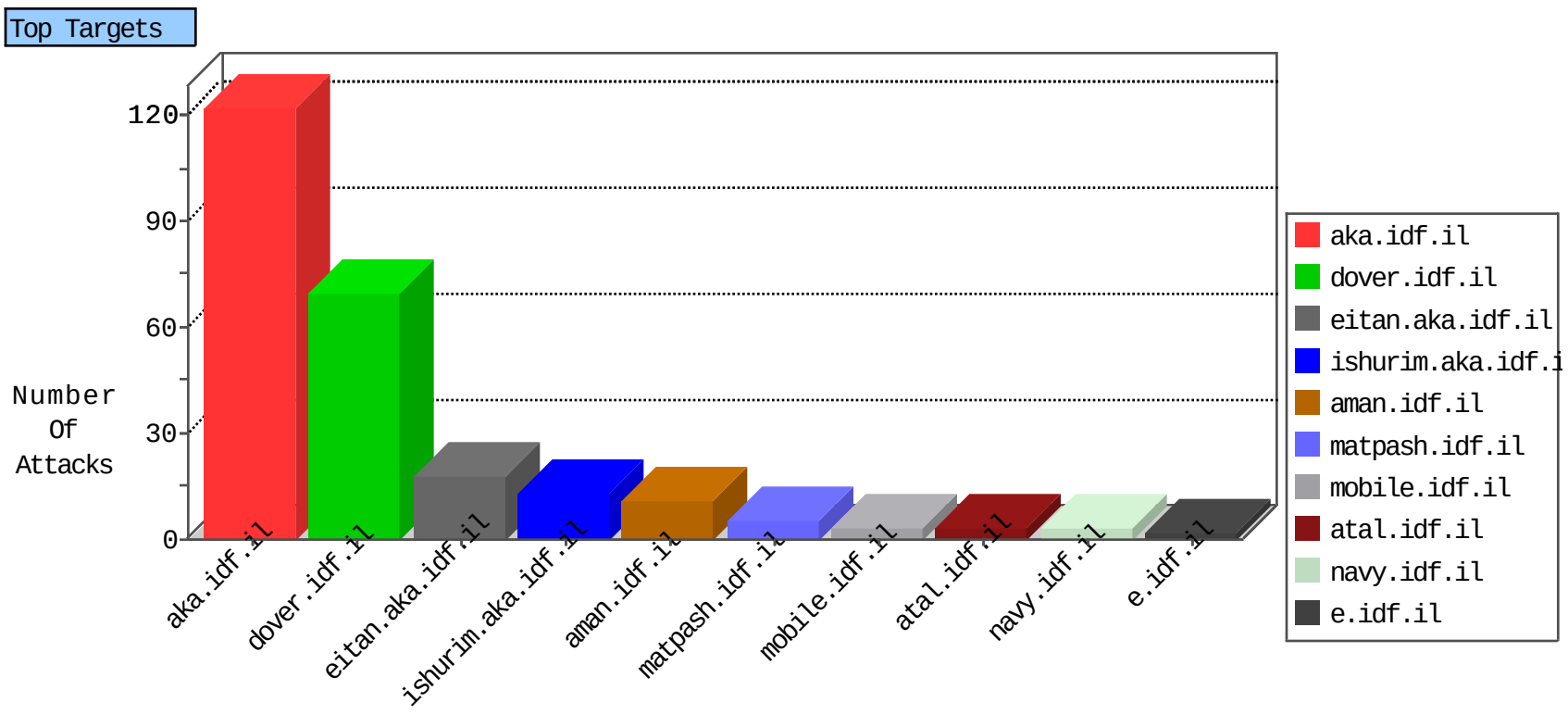
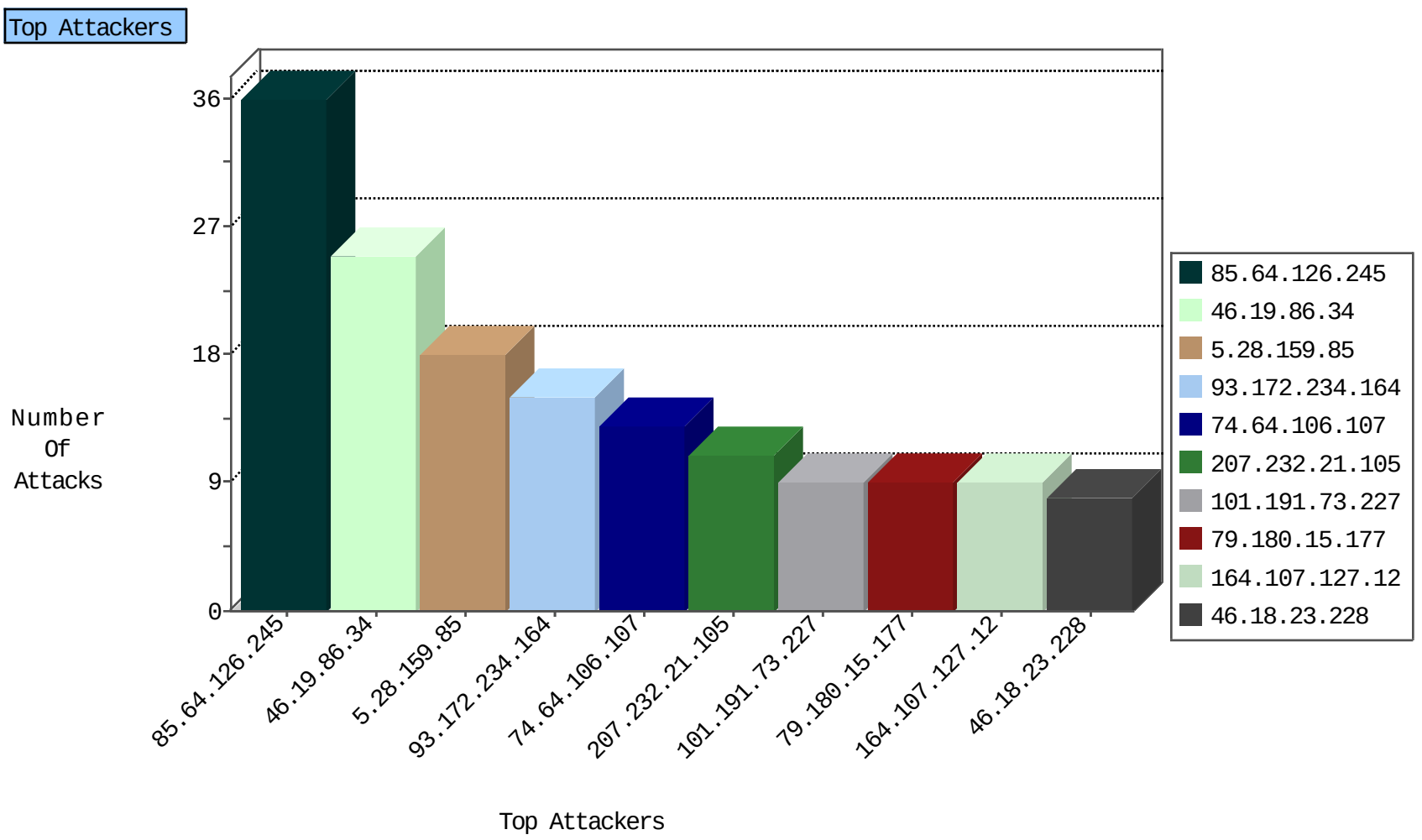
09-17-2016-02:04:08 to 09-17-2016-03:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-17-2016-02:04:08 to 09-17-2016-03:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	9
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-02:04:08 to 09-17-2016-03:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.157.151.57	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	2

