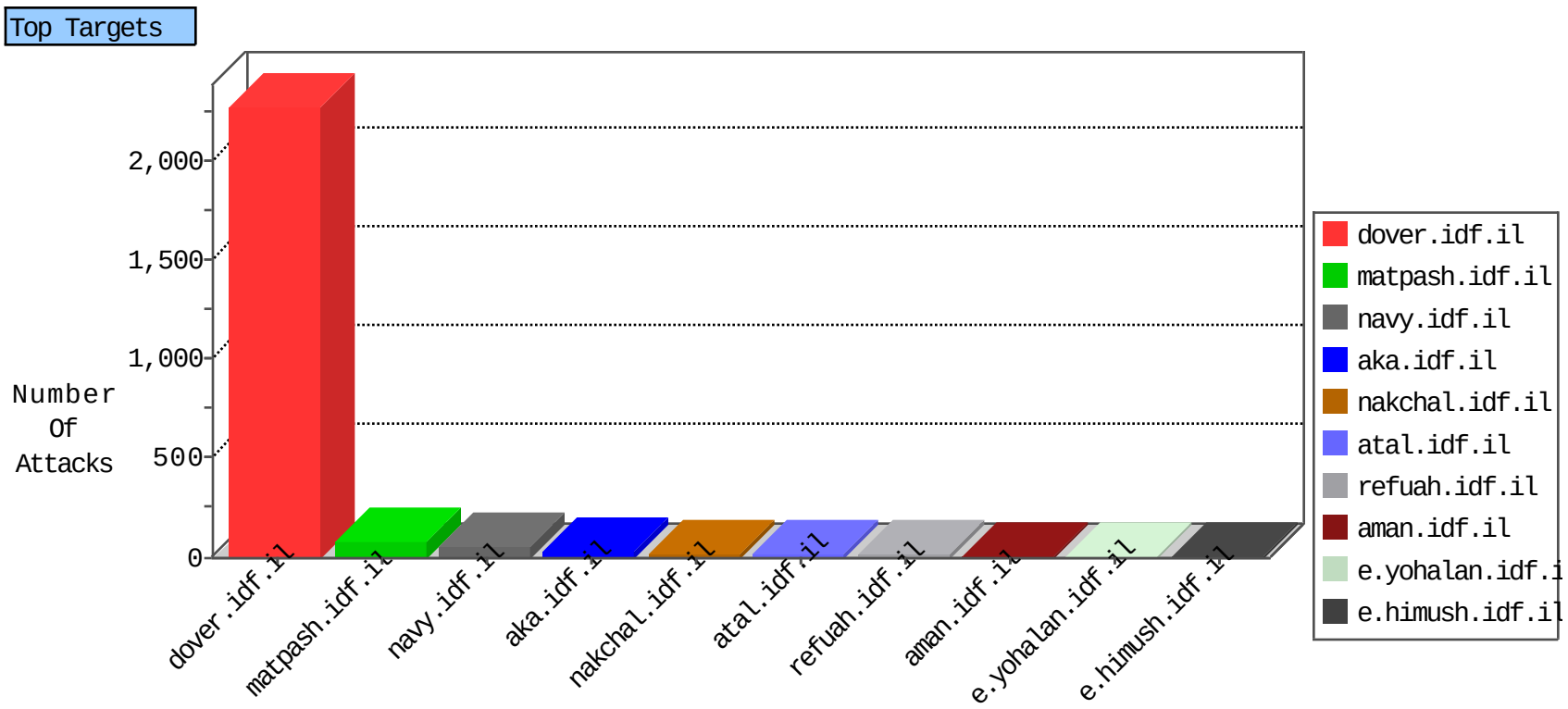
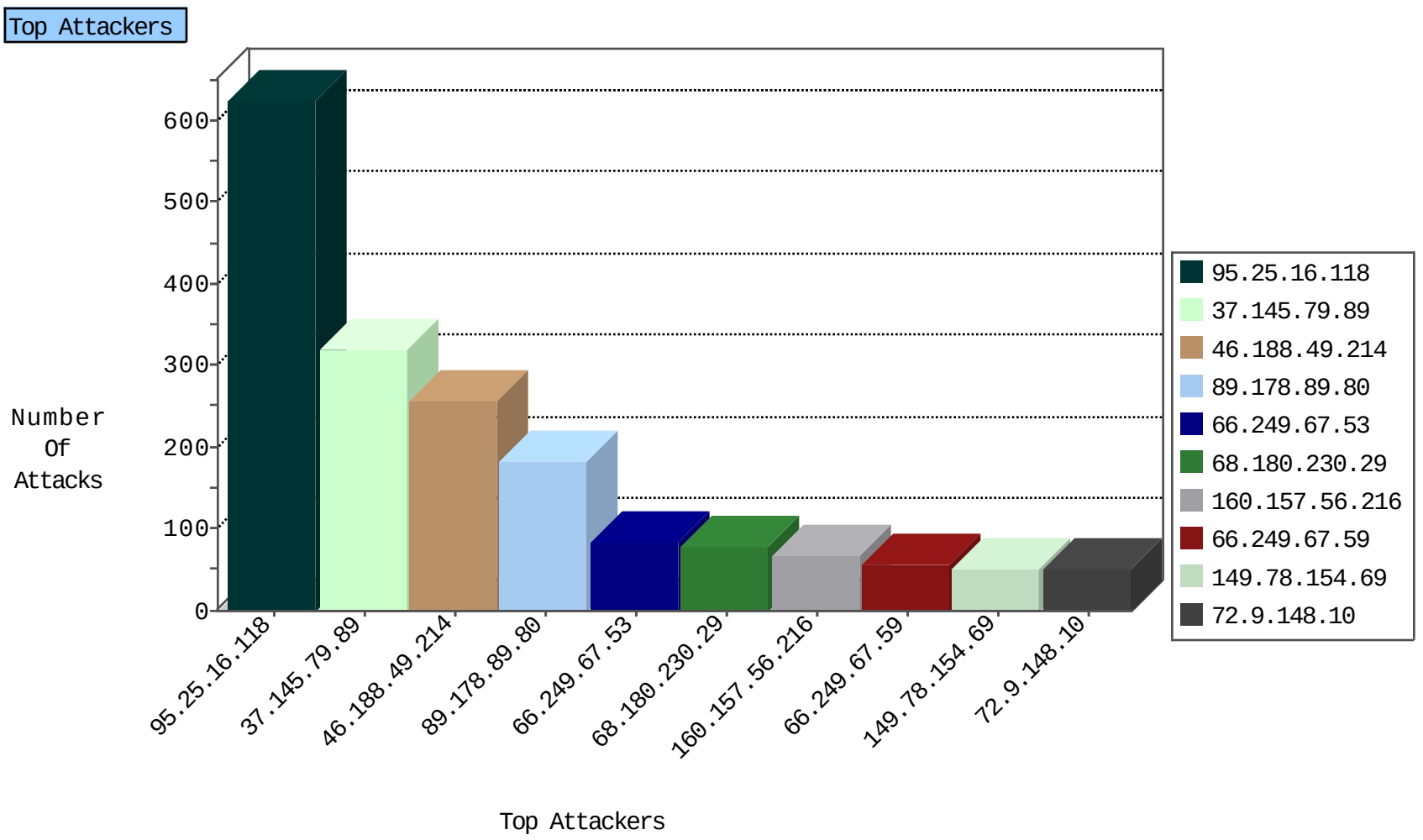
10-21-2015-03:04:02 to 10-21-2015-04:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-03:04:02 to 10-21-2015-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.7.15.115	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1403
220.181.108.150	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	11
207.46.13.178	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.174.93.146	Netherlands	147.237.76.197	e.himush.idf.il	Invalid TCP Flags	drop	1
93.174.93.146	Netherlands	147.237.77.235	sviva.idf.il	Invalid TCP Flags	drop	1
89.248.172.98	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.146	Netherlands	147.237.72.217	e.idf.il	Invalid TCP Flags	drop	1

