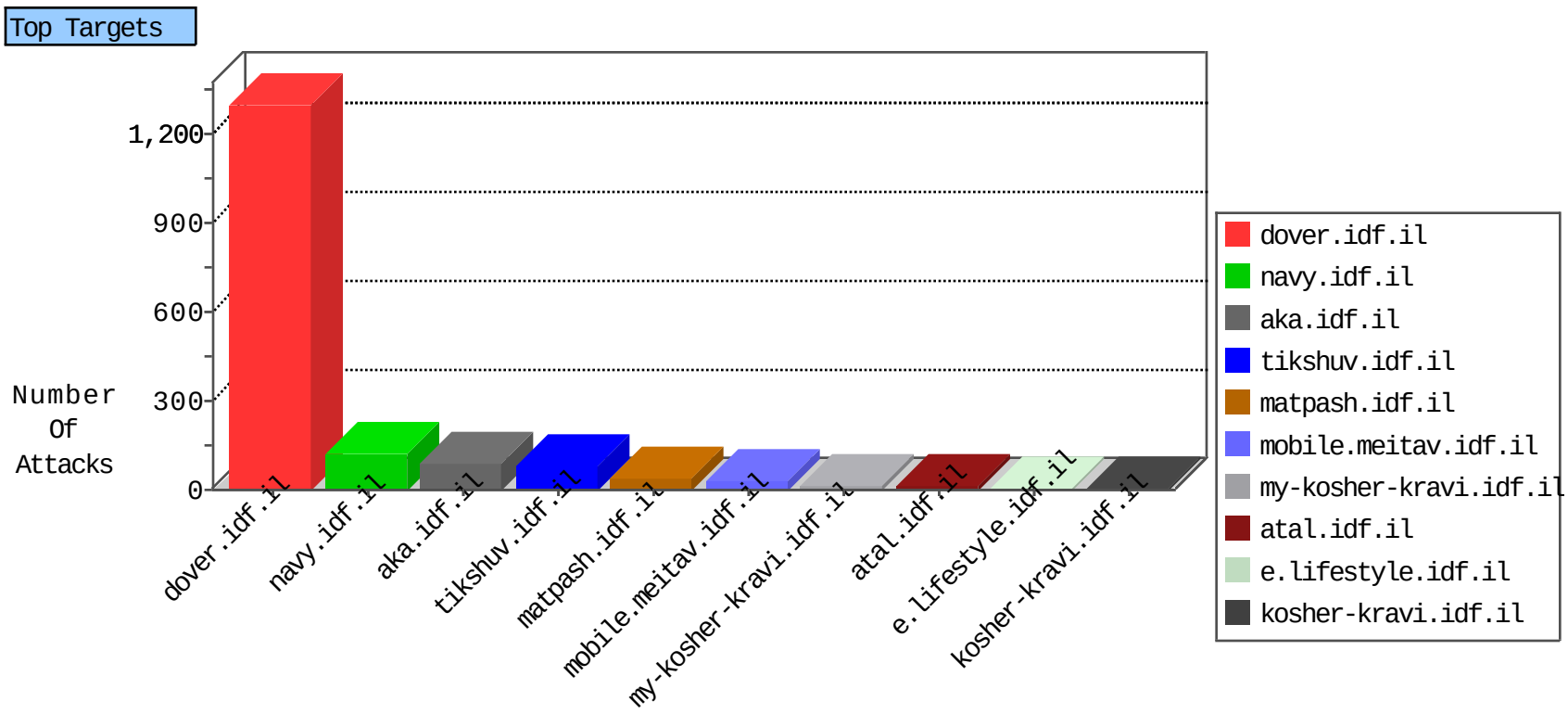
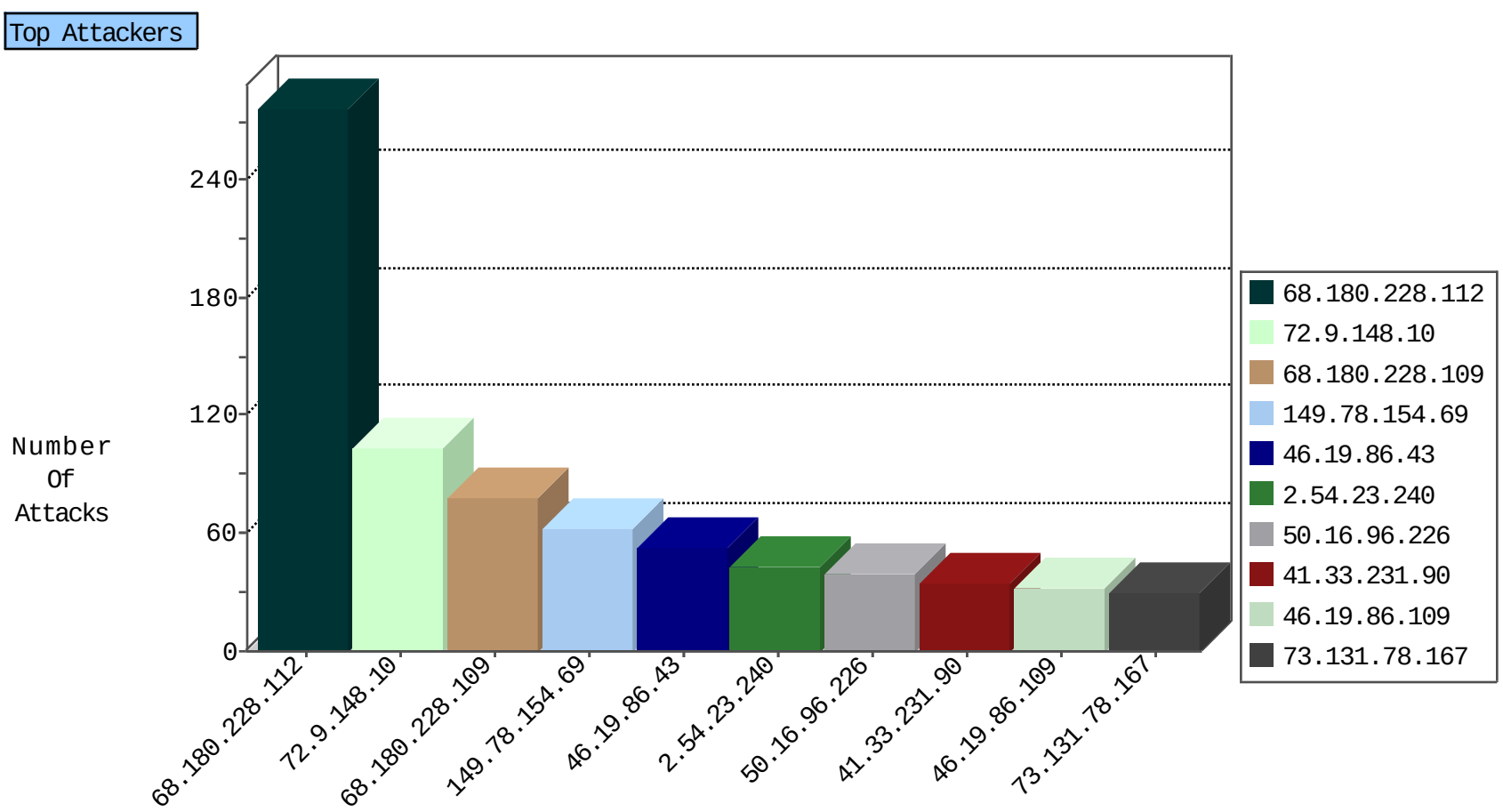
10-19-2015-04:04:08 to 10-19-2015-05:04:08

