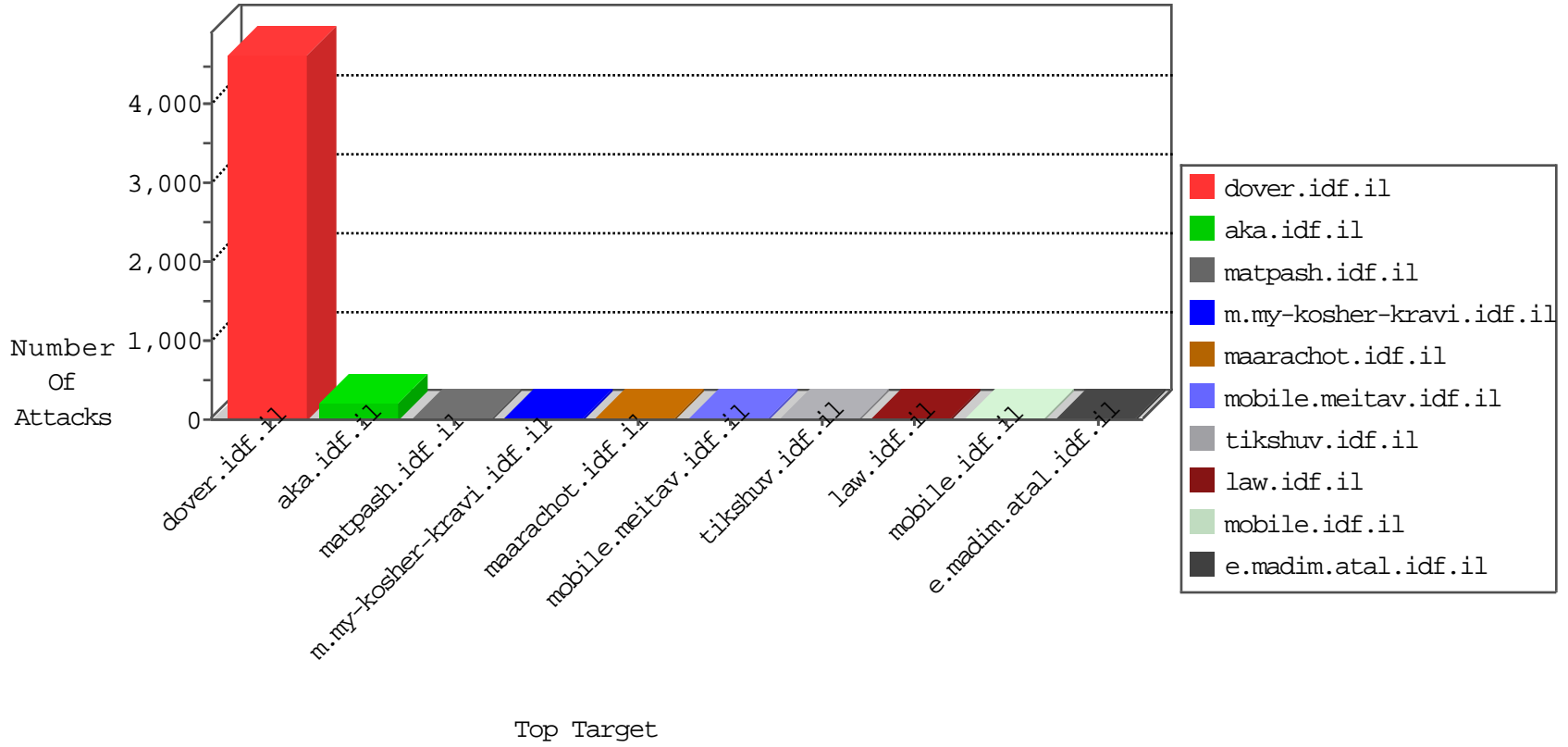




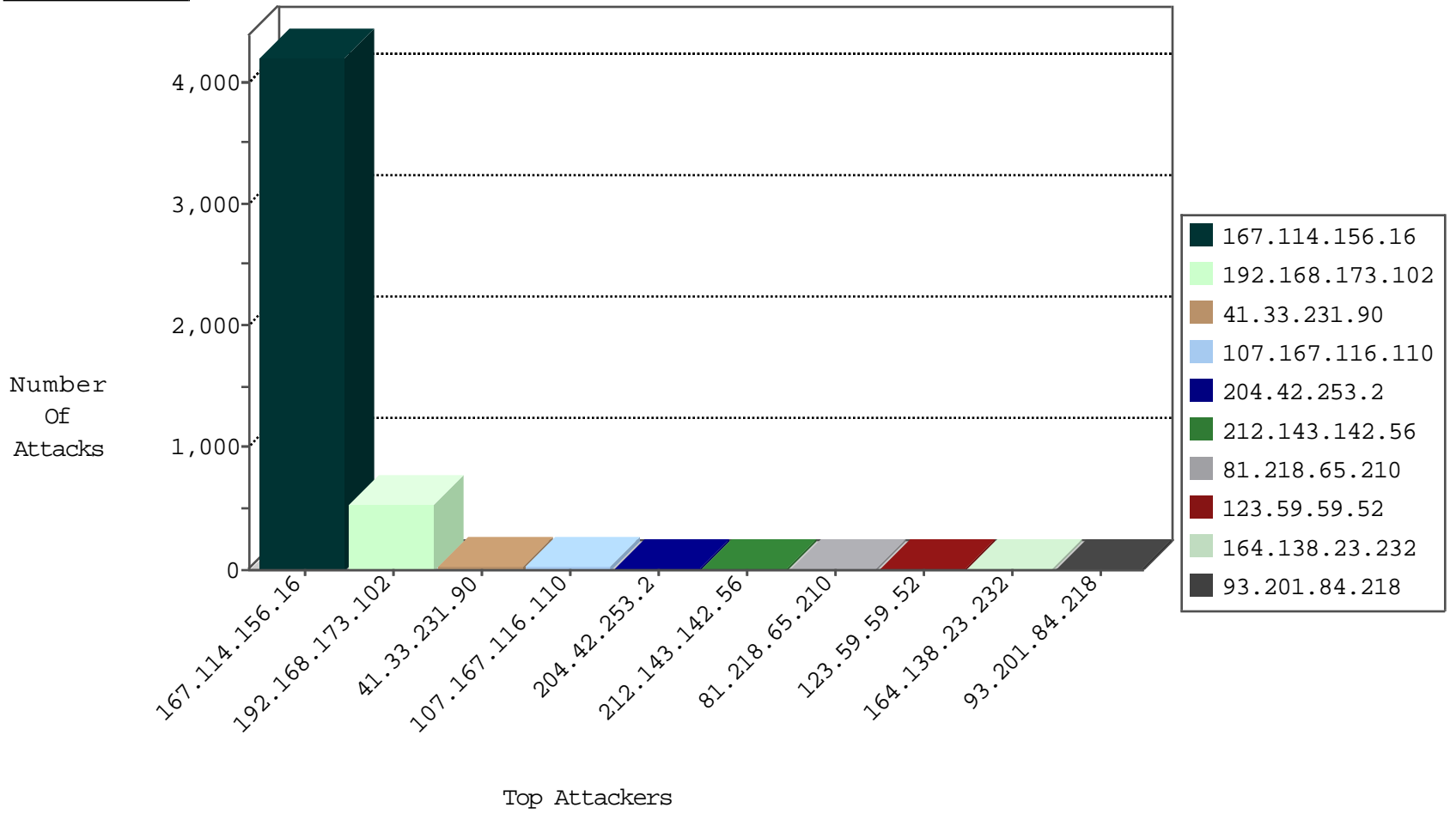
IDF Under Attack Daily Report



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	4194
123.59.59.52	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
185.70.184.164	Netherlands	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
93.201.84.218	Germany	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
93.201.84.218	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.201.84.218	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
93.201.84.218	Germany	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-04:04:04 to 04-08-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	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
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
210.44.52.150	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
179.43.144.37	147.237.0.17	Switzerland	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.240.213.93	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
119.195.228.221	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.113	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.205	United States	prisha.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
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	337
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	203
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
107.167.116.110	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
121.54.54.61	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.111	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.4.189.77	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.88.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
204.155.30.109	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
195.88.209.6	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.114	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
98.252.230.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.60	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.47	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
64.231.205.119	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.99	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.236	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.164	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.60	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.47	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.103	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.222.103.234	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
199.87.154.251	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.24	United States	147.237.0.33	idf.il	drop		drop	1
185.11.180.67	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
41.107.8.89	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.165	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.84.157	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
65.19.167.131	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
180.76.15.12	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
5.22.131.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.104	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
98.25.150.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.27	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.106.92.47	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
41.176.207.10	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.240.213.93	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
184.105.139.84	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.4.189.77	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.113	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
98.252.230.244	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
154.120.73.31	Nigeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/klali.aspx	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
154.120.73.31	Nigeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.140	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
123.59.59.52	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.qyer.com/1149-he/lifestyle.aspx	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
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.178	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/17012011masaiyot.aspx	Block	1
154.120.73.31	Nigeria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.163	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
157.55.39.241	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.88.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
154.120.73.31	Nigeria	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.88.101	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1