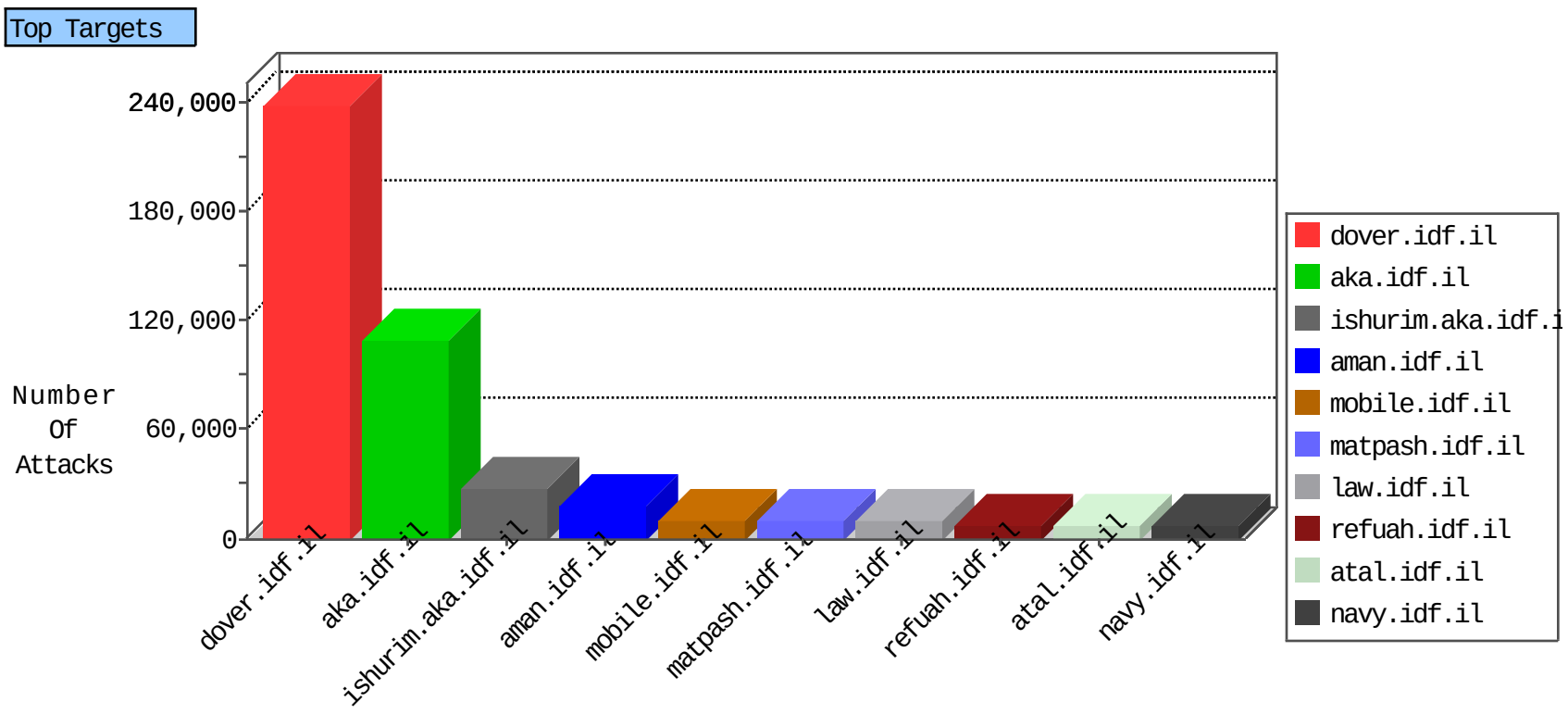
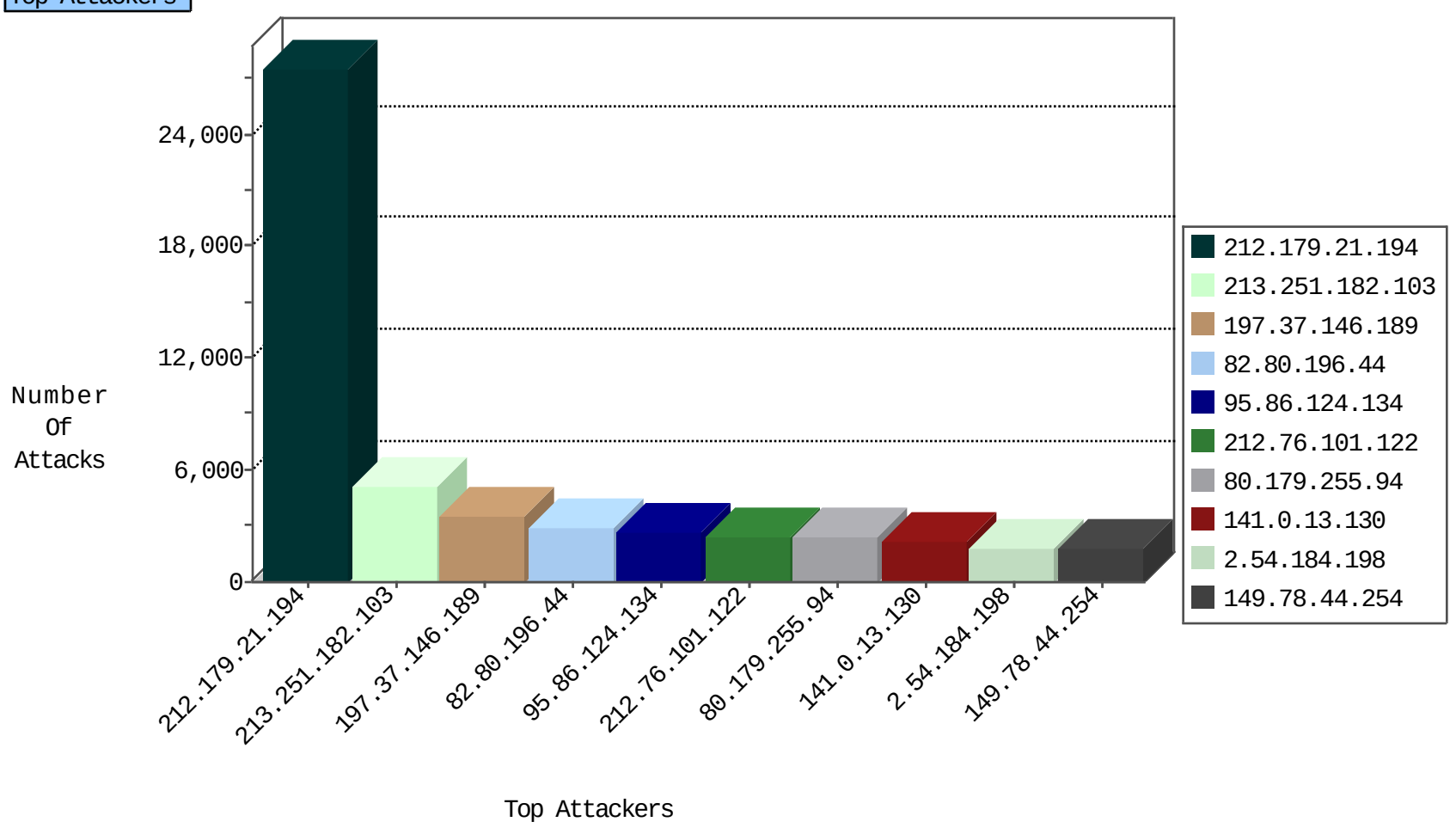
10-28-2015 to 10-29-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-28-2015 to 10-29-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	TCP handshake violation, first packet not syn	drop	771316
68.180.228.49	United States	147.237.76.30	himush.idf.il	TCP handshake violation, first packet not syn	drop	178147
77.235.133.57	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	146658
66.249.93.203	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	69809
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	65055
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37105
66.249.64.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34960
106.79.130.100	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34139
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	30199
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	29776
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	29498
37.105.195.79	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14788
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	14373
66.249.69.69	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	11106
66.249.64.153	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	9860
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	8885
82.145.210.64	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6974
66.249.67.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6883
89.138.228.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6097
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6045
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5902
66.249.67.202	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5755
66.249.64.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5618
66.249.64.159	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	5436
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	5264
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	4916
2.89.113.46	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4900
66.249.78.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4739
5.141.12.212	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4726
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4698
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4206
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4129
65.29.36.51	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3728
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3724
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3479
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3474
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3417
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3271
199.203.53.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2961
66.249.64.236	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2936
66.249.64.161	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2516
109.110.121.24	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2495
66.249.64.156	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2366
41.29.77.248	South Africa	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2285
145.83.2.6	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2180
66.249.78.204	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1984
66.249.93.207	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1897
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1845
66.249.64.151	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1590
37.139.52.36	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1573

