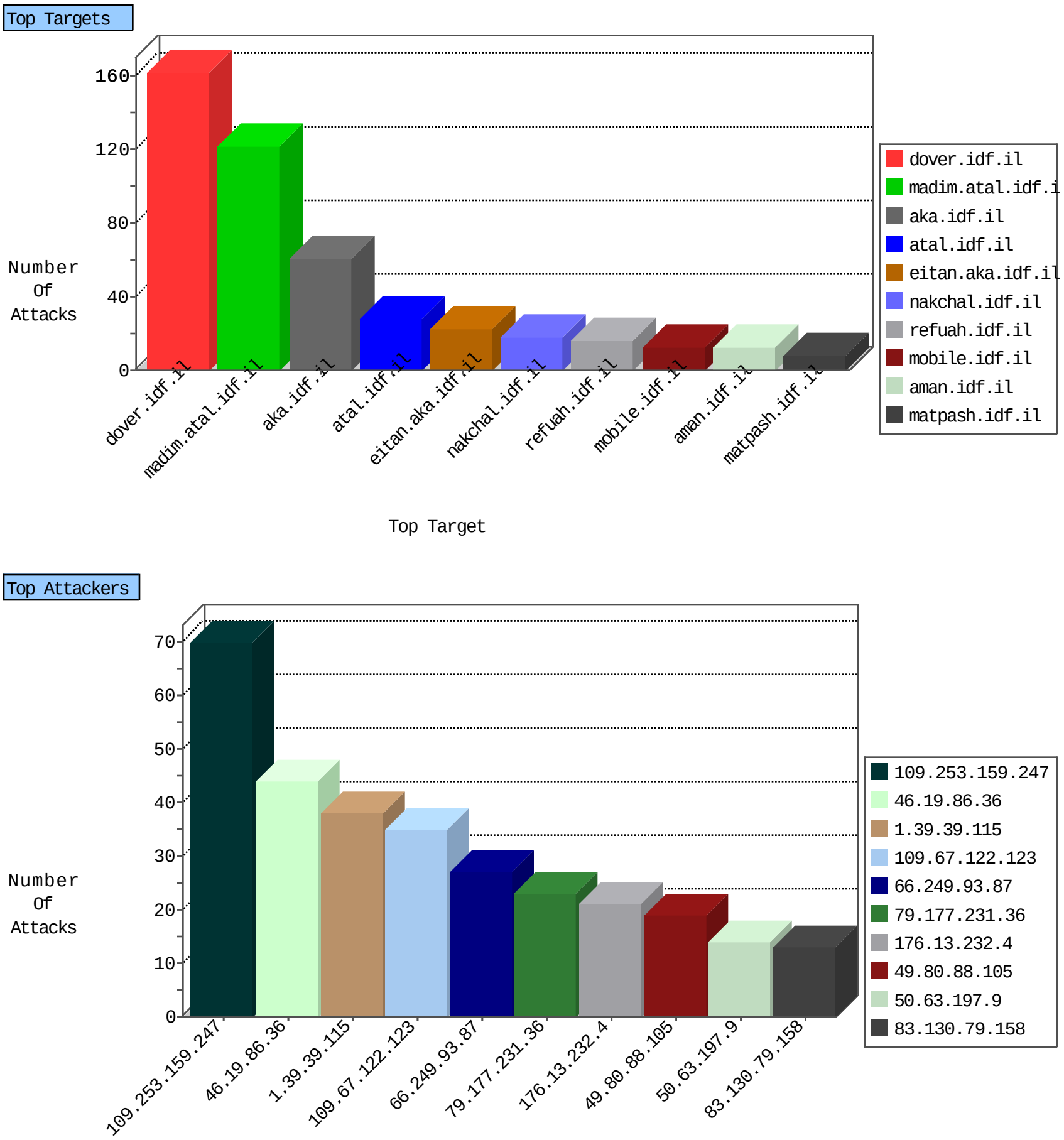
09-23-2016-08:04:00 to 09-23-2016-09:04:00

IDF Under Attack Daily Report



09-23-2016-08:04:00 to 09-23-2016-09:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.218.200.137	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
173.244.198.5	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-23-2016-08:04:00 to 09-23-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.63.197.9	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6

09-23-2016-08:04:00 to 09-23-2016-09:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
1.39.39.115	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	20
50.63.197.9	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
118.41.95.172	147.237.77.227	Korea, Republic of	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.240.250.154	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
74.82.47.23	147.237.77.233	United States	atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.76.201	Kenya	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.39	Indonesia	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
216.81.230.167	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
114.143.115.26	147.237.77.179	India	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
113.221.22.4	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.33	Latvia	idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.76.177	Kenya	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
198.199.89.155	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

09-23-2016-08:04:00 to 09-23-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.87	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
79.177.231.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
176.13.232.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
1.39.39.115	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.16.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
83.130.79.158	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
212.117.150.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
66.249.75.149	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.36	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.149.199	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
83.130.79.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.36	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
1.39.39.115	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.167.103.119	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.36	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.26.149.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.131	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
12.3.236.226	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.36	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
81.218.66.211	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.74	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
91.135.102.181	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.3.147.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
141.207.131.240	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
91.135.102.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.53.157.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
49.204.145.110	India	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.197.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.141	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.69.36.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
162.209.180.155	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
106.51.173.226	India	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.27	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.16.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1

09-23-2016-08:04:00 to 09-23-2016-09:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.159.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
109.67.122.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
49.80.88.105	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 49.80.88.105	Block	13
2.55.156.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
84.94.167.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
93.172.145.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
49.80.88.105	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
176.13.246.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.94.167.80	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.94.167.80	Block	2
80.246.137.161	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2347.jpg	Block	1
109.65.176.14	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.127.22.39	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
49.80.88.105	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/default.aspx	Block	1
197.33.105.184	Egypt	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
84.94.167.80	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
66.249.69.106	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.26.148.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
79.177.231.36	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
213.186.177.198	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
84.108.239.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method atana in URL	Block	1
123.194.163.231	Taiwan	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Cookie Tampering on cookie wb48617274: Expected 9899ED15, Observed F590FD3A	None	1
66.249.64.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19178-he/dover.aspx	Block	1

09-23-2016-08:04:00 to 09-23-2016-09:04:00