10-21-2015-03:04:02 to 10-21-2015-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-03:04:02 to 10-21-2015-04:04:02

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	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
125.65.165.215	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.167.117.171	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
99.100.37.115	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
182.72.109.162	147.237.76.198	India	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
174.128.228.82	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.156.233.50	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
62.219.83.119	147.237.0.17	Israel	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
174.128.228.82	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1

10-21-2015-03:04:02 to 10-21-2015-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.25.16.118	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	625
37.145.79.89	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	319
46.188.49.214	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	256
89.178.89.80	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	183
160.157.56.216		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	33
66.102.8.168	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
74.108.31.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
185.12.246.126	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
216.4.56.168	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.102.8.178	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
76.224.186.219	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
219.74.36.64	Singapore	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
219.74.35.174	Singapore	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
50.29.98.99	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
157.55.39.9	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
209.133.111.211	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
172.1.148.108	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
172.91.140.213		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
74.80.213.22	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
216.4.56.142	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
186.177.77.155	Costa Rica	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
109.67.164.149	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.207.141.235	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	SAM rule	drop	6
220.255.98.151	Singapore	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop		drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
108.41.12.133	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
66.249.67.53	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
74.80.213.22	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
203.127.58.235	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
66.249.67.65	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.120.148.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
104.60.21.208	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4

10-21-2015-03:04:02 to 10-21-2015-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	78
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
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	26
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
220.181.108.159	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	13
157.55.39.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	13
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
31.193.51.78	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
182.118.70.85	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/sa_swfobject.js	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	13
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	13
183.136.142.167	China	147.237.76.31	nakchal.idf.il	URL is Above Root Directory nakhal.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
98.27.190.59	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	13
67.190.66.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	13
128.199.95.16	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/l12.tar	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13

10-21-2015-03:04:02 to 10-21-2015-04:04:02