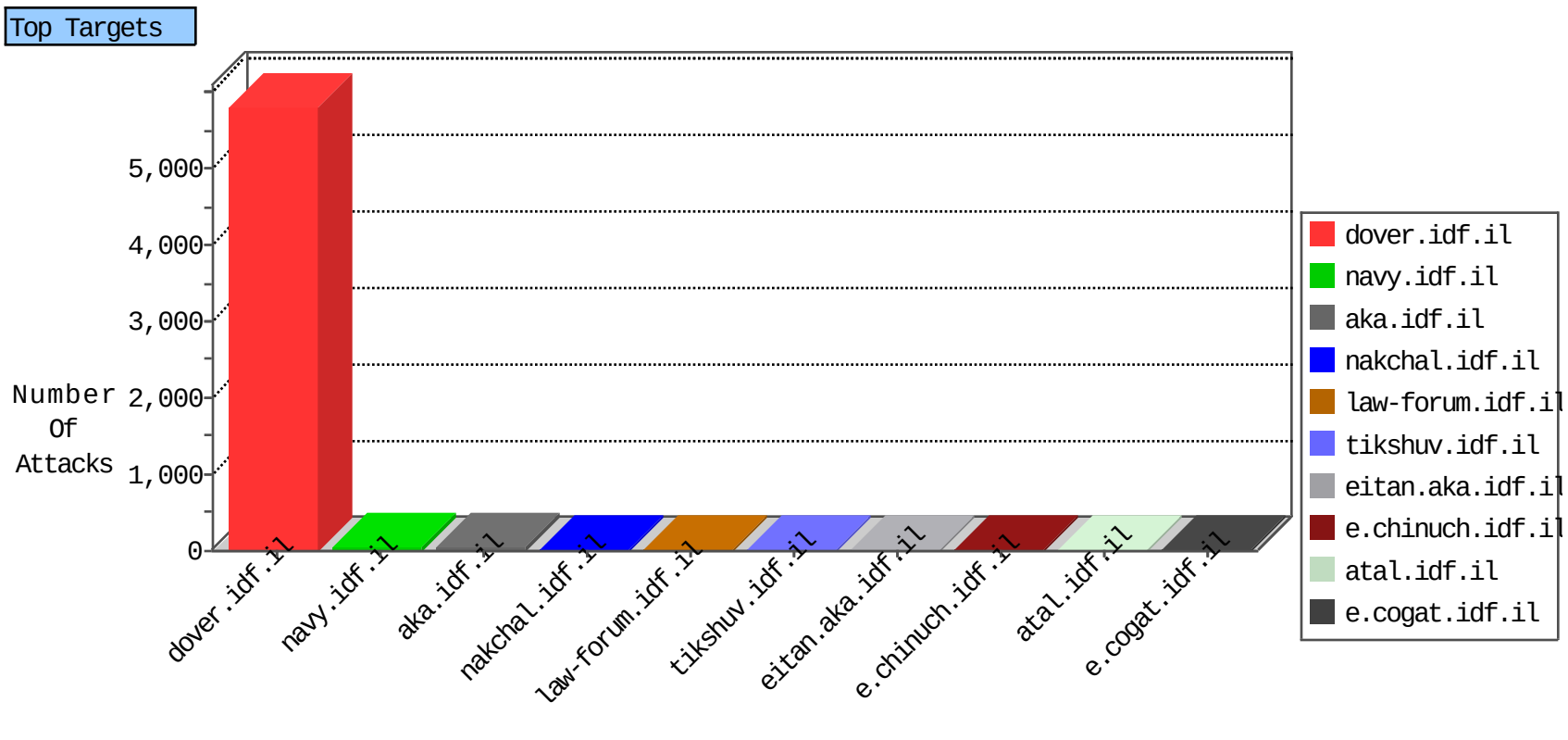
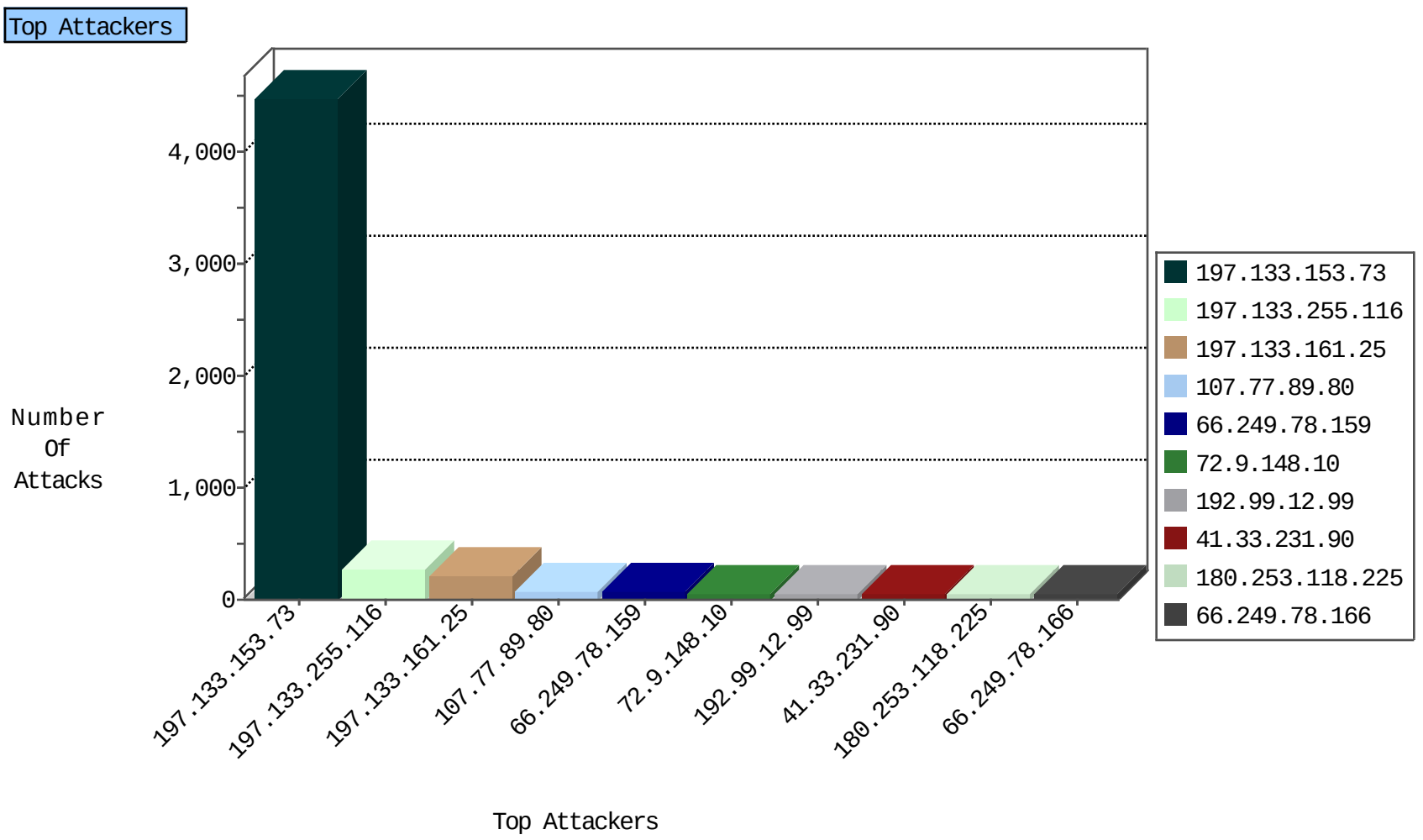
10-22-2015-04:04:00 to 10-22-2015-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-22-2015-04:04:00 to 10-22-2015-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.64.105.199	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
183.60.48.25	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

