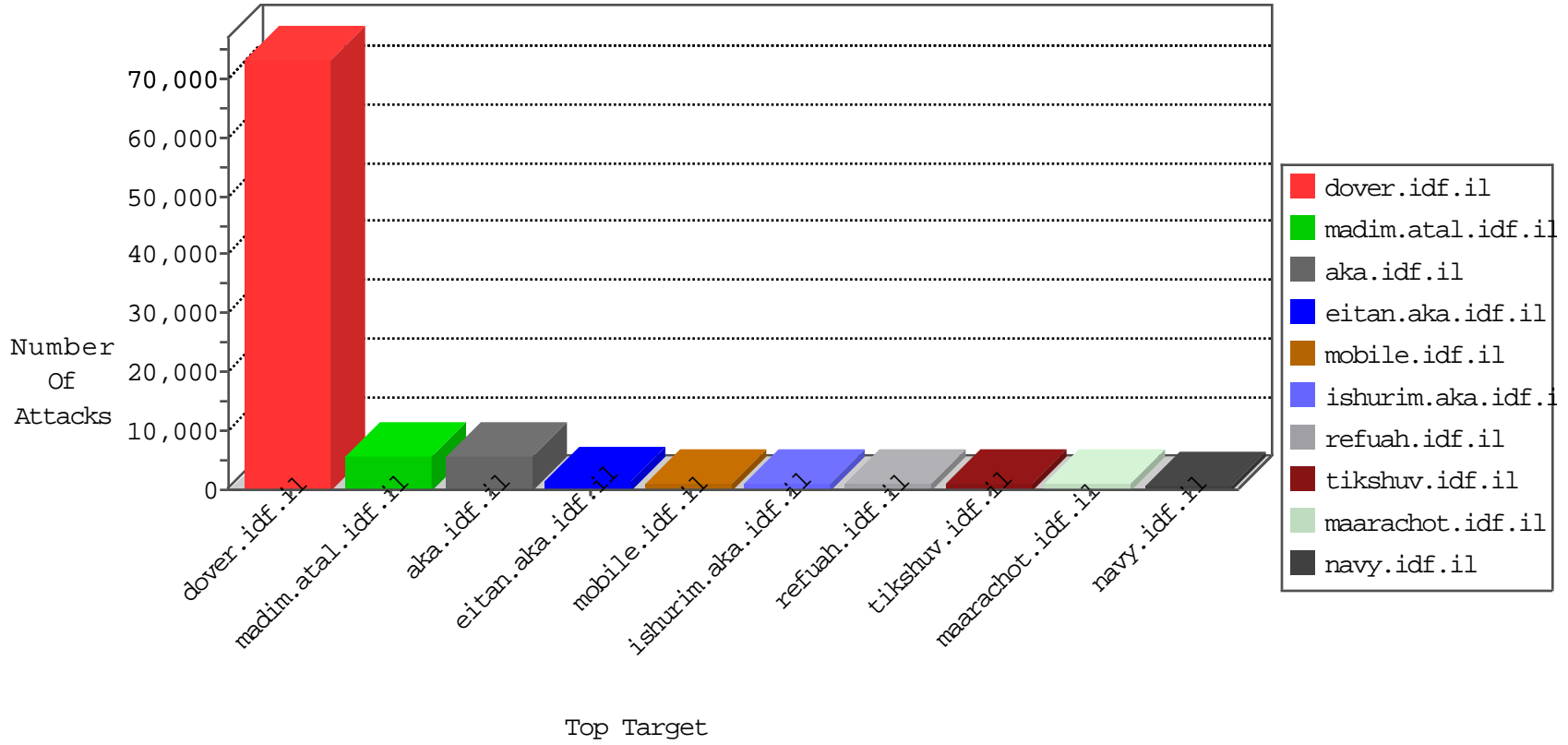


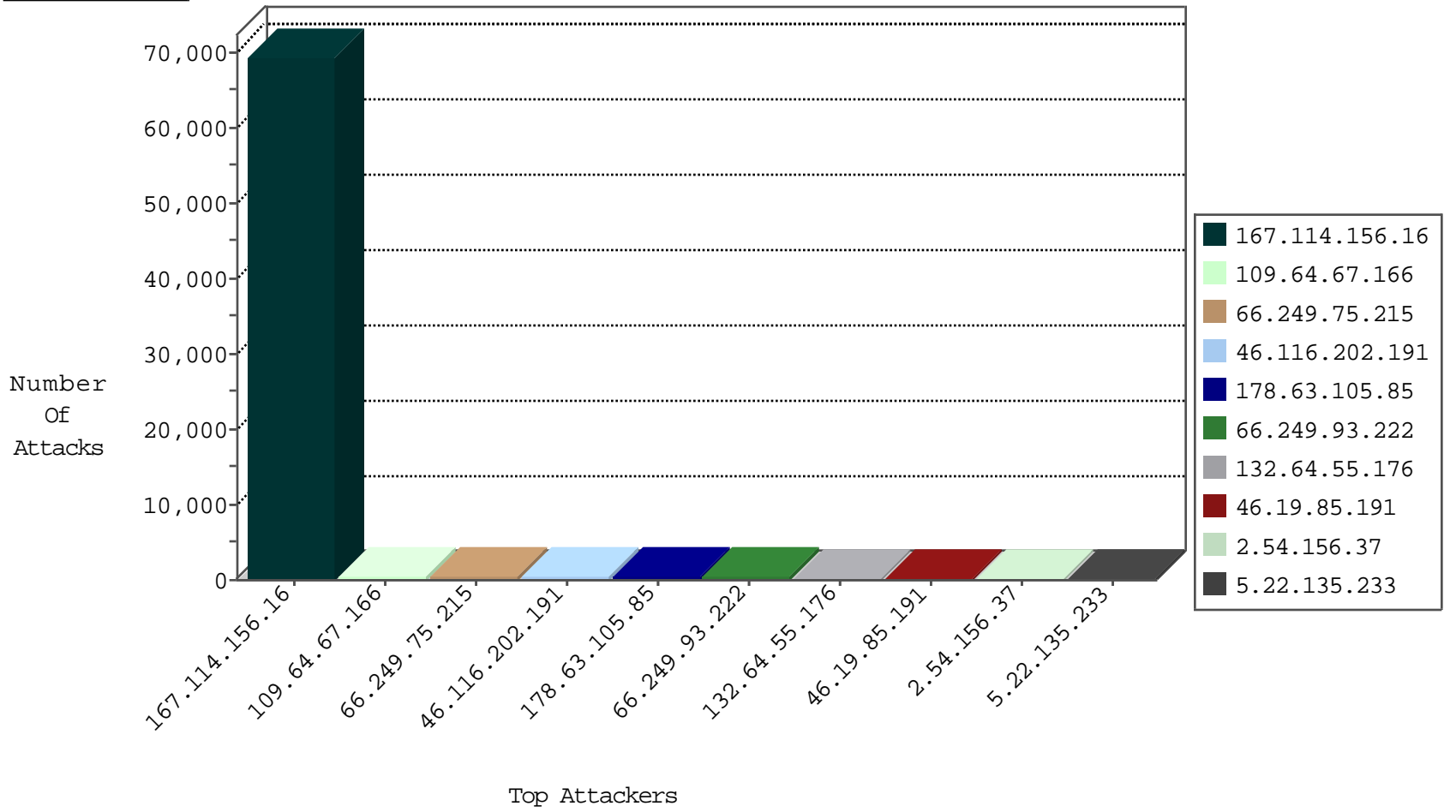
# IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	90688
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	7838
41.254.9.161	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4352
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	624
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	584
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	445
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	365
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
104.48.120.241	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	328
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	288
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	103
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	48
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	42
46.19.85.59	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	34
193.43.246.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
79.180.193.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
46.120.160.160	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	14
109.253.134.92	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
66.249.91.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
212.235.98.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
77.126.144.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
91.214.5.128	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
91.231.192.149	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
103.235.242.51	China	147.237.0.19	madim.atal.idf.il	L4 Source or Dest Port Zero	drop	8
37.26.149.255	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
46.19.85.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.66.48.27	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.182.177.6	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.108.152.18	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.67.148.213	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.110.110.138	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
176.13.17.65	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
216.249.107.200	United States	147.237.72.166	aka.idf.il	Anomaly-TCP-shorthead	dest-reset	5
109.253.138.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.85.106	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
212.143.191.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
213.159.209.5	Russian Federation	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	4
79.182.178.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
103.235.242.51	China	147.237.0.33	idf.il	L4 Source or Dest Port Zero	drop	4
216.249.107.200	United States	147.237.72.166	aka.idf.il	Anomaly-TCP-SYN-FIN	dest-reset	4
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
109.65.133.31	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
103.235.242.51	China	147.237.77.227	e.hamaz.idf.il	L4 Source or Dest Port Zero	drop	3
168.235.196.224	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
84.111.65.41	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
103.235.242.51	China	147.237.8.50	e.tikshuv.idf.il	L4 Source or Dest Port Zero	drop	3
81.218.165.186	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
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	41
213.151.37.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
46.121.153.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
5.22.131.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	21
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	20
79.176.103.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
2.54.40.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
87.70.1.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
5.102.224.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
5.29.127.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
84.94.47.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
194.90.242.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.64.106.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
80.246.130.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
46.19.86.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
132.248.44.99	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
79.182.98.136	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.19.86.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
207.46.13.141	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
81.218.131.145	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.133.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.210.115.133	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	8
