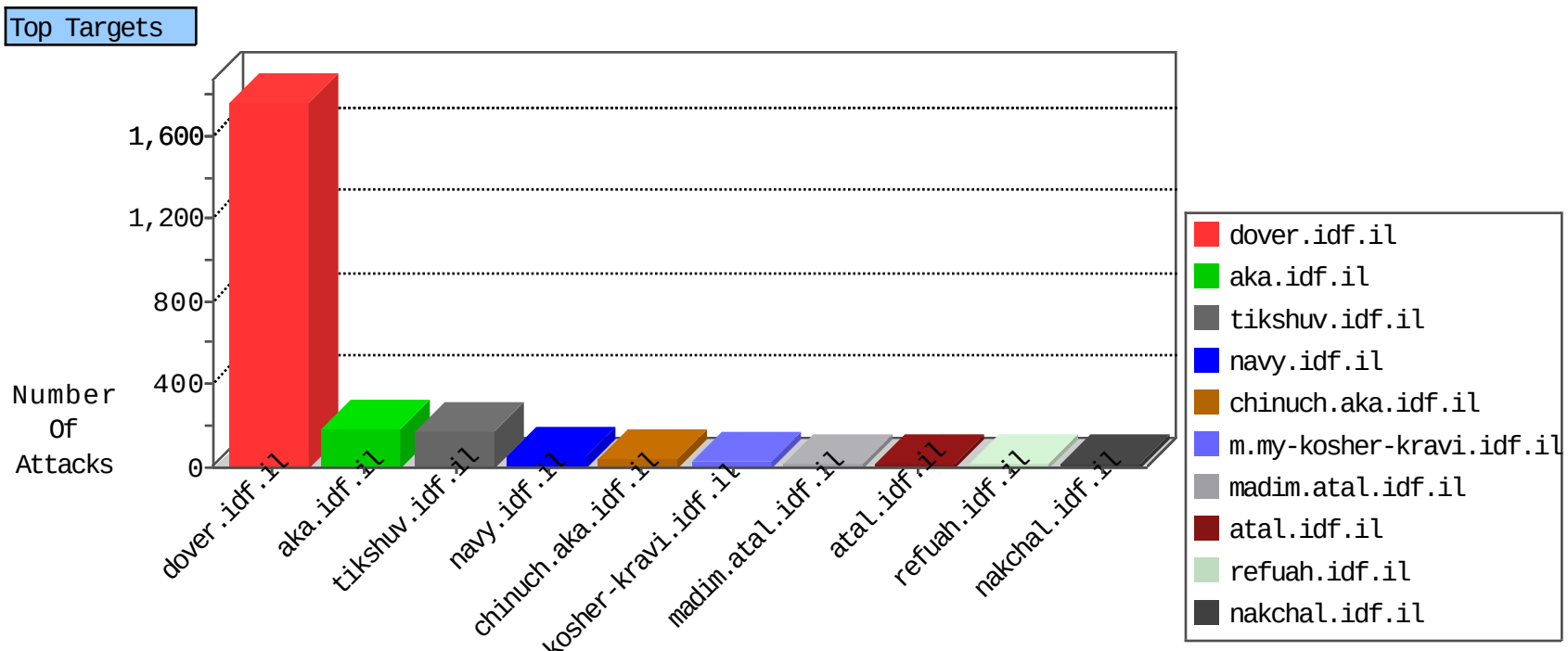
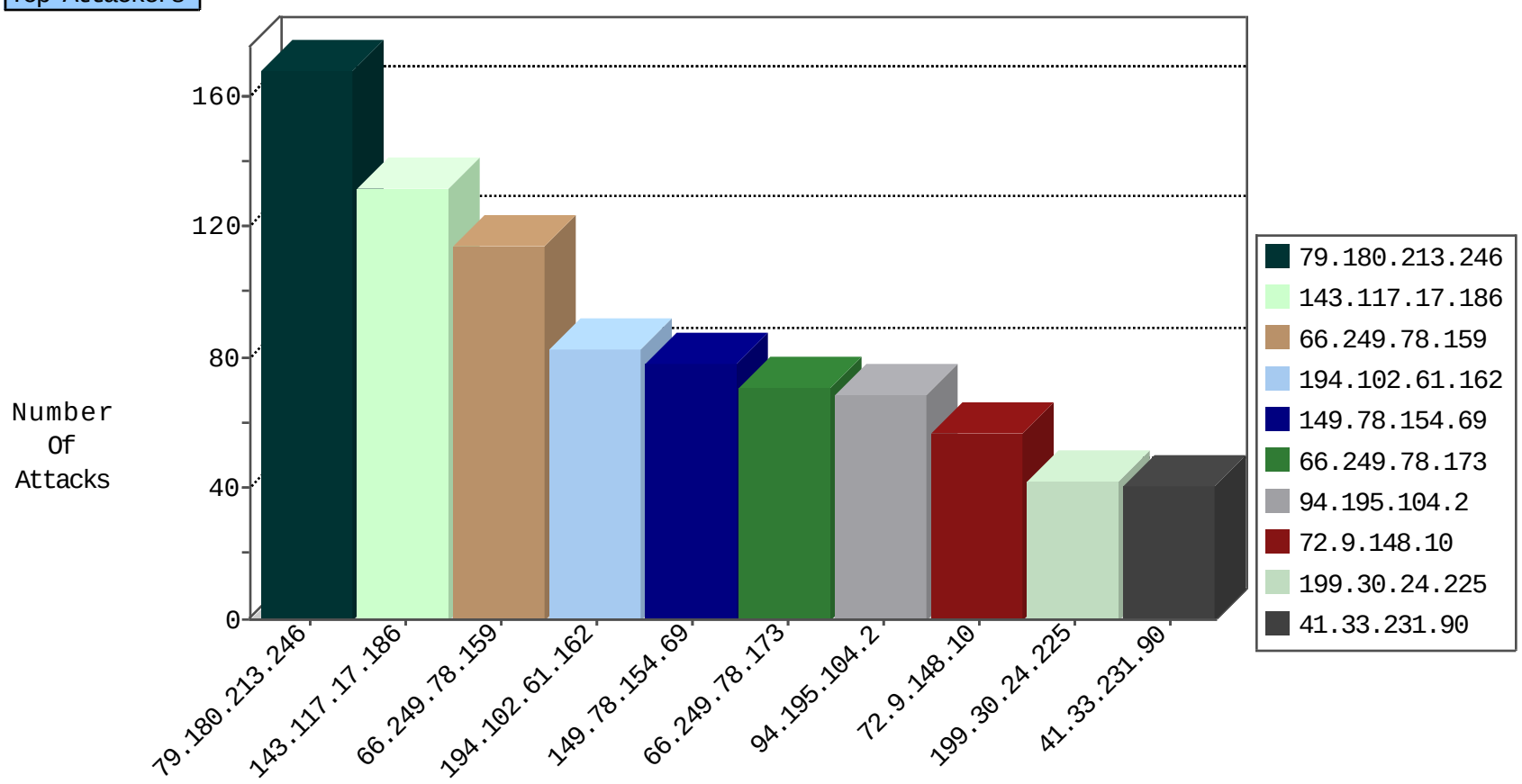
10-22-2015-00:04:04 to 10-22-2015-01:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-22-2015-00:04:04 to 10-22-2015-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.206.27	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	20
46.19.86.80	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.9.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.136.94	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
91.106.102.150	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
185.61.136.94	Ukraine	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
110.216.2.154	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

