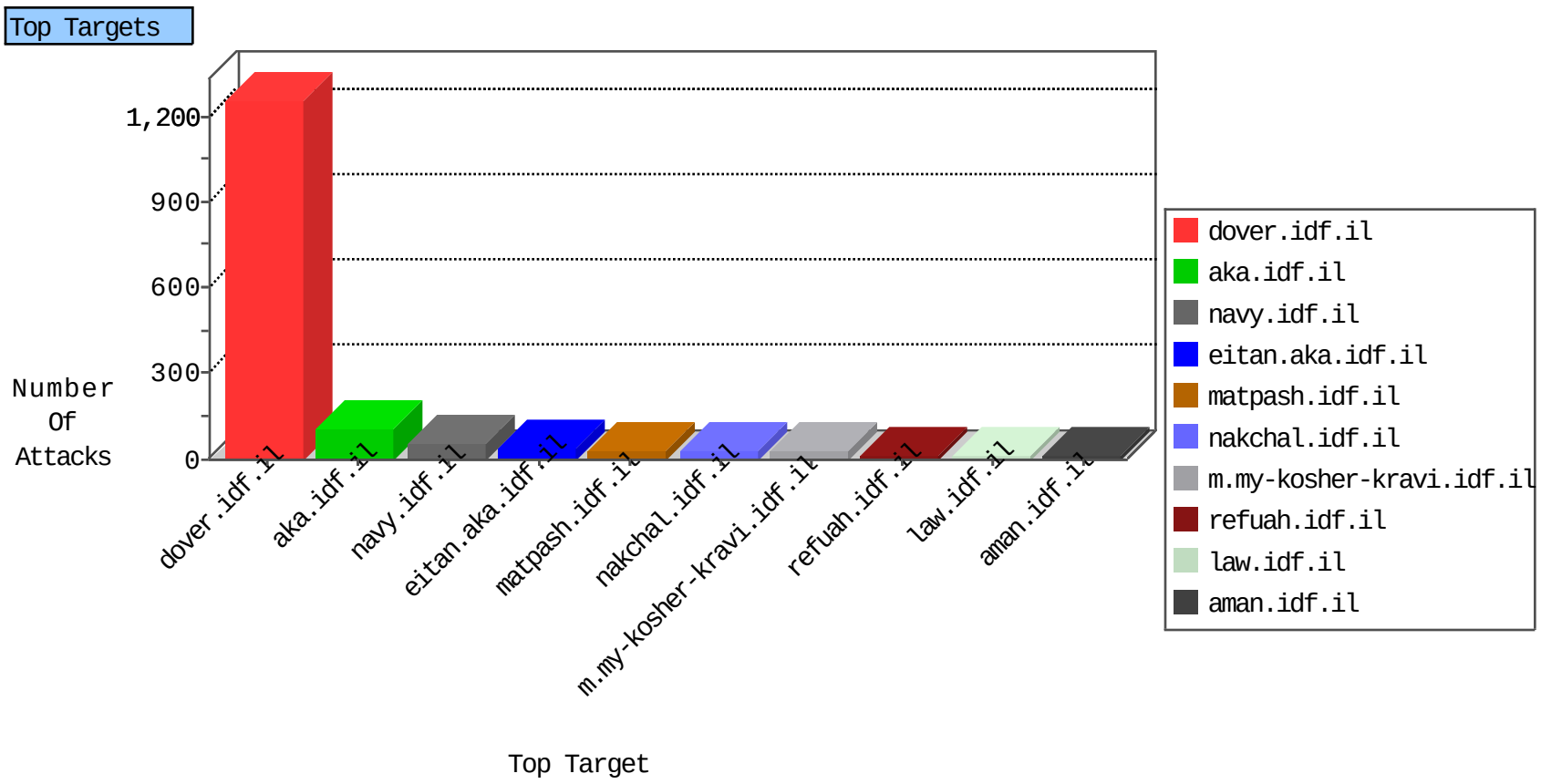
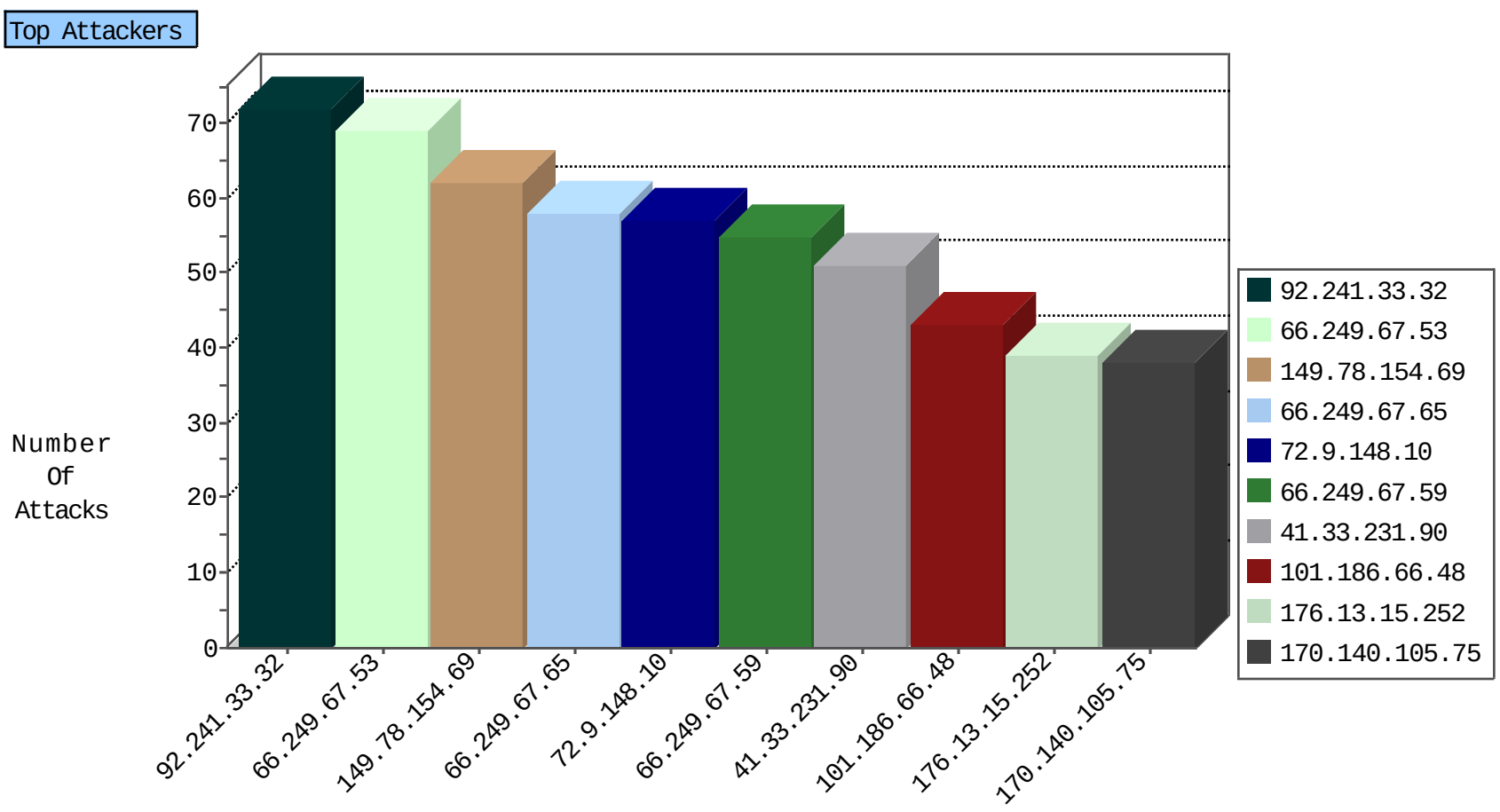
10-25-2015-05:04:01 to 10-25-2015-06:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-05:04:01 to 10-25-2015-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.88	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
83.222.109.40	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

