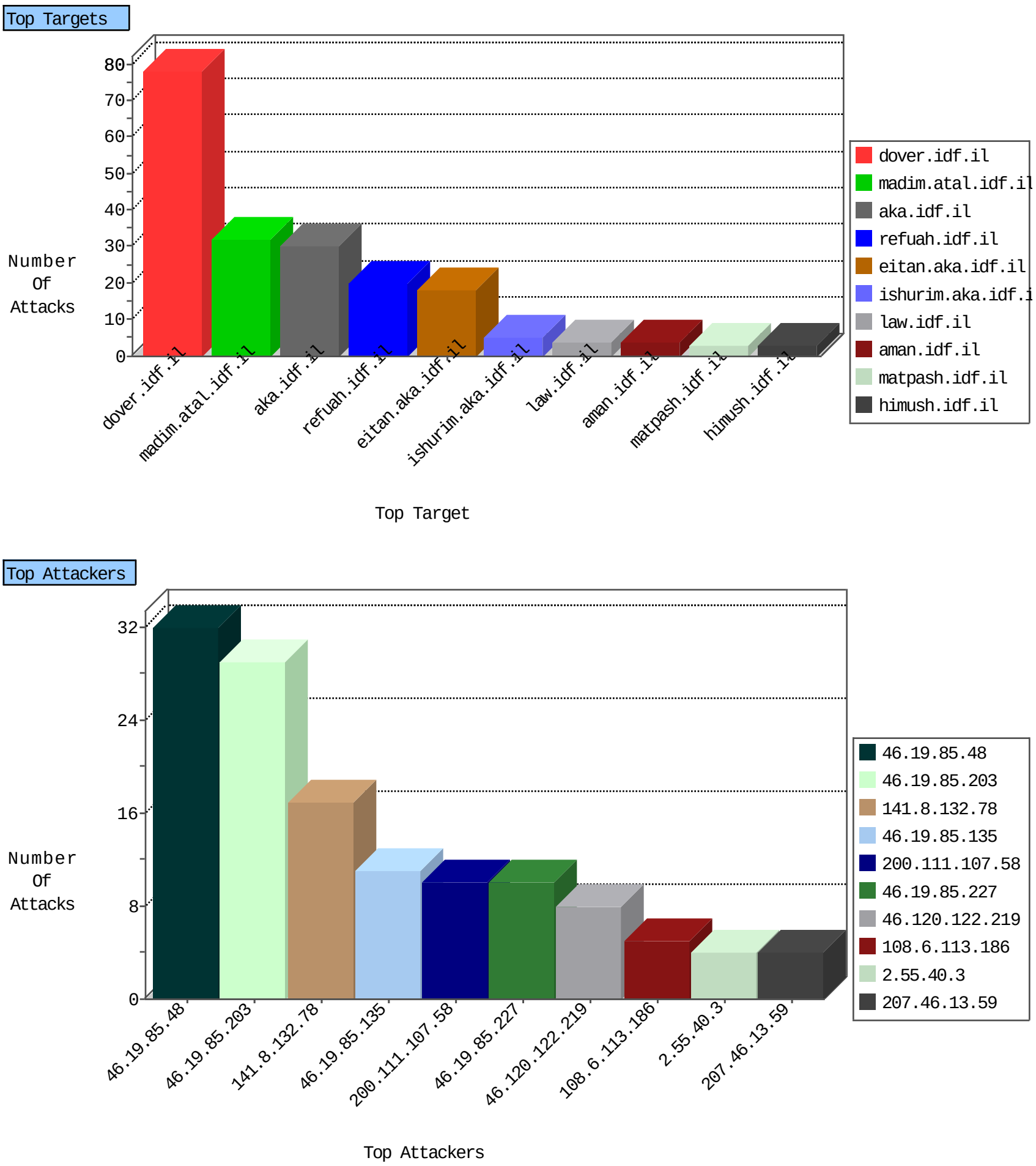
09-13-2016-06:04:09 to 09-13-2016-07:04:09

IDF Under Attack Daily Report



09-13-2016-06:04:09 to 09-13-2016-07:04:09

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
164.107.127.12	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	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
170.140.119.70	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.41	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.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
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.226	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

09-13-2016-06:04:09 to 09-13-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-13-2016-06:04:09 to 09-13-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
45.79.71.122	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
45.79.103.178	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
200.195.135.82	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 2048	1
200.195.135.82	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -f -sS	1
200.111.107.58	147.237.76.147	Chile	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.254.9.91	147.237.8.50	Sweden	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 1024	1
200.111.107.58	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
179.181.219.0	147.237.77.205	Brazil	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

09-13-2016-06:04:09 to 09-13-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
108.6.113.186	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
95.35.174.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.59	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.112	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.1.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.55.40.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.202	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.55.40.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
200.111.107.58	Chile	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.230.86.155	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.255.253.9	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.23	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
200.111.107.58	Chile	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.161.112.91	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.255.253.66	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.30	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.8.132.49	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
200.111.107.58	Chile	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.212	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.23	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.24	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
130.193.51.3	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
189.236.168.105	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.26.149.141	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.29.24.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
200.111.107.58	Chile	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.235	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.28	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.255.253.23	Russian Federation	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
139.162.37.147	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.143.118.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
200.111.107.58	Chile	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.29.24.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.66.27.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
200.111.107.58	Chile	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.255.253.27	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-13-2016-06:04:09 to 09-13-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.203	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	29
77.139.236.25	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
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
176.13.240.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
192.138.214.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.181.117.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
89.237.67.183	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
46.19.86.123	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.253.204.9	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1

09-13-2016-06:04:09 to 09-13-2016-07:04:09