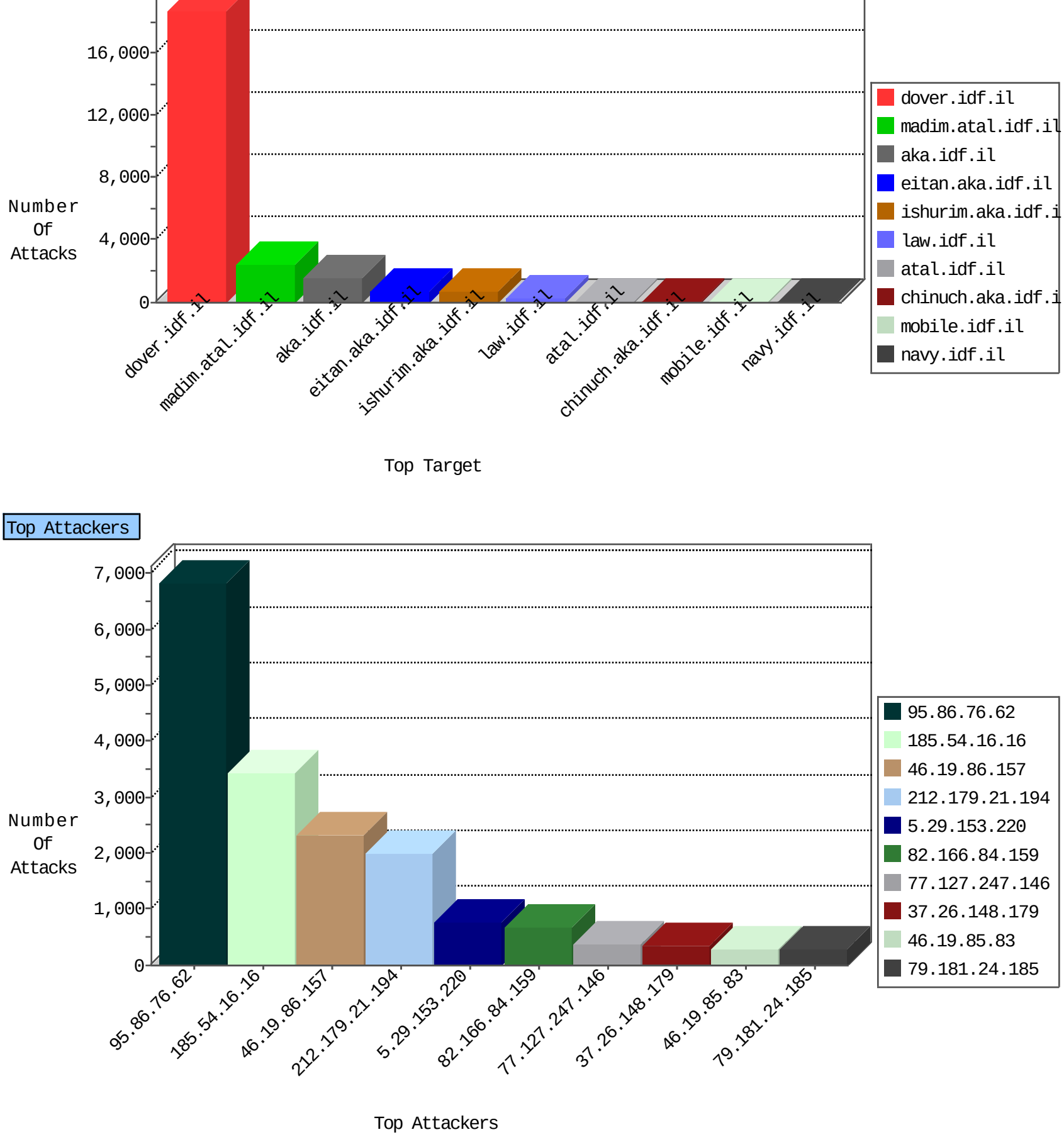
10-26-2015-12:04:05 to 10-26-2015-13:04:05

