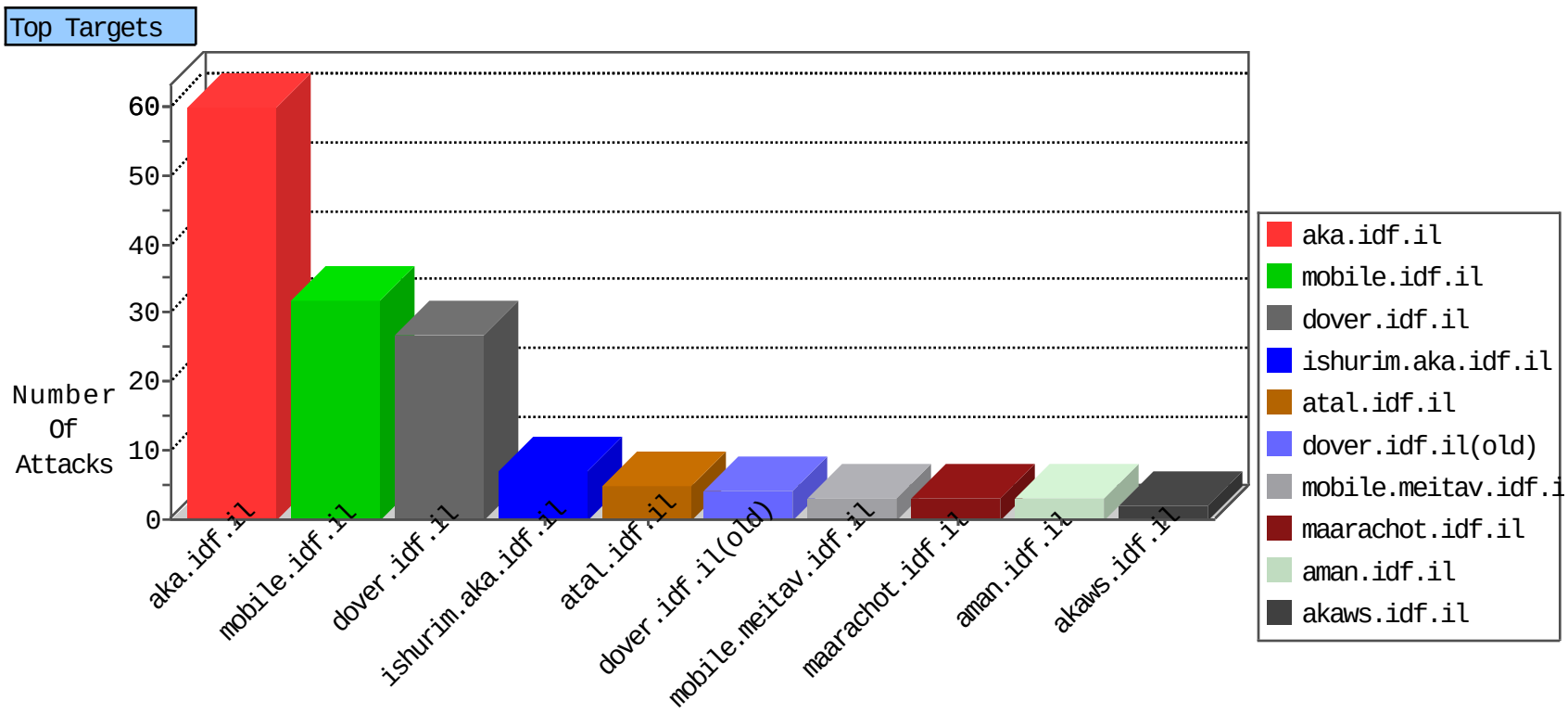
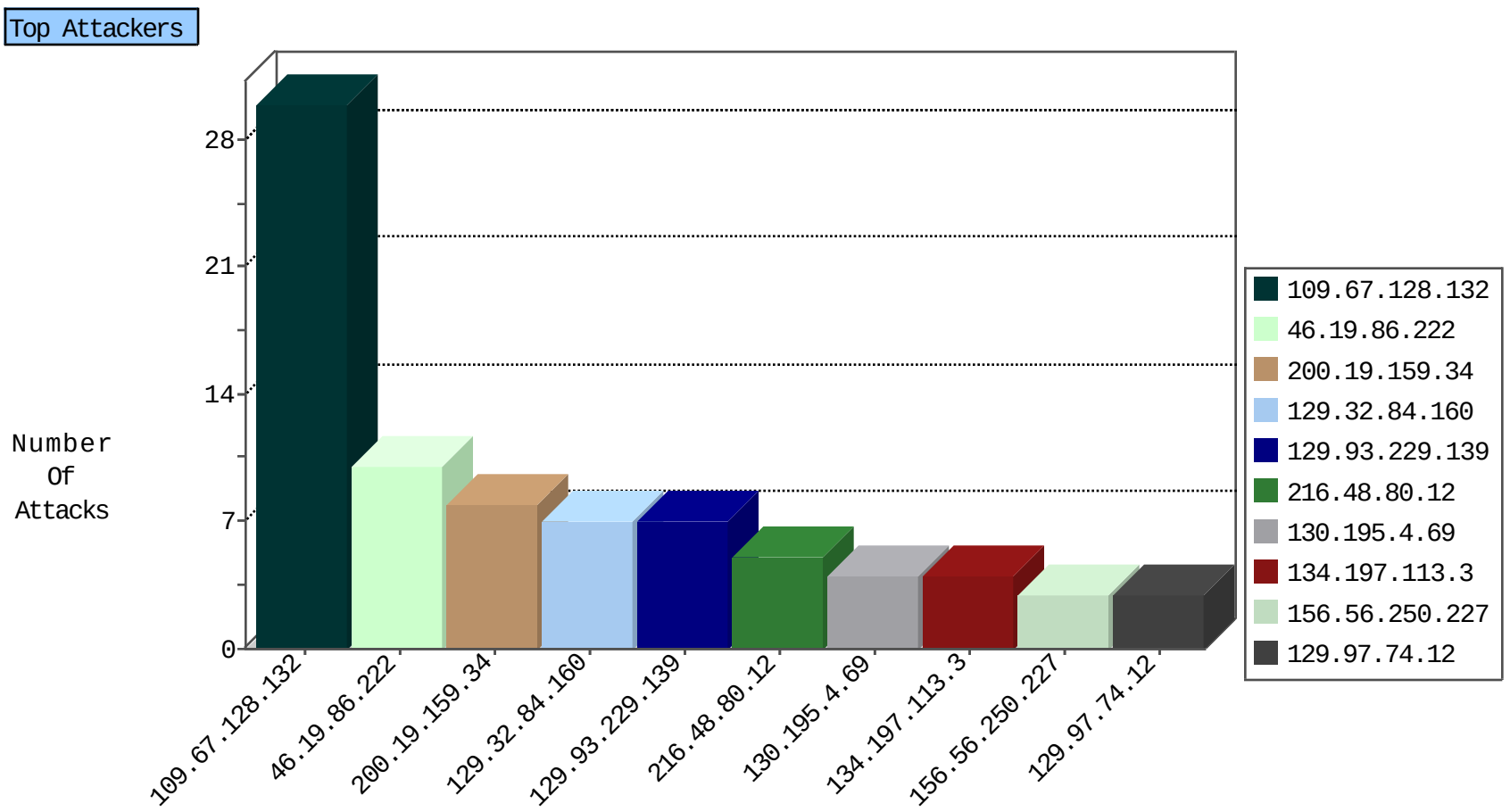
09-17-2016-07:04:01 to 09-17-2016-08:04:01

