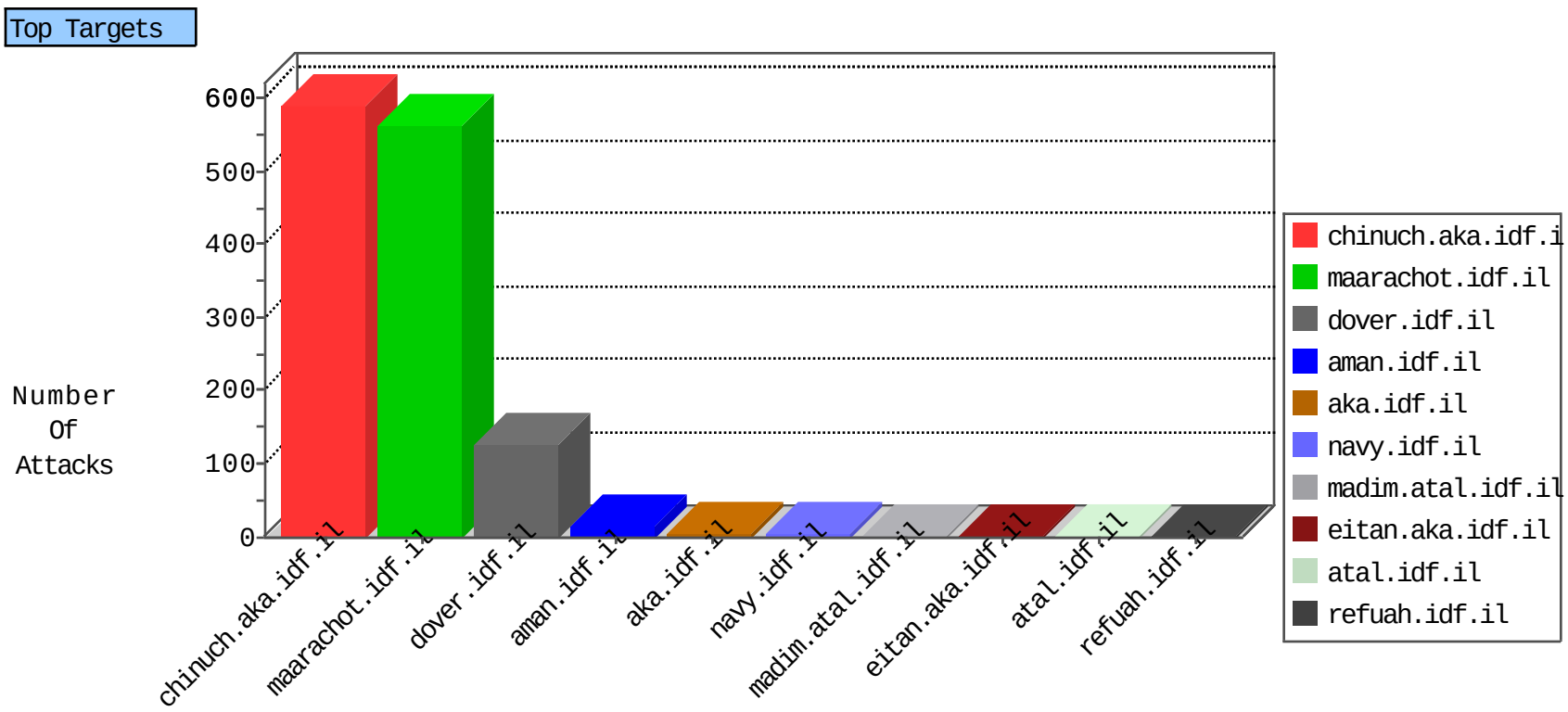
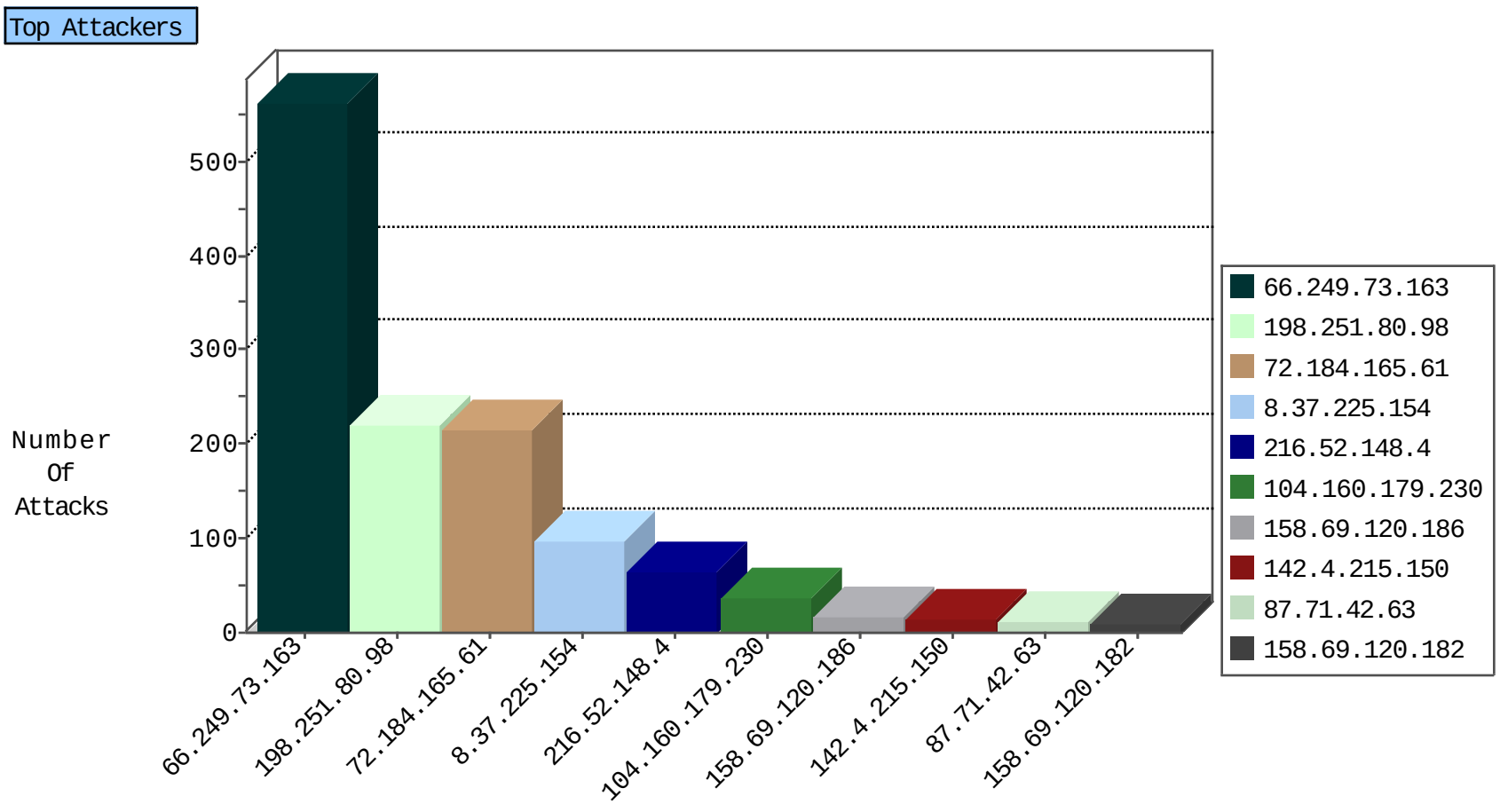
09-24-2016-07:04:08 to 09-24-2016-08:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-07:04:08 to 09-24-2016-08:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.231.197	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
204.12.220.86	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
204.12.220.85	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
63.141.242.194	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
185.128.40.162	Switzerland	147.237.76.30	himush.idf.il	Black List	drop	1
63.141.242.196	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
198.204.224.234	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
142.54.174.86	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	1

