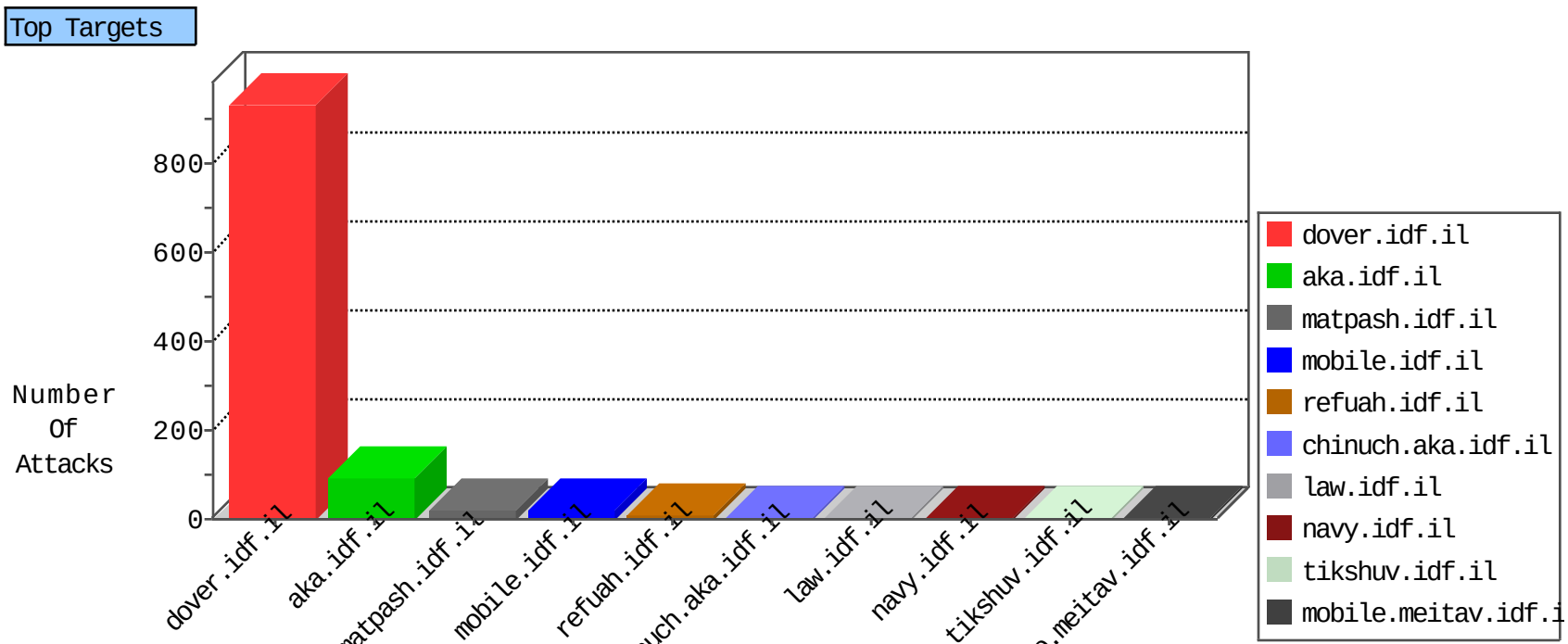
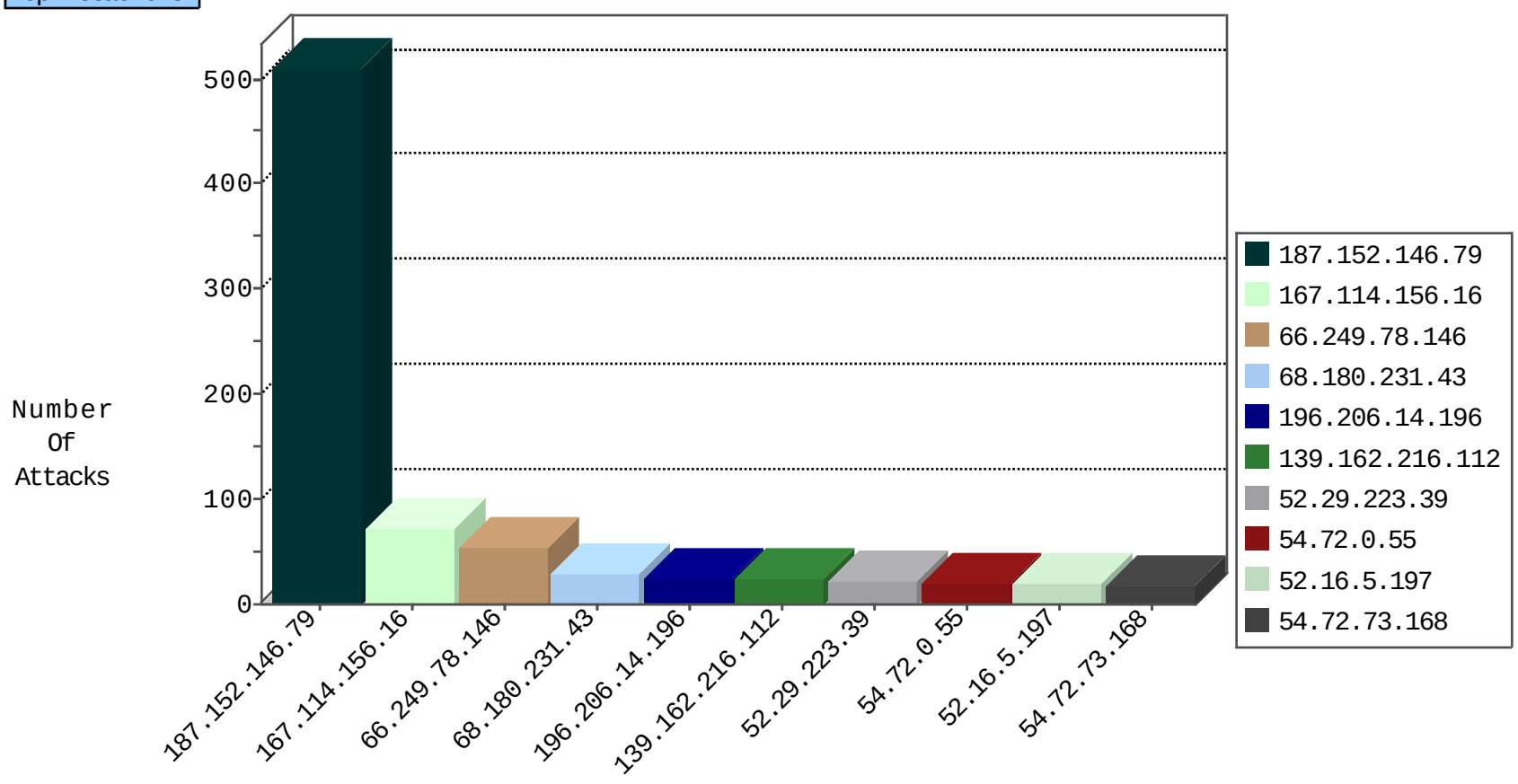
04-29-2016-05:04:02 to 04-29-2016-06:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-29-2016-05:04:02 to 04-29-2016-06:04:02