10-28-2015 to 10-29-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.184.106	United States	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	33
5.249.138.60	Italy	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	30
87.106.15.191	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	27
151.236.50.27	United Kingdom	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	27
138.134.192.10	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
188.165.246.177	France	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	22
212.227.89.212	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	21
113.52.133.86	Hong Kong	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	21
23.91.70.77	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	18
94.231.110.223	Denmark	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	18
212.114.110.141	Netherlands	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	16
81.169.186.84	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	15
46.22.131.43	Ireland	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	15
92.39.241.111	France	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	15
37.128.146.58	Netherlands	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	15
85.214.142.233	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	14
85.214.136.8	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	14
82.165.39.81	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
217.160.93.86	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
74.208.199.191	United States	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
85.214.109.173	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
94.102.153.186	United Kingdom	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
162.244.66.58	United States	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
130.193.82.202	United Kingdom	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	12
149.202.52.100	Germany	147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	11
81.169.224.5	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	10
81.169.172.208	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	10
95.110.188.8	Italy	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
91.142.210.18	Spain	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
209.95.43.10	United States	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
85.214.213.91	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
81.169.159.137	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
87.106.109.190	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
85.214.129.80	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
144.76.67.145	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
82.98.156.47	Spain	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	9
85.214.141.253	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
93.104.211.56	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
87.106.109.57	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
85.214.128.88	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
5.249.140.179	Italy	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
85.214.55.57	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	8
192.116.239.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
85.214.103.41	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	6
95.110.185.153	Italy	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	6
87.106.216.158	Germany	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	6
80.80.231.10	Switzerland	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	6
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
74.208.205.59	United States	147.237.77.216	dover.idf.il	4684: IP: IPv6 Tunneling Over IPv4	Block	6

