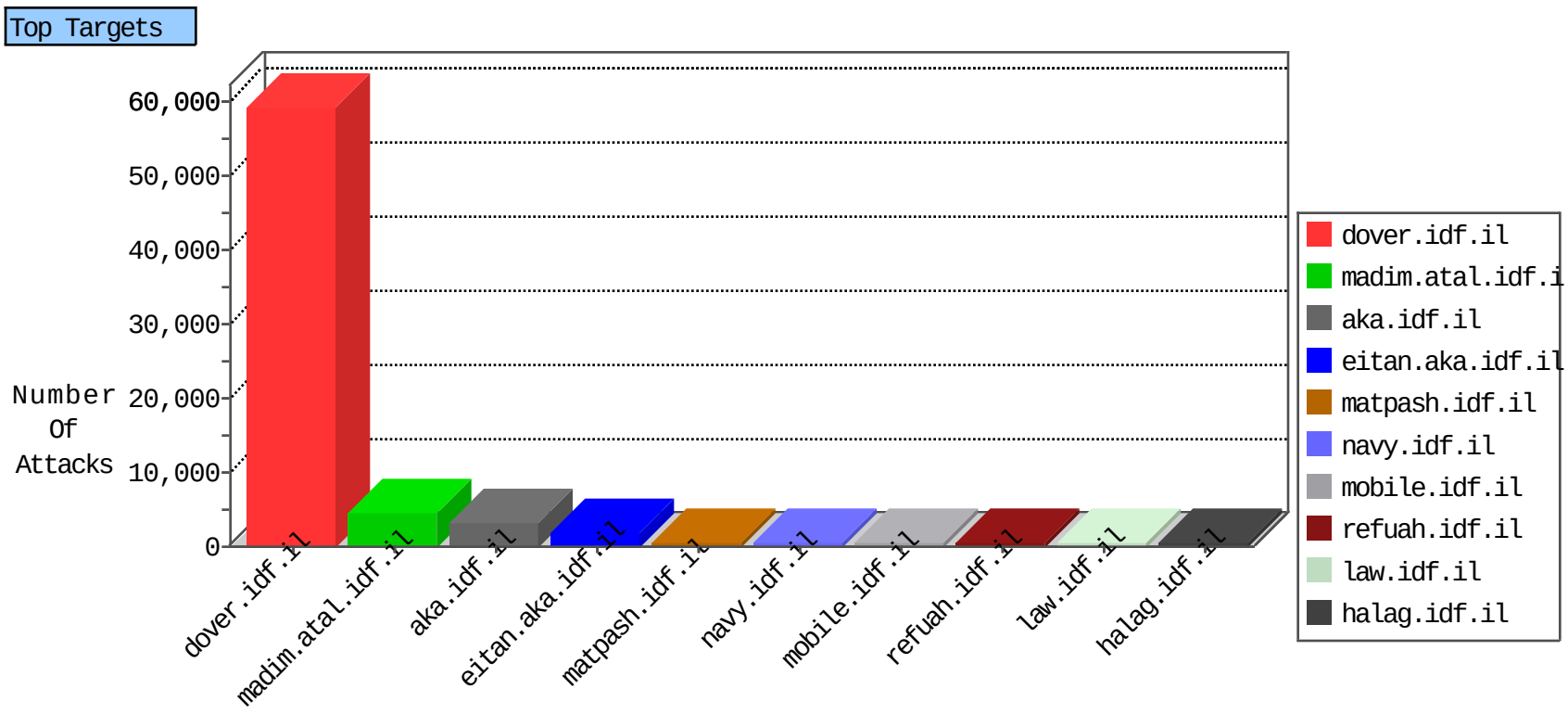
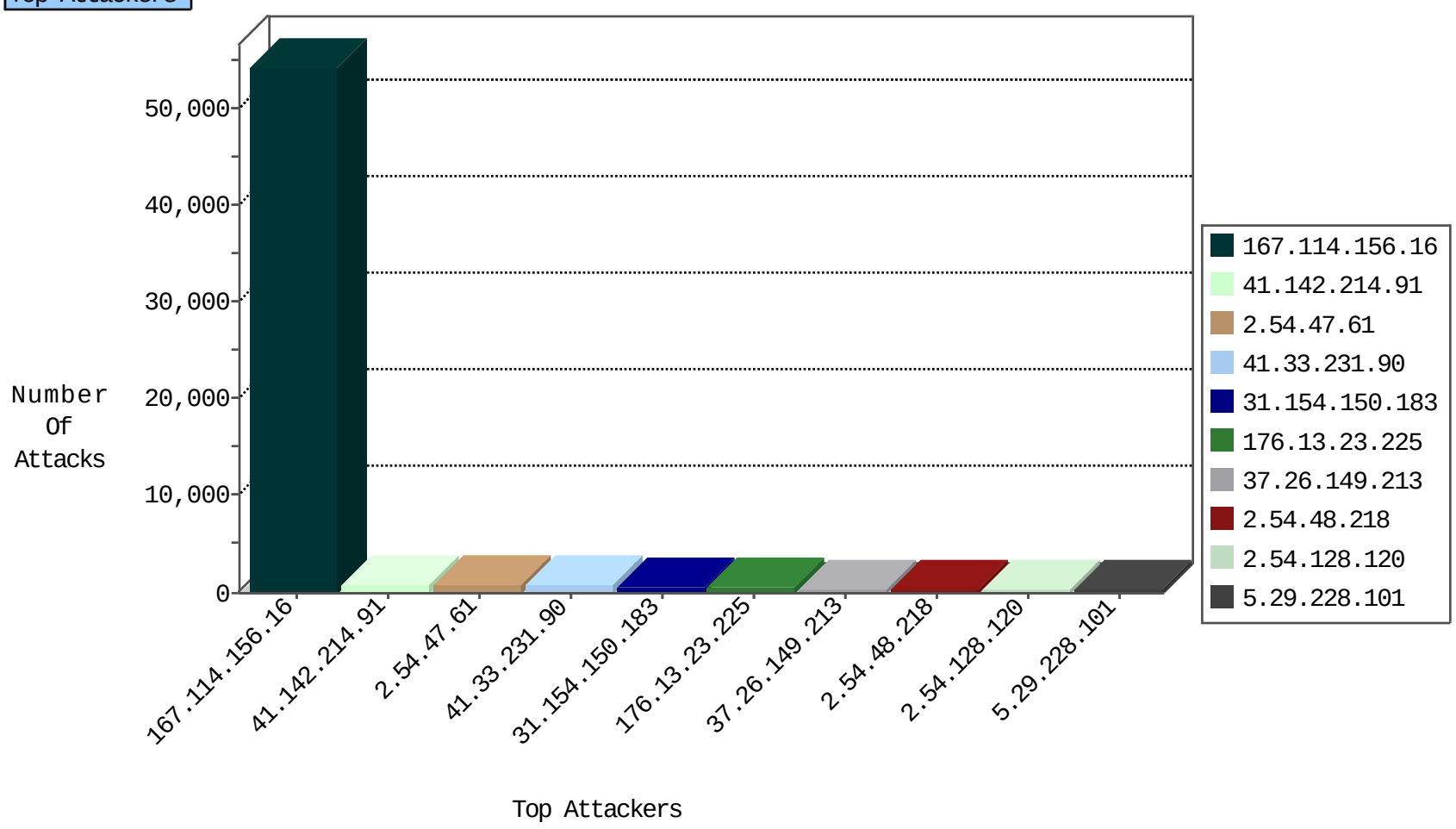
12-25-2015 to 12-26-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-25-2015 to 12-26-2015

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	89558
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5121
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3213
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	597
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	261
66.249.64.165	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	90
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	83
80.246.136.39	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
107.170.42.128	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
216.4.56.168	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	4
107.170.102.81	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
198.58.103.92	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.66.145.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	3
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
149.88.114.180	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
117.27.146.44	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
68.116.5.134	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
207.46.13.21	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
184.21.5.214	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
71.6.135.131	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.92	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
187.67.19.25	Brazil	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
82.145.229.7	Turkey	147.237.76.148	gqcenter.aka.idf.il	Block_Ip_Web_In	drop	1
77.247.178.132	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.81	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.50.250.4	Canada	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
107.150.98.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.69	Switzerland	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
172.98.67.67		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
79.178.35.76	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

12-25-2015 to 12-26-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.16.50	United States	147.237.77.216	dover.idf.il	C014: HTTP: Fuck in url	Block	26
95.10.174.221	Turkey	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	2
198.20.69.74	United States	147.237.76.199	e.nakchal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
95.10.174.221	Turkey	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
157.55.39.227	United States	147.237.77.233	atal.idf.il	C091: HTTP: Access to - admin.asp	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
45.33.104.237		147.237.72.167	ishurim.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
157.55.39.228	United States	147.237.77.233	atal.idf.il	C091: HTTP: Access to - admin.asp	Block	1
198.27.82.153	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
186.213.6.138	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
78.46.174.197	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
62.210.152.87	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.76.44	e.refuah.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
62.210.162.217	France	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

12-25-2015 to 12-26-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.85	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	116
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	94
95.10.174.221	147.237.77.74	Turkey	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
66.249.81.166	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	8
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
74.143.224.18	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
95.10.174.221	147.237.77.216	Turkey	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
209.66.70.253	147.237.77.176	United States	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	4
49.14.84.61	147.237.8.45	India	e.eitan.idf.il	GPL SCAN nmap TCP	4
218.104.49.211	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	3
91.200.12.139	147.237.77.216	Ukraine	dover.idf.il	ET WEB_SERVER Poison Null Byte	3
