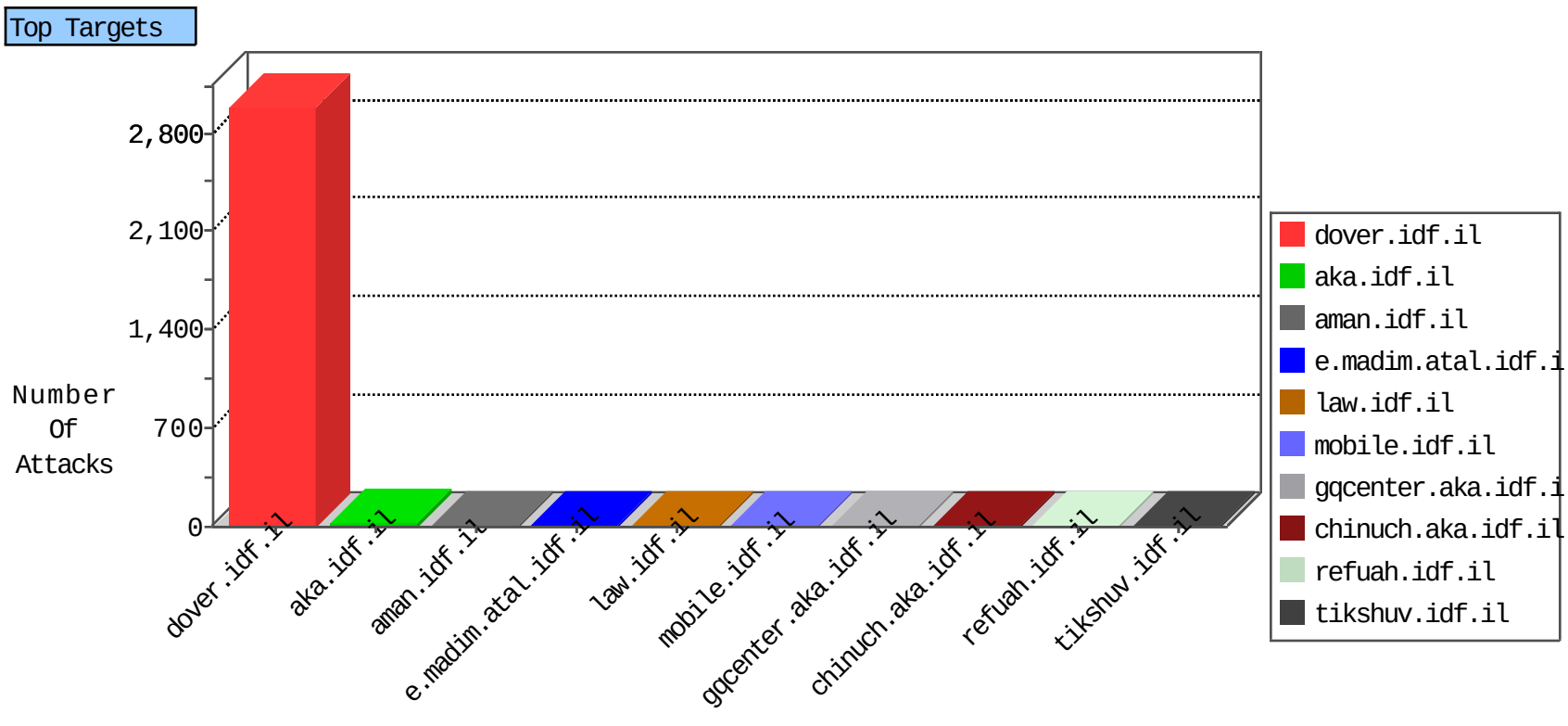
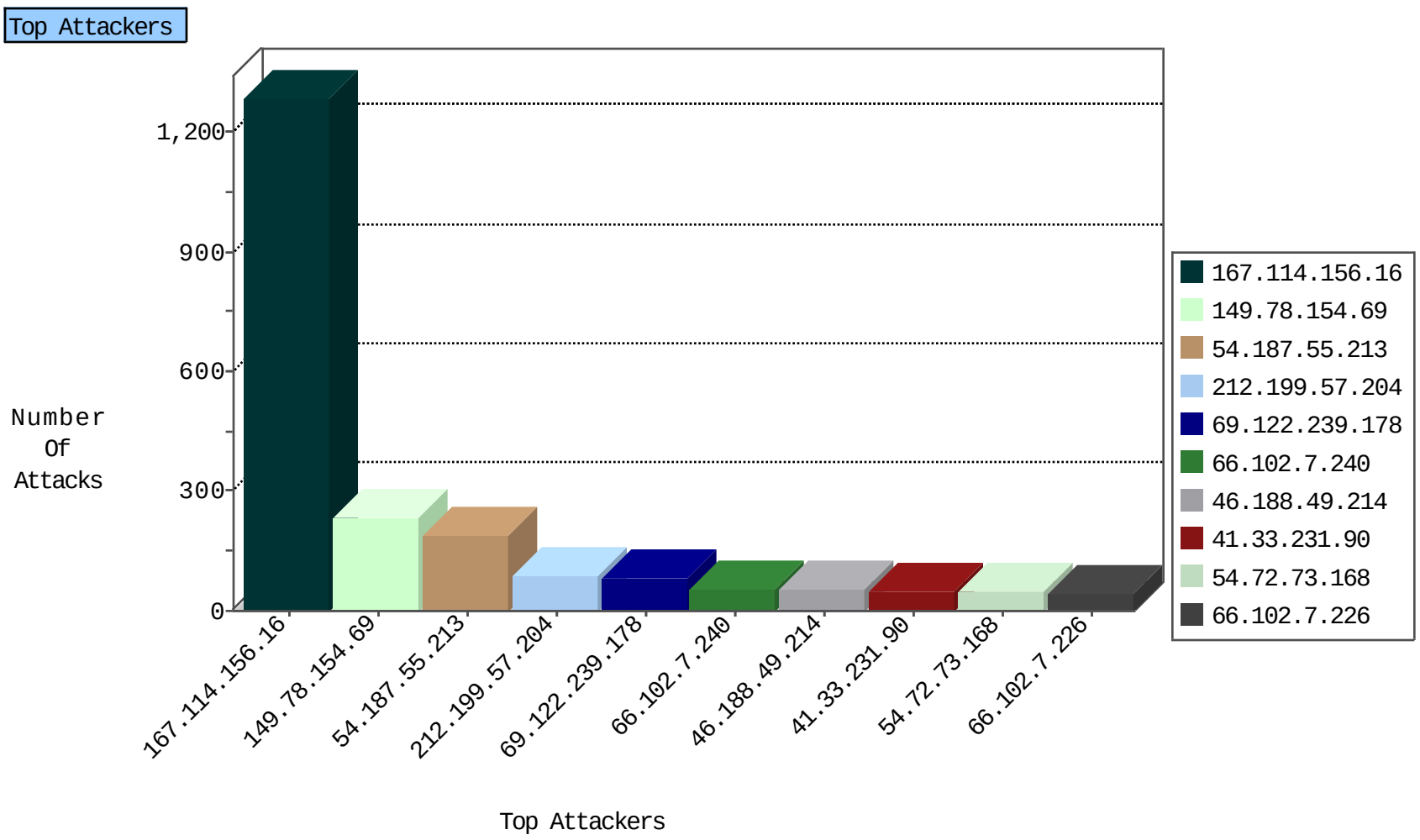
11-08-2015-05:04:09 to 11-08-2015-06:04:09

