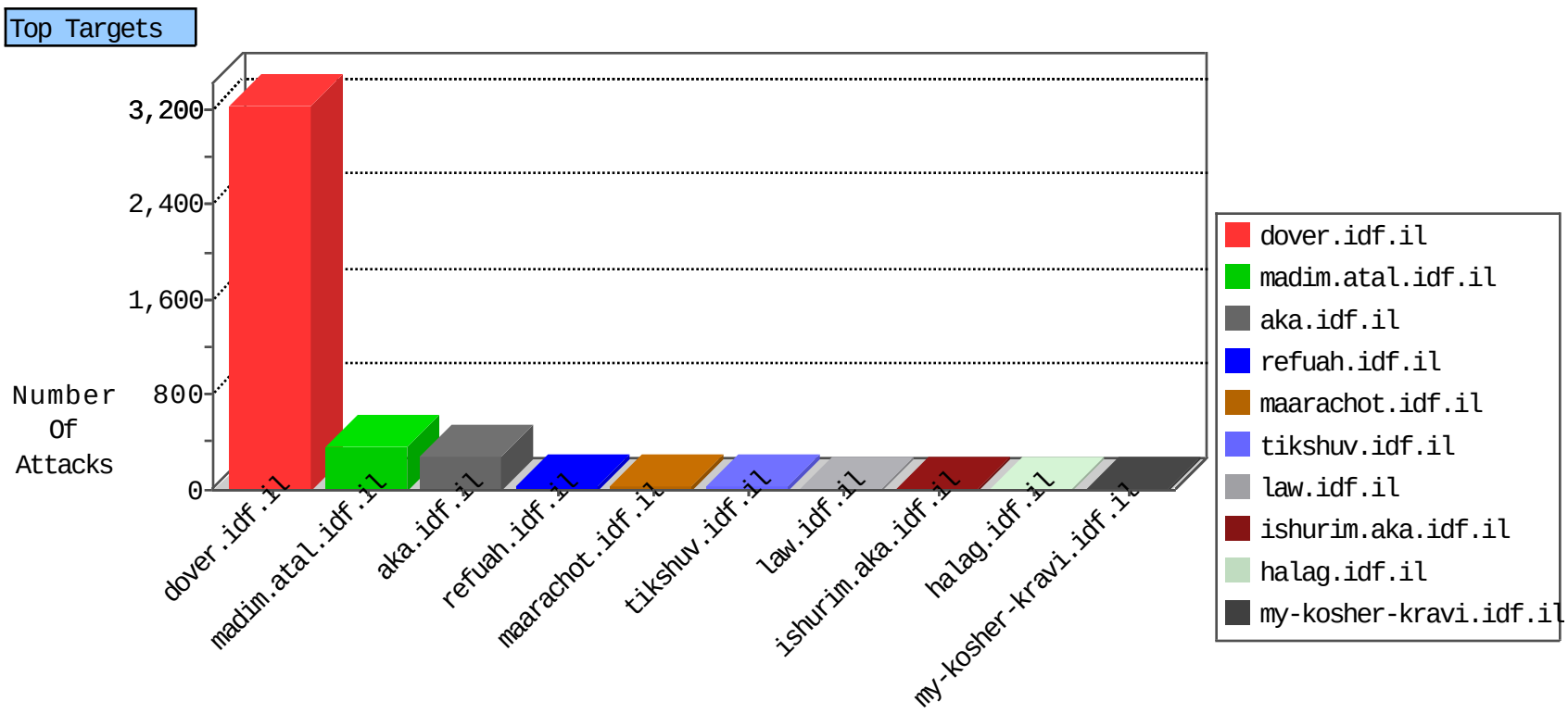
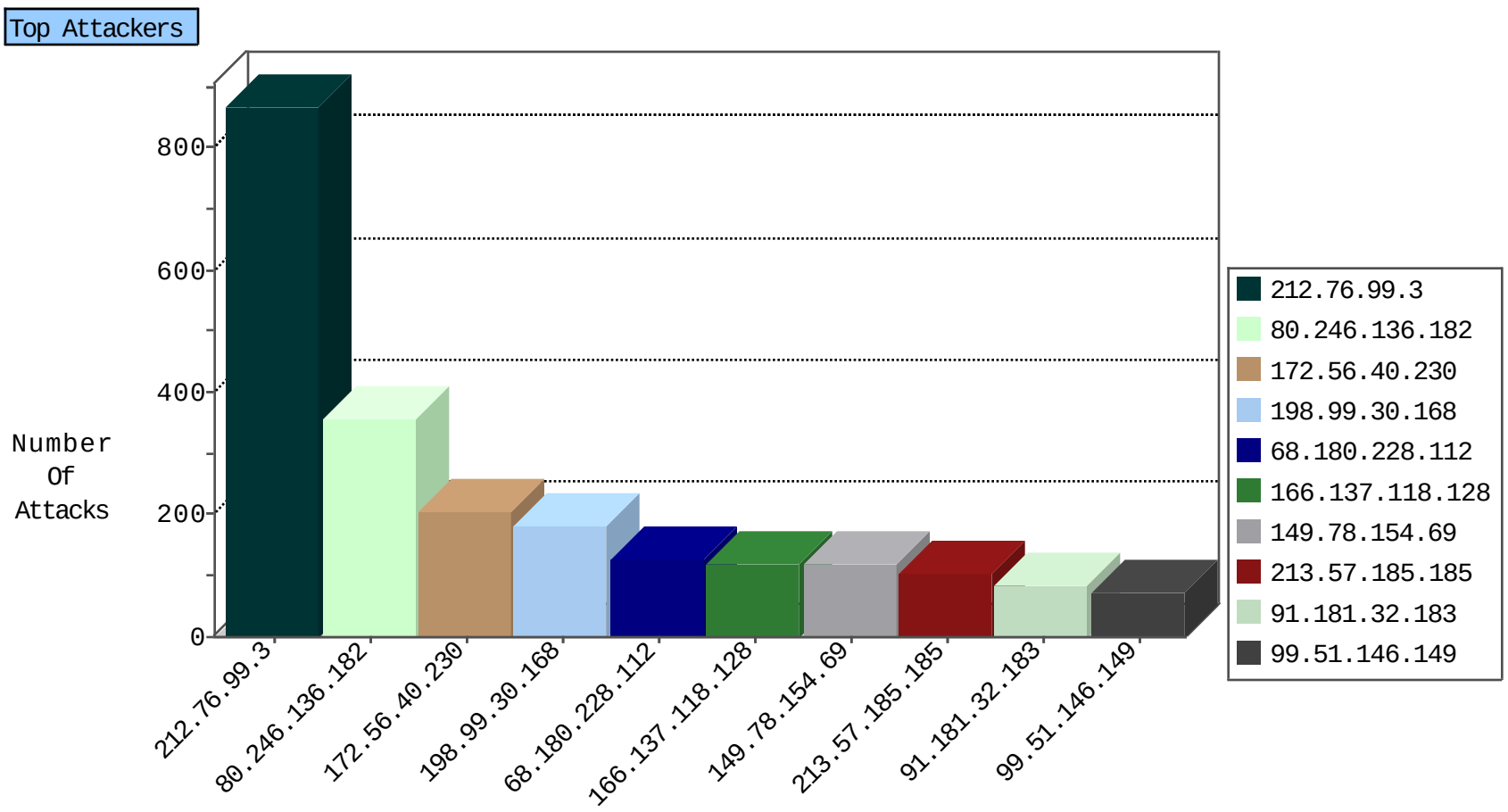
10-19-2015-01:04:46 to 10-19-2015-02:04:46