81.218.251.251	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
5.29.213.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.210.115.133	France	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	8
109.253.200.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.210.115.133	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	8
84.228.249.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
62.210.115.133	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	8
85.250.6.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
93.172.161.116	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.44	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
207.232.36.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
212.199.103.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
79.181.102.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
93.173.3.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.64.53.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.166.159.241	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.29.38.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.88.200.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.67.131.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.26.147.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.142.68.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.130.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.215	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	551
66.249.93.222	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	341
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	64
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	44
80.246.133.239	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	12
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	7
64.31.44.6	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
37.205.0.49	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	6
216.249.107.200	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
175.100.5.215	147.237.77.226	Cambodia	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	3
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
132.248.44.99	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
80.246.130.92	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
181.214.92.181	147.237.77.212	Chile	e.dover.idf.il	ET SCAN Potential SSH Scan	2
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	2
175.100.5.215	147.237.77.205	Cambodia	prisha.idf.il	ET SCAN Potential SSH Scan	2
81.218.241.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.26	147.237.77.216	United States	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
132.248.44.99	147.237.0.15	Mexico	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
37.26.146.211	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
149.56.41.141	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
217.21.4.68	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
93.189.26.18	147.237.0.19	Austria	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
80.246.130.243	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
85.64.234.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.98	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
23.96.109.87	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
95.35.131.202	147.237.77.234	Israel	halag.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
79.176.61.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.48.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
42.116.139.91	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.169.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.12	147.237.77.235	Romania	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
208.71.68.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
37.139.27.231	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.10.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.117.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.86.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.233.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
23.96.109.87	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
164.39.11.198	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.11.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1293
109.64.67.166	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	552
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	521
46.116.202.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	488
132.64.55.176	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	285
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	264
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	177
194.54.168.65	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	143
