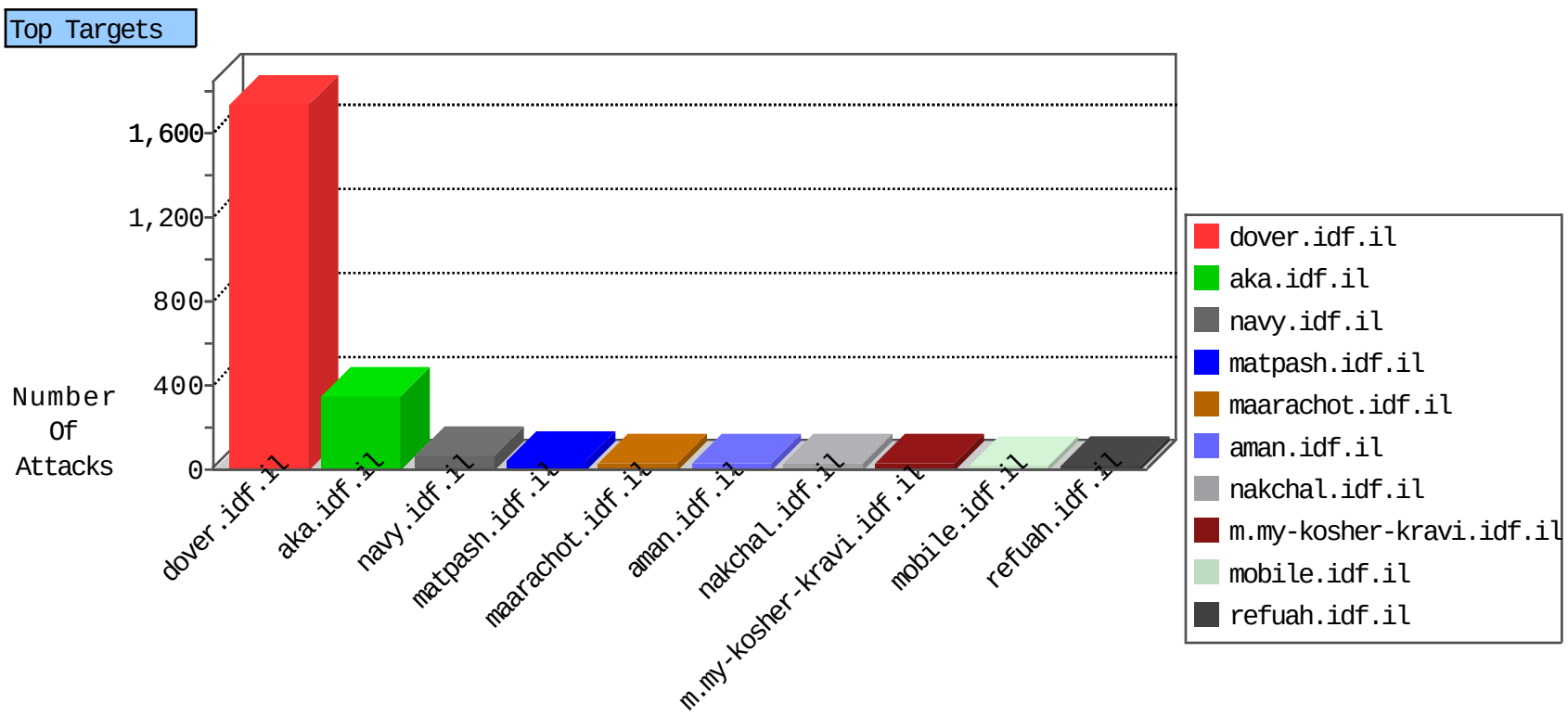
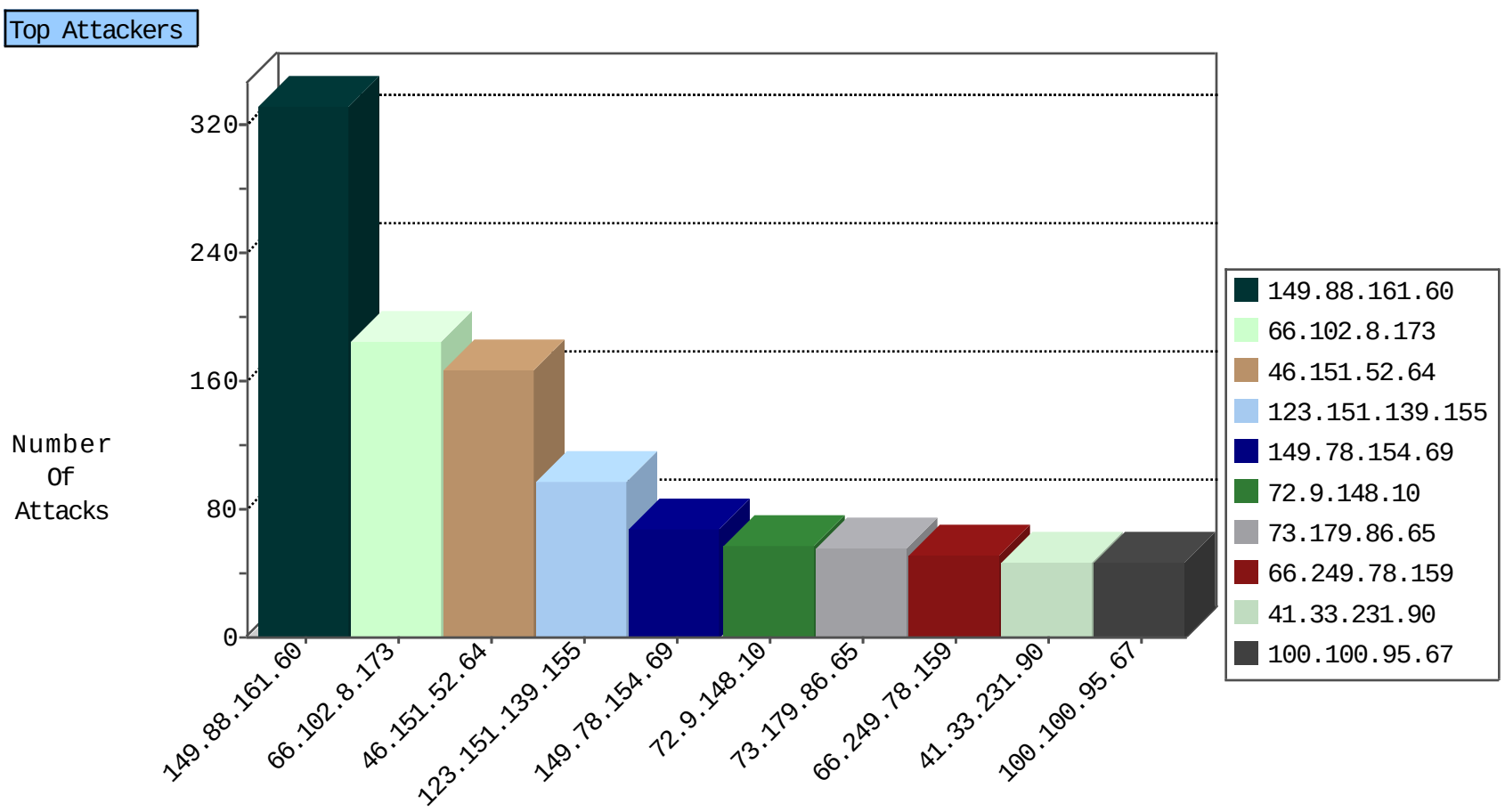
10-23-2015-05:04:04 to 10-23-2015-06:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-23-2015-05:04:04 to 10-23-2015-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.128.73.6	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	3
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	3
185.61.136.94	Ukraine	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
207.6.169.253	Canada	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