10-22-2015-00:04:04 to 10-22-2015-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-22-2015-00:04:04 to 10-22-2015-01:04:04

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.248.116.57	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP admin.php access	2
139.162.141.72	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
66.102.8.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
45.33.7.101	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
45.33.0.185	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
41.248.116.57	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP Phorum admin access	1
190.124.35.115	147.237.0.35	Nicaragua	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.33.7.101	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1

10-22-2015-00:04:04 to 10-22-2015-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
143.117.17.186	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
194.102.61.162	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
94.195.104.2	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
212.14.228.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
100.37.157.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
83.208.62.25	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
82.145.221.239	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
69.203.14.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
2.52.63.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
71.57.133.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
78.123.122.242	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
74.90.9.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
37.142.231.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
91.10.167.47	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
197.133.182.83	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.181.120.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
77.42.129.119	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.64.200.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.19.165		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.43.173.30	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
104.175.65.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.102.9.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.142.64.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
93.172.151.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.127.208.196		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
78.55.193.221	Germany	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
37.239.8.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
105.228.222.74	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.64.81.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
96.254.126.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

10-22-2015-00:04:04 to 10-22-2015-01:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.213.246	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation SearchText in www.tikshuv.idf.il/938-he/tikshuv.aspx	Block	168
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	56
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
199.30.24.225	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	42
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
83.130.113.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
178.255.87.242	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	14
77.125.119.229	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
31.154.91.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	14
202.102.99.80	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	14
109.67.11.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=bf6bf9b5kkkkkkk_bf6bf9b5	Block	14
77.126.253.238	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/request.aspx	None	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	14
188.165.15.89	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	14
213.172.183.61	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
176.13.19.249	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	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	14
188.165.15.89	France	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/smalim/smalim.aspx	None	14
82.166.125.124	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	14
176.13.19.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.19.249	None	14
5.8.242.73	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	14

10-22-2015-00:04:04 to 10-22-2015-01:04:04