109.253.143.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
109.67.119.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
94.230.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	93
176.13.1.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
94.230.86.247	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	92
79.179.55.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
87.71.96.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
89.139.130.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
31.210.186.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	63
185.120.126.195		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	59
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	55
37.26.146.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	53
31.168.122.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	49
89.138.127.226	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
149.88.204.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	47
176.13.16.58	Israel	147.237.0.19	medim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	42
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	41
2.54.51.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	41
46.19.85.244	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
31.210.187.91	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	36
212.29.210.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
37.46.38.137	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
80.246.133.233	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
79.183.151.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
212.29.210.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	33
191.243.161.25	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	33
191.243.161.25	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
109.65.66.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
87.70.74.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
89.139.190.247	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
80.246.139.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	275
2.54.156.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	221
5.22.135.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	214
176.13.6.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
2.52.45.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	189
87.70.96.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	182
2.54.141.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	179
176.13.11.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
2.54.60.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	158
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
2.52.129.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
2.54.39.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
185.32.179.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
176.13.6.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
2.54.157.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
2.54.37.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.54.52.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
37.26.149.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
212.199.57.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
109.253.222.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
2.52.190.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
2.54.53.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.54.136.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.52.155.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.26.146.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
109.253.158.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
37.26.149.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.54.58.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.52.15.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.52.128.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.13.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
109.253.218.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.147.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.52.181.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
2.54.5.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
37.26.149.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
212.25.85.54	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	38
2.54.39.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.54.58.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.253.143.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
109.253.146.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
185.32.179.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29