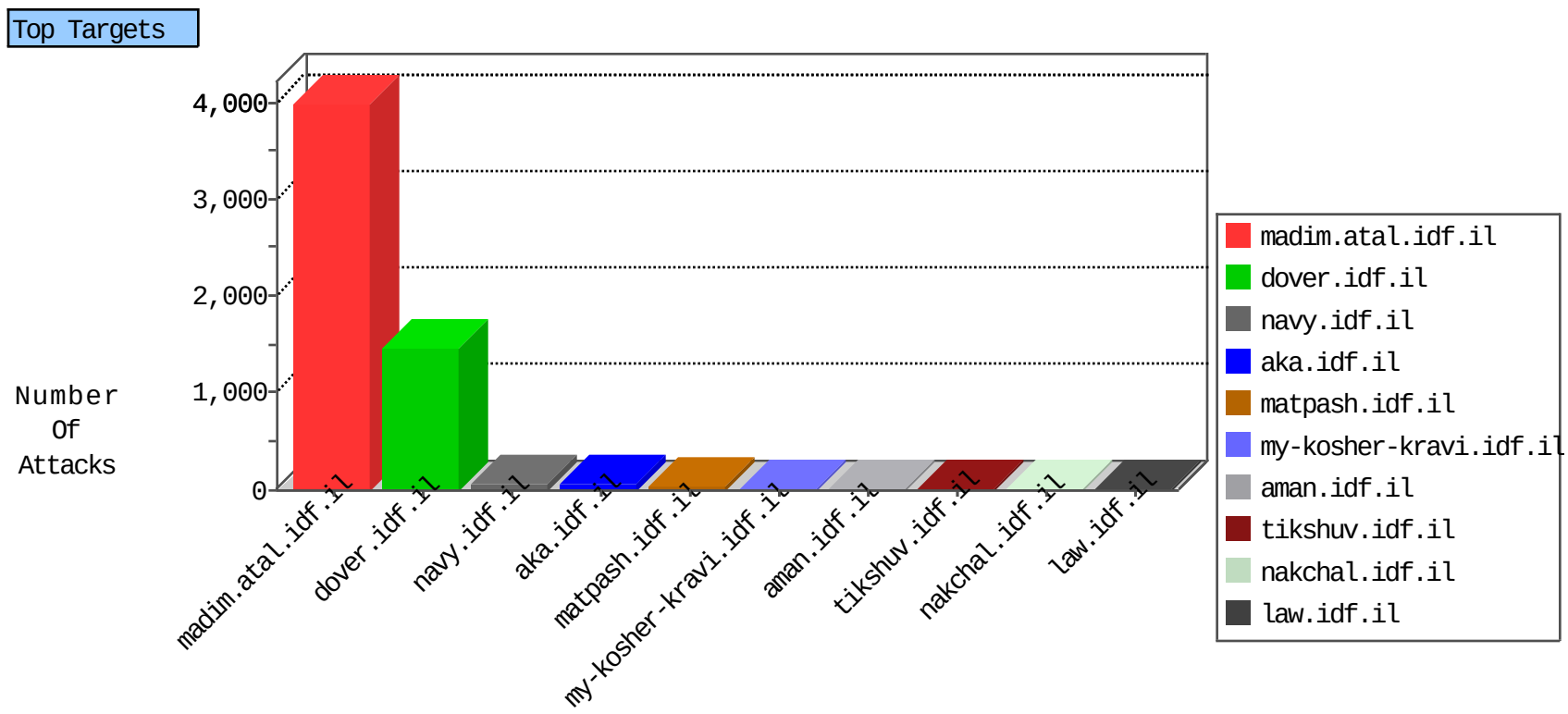
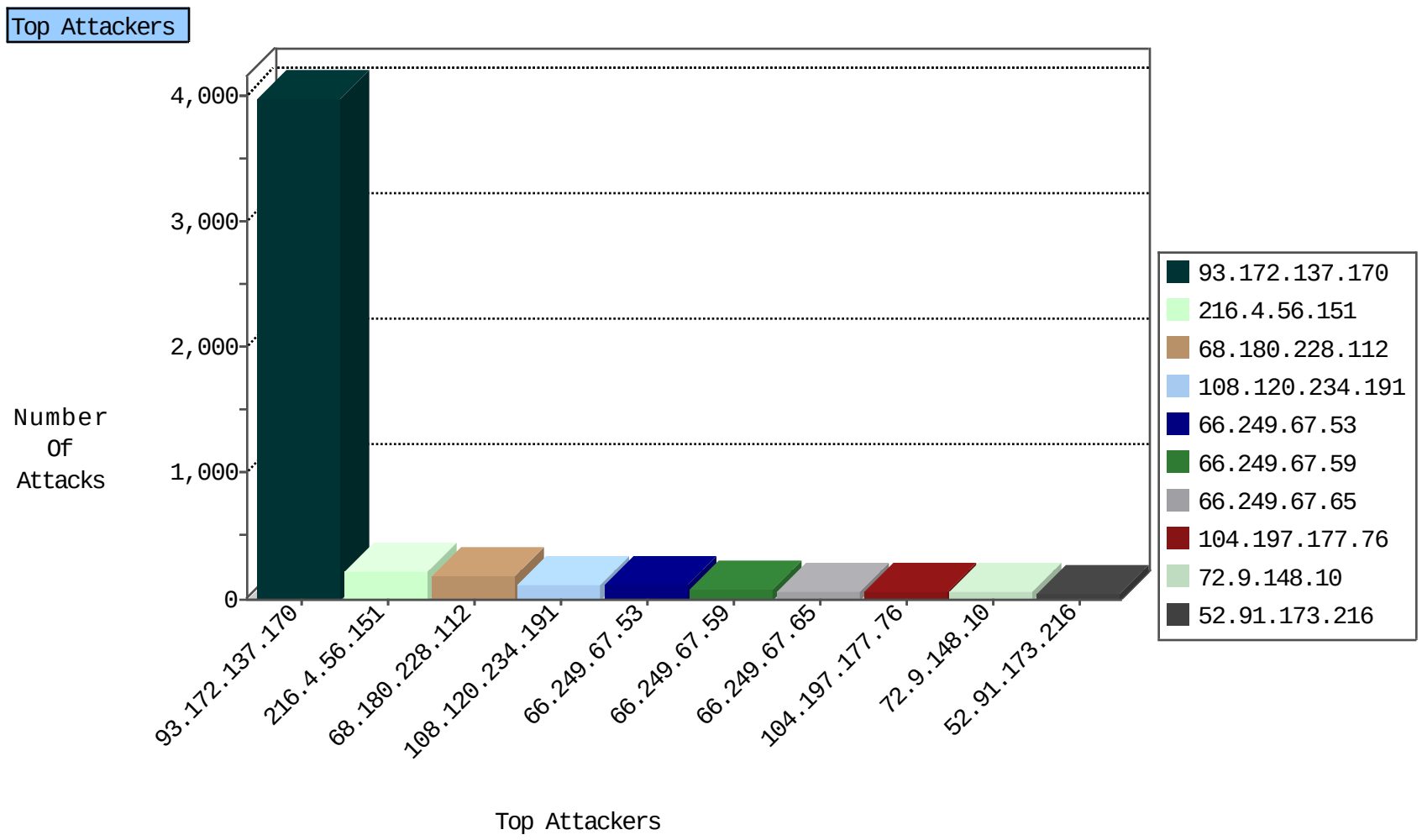
10-25-2015-04:04:07 to 10-25-2015-05:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-04:04:07 to 10-25-2015-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.108.21.16	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
5.8.201.254	Russian Federation	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1

