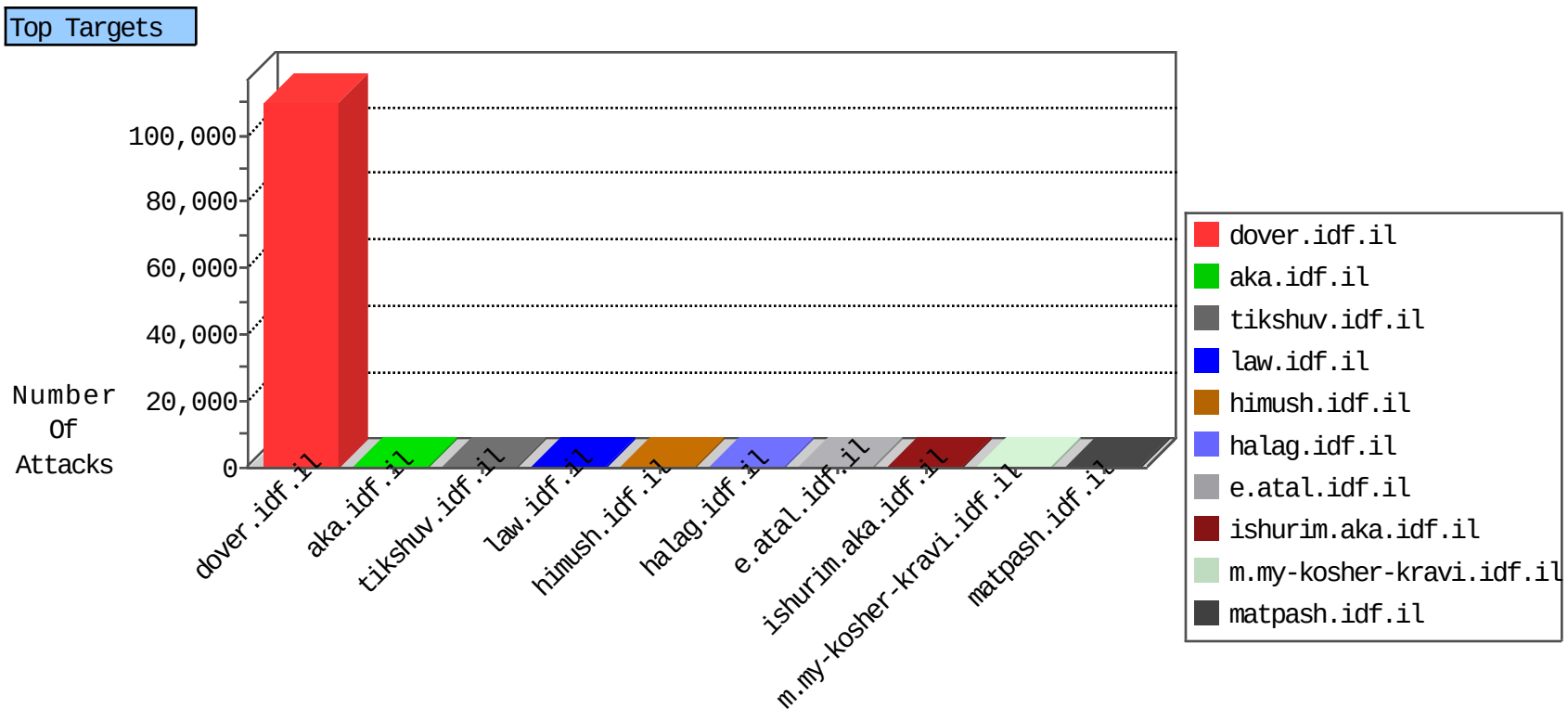
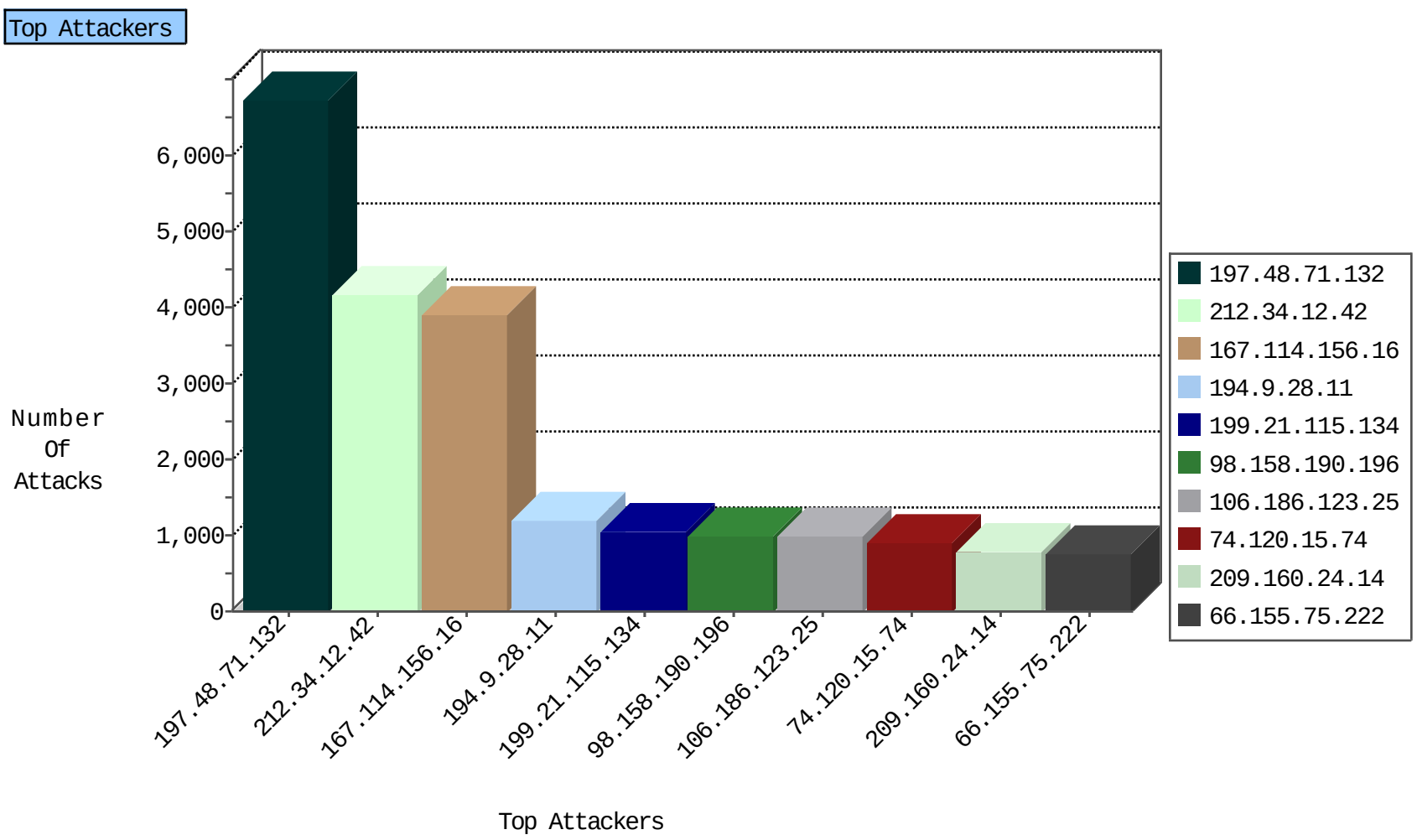
04-08-2016-02:04:00 to 04-08-2016-03:04:00

