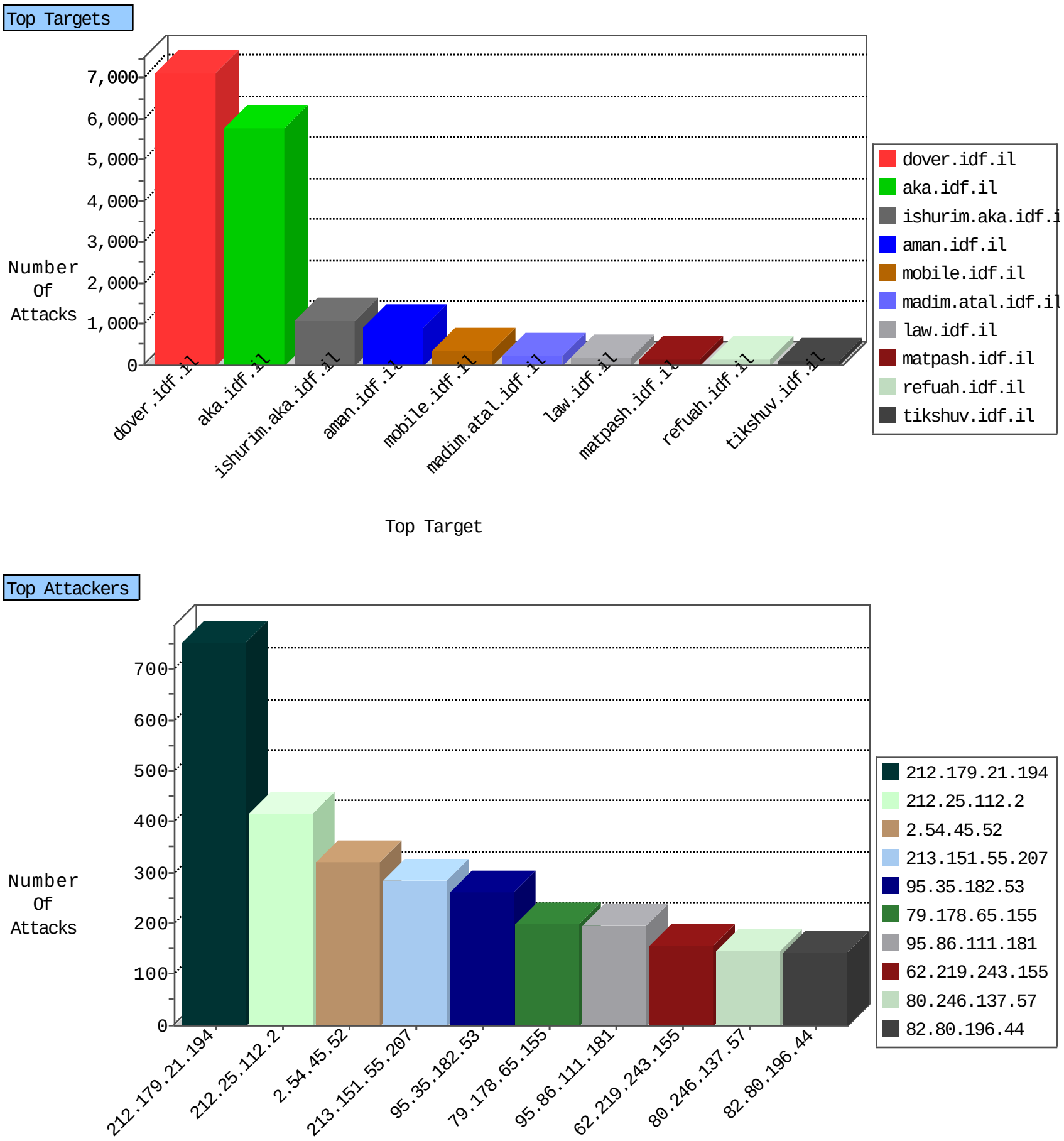
10-28-2015-10:04:04 to 10-28-2015-11:04:04