218.104.49.211	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	3
104.255.67.115	147.237.72.166		aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
94.102.48.195	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.104.49.211	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.181	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.83.155	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
87.68.55.8	147.237.77.74	Israel	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	2
176.12.147.154	147.237.77.74	Israel	law.idf.il	GPL SCAN myscan	2
80.246.130.11	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.81.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.216	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.78.69	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.102.48.195	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	2
88.80.190.113	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
162.222.185.165	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	2
81.218.247.58	147.237.8.28	Israel	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
81.218.247.58	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
176.12.147.154	147.237.77.74	Israel	law.idf.il	INDICATOR-SCAN myscan	2
66.249.81.212	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.139	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.104.49.211	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
31.168.181.151	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
218.104.49.211	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
212.72.12.2	147.237.77.212	Oman	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
81.218.247.58	147.237.72.167	Israel	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
187.160.210.68	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
166.63.122.229	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1

12-25-2015 to 12-26-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	838
2.54.47.61	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	759
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	637
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	575
37.26.149.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	438
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	179
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	142
41.142.214.91	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	131
141.0.15.33	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	128
46.19.86.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	118
216.185.58.7	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	108
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	95
8.37.231.89	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	89
46.19.85.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
2.54.155.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	65
66.249.69.122	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	49
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	48
84.228.78.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	48
84.228.78.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
184.21.5.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
79.177.160.225	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
66.249.93.146	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
213.57.128.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	39
213.57.128.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	39
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
63.141.204.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	34
213.57.128.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	33
188.139.250.137	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
188.139.250.137	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
95.221.252.232	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
77.126.95.184	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.26	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
193.251.135.74	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	23
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
176.13.19.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
