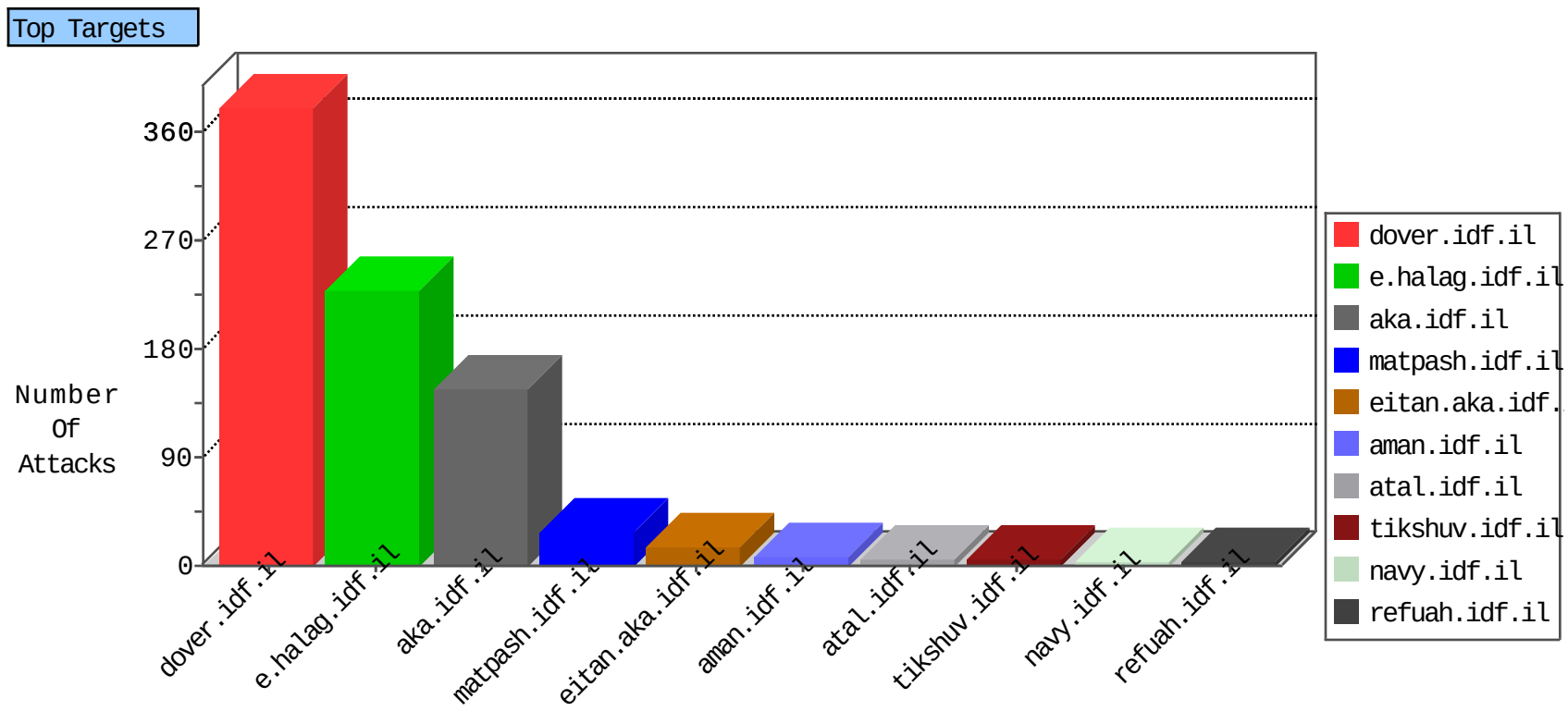
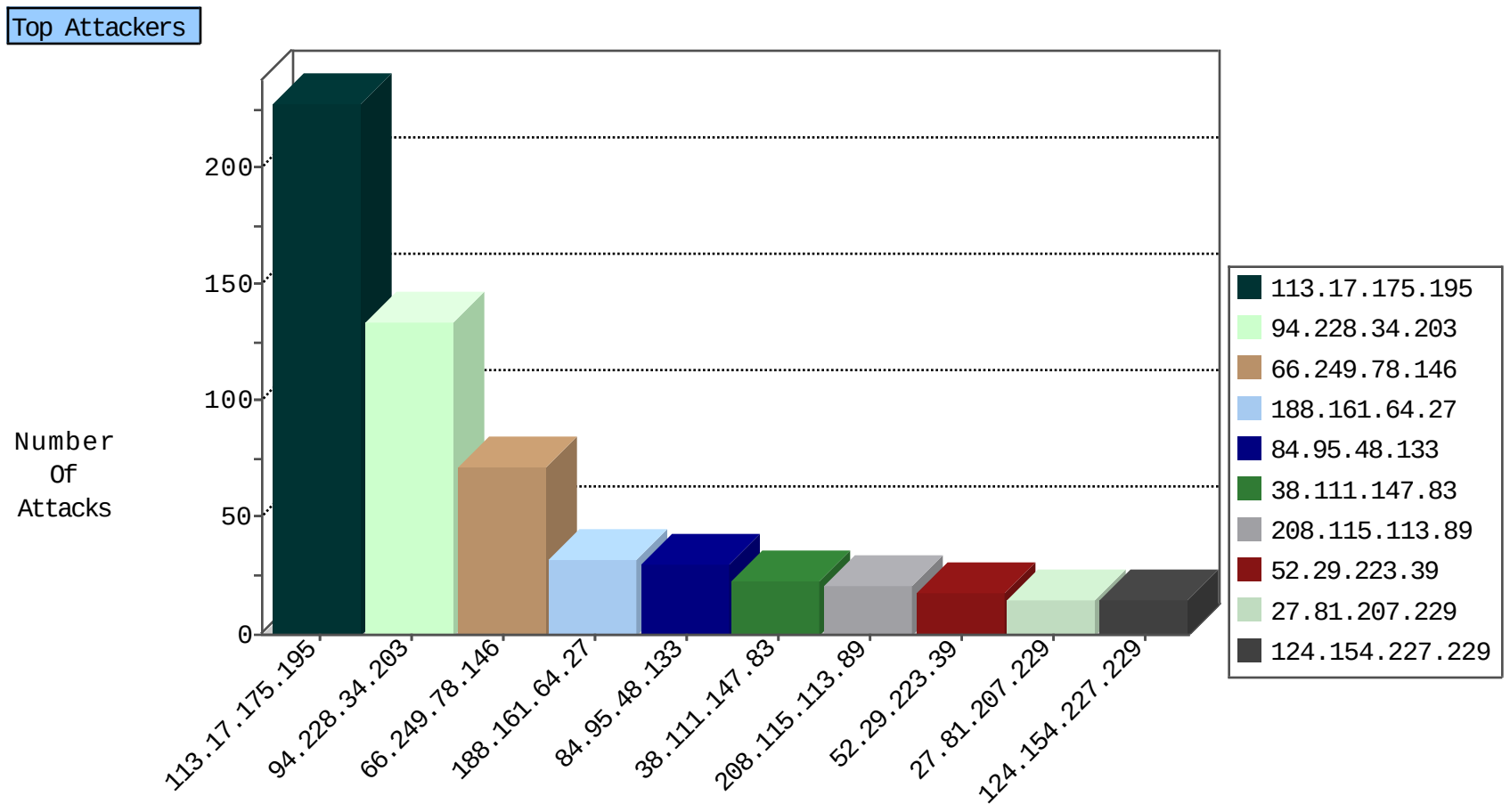
04-25-2016-05:04:06 to 04-25-2016-06:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-05:04:06 to 04-25-2016-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	228
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
188.138.17.205	France	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
205.251.197.151	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
5.196.72.168	France	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
5.196.72.168	France	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

