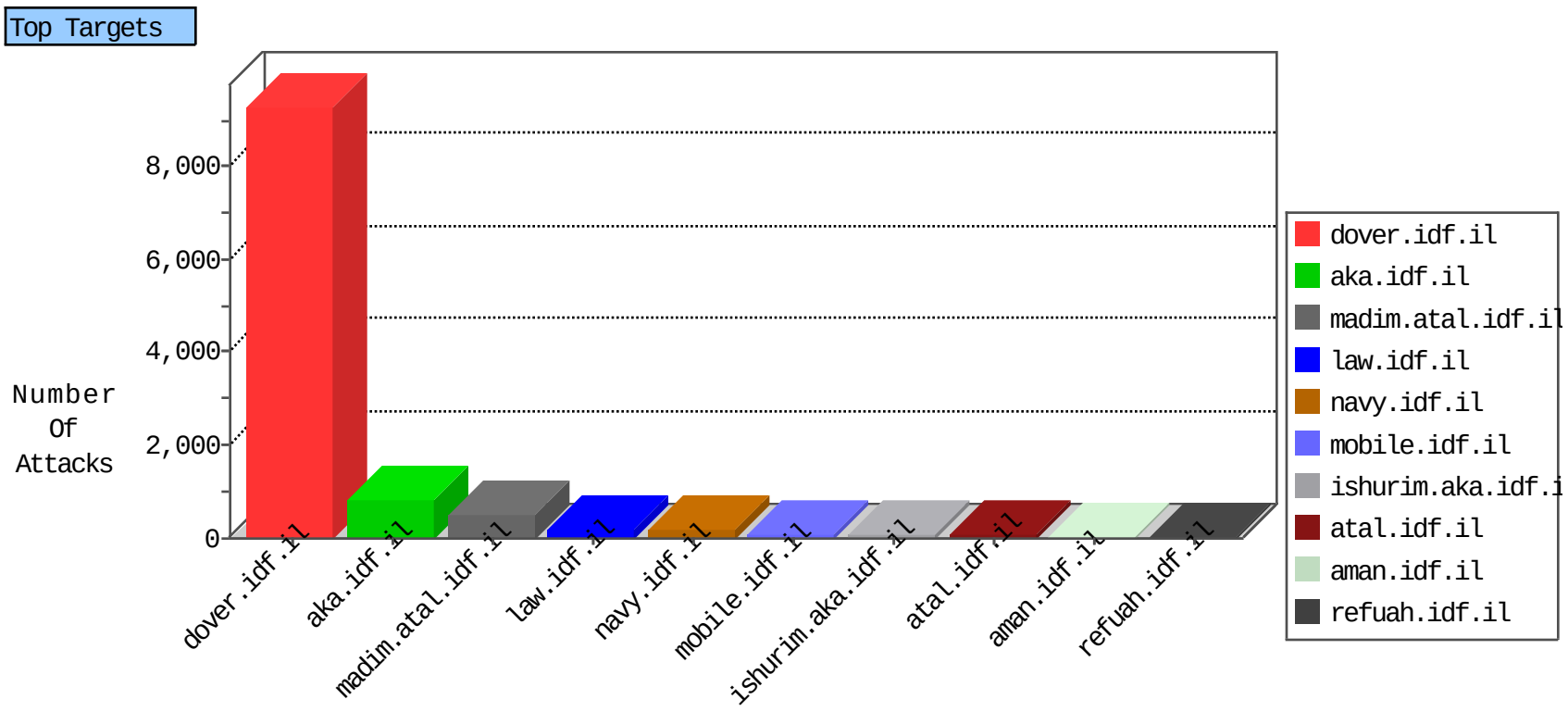
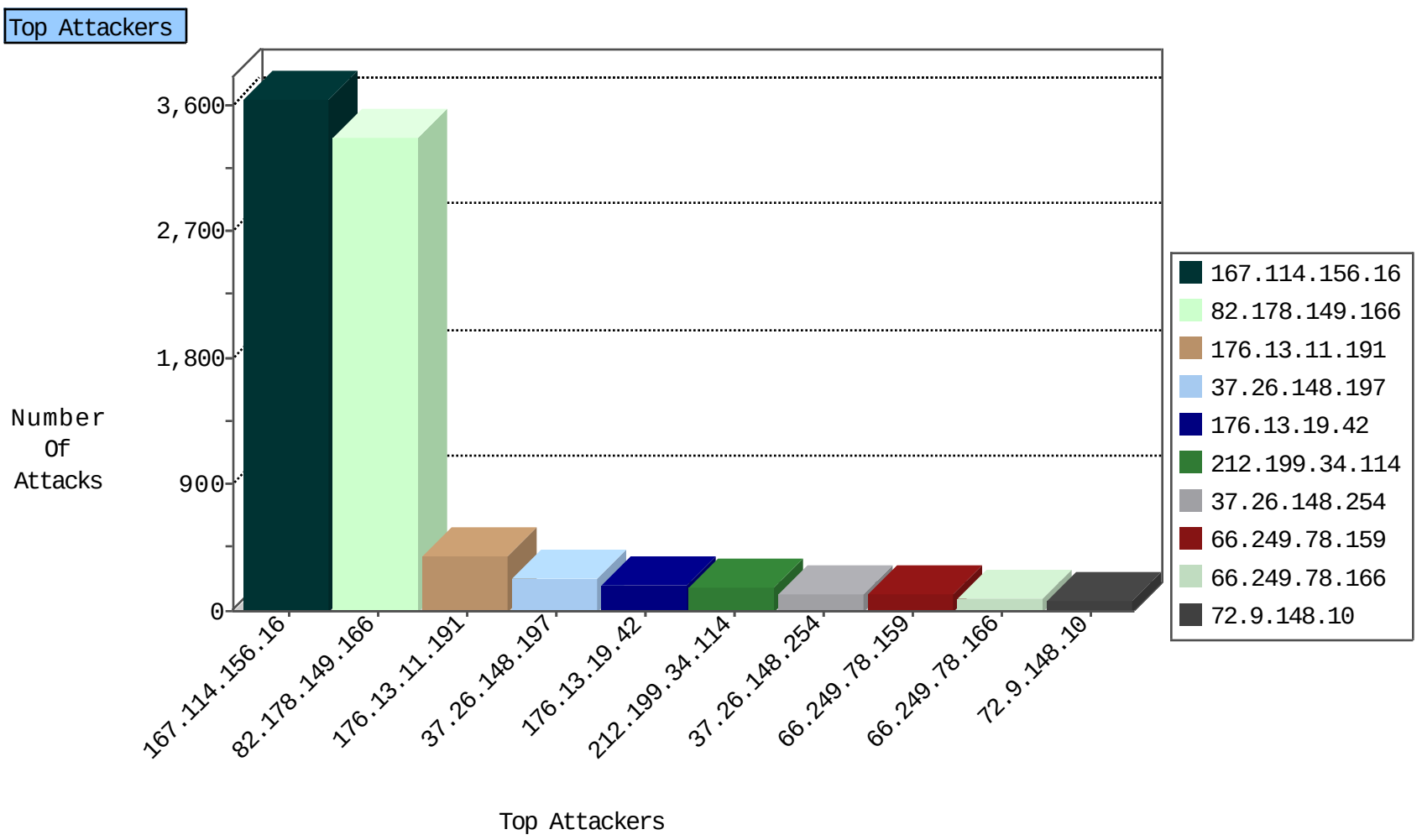
12-28-2015-14:04:04 to 12-28-2015-15:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015-14:04:04 to 12-28-2015-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.178.149.166	Oman	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	6021
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4710
167.114.156.16	Canada	147.237.77.216	dover.idf.i	DOS-Tool-SwitchbladG	dest-reset	3070
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood out of context	drop	173
37.26.148.197	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	117
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
66.249.78.159	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	78
66.249.78.166	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	72
37.26.148.254	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	71
37.26.148.197	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	67
82.145.211.80	Europe	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	45
66.249.66.31	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	43
72.9.148.10	United States	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	40
198.103.104.11	Canada	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	36
204.13.200.200	United States	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	36
66.249.93.107	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	34
83.7.81.10	Poland	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	30
66.249.78.173	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	30
37.8.111.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	29
83.137.1.204	United Kingdom	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	27
66.249.93.103	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	26
64.233.172.171	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	25
37.26.148.254	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	22
66.102.8.233	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	20
82.102.220.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	20
108.132.181.139	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	19
66.249.66.25	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	17
37.26.148.197	Israel	147.237.77.216	dover.idf.i	SYN Flood delete reset	drop	17
37.26.148.138	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	17
107.178.194.79	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	15
107.178.194.87	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	15
72.9.148.10	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	15
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	13
116.110.88.226	Vietnam	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	13
82.178.149.166	Oman	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	13
182.210.136.201	Korea, Republic of	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	12
37.26.148.138	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	12
66.249.66.28	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	11
66.249.93.99	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	11
82.178.149.166	Oman	147.237.77.216	dover.idf.i	F_Dover_Under_Attack_Con_Http	drop	10
66.249.93.99	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
66.249.81.212	Israel	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	10
202.188.229.226	Malaysia	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	9
183.80.212.68	Vietnam	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	9
