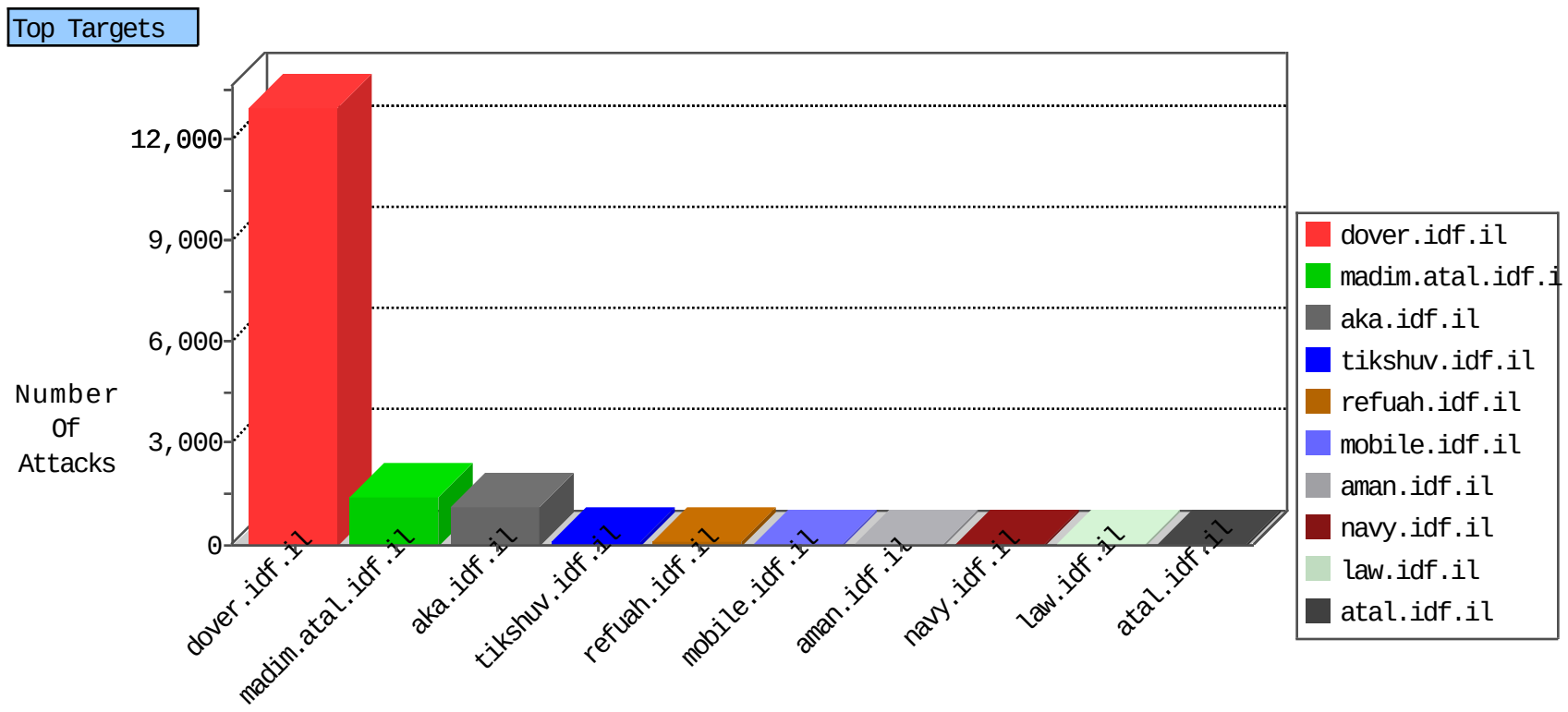
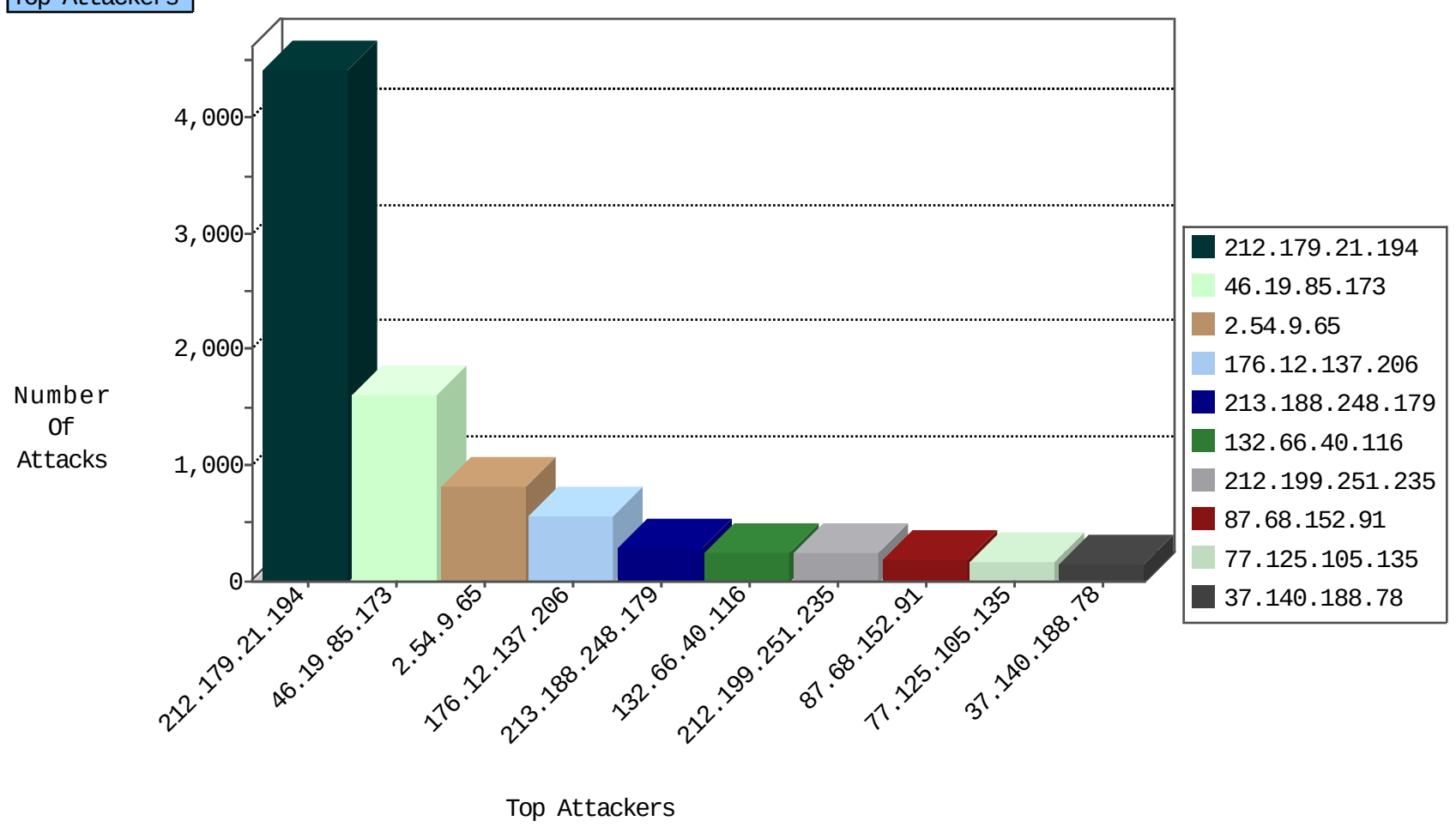
10-20-2015-17:04:01 to 10-20-2015-18:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-20-2015-17:04:01 to 10-20-2015-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.235.236.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	367
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	217
46.19.86.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
5.102.195.150	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
31.168.173.37	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	27
84.110.145.188	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
79.178.16.25	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
87.69.170.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
89.139.2.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
213.57.105.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
176.12.139.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
31.154.160.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
77.125.105.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.183.121.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
84.111.61.128	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
189.229.77.10	Mexico	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
81.218.67.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
132.66.40.116	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
74.56.165.49	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.179.48.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.91.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.173.36.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.22.130.49	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.228.131.141	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.150.249.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.172.146.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.22.130.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
217.72.121.65	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.43.77.209	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
132.66.40.116	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.111.61.128	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
93.172.162.27	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.136.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.77.185.183	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
207.232.40.193	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.52.162.247	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.146.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.142.110.3	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
77.127.109.42	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
198.154.61.16	United States	147.237.76.34	yohalan.idf.i	Block_Ntp_All_Net	drop	1
93.174.93.146	Netherlands	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
87.128.44.73	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
82.166.22.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.178.124.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
37.26.146.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.185.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.85.224	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.108.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.178.124.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-20-2015-17:04:01 to 10-20-2015-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-17:04:01 to 10-20-2015-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.241.220.201	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.199	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.1.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.210.129.188	147.237.0.33	France	idf.il	ET SCAN NMAP -sS window 4096	1