IDF Under Attack
Daily Report



Top Target



Top Attackers

10-19-2015-01:04:46 to 10-19-2015-02:04:46

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.194.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
79.181.130.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
198.99.30.168	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
85.64.232.99	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
109.66.203.52	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.25.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
87.68.56.28	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.182.211.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
208.54.5.209	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
99.51.146.149	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
208.80.155.215	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.2.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.94.92.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
68.231.217.209	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.2.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
198.99.30.168	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-19-2015-01:04:46 to 10-19-2015-02:04:46

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-01:04:46 to 10-19-2015-02:04:46

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
193.107.16.206	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.199	Sweden	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
123.196.116.66	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
123.196.116.66	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
123.196.116.66	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.194	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
202.44.235.239	147.237.77.74	Thailand	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.37.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.107.16.206	147.237.77.233	Russian Federation	atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.105.134.220	147.237.0.15	Sweden	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
123.196.116.66	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
123.196.116.66	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
111.93.198.54	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-19-2015-01:04:46 to 10-19-2015-02:04:46

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.76.99.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	869
172.56.40.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	205
198.99.30.168	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	176
166.137.118.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
91.181.32.183	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
99.51.146.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
77.125.135.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
162.229.85.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
85.65.100.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
46.120.106.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
37.26.148.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.41.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
37.231.122.223	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
188.247.77.32	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
188.134.27.26	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
174.114.210.58	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
99.237.149.73	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.182.106.51	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.12.141.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
72.229.180.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
98.245.109.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
79.176.185.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.57.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.2.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.228.166.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
50.153.22.128	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
201.52.174.106	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
67.160.236.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.68.56.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

10-19-2015-01:04:46 to 10-19-2015-02:04:46

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.182	Block	325
213.57.185.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.185.185	Block	104
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	91
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
37.26.148.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
149.78.165.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	26
194.187.168.23	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	13
77.237.146.28	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	13
46.117.110.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
157.55.39.207	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/×³×Ÿ Â¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³×ŸÂ¿Â½×³Â ×³×ŸÂ¿Â½×³Ã—	Block	13
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/story.aspx	Block	13
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	13
64.19.78.243	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	13
173.208.207.178	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	13
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	13
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	13
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
176.12.141.239	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	13
66.249.93.145	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
66.249.65.17	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	13
183.57.154.31	China	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../resources/scripts/generalfunctions.js	Block	13
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	13

10-19-2015-01:04:46 to 10-19-2015-02:04:46