IDF Under Attack Daily Report





11-08-2015-05:04:09 to 11-08-2015-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2258
66.249.64.186	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	854
123.230.208.137	Japan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
42.117.28.91	Vietnam	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
178.175.142.50	Moldova, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
180.143.222.34	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.6	Iceland	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

11-08-2015-05:04:09 to 11-08-2015-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-08-2015-05:04:09 to 11-08-2015-06:04:09

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	4
31.6.71.154	147.237.8.27	Poland	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
207.126.160.10	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
177.43.249.41	147.237.72.156	Brazil	aman.idf.il	ET SCAN NMAP -sS window 4096	1
177.43.249.41	147.237.72.156	Brazil	aman.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.77.243	Canada	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.172.154	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.8	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
217.20.64.39	147.237.0.33	Russian Federation	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.6.71.154	147.237.77.178	Poland	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.77.176	Korea, Republic of	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
177.43.249.41	147.237.72.156	Brazil	aman.idf.il	ET SCAN NMAP -sS window 2048	1
123.151.149.222	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.243	Canada	mobile.idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
74.117.133.194	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-08-2015-05:04:09 to 11-08-2015-06:04:09

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	233
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	187
212.199.57.204	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	88
69.122.239.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	81
46.188.49.214	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
66.102.7.240	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
69.132.192.189	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
66.102.7.226	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
178.167.254.170	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
66.102.7.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
24.114.53.150	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
199.119.233.189	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
157.55.39.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
157.55.39.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.102.7.240	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
162.243.199.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.102.7.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.102.7.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
71.81.216.247	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
157.55.39.175	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
109.67.31.201	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
89.138.50.171	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
188.165.15.14	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
93.173.137.129	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
84.94.32.197	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
97.74.24.188	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
198.58.102.96	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
40.77.167.2	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
40.77.167.9	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
40.77.167.20	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6

11-08-2015-05:04:09 to 11-08-2015-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.37.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.111.68	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
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	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
104.236.122.112		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.37.36	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/coni/english/main_index.stm al-aqsa letter to bethlehem municipality	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.65	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
64.237.45.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
157.55.39.141	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.33.204.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
72.64.94.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/home/def...78&catid=38978	Block	1
2.52.49.89	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/17487.jpg	Block	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8675-he/refuah.aspx	Block	1
79.111.218.222	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/69047.pdf	Block	1

11-08-2015-05:04:09 to 11-08-2015-06:04:09