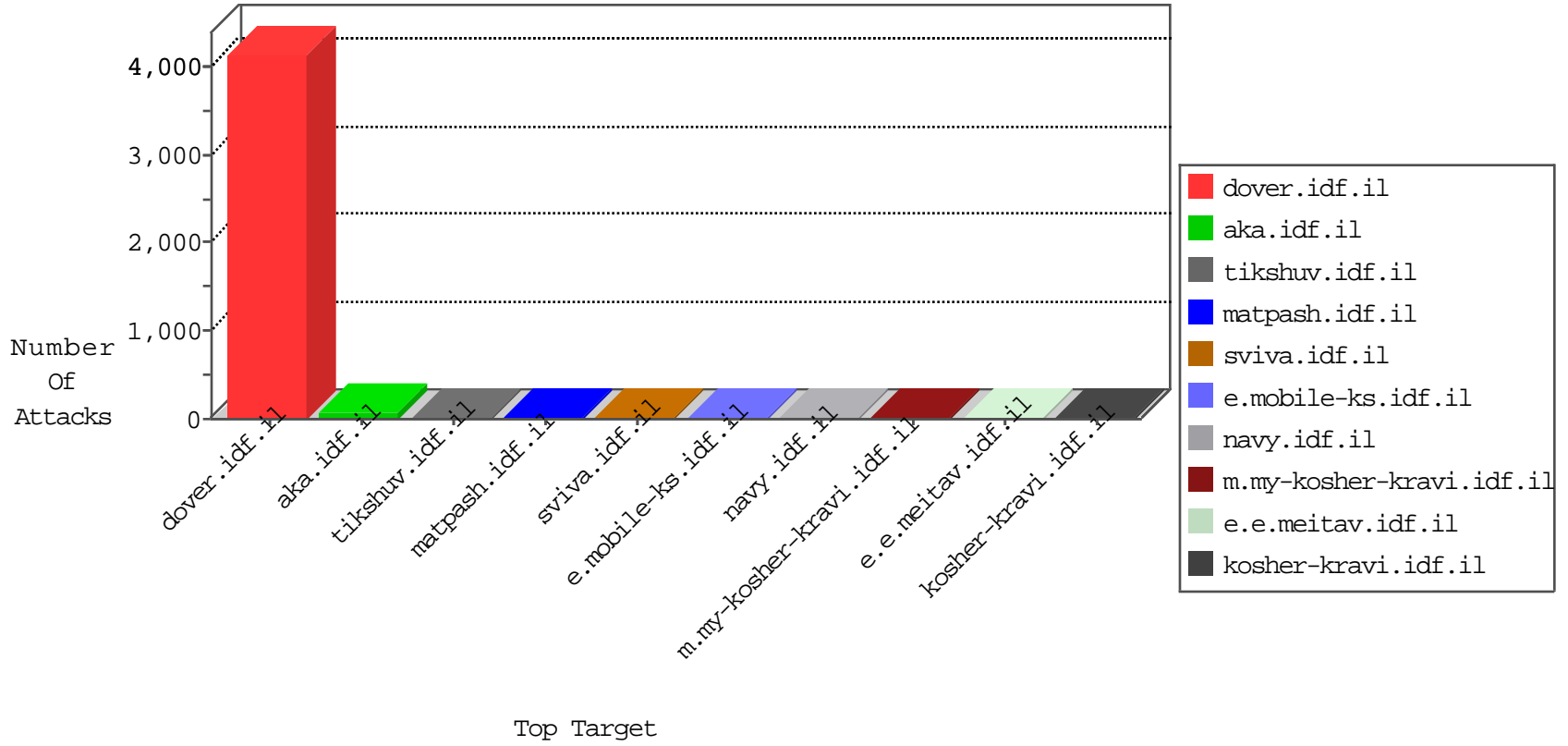




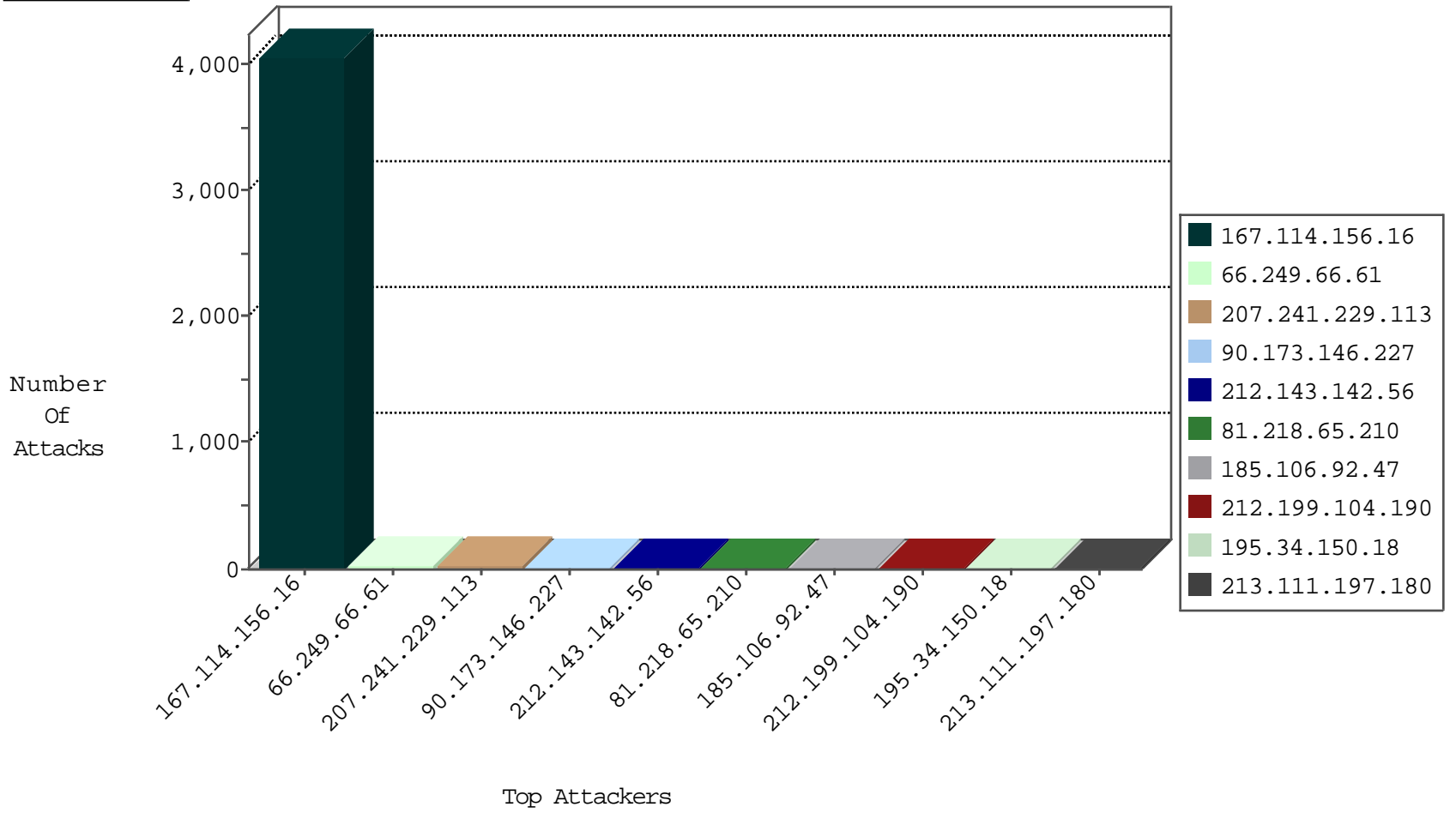
IDF Under Attack Daily Report



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	4064
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
185.94.111.1	Russian Federation	147.237.76.198	e.yohanan.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.31	United States	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	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
90.173.146.227	147.237.8.28	Spain	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
90.173.146.227	147.237.0.34	Spain	tikshuv.idf.il	ET SCAN Potential SSH Scan	3
41.78.73.30	147.237.77.235	Somalia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.47	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.47	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
124.106.101.188	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.218.60.60	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN NMAP -sS window 4096	1
90.173.146.227	147.237.0.19	Spain	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
41.78.73.30	147.237.77.235	Somalia	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
41.78.73.30	147.237.77.235	Somalia	sviva.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.63	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.47	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.47	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
122.117.61.154	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.184.2.29	147.237.76.30	Japan	himush.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.139	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
207.241.229.113	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	27
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.199.104.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
219.74.104.51	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
220.255.146.215	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.85.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
203.127.96.251	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.173.49.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
119.73.253.4	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.88.182.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.31	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
14.9.99.64	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.223	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.103	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.255.5.147	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
141.212.122.223	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
98.174.159.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.92	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.104	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.255.5.147	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.242.249.11	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.179.118.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.137.74.189	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.92	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.107	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.222	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.81.14.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.87	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.96	United States	147.237.0.35	akaws.idf.il	drop		drop	1
71.6.146.185	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.236	United States	147.237.76.148	ggpenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.222	United States	147.237.76.86	navy.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
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/nav.css	Block	1
213.111.197.180	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.111.197.180	Block	1
71.6.146.185	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
220.255.199.100	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
213.111.197.180	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-he/shared/usercontrols/headerupper/	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
203.127.96.213	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.111.197.180	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
93.172.149.126	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
207.46.13.53	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/contactus.aspx	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/npm/	Block	1
46.19.85.0	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
216.218.206.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.111.197.180	Ukraine	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
220.255.146.134	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.23	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9739-he/refuah.aspx	Block	1