107.170.91.224	United States	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	9
46.60.34.134	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	8
105.227.2.29	South Africa	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	8
198.103.104.11	Canada	147.237.77.216	dover.idf.i	SYN Flood delete reset	drop	8
141.0.14.141	Europe	147.237.77.216	dover.idf.i	SYN Flood out of context	drop	8

12-28-2015-14:04:04 to 12-28-2015-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-14:04:04 to 12-28-2015-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	1705
46.60.34.134	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
37.142.64.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
151.217.178.63	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.77.176		matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.201.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.47.229.34	147.237.76.147	France	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
177.206.240.42	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.238	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
169.50.71.180	147.237.77.233	Switzerland	atal.idf.il	ET SCAN NMAP -sS window 4096	1
151.217.178.63	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.55	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.55	147.237.0.35		akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.47.229.34	147.237.77.235	France	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.145.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.47.229.34	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.22.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.169.70.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-28-2015-14:04:04 to 12-28-2015-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1796
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop	SAM rule	drop	918
212.199.34.114	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	169
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	89
176.13.19.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	85
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop		drop	74
37.26.148.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
82.178.149.166	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
85.65.132.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
37.26.148.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
37.26.146.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.57.143.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
5.22.134.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
109.253.150.180	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
37.8.111.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
181.178.27.22	Panama	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
37.26.148.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
79.176.178.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
176.13.19.229	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
109.253.150.180	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	14
79.176.178.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
80.250.157.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
46.19.86.169	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
123.30.135.76	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.172.249.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
37.26.148.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
