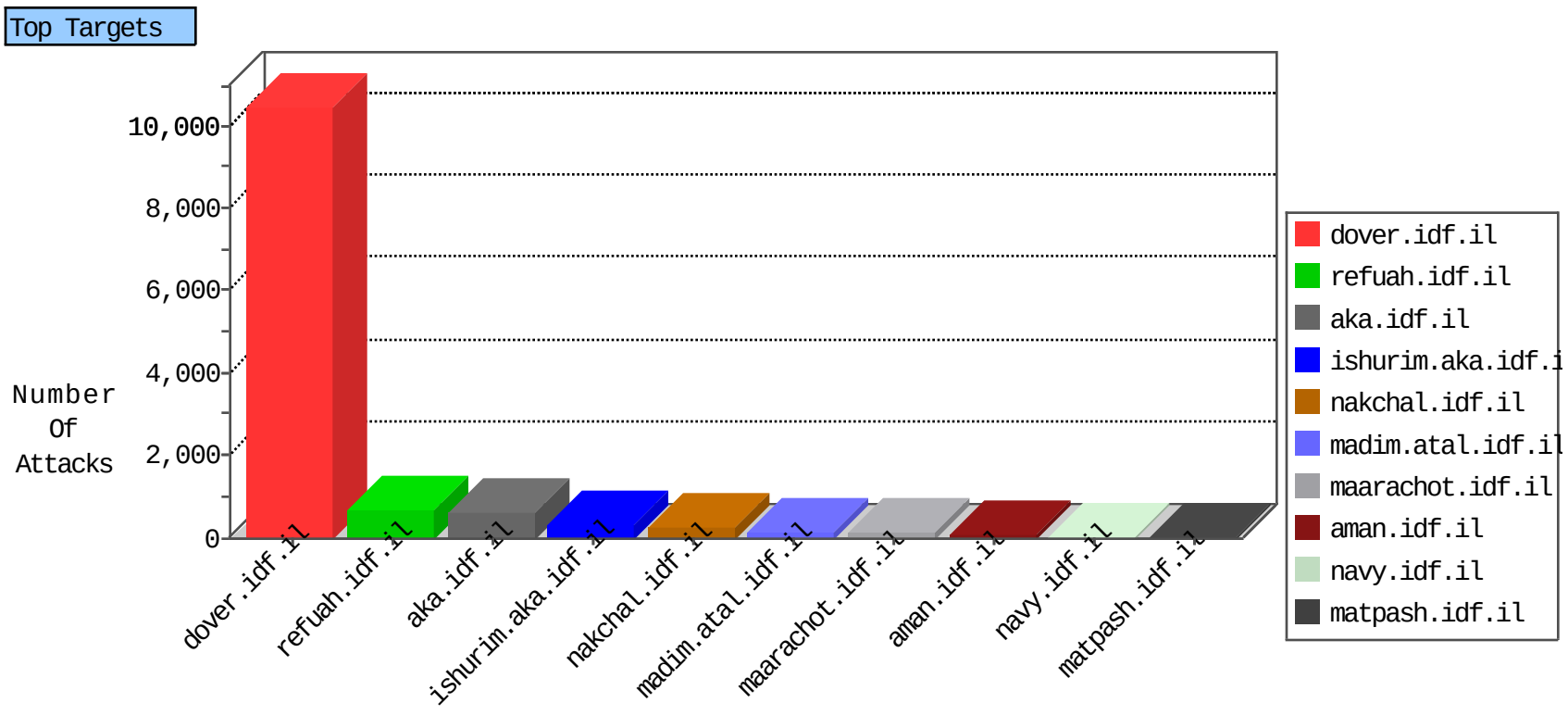
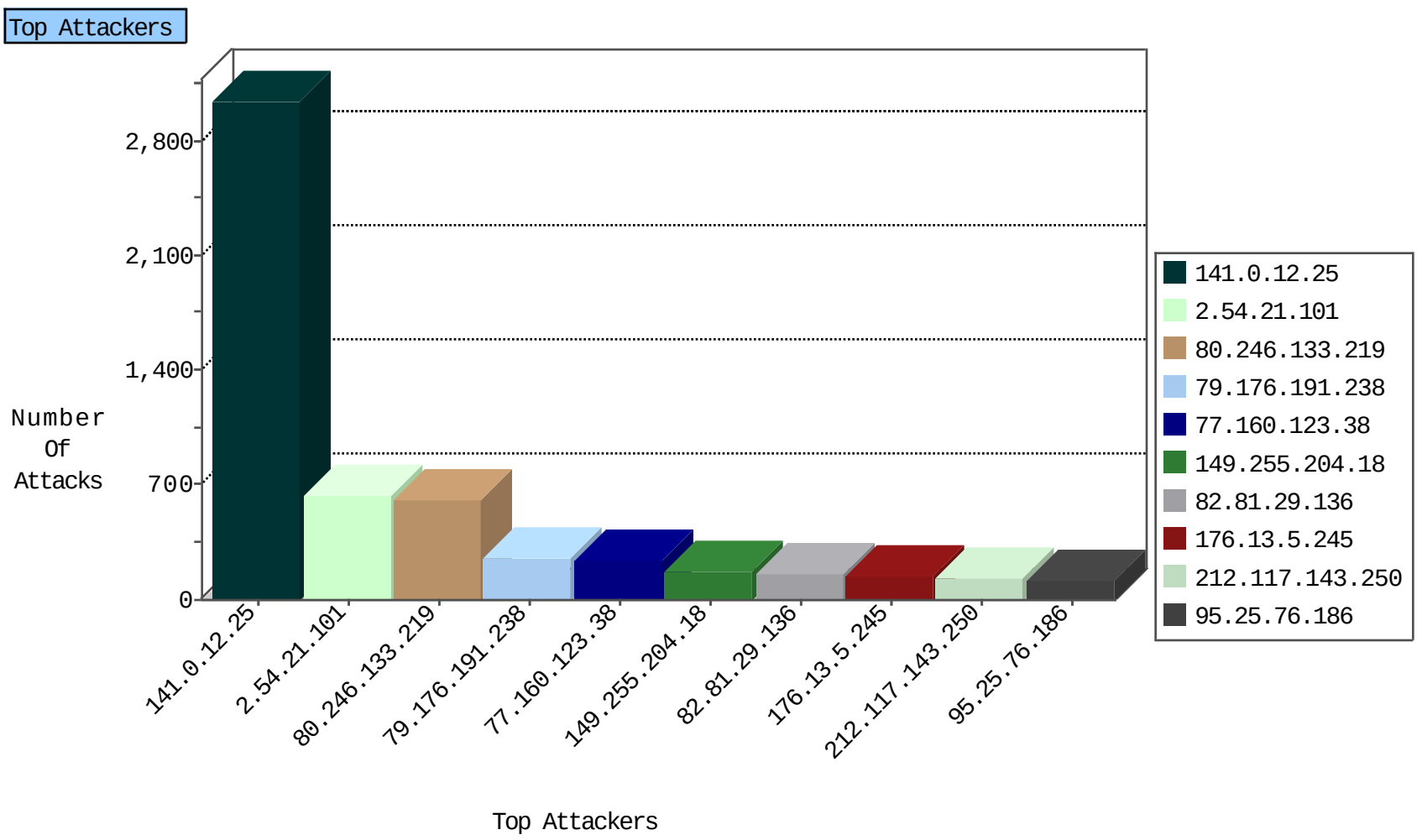
10-22-2015-12:04:08 to 10-22-2015-13:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-22-2015-12:04:08 to 10-22-2015-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.163	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2929
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1837
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	225
2.54.155.117	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	165
93.173.165.180	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
2.52.35.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.179.167.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
84.94.195.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.19.86.39	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
5.144.59.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
84.108.106.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
95.25.76.186	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.67.185.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
212.29.237.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.21.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.128.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
89.138.202.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.15.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.174.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.168.19.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
41.227.47.3	Tunisia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
192.117.12.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
31.168.178.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
132.73.50.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.178.59.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.149.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.179.71.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.41.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.151.59.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3
2.52.7.102	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.19.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.228.42.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.85.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.32.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.137.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.32.179.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.138.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.139.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.19.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.13.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
62.90.181.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
212.14.228.158	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.142.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.180.23	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.40.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
142.54.187.42	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
80.246.137.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
63.225.175.24	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-22-2015-12:04:08 to 10-22-2015-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.116.129	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
85.64.16.99	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-22-2015-12:04:08 to 10-22-2015-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.80.198.164	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
176.12.142.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
142.54.163.74	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.85.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.90.138.60	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.79.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.89.142	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.57.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.44.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
176.13.6.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
164.138.112.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
142.54.163.74	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.67.146.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.58.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
86.108.12.231	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.138.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.44.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
212.150.73.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1

