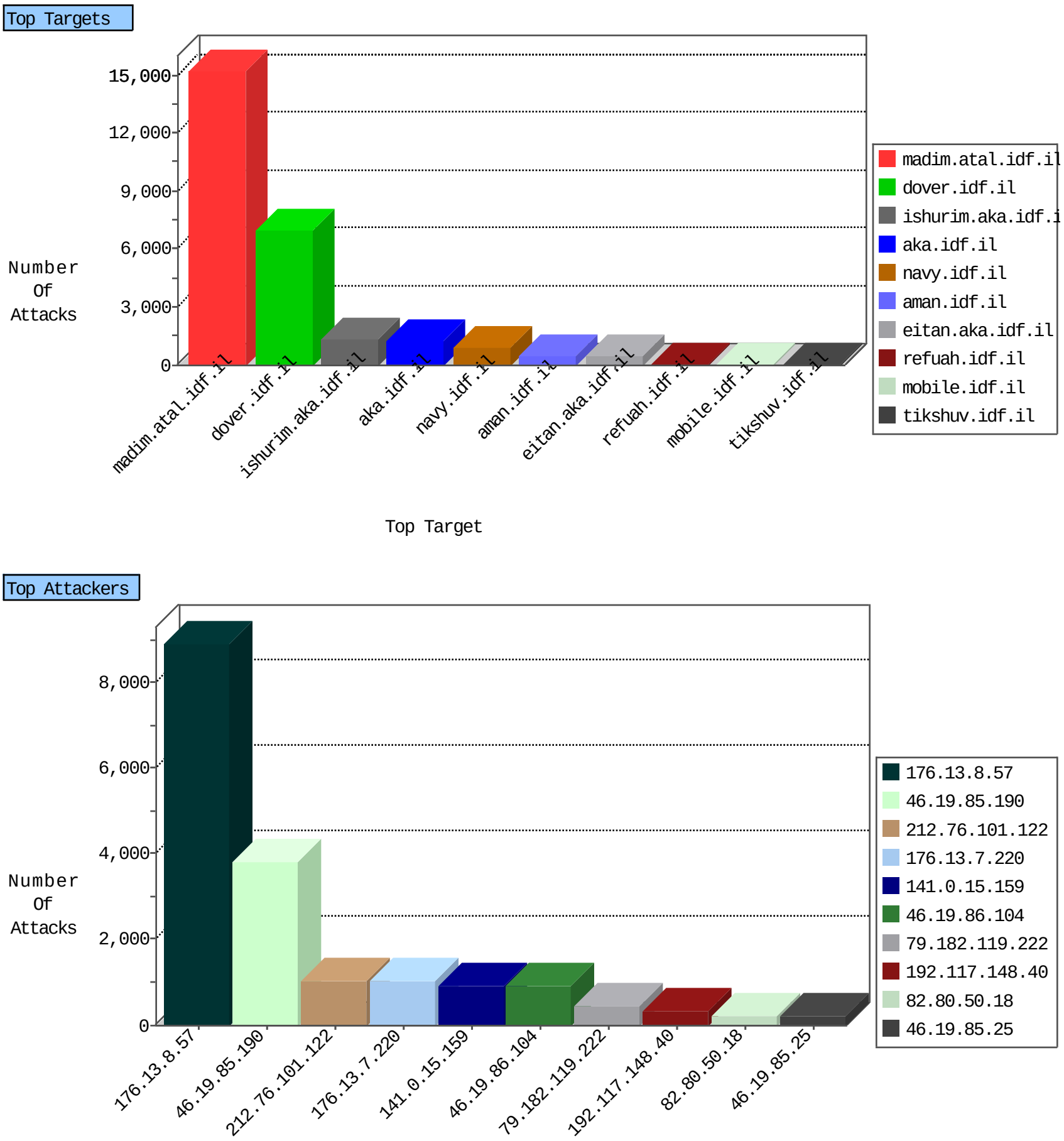
10-25-2015-10:04:09 to 10-25-2015-11:04:09

IDF Under Attack Daily Report



10-25-2015-10:04:09 to 10-25-2015-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	649
185.32.179.109	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	85
176.12.141.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
149.78.226.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
194.90.66.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	28
37.26.146.130	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
185.32.179.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
176.12.146.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.86.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
192.117.148.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
95.150.62.205	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.43	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.145.218.1	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
37.26.149.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.181.13.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
95.86.110.61	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.9.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.199.108.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.4.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.31.117.76	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.13.6.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.54.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.147.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.139.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.102.206.114	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.52.44.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.178.198.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5
84.94.105.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.6.64.106	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.7.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.137.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.85.170	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
82.81.193.82	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.12.141.217	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
104.34.104.186	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.11.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.34.139	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.32.179.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.32.179.101	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.26.147.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
80.246.140.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.86.121.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.173.160.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
209.88.198.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.95.251.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3

10-25-2015-10:04:09 to 10-25-2015-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.134.102.16	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
138.134.102.15	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6

10-25-2015-10:04:09 to 10-25-2015-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.254.3.213	147.237.72.166	Kenya	aka.idf.il	ET SCAN Potential SSH Scan	1
121.40.195.144	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.130.136.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.74.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.162.116.221	147.237.0.15	Sweden	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.29.213.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.156.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.124.35.115	147.237.77.233	Nicaragua	atal.idf.il	ET SCAN NMAP -sS window 4096	1
92.61.225.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.145.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.1.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.235.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.146.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-25-2015-10:04:09 to 10-25-2015-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1035
141.0.15.159	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	935
79.182.119.222	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	438
192.117.148.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	309
46.19.85.218	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	216
213.244.82.140	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	180
46.19.85.68	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	150
46.19.86.96	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
46.19.86.216	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.19.85.124	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
46.19.86.70	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.86.142	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
46.19.85.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
2.54.186.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	66
46.19.86.171	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
2.52.4.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
213.151.57.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.19.85.10	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.199	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.85.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
85.250.227.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
212.179.155.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
185.33.169.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.120.36.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
109.65.164.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
89.138.193.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.147	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
5.29.237.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.85.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
62.219.114.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.86.52	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
31.154.91.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.176.147.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.49	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
100.100.33.111		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
2.54.32.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
100.100.33.111		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	39
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
37.142.64.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.85.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
37.26.146.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
46.19.86.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
192.116.130.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33

10-25-2015-10:04:09 to 10-25-2015-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.8.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8912
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3766
176.13.7.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1025
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	868
82.80.50.18	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	126
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	98
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	84
82.80.50.18	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.50.18	Block	70
93.173.31.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.173.31.64	Block	70
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	42
176.13.25.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	42
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
176.13.25.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
176.13.26.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
176.13.25.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
176.13.26.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
82.80.50.18	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/4/	Block	28
176.13.24.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
176.13.27.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
37.26.146.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
176.13.25.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	27
176.13.27.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
37.26.146.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.26.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
2.54.27.220	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	14
176.13.25.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
176.13.24.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
176.13.26.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
113.33.228.2	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
31.168.199.226	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
176.13.25.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
176.13.16.88	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	14
182.118.54.219	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery/jquery-ui.js	Block	14
46.19.85.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
87.69.240.53	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.240.53 (Open Mode)	None	14
2.54.128.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.25.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
212.235.56.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.13.24.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
149.78.70.89	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/miluim/	Block	14
46.19.85.190	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	14

10-25-2015-10:04:09 to 10-25-2015-11:04:09