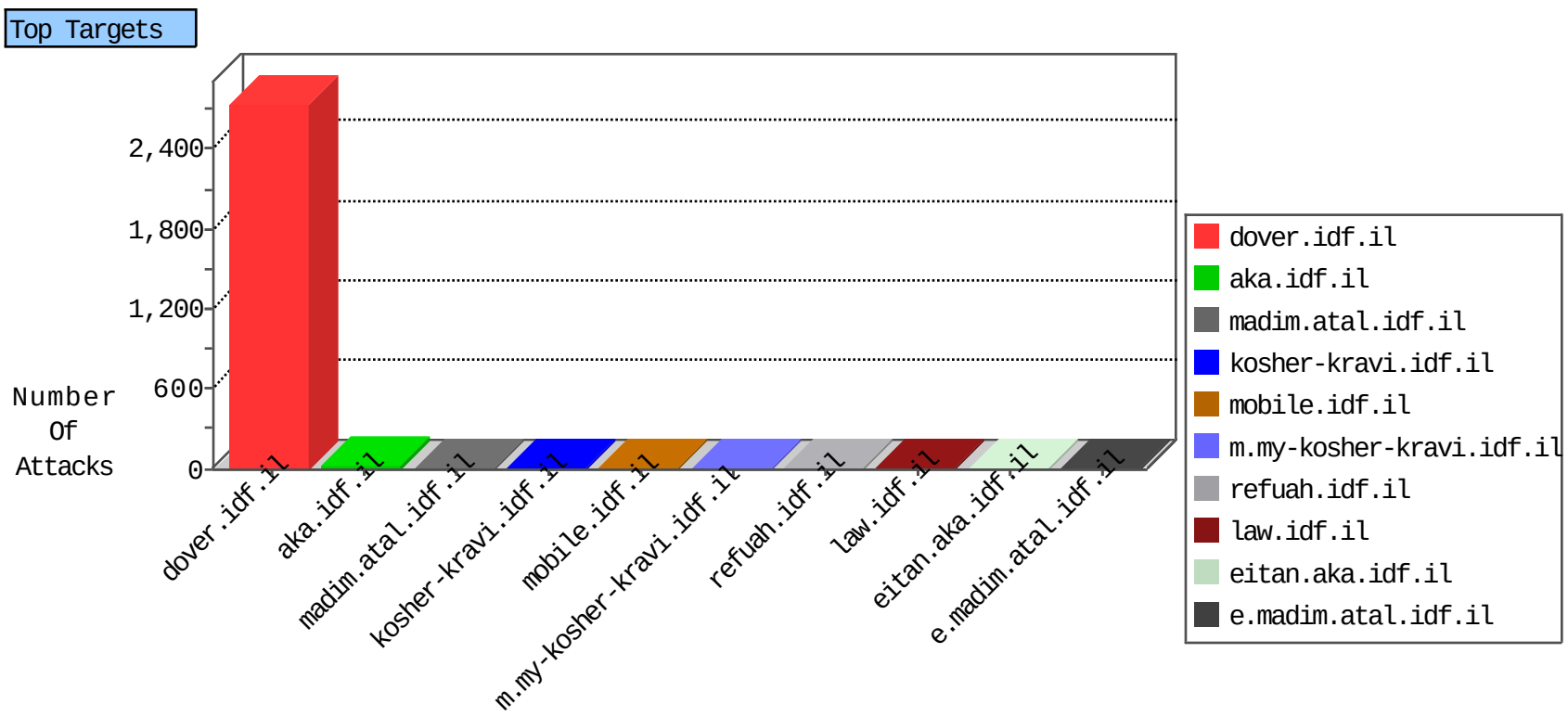
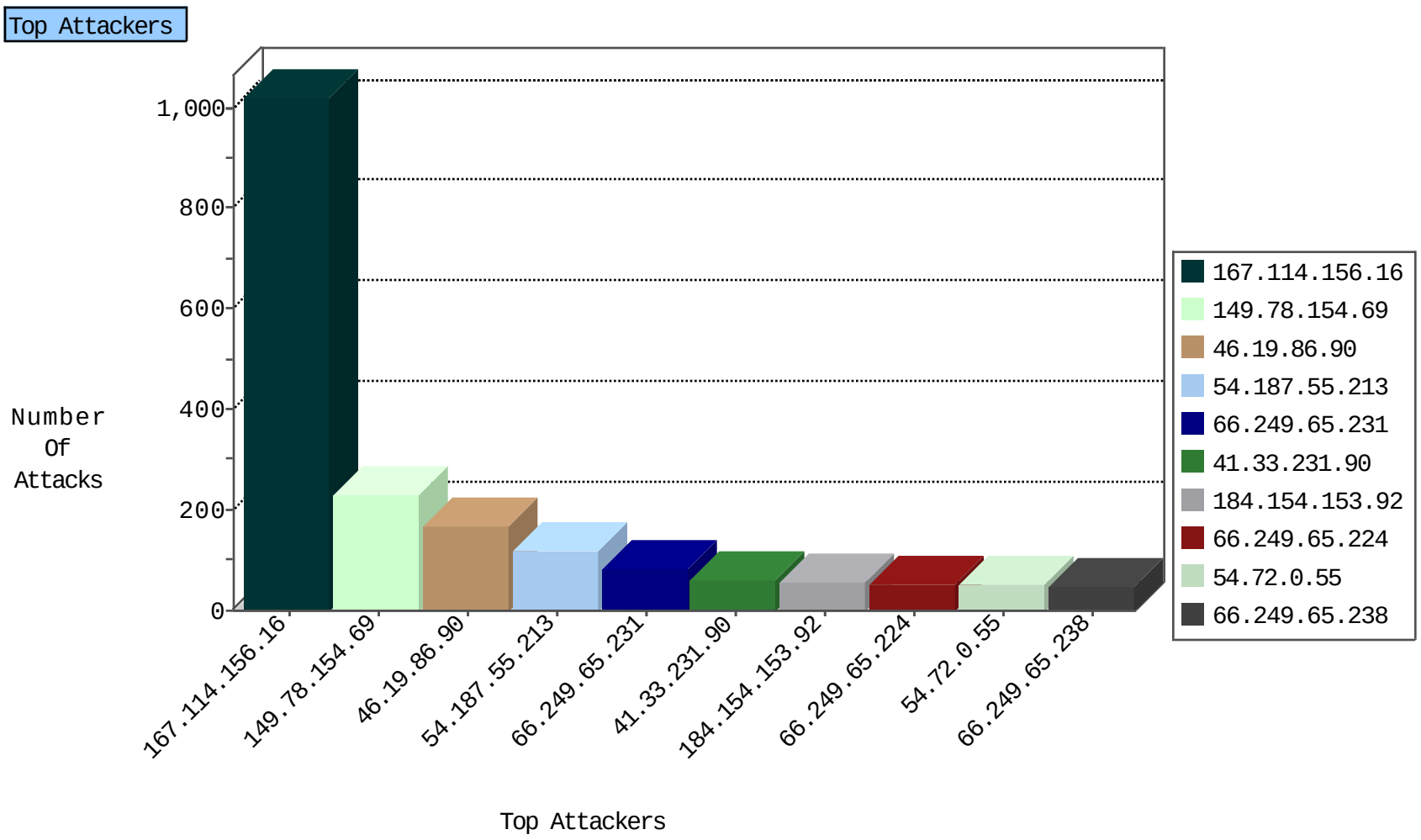
11-07-2015-04:04:00 to 11-07-2015-05:04:00