10-22-2015-12:04:08 to 10-22-2015-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.12.25	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3045
2.54.21.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	623
80.246.133.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	589
79.176.191.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	258
77.160.123.38	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	245
149.255.204.18	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	170
212.117.143.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
95.25.76.186	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	105
82.81.29.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
37.151.107.243	Kazakstan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
84.228.96.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
133.36.145.13	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
185.58.201.28	Lebanon	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	74
46.19.86.33	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.86.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
46.19.86.204	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.52.7.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
176.13.17.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
2.54.6.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
109.66.59.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
185.23.127.226	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
109.67.114.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.13.4.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
77.125.90.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
85.64.0.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.86.247	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
176.13.13.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.189	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
62.219.153.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
84.108.102.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
176.12.138.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	43
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
92.241.54.96	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
81.218.33.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
82.81.29.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.245	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.5.245	Block	140
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	84
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
64.79.85.205	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	56
64.79.85.205	United States	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	42
132.68.18.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	28
203.133.170.162	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	14
85.64.16.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	14
23.97.166.57	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
208.115.113.87	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
82.145.210.14	Europe	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1380	Block	14
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.65.17.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
80.246.133.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2418.jpg	Block	14
212.150.214.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	14
141.212.122.96	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /x	Block	14
84.55.42.31	Lithuania	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/horaot	Block	14
85.167.180.74	Norway	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
80.246.133.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/layout.css	Block	14
213.8.247.155	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	14
85.64.0.166	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker1 in www.idf.il/1780-he/dover.aspx	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	14
85.250.122.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
217.86.201.186	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
176.13.19.95	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding bHvZ(jejOp Bt/@ in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
85.64.16.99	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.16.99	Block	14
17.138.57.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	14
207.46.13.149	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx	Block	14
109.64.198.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
82.81.29.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	14
66.249.67.249	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	14