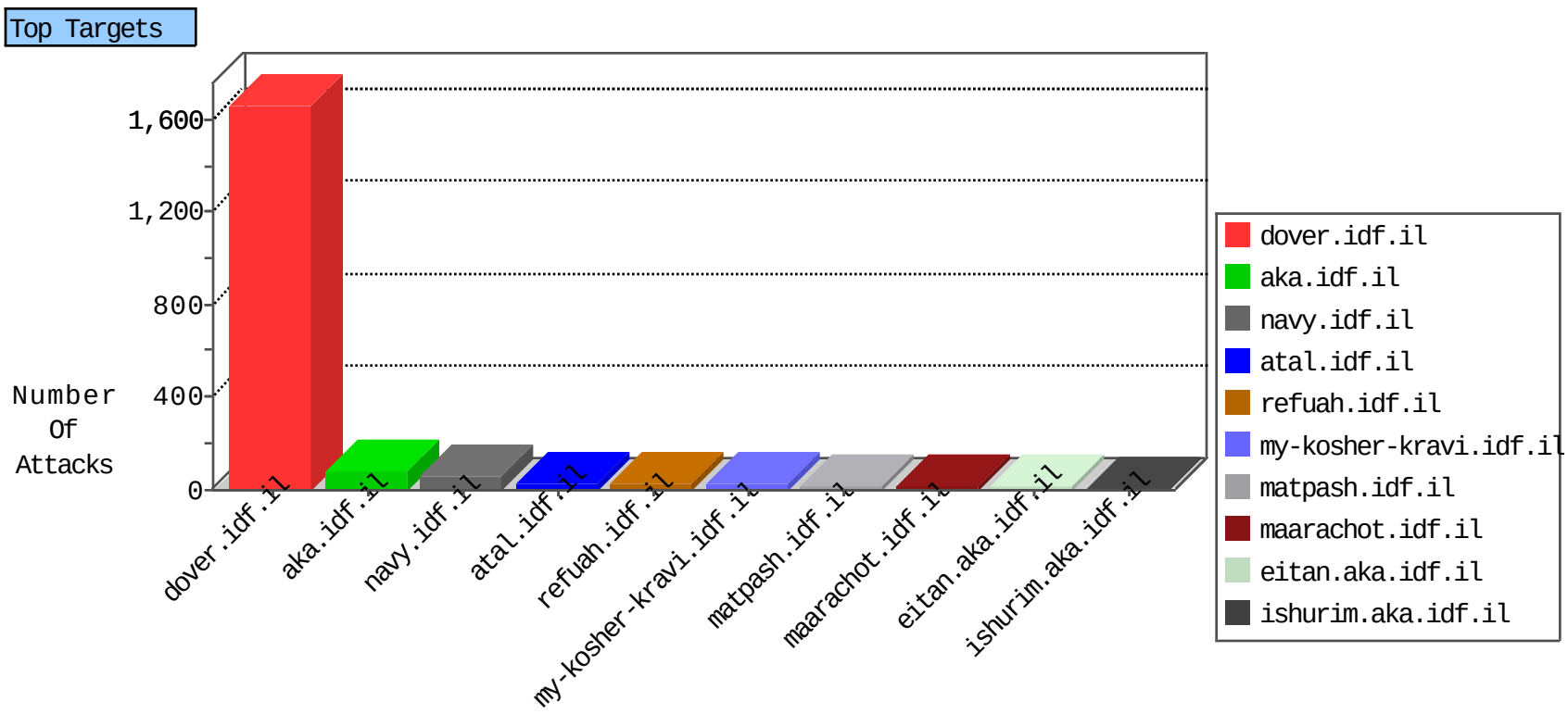
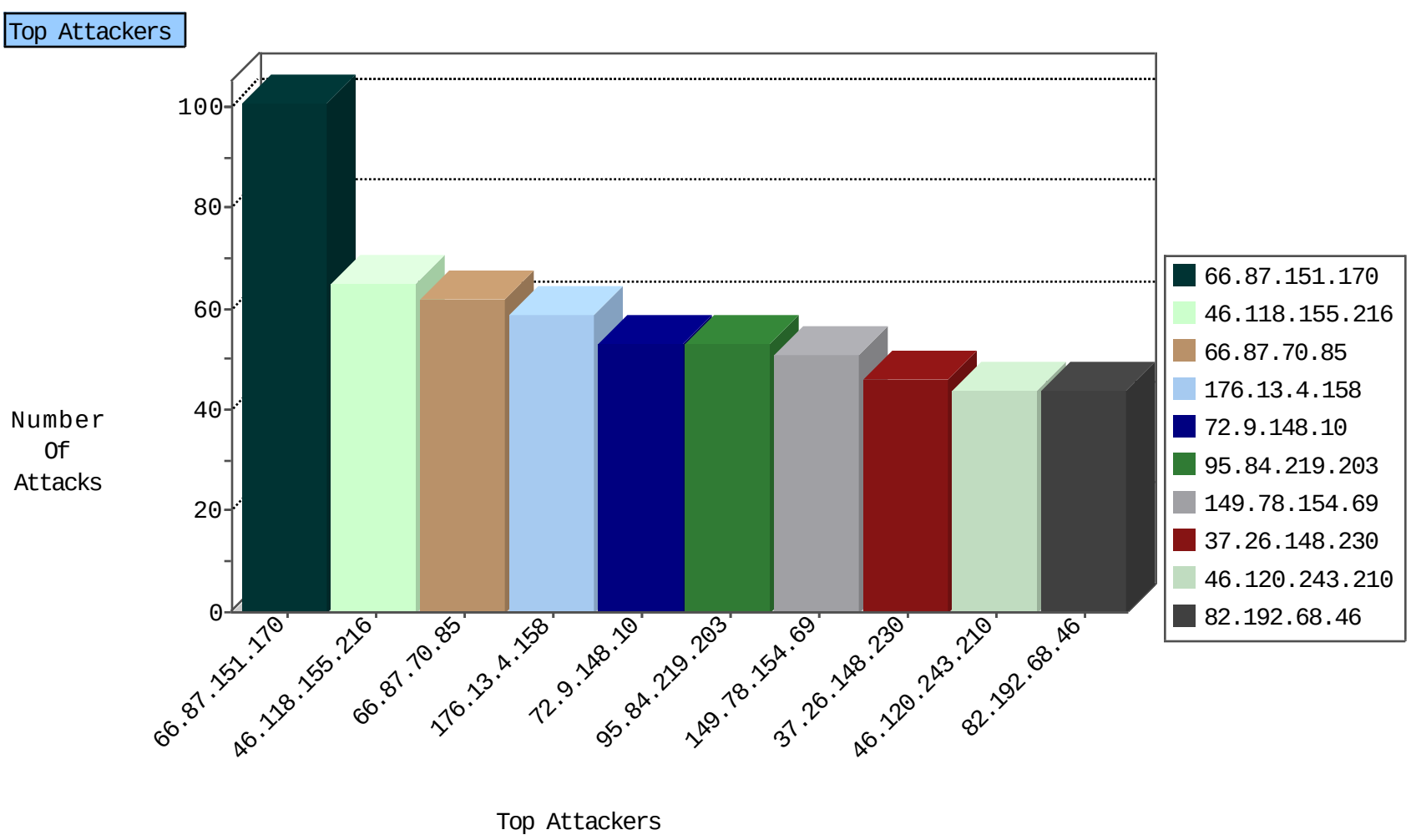
10-20-2015-01:04:54 to 10-20-2015-02:04:54