10-25-2015-04:04:07 to 10-25-2015-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.208.224	Canada	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

10-25-2015-04:04:07 to 10-25-2015-05:04:07

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	3
82.117.208.243	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.116.221	147.237.76.38	Sweden	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.126.145	147.237.0.16	Israel	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.141.171.107	147.237.8.46	Malaysia	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.227.150.72	147.237.76.30	Sweden	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-25-2015-04:04:07 to 10-25-2015-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.4.56.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	218
108.120.234.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
176.13.2.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
96.41.214.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
93.173.0.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
79.176.145.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
52.91.173.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
109.64.29.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.241.226.144	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	17
216.81.94.76	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.38.193.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
103.3.81.13	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
98.115.120.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
194.187.168.25	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
69.171.228.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
184.173.183.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.169.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
69.171.228.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
74.101.220.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

10-25-2015-04:04:07 to 10-25-2015-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.137.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 93.172.137.170	Block	3976
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1158-he/dover.aspx	Block	84
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	70
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	70
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	56
104.197.177.76	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.197.177.76	Block	42
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	42
213.21.33.35	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/327-en/patzar.aspx	Block	14
167.114.208.224	Canada	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/topcap.gif)	Block	14
188.143.232.43	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	14
167.114.208.224	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.240.88.17	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
104.197.177.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/products	Block	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/images/shared/mailthisclose.png	Block	14
46.121.247.189	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	14
180.76.15.31	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list5.htm	Block	14
82.118.237.101	Bulgaria	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/16900.jpg	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.151.52.35	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forums/forums.asp	Block	14
184.105.139.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	14
93.172.137.170	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	14
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	14
157.55.39.134	United States	147.237.76.86	navy.idf.il	Parameter Type Violation catId in www.navy.idf.il/navy/watercrafts.aspx	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.91.173.216	Block	14
188.143.232.24	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/901-en/cogat.aspx parameter fromDate	Block	14

10-25-2015-04:04:07 to 10-25-2015-05:04:07