IDF Under Attack Daily Report



10-26-2015-12:04:05 to 10-26-2015-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3582
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	497
66.249.78.148	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	465
212.64.228.100	Europe	147.237.72.167	ishurim.aka.idf.i	TCP handshake violation, first packet not syn	drop	431
185.54.16.16	United Arab Emirates	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	277
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	276
147.235.236.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	228
2.54.4.205	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
80.74.110.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	47
109.64.8.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	39
176.106.227.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
37.26.146.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
79.181.175.215	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
2.54.39.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
46.19.85.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
95.86.113.30	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
82.80.203.100	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
50.117.41.6	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.12.139.36	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.13.12.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
176.13.18.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.179.121.201	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.85.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
2.52.131.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	9
192.114.23.209	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
85.250.117.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.86.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.19.85.244	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	7
62.90.10.97	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.163.12	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
87.69.200.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
80.246.139.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.180.121.169	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.24.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
62.219.153.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.48.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.8.50.112	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.121.80.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.183.21.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.150.214.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.184.248	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
147.235.8.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
192.115.189.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

10-26-2015-12:04:05 to 10-26-2015-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.242.98	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
15.203.178.12	France	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
66.249.67.65	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

10-26-2015-12:04:05 to 10-26-2015-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	51
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	4
81.218.251.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
79.180.208.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.187.168.27	147.237.77.216	Poland	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.14.48.80	147.237.77.74	Chile	law.idf.il	Tehila - Perl LWP with fake user agent	1
37.142.177.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.54.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.53.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.171.139	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.58.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.48.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.17.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
77.127.88.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.90.105.94	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	portscan: TCP Distributed Portscan	1
176.13.13.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.19.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.171.139	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.93.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-26-2015-12:04:05 to 10-26-2015-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.86.76.62	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6832
185.54.16.16	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3433
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1992
82.166.84.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	393
77.127.247.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	364
37.26.148.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	347
79.181.24.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	271
46.19.85.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	212
213.151.58.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
50.117.41.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
212.64.228.100	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
81.218.48.37	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	96
195.60.232.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	86
46.19.86.214	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
62.0.53.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
46.19.86.7	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
37.26.148.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
212.150.59.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
108.56.149.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
5.156.135.126	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
2.54.173.91	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	61
46.19.86.58	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
46.19.86.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
2.54.39.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
80.178.210.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
95.86.113.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
192.114.23.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
85.65.165.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.12.138.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.73	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
78.80.132.2	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.173.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	42
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
2.54.173.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	42
2.54.173.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
81.218.173.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
77.125.157.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
81.218.116.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
81.218.20.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2314
82.166.84.159	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 82.166.84.159	Block	280
81.218.48.37	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/590-he/patzar.aspx	Block	79
95.86.113.30	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	70
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
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
46.19.86.104	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	28
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/salah.stm" target="_blank	Block	28
176.13.0.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	28
80.246.136.50	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
176.13.7.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
190.14.48.80	Chile	147.237.77.74	law.idf.il	PHP Attempt	Block	28
37.8.50.112	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	28
199.15.251.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	28
184.105.247.195	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	14
82.81.251.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	14
37.26.146.216	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
199.203.53.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Unsupported Cipher)	None	14
2.54.171.178	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
213.244.119.129	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx)	Block	14
190.14.48.80	Chile	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 190.14.48.80	Block	14
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	14
212.64.228.100	Europe	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Unsupported Legacy SSL Version)	None	14
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	14
5.102.254.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
80.246.136.200	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.116.172.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
89.138.24.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl60.x in www.aka.idf.il/main/sachar/payslips.aspx	None	14
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	14
79.176.48.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
212.117.136.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	14
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
190.14.48.80	Chile	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	14
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	14
1.46.41.33	Thailand	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 1.46.41.33	None	14
79.176.64.89	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 108 cookies	Block	14
212.150.82.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	14
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
176.13.18.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	14
37.26.146.216	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	14
64.41.200.102	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 64.41.200.102 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	14