IDF Under Attack Daily Report





10-20-2015-01:04:54 to 10-20-2015-02:04:54

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.252.90.99	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3212
157.166.167.129	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.253	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
173.252.80.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-20-2015-01:04:54 to 10-20-2015-02:04:54

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-20-2015-01:04:54 to 10-20-2015-02:04:54

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	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
124.248.40.133	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
62.219.83.119	147.237.8.45	Israel	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
124.248.40.133	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
62.219.83.119	147.237.8.45	Israel	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
62.219.83.119	147.237.8.45	Israel	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
124.248.40.133	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
124.248.40.133	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

10-20-2015-01:04:54 to 10-20-2015-02:04:54

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.151.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
66.87.70.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
176.13.4.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
95.84.219.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
37.26.148.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.120.243.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.86.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.145.8.163	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
178.62.213.221	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.52.8		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
172.56.40.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
174.29.254.251	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.231.215.137	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
17.142.152.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.241.225.195	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	18
17.142.152.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
80.246.133.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.86.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.0.70.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
93.184.73.16	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.183.152.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
17.142.145.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
17.142.152.68	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.52.8		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
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
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.166.167.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.66.145.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-20-2015-01:04:54 to 10-20-2015-02:04:54

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	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	39
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	13
176.13.1.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
52.8.52.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	13
182.118.60.194	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/clientscripts/op/controlscroller.js%3fsiteversion	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	13
45.45.135.17		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	13
80.246.130.230	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	13
52.8.142.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	13
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	13
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	13
80.246.133.106	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	13
54.193.16.162	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	13
207.232.21.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/library/manage/resource/getfilecontent.hh.asp	Block	13
66.249.69.11	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	13
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	13
110.53.251.65	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13

10-20-2015-01:04:54 to 10-20-2015-02:04:54