89.139.59.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
31.154.155.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
79.177.116.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
5.102.254.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
46.19.86.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
213.57.128.60	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
213.57.128.60	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
31.154.8.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
213.57.128.60	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
82.145.218.13	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.154.150.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 31.154.150.183	Block	297
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.23.225	Block	263
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	262
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	195
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	190
2.54.128.120	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.128.120	Block	188
5.29.228.101	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.228.101	Block	186
77.127.206.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	151
5.29.190.196	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
77.127.206.147	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 77.127.206.147	Block	149
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	144
2.54.128.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
2.54.47.61	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
31.154.150.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 31.154.150.183	Block	111
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
79.183.1.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
5.29.228.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
31.154.150.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
84.111.184.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
94.159.169.204	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.169.204	Block	81
213.57.159.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
37.26.147.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
2.54.48.218	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.48.218	Block	79
5.29.228.101	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 5.29.228.101	Block	78
213.57.151.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
2.54.188.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
46.19.86.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
79.183.1.34	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.183.1.34	Block	58
109.253.220.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.54.128.120	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.128.120	Block	56
2.54.12.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
37.26.147.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
2.54.171.148	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.171.148	Block	53
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	53
149.78.245.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
213.57.159.246	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.159.246	Block	46
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
176.13.23.225	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.23.225	Block	43
46.19.86.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
199.30.25.202	United States	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 199.30.25.202	Block	38
37.26.149.213	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.213	Block	37
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
213.57.151.200	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.151.200	Block	36
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	33
109.253.159.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
5.102.254.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.154.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.12.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
185.32.179.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
217.132.33.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26