89.248.160.196	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.220.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.31.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
8.37.227.26	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.161.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.46.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.168.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.52.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.241.220.201	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.40	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
58.177.42.42	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
165.228.233.142	147.237.76.199	Australia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
52.16.5.197	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.23.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.76.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.45.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.159.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.160.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.40.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.135.239	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.241.220.201	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
72.167.232.160	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

10-20-2015-17:04:01 to 10-20-2015-18:04:01

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	4426
46.19.85.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1617
213.188.248.179	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	280
132.66.40.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	245
87.68.152.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	194
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
37.60.41.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	149
131.137.245.209	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
41.105.241.210	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
5.22.130.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
109.67.148.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
79.182.216.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
37.142.242.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
144.76.235.107	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
109.65.209.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
79.77.185.183	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
131.137.245.206	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
2.54.32.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
176.12.145.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
46.19.86.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
131.137.245.208	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
109.65.178.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
77.125.105.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
46.19.85.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
84.95.84.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
91.199.69.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
79.176.12.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.52.162.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.85.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
5.102.195.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
100.100.39.115		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	45
37.26.146.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
5.29.136.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
109.66.31.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
84.111.61.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.248.204.175	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.76.111.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
37.26.146.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
5.22.129.194	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
79.178.55.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33

10-20-2015-17:04:01 to 10-20-2015-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.9.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	828
176.12.137.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	559
212.199.251.235	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	221
77.125.105.135	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	104
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	78
85.250.94.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	52
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	52
2.54.28.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	39
133.130.49.166	Japan	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
77.127.198.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	26
79.180.31.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	13
2.52.164.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	13
212.76.103.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/25459.ppt&sa=u&ved=0ca8qfjadahukewigsowynthiahxigz4khbzsbyu&sig2=qnohapjho_p0vjziiz6vwq&usg=afqjcnhw6mmn2bmtokzzleq-wb_k43txqw	Block	13
149.88.54.29	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	13
46.19.85.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
2.54.176.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
85.65.136.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
185.82.201.17		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php/admin	Block	13
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version __atssc=facebook%3B1	Block	13
109.67.28.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	13
79.183.199.17	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	13
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	13
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	13
5.22.129.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	13
77.127.67.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	13
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	13
109.160.134.81	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	13
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvs=562656512b768b26000;	Block	13
79.183.199.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.93.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyu	Block	13
176.12.147.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
46.117.132.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
5.28.138.155	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	13
93.173.241.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	13
77.127.198.28	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method _atuvc=1%7C42; in URL __atuvs=562656512b768b26000	Block	13
81.218.87.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
2.54.32.126	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	13
176.13.12.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.120.43.102	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	13
37.26.146.229	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	13
94.230.86.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
202.102.99.72	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/sa_swfobject.js	Block	13
149.78.164.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13

10-20-2015-17:04:01 to 10-20-2015-18:04:01