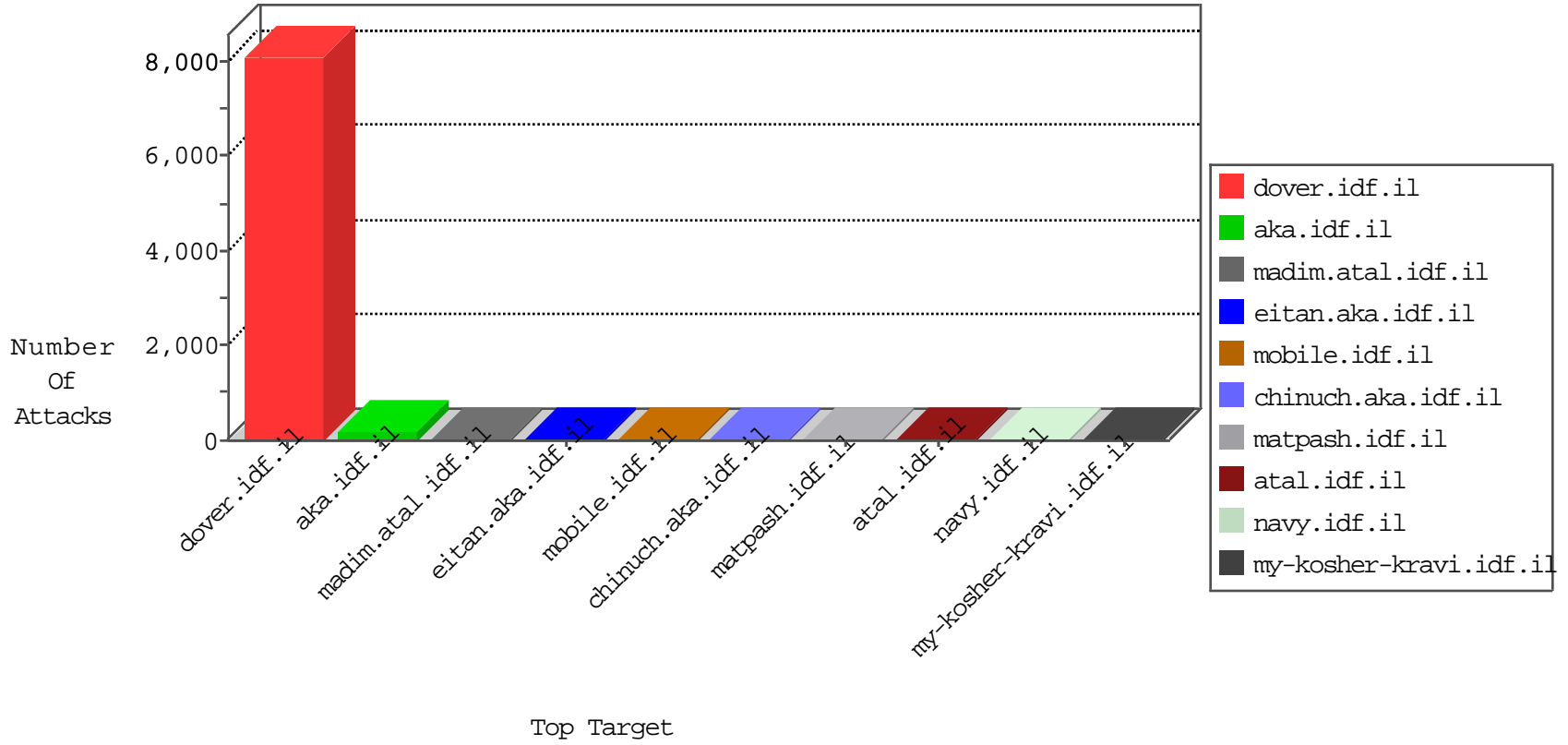


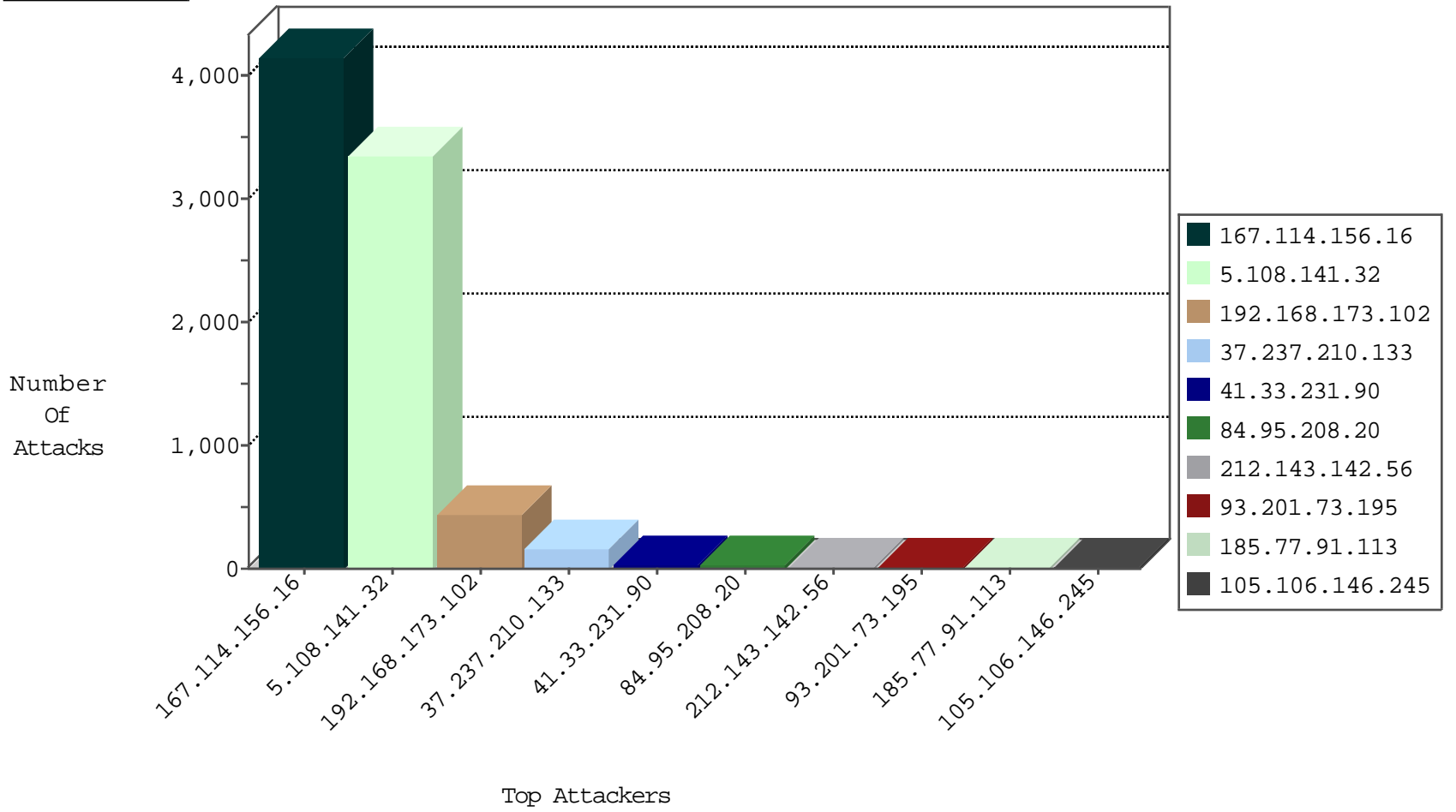
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4130
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	551
197.29.15.184	Tunisia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	415
37.237.210.133	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	118
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	2
184.105.247.242	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
93.201.73.195	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
93.201.73.195	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
93.201.73.195	Germany	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
93.201.73.195	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.201.73.195	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.238	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
93.201.73.195	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
93.201.73.195	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.54	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
122.117.115.27	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.108.132.58	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1637
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	1001
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	279
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	166
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	166
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.237.210.133	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	24
37.237.210.133	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.67.228.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
105.106.146.245	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.154	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.12.93	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
177.32.50.104	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
67.243.147.176	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
70.112.162.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
1.129.96.53	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.20	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
49.181.224.253	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.179.55.100	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.133.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.186.49.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.5	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.131.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.43	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
64.149.142.67	United States	147.237.76.86	navy.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
85.64.27.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.62.53.168	Russian Federation	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.77.91.113	Turkey	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
38.229.1.15	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.206	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.120	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.71.99.228	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.77.91.113	Turkey	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.146.185	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.8.80.15	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.170.111.152	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.77.91.113	Turkey	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.207	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
82.80.230.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	2
37.237.210.133	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
202.140.108.122	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
202.140.101.40	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
70.106.211.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
54.153.33.233	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
207.46.13.25	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	Block	1
202.140.101.45	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.6.146.185	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.66.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
202.140.108.63	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.78.17.175	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
217.160.63.130	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
70.85.16.6	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
202.140.108.64	Hong Kong	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
83.143.81.42	Norway	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/69687.pdf	Block	1
157.55.39.109	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
70.106.211.148	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1