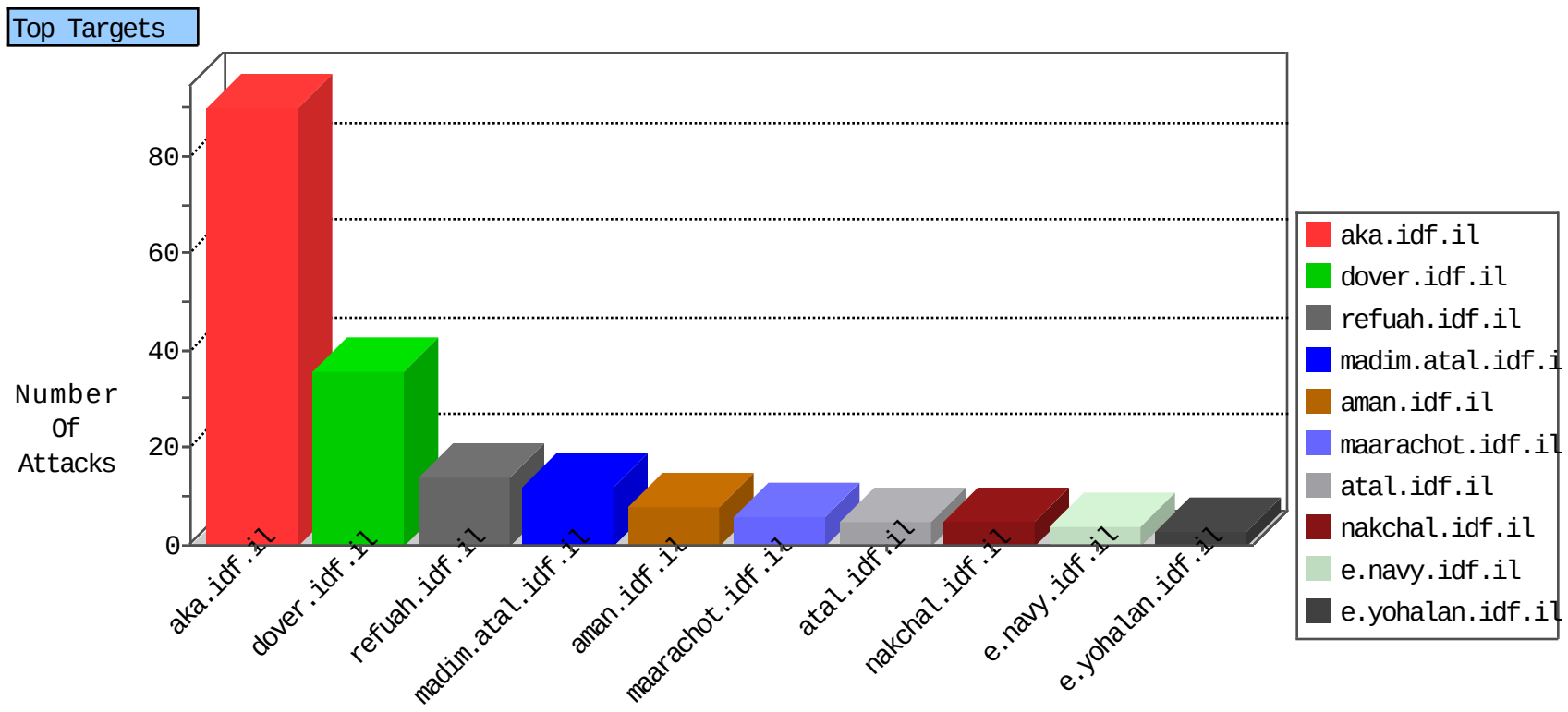
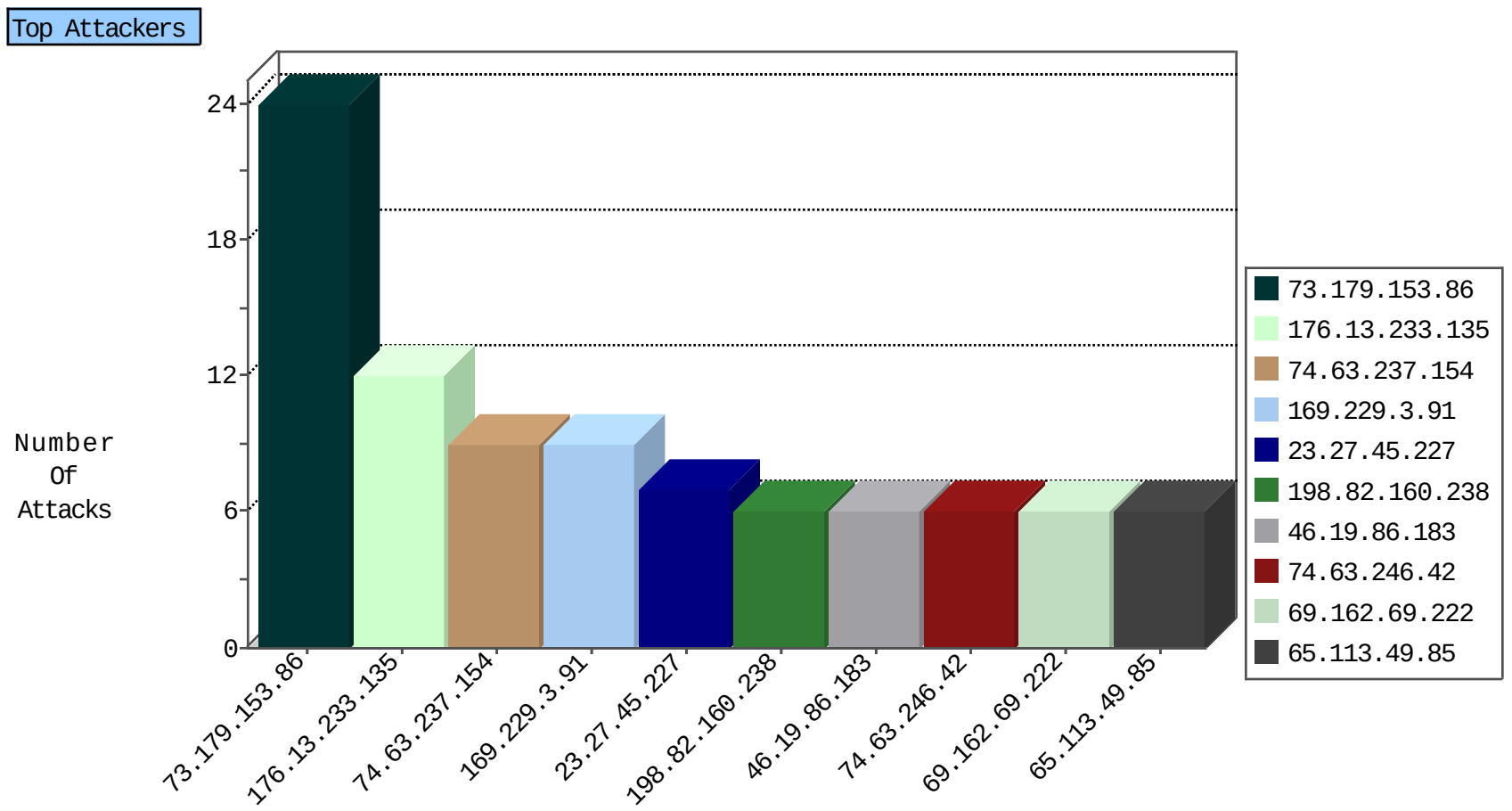
09-20-2016-01:09:39 to 09-20-2016-02:09:39