IDF Under Attack Daily Report





11-07-2015-04:04:00 to 11-07-2015-05:04:00

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	1883
78.47.67.232	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	3
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2

11-07-2015-04:04:00 to 11-07-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.180.21	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.191.165	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-07-2015-04:04:00 to 11-07-2015-05:04:00

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
115.72.103.148	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
210.61.150.154	147.237.77.121	Taiwan	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
182.90.68.83	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.174.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
40.115.58.160	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	147.237.77.121	Taiwan	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
180.93.225.52	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.174.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

11-07-2015-04:04:00 to 11-07-2015-05:04:00

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	230
46.19.86.90	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	169
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	96
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	58
184.154.153.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
54.224.21.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
104.131.195.214	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
207.46.13.184	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
157.55.39.181	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
40.77.167.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
66.249.65.231	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
198.58.102.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop		drop	14
66.249.65.238	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
77.244.254.230	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
85.64.176.188	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
195.154.194.59	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
68.83.104.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
40.77.167.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	10
40.77.167.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
195.154.211.147	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
128.148.231.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
40.77.167.39	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
75.126.221.55	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
157.55.39.63	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
40.77.167.56	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	SAM rule	drop	8
66.249.65.231	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
37.26.148.182	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
37.26.146.164	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
79.181.5.146	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6

11-07-2015-04:04:00 to 11-07-2015-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.211.26	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
176.13.15.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.127.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.154.211.26	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.154.211.26	Block	3
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	2
149.78.10.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in aka.idf.il/giyus/forms/	None	1
74.82.47.3	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;moduletogoto in aka.idf.il/giyus/login/	None	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2277.jpg	Block	1
78.47.67.232	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.164.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
193.200.150.125	Europe	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3384.jpg	Block	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
66.249.67.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
64.79.85.205	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1

11-07-2015-04:04:00 to 11-07-2015-05:04:00