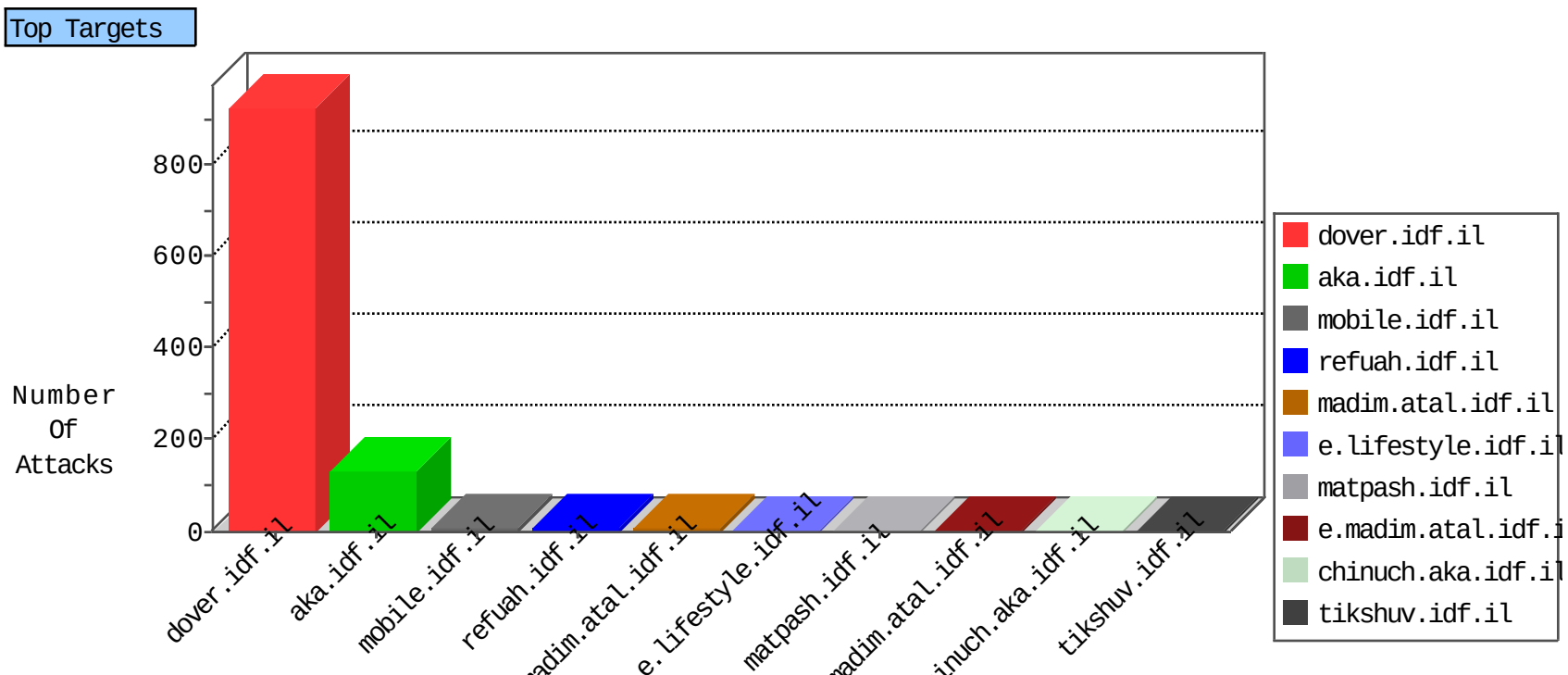
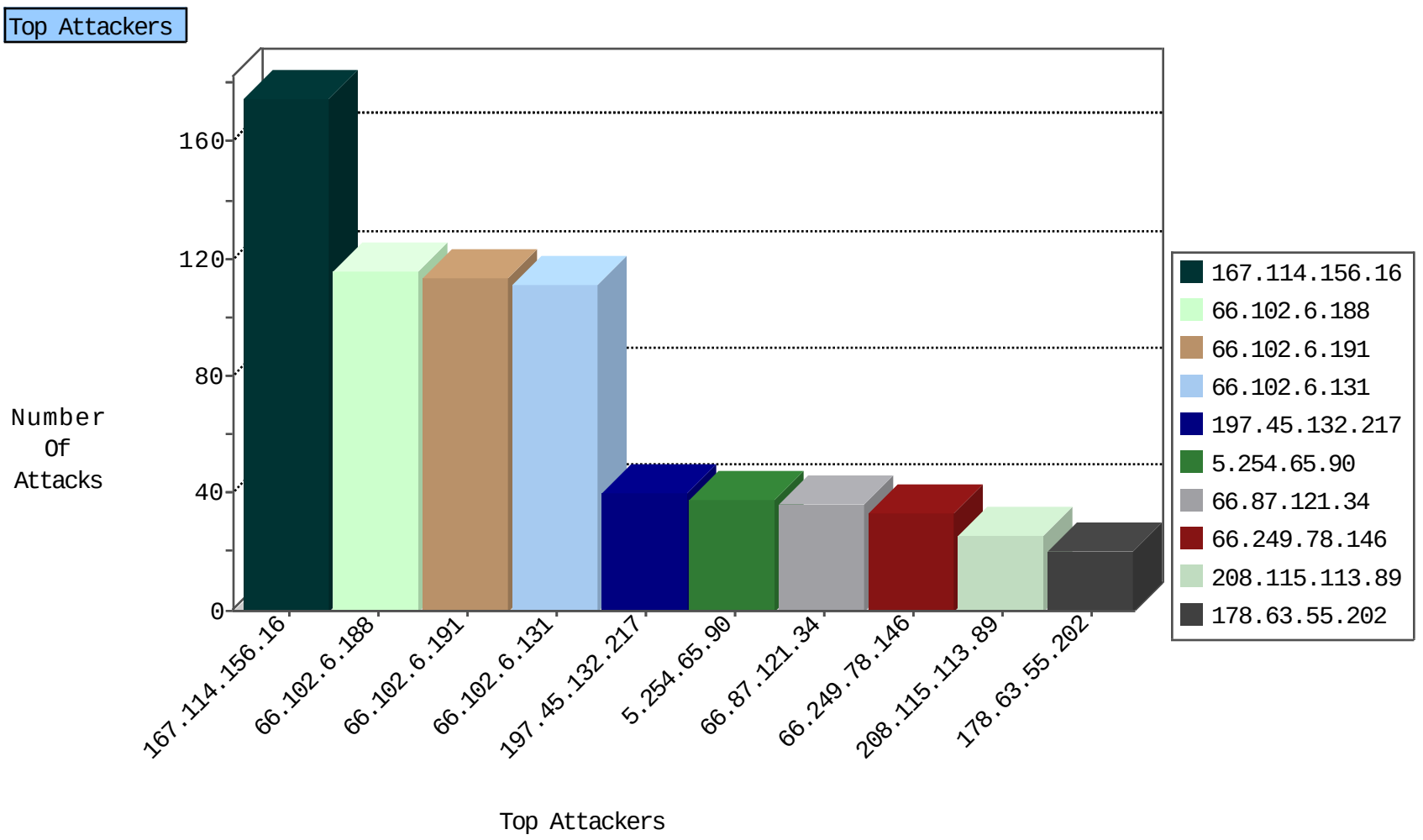
04-28-2016-07:04:01 to 04-28-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-07:04:01 to 04-28-2016-08:04:01