IDF Under Attack
Daily Report



10-28-2015-10:04:04 to 10-28-2015-11:04:04

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	558
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	270
213.151.35.218	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	134
46.19.85.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	54
79.180.152.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	41
82.80.144.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
176.13.14.23	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	39
95.35.182.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
176.106.226.240	Israel	147.237.72.156	aman.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	30
79.180.203.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.182.198.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	28
2.54.44.16	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	24
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
46.19.85.170	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	21
46.19.86.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
176.13.1.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
213.8.129.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
2.52.169.199	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	14
80.179.9.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
2.54.20.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.12.136.17	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
176.13.14.23	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
46.19.86.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.180.152.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
46.19.86.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
79.180.152.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
80.246.136.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
138.134.102.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
2.52.18.105	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.26.147.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
93.173.176.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
176.13.12.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.235.62.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
46.19.86.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
212.143.39.125	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
46.19.86.223	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
213.8.44.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
80.246.136.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
79.181.181.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
176.13.6.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
46.19.85.226	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
207.232.28.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
176.13.5.249	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	7
109.226.21.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
91.214.5.128	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.181.98	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
213.8.44.196	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.86.255	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
109.65.178.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5

10-28-2015-10:04:04 to 10-28-2015-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-28-2015-10:04:04 to 10-28-2015-11:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.143.39.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
169.57.5.20	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.88.198.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.146.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
107.167.112.100	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.104.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.28.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-28-2015-10:04:04 to 10-28-2015-11:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	511
212.25.112.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	414
2.54.45.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	321
213.151.55.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	286
95.35.182.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	239
79.178.65.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	167
62.219.243.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	158
80.246.137.57	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	133
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	122
107.167.112.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	89
2.54.40.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
2.54.188.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	67
37.26.146.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
79.180.208.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	66
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	66
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	64
80.179.198.10	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	62
109.226.21.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	59
212.179.159.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
80.179.16.76	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	51
37.26.147.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.85.153	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	49
79.176.64.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	46
192.115.248.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	45
157.55.39.31	United States	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	45
62.219.123.188	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	44
183.57.152.36	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
109.186.34.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	41
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	41
46.121.15.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	41
212.25.102.57	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	41
176.13.8.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	41
176.13.10.35	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	39
158.169.40.7	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	38
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	37
46.19.86.120	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	37
2.54.180.36	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	37
46.19.86.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.85.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.19.86.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
109.64.26.204	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	37
31.168.13.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	36
80.246.130.195	Israel	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	35

10-28-2015-10:04:04 to 10-28-2015-11:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
91.214.5.128	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
132.74.214.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
80.246.136.133	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	34
176.12.136.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.86.111.181	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	98
95.86.111.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	98
176.13.6.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	56
79.178.111.161	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
107.150.56.90	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 107.150.56.90	Block	28
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
80.246.139.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
87.68.163.174	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
2.52.24.91	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	28
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
87.68.163.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	28
2.54.51.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
176.13.5.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
77.125.14.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	28
77.127.233.157	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	28
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	28
149.88.129.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	24
199.203.84.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
2.54.173.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
46.19.86.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
80.246.140.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
176.13.3.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
37.26.149.194	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
37.26.147.178	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	14
79.176.43.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
85.65.60.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
185.120.126.6		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
2.54.63.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
80.246.137.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
176.12.142.125	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	14
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
79.183.101.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
109.186.156.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
31.154.91.36	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
62.219.161.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
84.95.251.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
176.228.151.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
2.54.11.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
2.52.133.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.178.180.6	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
212.235.62.94	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
2.54.186.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
46.19.86.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.8.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
2.54.153.196	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
46.19.86.120	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	14
176.12.151.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14

10-28-2015-10:04:04 to 10-28-2015-11:04:04