10-22-2015-04:04:00 to 10-22-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-22-2015-04:04:00 to 10-22-2015-05:04:00

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	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
169.229.3.91	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
79.143.180.44	147.237.76.42	Germany	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.76.42	Sweden	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
182.48.105.216	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
169.229.3.92	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.77.205	India	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
71.6.165.200	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.143.82.50	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
37.143.82.50	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
198.199.65.204	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.50	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.229.3.92	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1

10-22-2015-04:04:00 to 10-22-2015-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.133.153.73	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4387
197.133.255.116	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	268
197.133.161.25	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	219
107.77.89.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
197.133.153.73	Egypt	147.237.77.216	dover.idf.il	drop		drop	54
189.38.134.239	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
180.253.118.225	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
192.99.12.99	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
89.138.245.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
197.133.153.73	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
91.106.32.66	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
173.246.207.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	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
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
131.128.73.3	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.99.12.99	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
180.253.118.225	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
107.185.255.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.78	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
50.153.190.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.21.50.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
24.228.91.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.139	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.133.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.133.153.73	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
90.196.54.1	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
32.42.15.123	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
75.75.52.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.126.224.174	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.30.24.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.99.12.99	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
199.30.24.139	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

10-22-2015-04:04:00 to 10-22-2015-05:04:00

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	56
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	42
41.43.201.226	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22777-ar/dover.aspx)	Block	28
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17416.jpg	Block	14
77.237.146.28	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	14
178.49.154.143	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	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
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	14
91.121.83.118	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.121.83.118	Block	14
41.43.208.124	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22777-ar/dover.aspx)	Block	14
188.143.232.22	Russian Federation	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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/4/size220x0/17374.jpg	Block	14
91.121.83.118	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
192.99.12.99	Canada	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/see	Block	14
104.236.61.18		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	14
197.133.153.73	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
41.43.192.2	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx)	Block	14
140.207.198.223	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	14

10-22-2015-04:04:00 to 10-22-2015-05:04:00