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-20-2016-01:09:39 to 09-20-2016-02:09:39

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.29.178.14	Poland	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
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	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
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.208.4.197	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	2
129.22.150.78	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	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
141.22.213.35	Germany	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.167	ishurim.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
216.48.80.12	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
202.4.2.148	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.167	ishurim.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
202.4.4.147	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-20-2016-01:09:39 to 09-20-2016-02:09:39

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-20-2016-01:09:39 to 09-20-2016-02:09:39

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
74.63.246.42	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.237.154	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
69.162.69.222	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.254.234	147.237.76.200	Singapore	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.46.36.168	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.246.42	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
74.63.237.154	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.237.111.200	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-20-2016-01:09:39 to 09-20-2016-02:09:39

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
73.179.153.86	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
73.179.153.86	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.86.183	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
23.27.45.227	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
65.113.49.85	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
65.113.49.85	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.36	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.120.93.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
172.56.7.73	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.36	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
69.162.69.222	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.63	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.237.111.200	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.63.246.42	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
138.246.253.19	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.4.120.149	Germany	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
106.186.113.169	Japan	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.158.94	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.237.154	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.162.69.222	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
109.237.111.200	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1
46.4.85.112	Germany	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.246.42	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.237.154	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
141.212.122.48	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
108.29.132.251	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
5.86.3.31	Italy	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
74.63.237.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
173.35.169.75	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
69.162.69.222	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.222.60	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.4.85.112	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.63.246.42	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.63.237.154	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.54	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
108.29.132.251	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.86.3.31	Italy	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.63.237.154	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
199.212.66.27	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
69.162.69.222	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-20-2016-01:09:39 to 09-20-2016-02:09:39

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.233.135	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	12
23.27.45.227	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	2
176.13.233.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
217.132.63.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.87.238	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.108.87.238	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
181.215.98.148	United States	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
69.116.75.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
87.69.179.197	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
181.215.98.148	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/wp/wp-login.php	Block	1
73.7.32.83	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.50	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.46.13.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
79.180.54.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 127.0.0.1/callback.json	Block	1

09-20-2016-01:09:39 to 09-20-2016-02:09:39