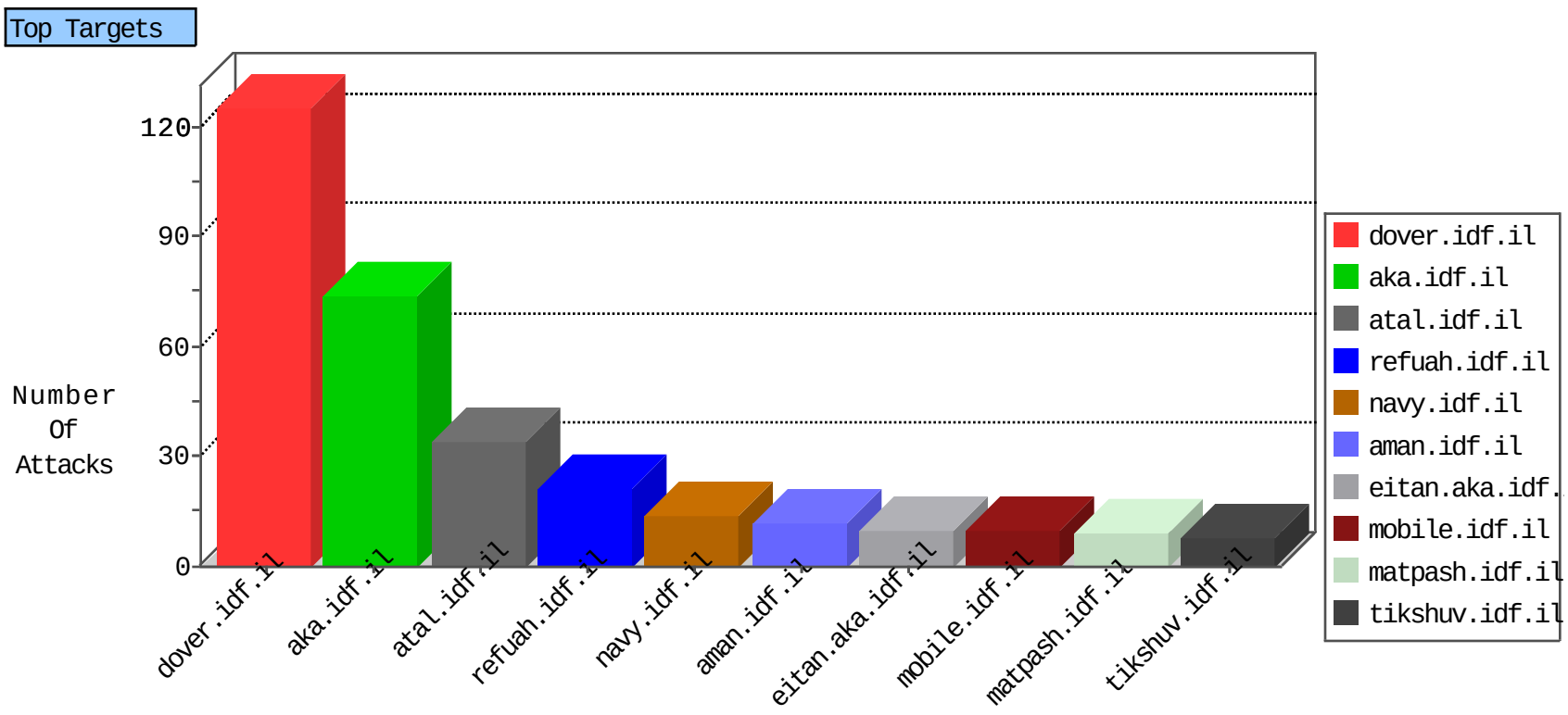
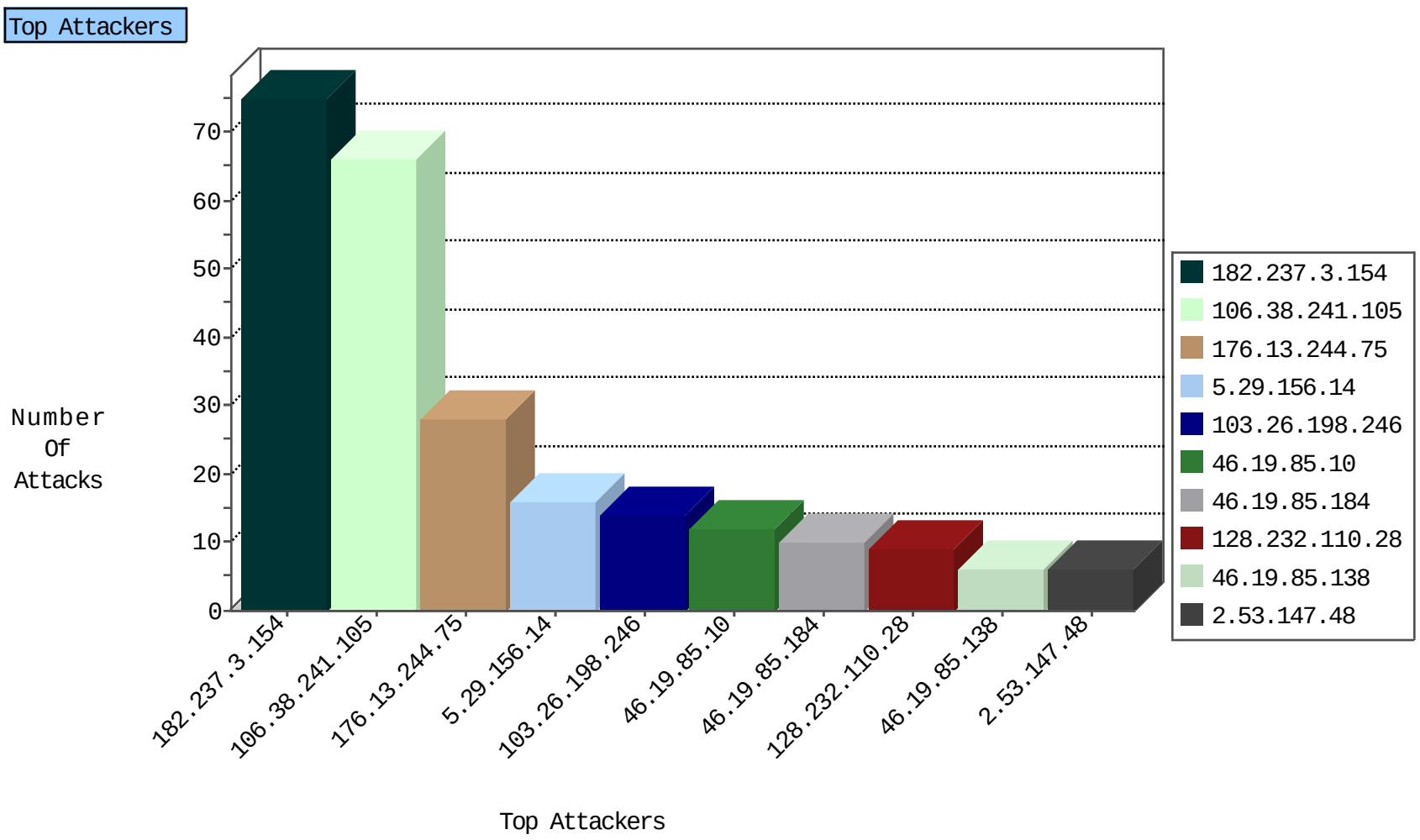
09-16-2016-07:04:01 to 09-16-2016-08:04:01