10-25-2015-05:04:01 to 10-25-2015-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-05:04:01 to 10-25-2015-06:04:01

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
218.84.212.119	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.254.90.133	147.237.77.179	Mexico	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
182.69.122.120	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.52.8	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
189.254.90.133	147.237.77.179	Mexico	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
184.58.241.45	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
120.150.29.211	147.237.72.167	Australia	ishurim.aka.idf.i	ET SCAN NMAP -sS window 4096	1

10-25-2015-05:04:01 to 10-25-2015-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.241.33.32	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
101.186.66.48	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
176.13.15.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
37.26.147.229	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.187.157.108	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
69.119.117.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
176.12.151.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
74.101.220.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
109.66.214.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
170.140.105.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.177.134.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
108.236.165.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
69.180.120.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	18
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.182.5.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
76.89.170.130	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
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
103.3.81.13	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
208.54.83.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
101.59.193.55	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.183.181.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
82.166.22.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
207.229.151.141	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.142.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
184.58.241.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.141.37	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.29.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

10-25-2015-05:04:01 to 10-25-2015-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	56
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	42
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	28
46.121.247.189	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
170.140.105.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/	Block	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/1133-he/dover.aspx	Block	14
5.79.74.89	Netherlands	147.237.77.74	law.idf.il	Suspicious Response Code	Block	14
85.64.22.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
183.245.117.208	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	14
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding KBK(:p3eUNwrW@P]RIXdXC3/ytr	None	14
149.88.126.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 66.249.67.59	Block	14
188.143.232.43	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
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	14
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/	Block	14
5.79.74.89	Netherlands	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17418.jpg	Block	14

10-25-2015-05:04:01 to 10-25-2015-06:04:01