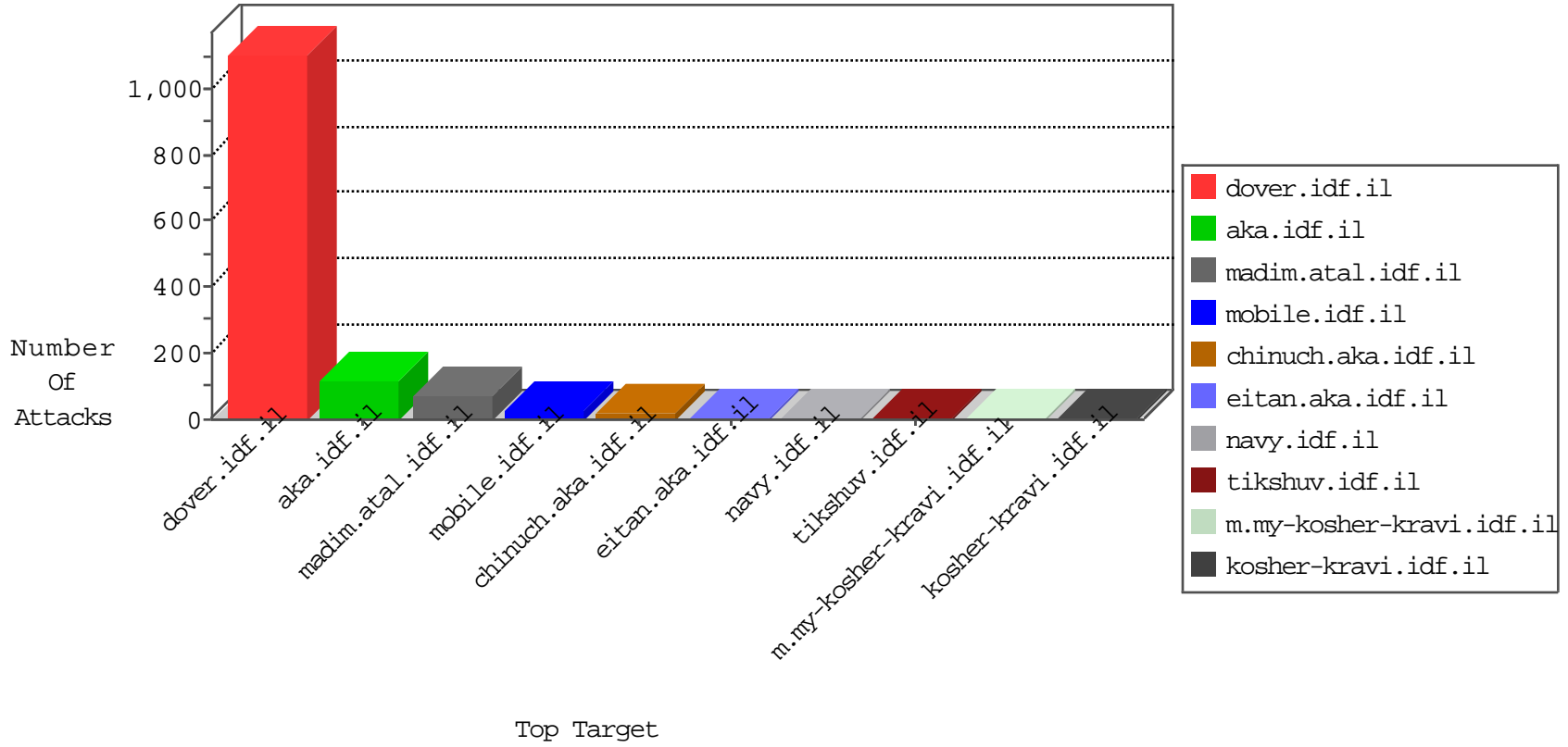


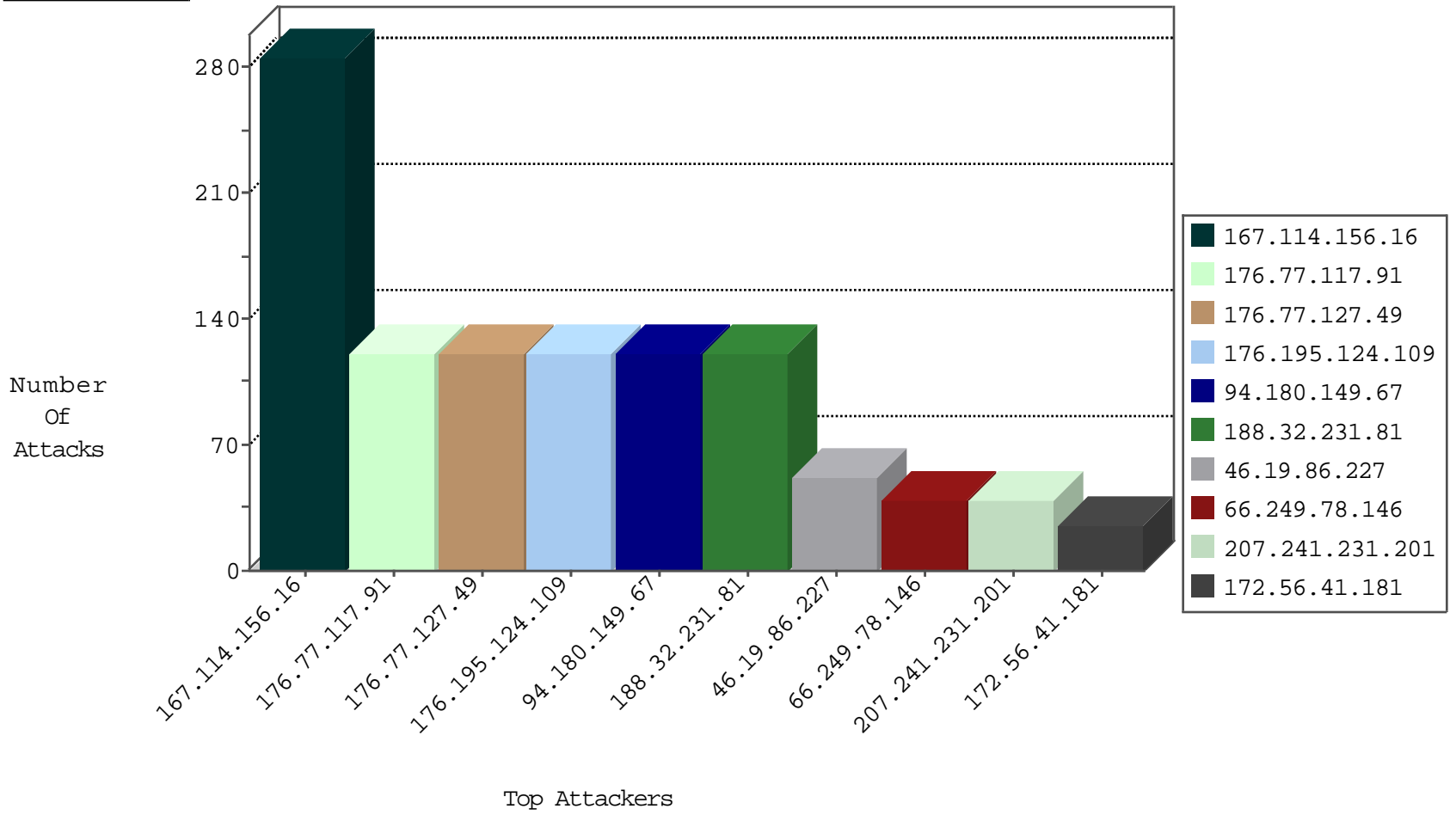
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	40091
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	13273
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1708
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
213.57.174.85	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
101.164.208.36	Australia	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
180.97.106.37	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
195.88.209.6	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
66.240.219.146	United States	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
173.193.130.54	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
173.65.154.27	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.8.19	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.147	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
106.120.173.76	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
81.17.17.135	147.237.0.17	Switzerland	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
52.90.202.117	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
173.193.130.54	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
173.193.130.54	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -f -sS	1
163.172.8.19	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.8.19	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
117.2.80.56	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.214.34.99	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
66.240.213.93	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
52.90.202.117	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
187.245.195.39	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.32.231.81	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
94.180.149.67	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
176.77.117.91	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
176.77.127.49	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
176.195.124.109	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
207.241.231.201	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	39
172.56.41.181	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
2.53.16.14	Israel	147.237.77.243	mobile.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
193.171.152.101	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.85.216	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.108.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.116.108.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.116.108.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
73.26.18.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
140.186.14.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.172.120.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
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
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.100.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.105.53.102	Philippines	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	3
37.46.38.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.183.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
188.120.154.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
124.105.53.102	Philippines	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.105.53.102	Philippines	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	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
124.105.53.102	Philippines	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
188.120.154.207	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.135.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.107.189.78	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.182.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	38
109.253.135.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.53.146.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
5.248.253.133	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
109.253.197.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/70005.doc	Block	1
106.120.173.76	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.219.160.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.166	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
67.19.79.218	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /robots.txt	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.124.7.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/15710.jpg	Block	1
98.207.46.126	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
149.50.98.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/main.asp	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/1/2801.jpg	Block	1
98.207.46.126	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1