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	HTTP-POST-Segmented-DoS	dest-reset	8527
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4723
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1383
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1053
85.250.118.189	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
37.157.249.183	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-28-2016-07:04:01 to 04-28-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.220.63.148	Korea, Republic of	147.237.77.235	sviva.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-28-2016-07:04:01 to 04-28-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.102.213.252	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
201.175.110.135	147.237.8.14	Mexico	e.orchot.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.36.35.241	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
211.220.63.148	147.237.77.235	Korea, Republic of	sviva.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1

04-28-2016-07:04:01 to 04-28-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
5.254.65.90	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.87.121.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
104.236.100.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.177.177.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.177.177.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
77.126.235.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.147.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
216.4.56.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.45.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.31.54.202	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
83.250.47.184	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.205.84.62	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
83.142.164.58	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.254.65.173	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.195.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.39.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.146.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.152.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.244	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.58.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.111.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-28-2016-07:04:01 to 04-28-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	3
2.53.165.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.249.55.100	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
14.102.56.34	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.181.172.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
212.199.57.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3395.jpg	Block	1
14.102.56.34	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
23.106.166.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/megurim/kishur/default.asp	None	1
149.88.37.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main-sachar	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
2.53.52.174	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/default.aspx	Block	1
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
157.55.39.133	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8913-he/refuah.aspx	Block	1

04-28-2016-07:04:01 to 04-28-2016-08:04:01