09-24-2016-07:04:08 to 09-24-2016-08:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-24-2016-07:04:08 to 09-24-2016-08:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	563
192.223.94.108	147.237.76.147	Bolivia	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
179.43.141.221	147.237.77.179	Switzerland	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
121.46.101.38	147.237.72.14	India	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.158	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.103	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
185.153.198.10	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
111.227.111.94	147.237.77.212	China	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.172.103	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.161.40.17	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

09-24-2016-07:04:08 to 09-24-2016-08:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
72.184.165.61	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	215
8.37.225.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	50
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	49
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	46
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	38
216.52.148.4	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	36
216.52.148.4	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	28
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
108.31.120.41	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	4
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
79.180.6.32	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
158.69.120.186	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
158.69.120.182	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.99.160.125	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
158.69.120.182	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
46.19.86.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
158.69.22.223	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.209.105.220	Cyprus	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.132.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
158.69.120.182	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
104.160.179.230	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
192.99.160.125	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.93.206.21	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.53	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.42	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
158.69.22.223	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
128.232.110.28	United Kingdom	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
141.212.122.53	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
158.69.120.182	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
142.4.215.150	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
192.99.160.125	Canada	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
158.69.22.223	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
184.105.139.92	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-24-2016-07:04:08 to 09-24-2016-08:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.42.63	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
85.250.109.150	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
89.237.75.254	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.237.75.254	Block	2
2.53.163.104	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
186.125.42.245	Argentina	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus ingles	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
89.237.75.254	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
115.28.28.62	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
85.250.190.153	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
115.28.28.62	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8746-he/refuah.aspx	Block	1
157.55.39.65	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1

09-24-2016-07:04:08 to 09-24-2016-08:04:08