IDF Under Attack Daily Report





04-08-2016-02:04:00 to 04-08-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.60.147.79	Switzerland	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	80466
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	11116
188.55.204.168	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5171
130.211.134.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4579
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3879
52.23.215.54	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2944
199.47.125.84	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2158
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2097
106.186.115.90	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2002
66.249.65.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1968
89.238.166.133	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1362
87.69.195.171	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1145
172.56.13.206	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1106
54.94.252.114	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1010
213.229.73.244	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	934
176.2.134.161	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	766
89.238.166.133	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	612
104.197.101.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	568
156.205.17.252	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	545
108.59.83.170	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	520
191.239.6.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	499
191.239.218.221	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	330
128.199.144.177	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	153
52.17.98.103	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	137
54.76.190.11	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
52.32.129.70	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	62
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	48
52.29.55.227	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	41
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	27
54.148.48.125	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24
52.76.122.5	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
46.101.7.191	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
54.179.4.123	Singapore	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
195.225.219.240	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
104.197.93.224	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
52.33.138.105	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
54.198.167.222	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
40.127.166.75	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
74.91.20.198	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	2
107.150.46.38	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
52.25.116.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
80.57.15.17	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
107.150.32.60	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
52.23.163.75	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
146.148.86.248	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
74.91.18.44	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
107.150.32.60	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	2
74.91.20.197	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	forward	2

04-08-2016-02:04:00 to 04-08-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
130.193.243.48	Iraq	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-08-2016-02:04:00 to 04-08-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.191.64.166	147.237.77.216	India	dover.idf.il	ET WEB_SERVER UA WordPress, probable DDOS-Attack	144
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.232.98.3	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
202.85.221.63	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.179.135	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.63.7.151	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.144.177	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.114.157.12	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.7.151	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
128.199.114.26	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.80.70.219	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.83.109	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.3.202.115	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
128.199.67.254	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.3.202.115	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
119.93.147.111	147.237.0.34	Philippines	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.37	147.237.76.39	Switzerland	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
110.143.44.114	147.237.0.35	Australia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
209.148.94.140	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.199.238.240	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.232.98.3	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
202.174.92.238	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.195.155	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
202.85.221.63	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -f -sS	1
128.199.145.23	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.114.157.12	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
45.63.7.151	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.129.191	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.80.70.219	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 3072	1
128.199.86.239	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.80.70.219	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -f -sS	1
128.199.76.58	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.3.202.115	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
128.199.65.246	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.3.202.115	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
115.28.247.220	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.247.177	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
107.6.130.113	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
128.199.222.66	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

04-08-2016-02:04:00 to 04-08-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3387
197.48.71.132	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2646
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2067
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1565
194.9.28.11	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1180
199.21.115.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1041
98.158.190.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	992
106.186.123.25	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	988
74.120.15.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	889
209.160.24.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	774
151.236.48.204	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	758
66.155.75.222	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	756
23.236.48.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	749
23.251.156.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	731
23.97.58.45	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	698
106.187.51.76	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	696
162.212.56.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	671
130.211.158.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	661
130.211.172.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	615
146.148.35.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	602
183.82.51.188	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	597
199.223.233.140	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	573
104.197.119.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	564
146.148.119.116	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	562
104.155.83.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	557
193.107.252.143	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	547
213.171.205.177	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	541
62.249.169.200	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	521
146.148.61.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	521
108.59.83.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	518
88.208.192.244	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	513
74.120.15.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	505
106.187.93.83	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	501
104.197.1.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	486
146.148.86.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	486
130.211.133.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	486
104.196.9.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	462
212.34.12.42	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	459
88.208.238.77	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	457
80.57.15.17	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	446
107.155.108.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	435
43.252.89.111	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	428
106.187.94.248	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	423
104.197.107.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	415
64.77.72.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	401
23.94.134.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	397
104.155.27.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	395
80.98.89.250	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	394
82.223.121.70	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	390
107.167.177.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	389

04-08-2016-02:04:00 to 04-08-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
185.120.125.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
70.39.187.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22927-ar/dover.aspx.alah	Block	1
205.204.95.90	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
107.150.46.37	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.867bb.com/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/null	Block	1
74.91.18.44	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.867bb.com/	Block	1
5.8.37.203	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/story.aspx	Block	1
207.46.13.1	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
157.55.39.194	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1093-7963-he/מאיר שחמו.aspx	Block	1
74.91.20.198	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.867bb.com/	Block	1
40.77.167.69	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/general/eitan.aspx	Block	1
185.27.217.10	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
107.150.32.60	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.867bb.com/	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-08-2016-02:04:00 to 04-08-2016-03:04:00