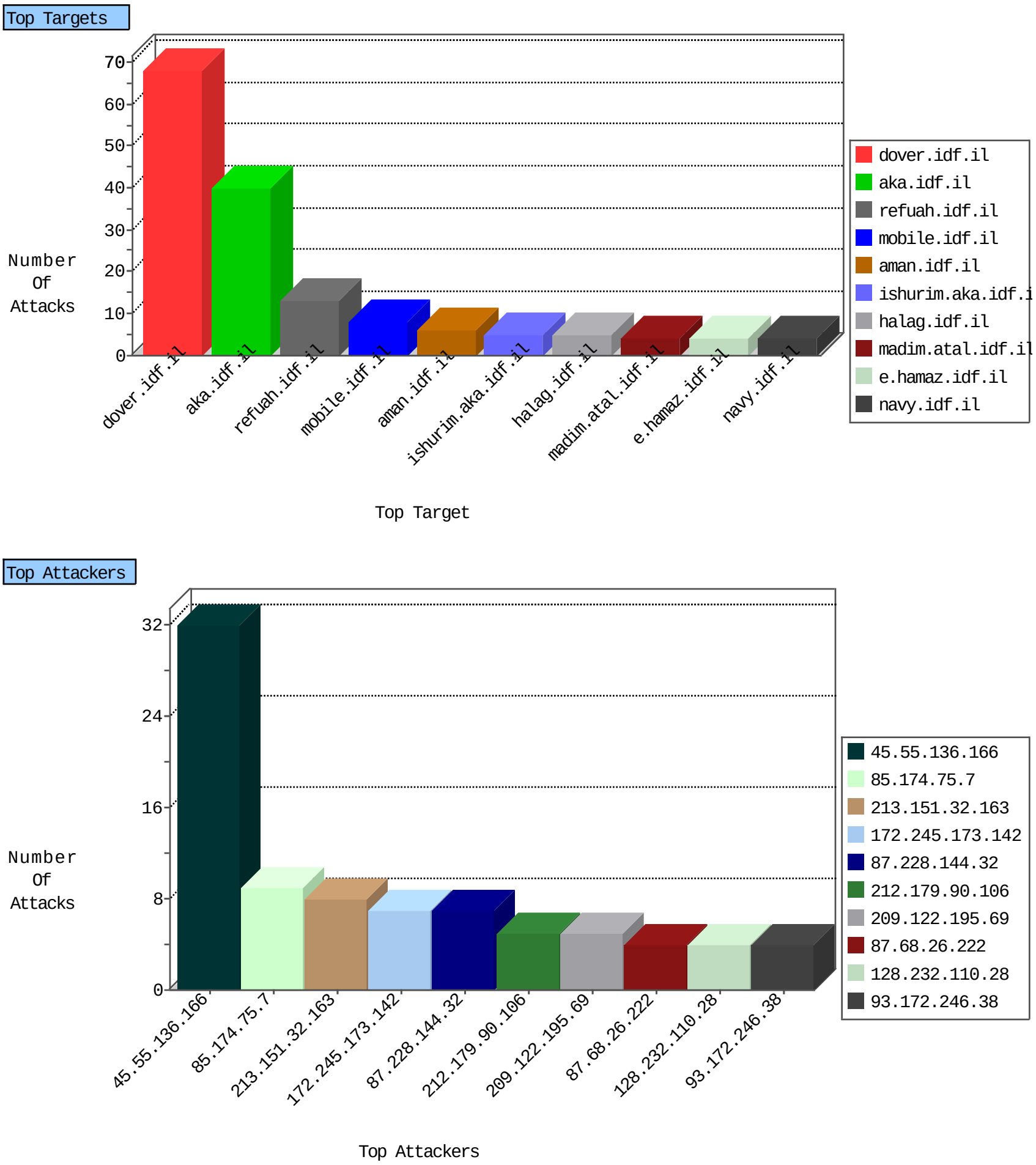
09-14-2016-05:04:09 to 09-14-2016-06:04:09

IDF Under Attack
Daily Report



09-14-2016-05:04:09 to 09-14-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.138	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	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.68	Switzerland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	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
128.42.142.45	United States	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
160.80.221.39	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-05:04:09 to 09-14-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.44.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
185.38.14.215	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-14-2016-05:04:09 to 09-14-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.174.75.7	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	2
52.166.249.197	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
85.174.75.7	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.174.75.7	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
85.174.75.7	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
52.166.249.197	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
189.161.173.106	147.237.0.19	Mexico	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.0.253	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
172.245.173.142	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.174.75.7	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
85.174.75.7	147.237.8.27	Russian Federation	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.174.75.7	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
67.211.219.120	147.237.76.176	United States	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
52.166.249.197	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

09-14-2016-05:04:09 to 09-14-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.55.136.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
209.122.195.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.228.144.32	Cyprus	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
49.151.29.140	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.172.246.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
87.68.26.222	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
209.66.119.150	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
87.68.26.222	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.228.167.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.225.162.149	Ukraine	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.33.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.172.246.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
87.228.144.32	Cyprus	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.140.0.23	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
168.1.128.61	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.210.187.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.226.113.7	Germany	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
194.153.113.13	Germany	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
172.245.173.142	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
50.116.3.158	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
128.232.110.28	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
184.105.247.235	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.245.173.142	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
98.231.98.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.228.144.32	Cyprus	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
172.245.173.142	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
69.116.196.213	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.113	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
89.248.174.4	Netherlands	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
184.105.247.243	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.245.173.142	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.169	Japan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
88.57.44.81	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.127.12.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.114	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.27.106.241	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
87.228.144.32	Cyprus	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
172.245.173.142	United States	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-14-2016-05:04:09 to 09-14-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.202	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
99.253.201.44	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
194.153.113.13	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
115.28.28.62	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
204.79.180.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	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
68.180.229.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
157.55.39.19	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
84.229.68.6	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1

09-14-2016-05:04:09 to 09-14-2016-06:04:09