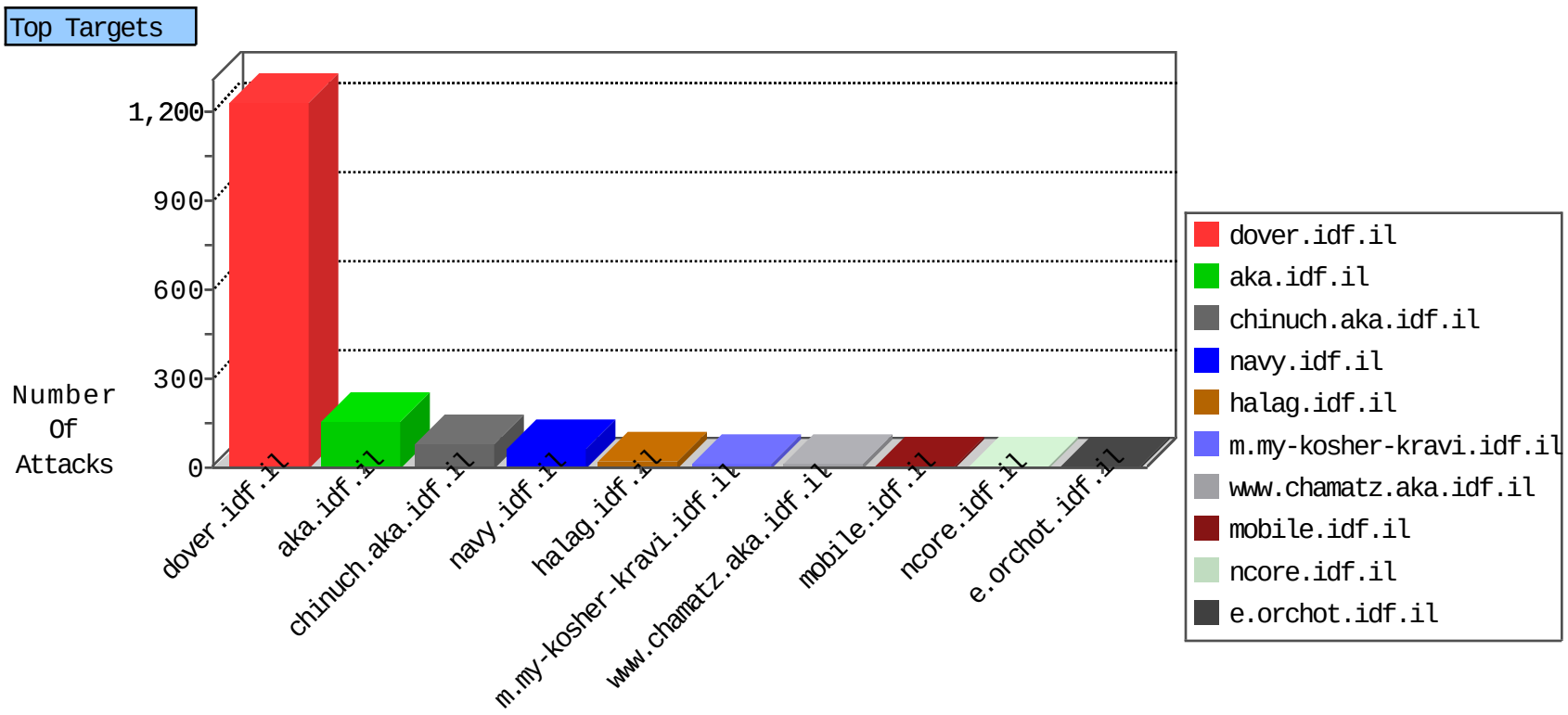
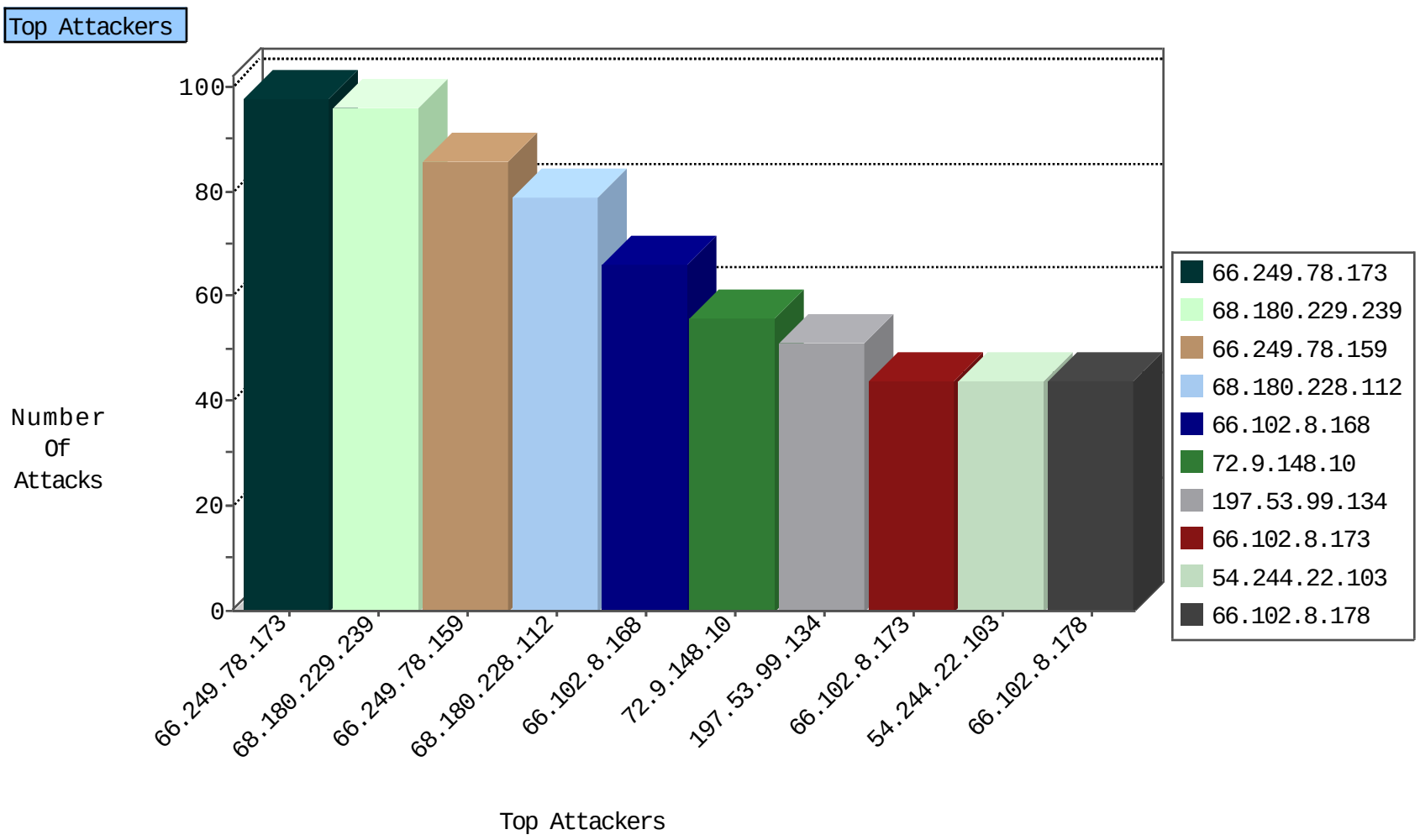
10-23-2015-04:04:01 to 10-23-2015-05:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-23-2015-04:04:01 to 10-23-2015-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.146.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
82.80.146.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
95.86.120.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	3
66.102.8.152	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
98.71.194.96	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.102.254.79	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
61.154.37.239	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-23-2015-04:04:01 to 10-23-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-04:04:01 to 10-23-2015-05:04:01