IDF Under Attack Daily Report





09-16-2016-07:04:01 to 09-16-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.29.178.14	Poland	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	4
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
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
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	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
131.247.2.241	United States	147.237.72.217	e.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
164.107.127.12	United States	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
165.242.90.129	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	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
192.33.90.67	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.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

09-16-2016-07:04:01 to 09-16-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-16-2016-07:04:01 to 09-16-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.58.102.178	147.237.8.14	United Kingdom	e.orchot.idf.il	GPL SCAN superscan echo	4
193.201.225.73	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.23.181.171	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.193.252.231	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
66.212.179.106	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.185.138	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.185.138	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
193.23.181.171	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.23.181.171	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
66.212.179.106	147.237.77.243	Canada	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
40.84.185.138	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1

09-16-2016-07:04:01 to 09-16-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
182.237.3.154	Hong Kong	147.237.77.216	dover.idf.il	drop	SAM rule	drop	74
176.13.244.75	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	8
46.19.85.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	7
103.26.198.246	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
106.38.241.105	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	6
5.29.156.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
103.26.198.246	Malaysia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
106.38.241.105	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
2.53.147.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	5
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	5
106.38.241.105	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.166.112	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.60.246	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.244.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.29.156.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.156.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
103.47.14.226	India	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.244.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.29.156.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
87.70.55.128	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
103.26.198.246	Malaysia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
87.70.55.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
122.173.44.48	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.236	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.46.41.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.129.20	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.67.49.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
199.241.27.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.8.73.217	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.104	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-16-2016-07:04:01 to 09-16-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.80.155.222	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
213.57.87.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.192	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.	Block	1
40.77.167.81	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
79.181.125.23	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
79.181.125.23	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.181.125.23	Block	1
73.109.70.161	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	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
5.28.178.70	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
76.167.225.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
5.39.85.81	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1

09-16-2016-07:04:01 to 09-16-2016-08:04:01