09-17-2016-02:04:08 to 09-17-2016-03:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.0.21.98	147.237.76.86	Colombia	navy.idf.il	ET SCAN NMAP -sS window 3072	1
133.242.4.52	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
121.141.225.10	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.2.213.159	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.223.81.8	147.237.77.216	Bolivia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
161.18.12.66	147.237.77.212	Colombia	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
133.208.21.66	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
121.141.225.10	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.141.225.10	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.69.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

09-17-2016-02:04:08 to 09-17-2016-03:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.28.159.85	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
74.64.106.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
85.64.126.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
46.19.86.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
207.232.21.105	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
101.191.73.227	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
85.64.126.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.64.126.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.64.126.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.48	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.126.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.15.177	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
5.102.203.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.34	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
93.172.234.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
93.172.234.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
93.172.234.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.18.23.228	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.18.23.228	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.8.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.128.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.147.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
77.237.138.202	Czech Republic	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.102.195.83	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
80.246.137.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
71.6.158.166	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
221.181.73.62	China	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.180.15.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.186.113.169	Japan	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
156.212.71.48	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
79.180.15.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
221.181.73.62	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
107.150.53.122	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.62.53.168	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
79.180.15.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.181.73.62	China	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
80.246.137.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.181.73.62	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-17-2016-02:04:08 to 09-17-2016-03:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.21.105	Israel	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.e.lc4.gov.il/	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
157.55.39.21	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
50.35.76.135	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
157.55.39.76	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.85.131.80	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to www.e.lc4.gov.il/favicon.ico	Block	1
77.139.143.38	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
180.76.15.8	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
180.76.15.158	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
2.55.128.123	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1

09-17-2016-02:04:08 to 09-17-2016-03:04:08