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	3
66.249.65.18	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	147.237.76.198	United States	e.yohalan.idf.il	ET DROP Dshield Block Listed Source	1
183.107.197.143	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.157.71.176	147.237.76.86	China	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.235.195.234	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
1.235.195.234	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN NMAP -f -sS	1
209.41.67.92	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
158.85.158.198	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
45.33.7.101	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN NMAP -sS window 2048	1

10-23-2015-04:04:01 to 10-23-2015-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
197.53.99.134	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
74.101.93.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
71.253.235.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
185.26.182.31	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
187.65.73.214	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.80.146.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
65.55.219.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.247.76.65	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.229.239	United States	147.237.72.166	aka.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
176.12.138.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.133.43	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.70	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
221.121.151.230	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.72	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
166.137.126.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
157.55.39.237	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.203.242	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
95.86.120.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.192	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
134.191.232.71	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	4
220.255.97.210	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.137.118.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

10-23-2015-04:04:01 to 10-23-2015-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	70
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	70
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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	42
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.67.146	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
137.116.71.170	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/robots.txt	Block	14
66.249.67.209	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
91.55.189.242	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
66.249.67.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
176.28.46.163	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
66.249.67.217	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
92.78.142.231	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	14
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17404.jpg	Block	14
68.196.137.237	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
46.121.111.234	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
93.196.106.230	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.201	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	14
110.34.28.229	Nepal	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14816-he/dover.a	Block	14
79.197.206.128	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14

10-23-2015-04:04:01 to 10-23-2015-05:04:01