IDF Under Attack
Daily Report





10-19-2015-04:04:08 to 10-19-2015-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
61.241.197.119	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
5.29.251.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-19-2015-04:04:08 to 10-19-2015-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-19-2015-04:04:08 to 10-19-2015-05:04:08

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	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
31.184.195.114	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.55.151.117	147.237.72.167	Netherlands	ishurim.aka.idf.i	ET WEB_SERVER Muieblackcat scanner	1
117.135.163.104	147.237.8.24	China	e.lifestyle.idf.i	ET SCAN NMAP -sS window 4096	1
117.135.163.104	147.237.8.24	China	e.lifestyle.idf.i	ET SCAN NMAP -f -sS	1
99.160.189.94	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.33	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.78.194.100	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
31.184.195.114	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.195.135.82	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
169.55.151.117	147.237.72.167	Netherlands	ishurim.aka.idf.i	SERVER-WEBAPP Setup.php access	1
121.40.195.144	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	147.237.8.24	China	e.lifestyle.idf.i	ET SCAN NMAP -sS window 2048	1
104.197.123.148	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

10-19-2015-04:04:08 to 10-19-2015-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
46.19.86.43	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
2.54.23.240	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
46.19.86.109	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	30
17.142.152.110	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
17.142.152.68	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
166.170.5.47	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
184.91.174.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
17.142.152.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
24.146.241.146	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
17.142.152.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
17.142.152.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
190.179.218.21	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
46.19.85.30	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
17.142.152.81	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
76.101.194.250	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
17.142.145.3	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
17.142.152.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
17.142.152.86	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
65.96.42.162	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
50.16.96.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
17.142.145.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
32.42.15.123	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
24.114.51.73	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
99.116.172.193	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
17.142.152.94	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.87.120.115	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
99.102.168.12	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
173.84.92.223	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
67.68.86.219	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
17.142.152.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.144.168.50	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
157.55.39.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
109.66.26.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
107.77.76.110	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
5.29.251.38	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
207.46.13.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
73.131.78.167	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4

10-19-2015-04:04:08 to 10-19-2015-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	181
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	104
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	78
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 68.180.228.112	Block	65
162.243.38.196	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.38.196	Block	26
50.16.96.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	26
73.131.78.167	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
79.181.155.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
66.249.93.145	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
95.211.168.172	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	13
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
54.193.120.241	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover...	Block	13
123.125.71.22	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
74.82.47.2	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	13
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	13
140.207.198.111	China	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	13
31.184.238.55	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forums/forums.asp	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/17360.jpg	Block	13
79.176.120.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dov.	Block	13
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	13
46.19.86.39	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	13

10-19-2015-04:04:08 to 10-19-2015-05:04:08