04-25-2016-05:04:06 to 04-25-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-05:04:06 to 04-25-2016-06:04:06

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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
5.196.199.232	147.237.76.30	France	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.201	Lithuania	e.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.43	147.237.77.205	Switzerland	prisha.idf.il	ET SCAN Potential SSH Scan	1
98.126.212.154	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.126.212.154	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.198	Lithuania	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
179.43.144.43	147.237.77.226	Switzerland	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
101.99.28.51	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
98.126.212.154	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
98.126.212.154	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
195.154.54.169	147.237.8.24	France	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2016-05:04:06 to 04-25-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.203	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
84.95.48.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
188.161.64.27	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
38.111.147.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
27.81.207.229	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
188.161.64.27	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
67.239.39.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
124.154.227.229	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.2.186	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.71.70.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
108.242.228.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.29.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.200.66.222	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.151	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
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.154.227.229	Japan	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.158.152.52	Russian Federation	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
68.180.231.43	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
73.36.242.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.39.222.159	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.101.67.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.167	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.128	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.222.159	Netherlands	147.237.76.147	chinuch.aka.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
74.125.182.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.137	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-25-2016-05:04:06 to 04-25-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	7
38.111.147.83	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 38.111.147.83	Block	4
31.204.128.94	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 31.204.128.94	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
157.55.39.118	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/portalmiluim/templates/www.behazdaa.org.il	Block	1
79.180.20.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/default.aspx	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
125.26.37.108	Thailand	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/	Block	1
38.111.147.83	United States	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 38.111.147.83	Block	1
180.76.15.142	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
81.171.81.118	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
31.204.128.94	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
66.249.79.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
58.7.246.183	Australia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.7.246.183	Block	1
208.115.111.71	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2.htm	Block	1
81.171.81.118	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in www.tikshuv.idf.il/site/general.aspx	Block	1
38.111.147.83	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/shared/usercontrols/headerupper/	Block	1
141.212.122.129	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
66.249.89.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
58.7.246.183	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ reserver	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
141.212.122.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /x	Block	1
64.9.58.217	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
125.26.37.108	Thailand	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1

04-25-2016-05:04:06 to 04-25-2016-06:04:06