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	TCP handshake violation, first packet not syn	drop	21891
52.91.40.35	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3015
196.206.14.196	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1903
52.29.223.39	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1502
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	14
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
5.206.231.84	Portugal	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
5.206.231.84	Portugal	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
162.243.126.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.206.231.84	Portugal	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
5.206.231.84	Portugal	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
220.124.151.130	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

04-29-2016-05:04:02 to 04-29-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.227.0.76	United States	147.237.0.15	kosher-kravi.idf.il	0947: HTTP: test-cgi Access	Block	1
173.227.0.76	United States	147.237.0.17	m.my-kosher-kravi.idf.il	0947: HTTP: test-cgi Access	Block	1

04-29-2016-05:04:02 to 04-29-2016-06:04:02

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
174.37.194.144	147.237.76.42	United States	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
161.202.120.149	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.178	Italy	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
220.124.151.130	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
220.124.151.130	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
188.2.153.226	147.237.0.33		idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
161.202.120.149	147.237.77.233	Japan	atal.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.149	147.237.77.205	Japan	prisha.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.149	147.237.76.201	Japan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.178	Italy	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
107.158.255.194	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
220.124.151.130	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
161.202.120.149	147.237.77.226	Japan	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
161.202.120.149	147.237.77.170	Japan	maarachot.idf.il	ET SCAN Potential SSH Scan	1

04-29-2016-05:04:02 to 04-29-2016-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
187.152.146.79	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	511
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
196.206.14.196	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
158.69.228.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
116.25.105.99	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.136.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.209	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.15.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
52.91.40.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
177.180.10.138	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
104.197.57.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
1.36.146.89	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
181.30.30.166	Argentina	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.142.162.50	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.177	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.132.16.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.15.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.84.181	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.191.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.90.243.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
24.184.96.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.65.31.90	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
216.135.125.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.247.219	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

04-29-2016-05:04:02 to 04-29-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
74.89.106.151	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/	Block	1
54.189.233.254	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
148.251.70.201	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
174.37.194.144	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.136.155	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	1
54.203.102.190	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/994-8301-he/miluim.aspx	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.246	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.15.15	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
116.25.105.99	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 116.25.105.99	Block	1
54.203.165.22	United States	147.237.0.34	tikshuv.idf.il	Distributed Parameter Type Violation on www.tikshuv.idf.il/modules/forums/forum.aspx parameter ForumId	Block	1
164.132.161.6	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluiml	Block	1
66.249.79.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.116.63.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.247.194	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
116.25.105.99	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/3	Block	1
164.132.161.96	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17275-he/חיל האוויר תק ף שלוש מטרות טרור ברצועה בתגובה לירי הרקטות.aspx	Block	1
54.185.208.247	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1379-he/dover.aspx parameter PageNum	Block	1
198.58.103.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
131.253.25.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	1
174.37.194.144	United States	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 174.37.194.144 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

04-29-2016-05:04:02 to 04-29-2016-06:04:02