10-28-2015 to 10-29-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	67
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	55
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	27
188.165.246.177	147.237.77.74	France	law.idf.il	SQL Injection - Select From	24
66.135.63.82	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
2.54.7.136	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
93.89.16.110	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	5
176.98.69.225	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP backup access	5
66.249.78.173	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
185.58.201.28	147.237.77.233	Lebanon	atal.idf.il	ET SCAN NMAP -sA (2)	3
46.19.85.127	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
198.255.151.117	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
79.180.193.73	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
66.249.81.218	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
37.19.119.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
185.58.201.28	147.237.76.42	Lebanon	refuah.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	2
66.249.67.216	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.66.128.217	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
169.57.5.20	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
77.235.133.57	147.237.77.216	Lebanon	dover.idf.il	portscan: TCP Distributed Portscan	2
176.13.23.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.76.202	Italy	e.halag.idf.il	ET SCAN NMAP -f -sS	1
37.142.68.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.154.229.204	147.237.77.216	United Kingdom	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
219.91.186.104	147.237.76.86	India	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.52.143.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.166.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.248.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.126.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.53.247.3	147.237.77.216	Macau	dover.idf.il	ET SCAN Potential SSH Scan	1
46.120.104.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.116.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.146.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.245.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.228.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.16.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.201.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.210	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
149.202.52.100	147.237.76.31	Germany	nakchal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.19.85.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.161.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-28-2015 to 10-29-2015

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	25423
197.37.146.189	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2992
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2425
213.251.182.103	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2380
80.179.255.94	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	2153
141.0.13.130	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2127
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	1947
2.54.184.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1819
149.78.44.254	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1785
212.25.102.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1755
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1614
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	1574
91.193.51.174	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1556
79.176.160.189	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1422
195.226.71.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1381
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1353
176.12.142.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1319
105.156.37.33	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1273
46.19.85.1	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	1168
46.19.85.127	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	1080
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1045
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	1007
5.28.139.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	959
46.19.85.123	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	854
149.78.235.34	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	735
52.16.5.197	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	726
85.64.66.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	680
2.52.179.39	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	680
2.54.12.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	665
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	661
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	654
209.88.198.1	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	647
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	646
46.19.85.84	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	643
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	632
5.22.129.216	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	629
72.11.211.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	616
68.180.228.59	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	606
79.181.119.151	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	576
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	568
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	564
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	562
207.46.13.58	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	531
2.54.165.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	530

10-28-2015 to 10-29-2015

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
31.154.19.5	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	529
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	529
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	525
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	524
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	524
37.26.146.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	521

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2730
95.86.124.134	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 95.86.124.134	Block	2590
213.151.52.202	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.52.202	Block	1106
149.78.85.39	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	630
85.65.13.4	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.13.4	Block	480
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	308
105.156.37.33	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.156.37.33	Block	272
176.12.145.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	255
87.68.241.254	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	240
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	229
79.176.35.28	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	225
79.176.35.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	225
77.125.136.36	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.136.36	Block	210
31.154.145.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.145.153	Block	195
109.65.194.97	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	180
95.86.111.181	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	168
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	168
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	165
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	158
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	155
176.12.145.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	150
79.178.175.207	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	150
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	150
79.178.175.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	150
84.108.37.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	140
84.108.37.223	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	138
172.56.37.84	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	135
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	135
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	135
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	129
176.13.1.24	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	126
5.29.193.157	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	126
5.29.193.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	126
107.6.154.229	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 107.6.154.229	Block	120
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	118
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	116
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	115
5.22.129.253	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	113
5.22.129.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	113
79.178.111.161	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	112
79.178.133.75	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	112
79.178.133.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	112
82.102.170.200	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	105
213.151.57.156	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.57.156	Block	105
79.182.196.134	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	105
2.54.48.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	105
82.102.170.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	105
79.182.196.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	105
2.52.27.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	105
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	104