10-23-2015-05:04:04 to 10-23-2015-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-05:04:04 to 10-23-2015-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.63.55.158	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
36.72.228.72	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
218.108.132.58	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
195.68.62.253	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
182.48.105.216	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.138	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.0.35	Turkey	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
209.41.67.92	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
123.189.5.231	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.138	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
50.252.197.194	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 3072	1

10-23-2015-05:04:04 to 10-23-2015-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.88.161.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	286
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	114
123.151.139.155	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
100.100.95.67		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	47
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
154.5.172.145	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
219.74.36.138	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
75.20.145.47	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.24.155.132	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
219.74.38.242	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.10.241		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
121.7.37.167	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
220.255.193.82	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
220.255.193.82	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
186.4.197.32	Ecuador	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.255	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.11.40.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.41.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.172.184.58	Israel	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	11
100.100.10.241		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
220.255.103.48	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
81.218.48.37	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
220.255.146.30	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.233.172.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.237	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
96.41.154.239	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
111.30.132.194	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
219.74.36.138	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
219.74.38.242	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
220.255.97.210	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

10-23-2015-05:04:04 to 10-23-2015-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.151.52.64	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	84
46.151.52.64	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.151.52.64	Block	70
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
73.179.86.65	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	56
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	28
66.249.75.7	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
130.185.139.213	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
46.151.52.64	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	14
79.178.136.212	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.178.136.212	Block	14
66.249.75.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	14
5.29.62.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	14
137.116.71.170	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/robots.txt	Block	14
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
54.209.60.63	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=66a5eaaekkkkkkk_66a5eaae	Block	14
79.178.136.212	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
31.193.51.17	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1226-	Block	14
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
66.249.67.178	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
103.53.225.47		147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 103.53.225.47	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
157.55.39.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sachar	Block	14
66.249.67.193	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/robots.txt	Block	14
103.53.225.47		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/user	Block	14
176.12.145.205	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.145.205	None	13
176.12.145.205	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	13

10-23-2015-05:04:04 to 10-23-2015-06:04:04