2.54.31.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.95.215.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
116.111.40.250	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.148.244	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
105.227.2.29	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.159.217	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

12-28-2015-14:04:04 to 12-28-2015-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.11.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	156
176.13.11.191	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.11.191	Block	140
176.13.11.191	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	89
176.13.1.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
77.126.148.45	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.148.45	Block	7
207.46.13.19	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	4
212.199.251.235	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
212.199.251.235	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.199.251.235	Block	3
37.142.206.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.199.99.36	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
40.77.167.25	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.149.150	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
37.142.64.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	3
207.46.13.4	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.4	Block	3
79.181.61.156	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
192.114.91.246	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
176.13.0.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.141.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.62.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.2.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
176.12.141.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.109	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.37.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.174.152	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
207.46.13.134	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.13.12.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
2.54.31.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.228.175.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.186.200	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.195	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/Ã—â€™Ã—â„¢Ã—Å“ Ã—â„¢Ã—â€¢Ã—Â Ã—â€¢Ã—ª	Block	1
2.54.134.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
196.22.142.59	South Africa	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvs=56812c53e8680ba9000; _pk_id.20.8afc=76c78fbb0e4f0f6a.1439828187.5.1443114444.1443114444.; _pk_ref.20.8afc=%5B%22%22%2C%22%22%2C1443114444%2C%22https%3A%2F%2Fwww.google.com%2F%22%5D; ASP.NET_SessionId=dg133h45wp45ry45fv1jhf45	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
213.57.166.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
2.52.182.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.157.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.11.191	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
66.249.66.22	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.141.173	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.149.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.230.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

12-28-2015-14:04:04 to 12-28-2015-15:04:04