IDF Under Attack Daily Report





09-17-2016-07:04:01 to 09-17-2016-08:04:01

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	8
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.32.84.160	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	4
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
165.242.90.128	Japan	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
156.56.250.227	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	3
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	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
216.48.80.12	Canada	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.167	ishurim.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
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-17-2016-07:04:01 to 09-17-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-17-2016-07:04:01 to 09-17-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.7.217.235	147.237.72.156	Brazil	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
128.127.0.45	147.237.76.39	Italy	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.76.148	Russian Federation	gqcenter.aka.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
202.155.58.28	147.237.8.46	Indonesia	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.39	Italy	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
128.127.0.45	147.237.76.39	Italy	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-17-2016-07:04:01 to 09-17-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.67.128.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
172.58.201.124	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
71.236.178.153	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.9.151.22	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.85.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
217.132.108.84	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.218.12	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.138.43.160	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
184.105.247.227	United States	147.237.8.24	e.lifestyle.idf.	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.17	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.244	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.70.30.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.82	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.18	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.28	United States	147.237.76.176	test.ncore.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
172.58.184.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.138.43.160	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
120.132.84.59	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-17-2016-07:04:01 to 09-17-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.65.96	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
66.249.64.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
109.253.218.12	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
73.5.123.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
66.249.64.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	1
157.55.39.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.30	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1

09-17-2016-07:04:01 to 09-17-2016-08:04:01