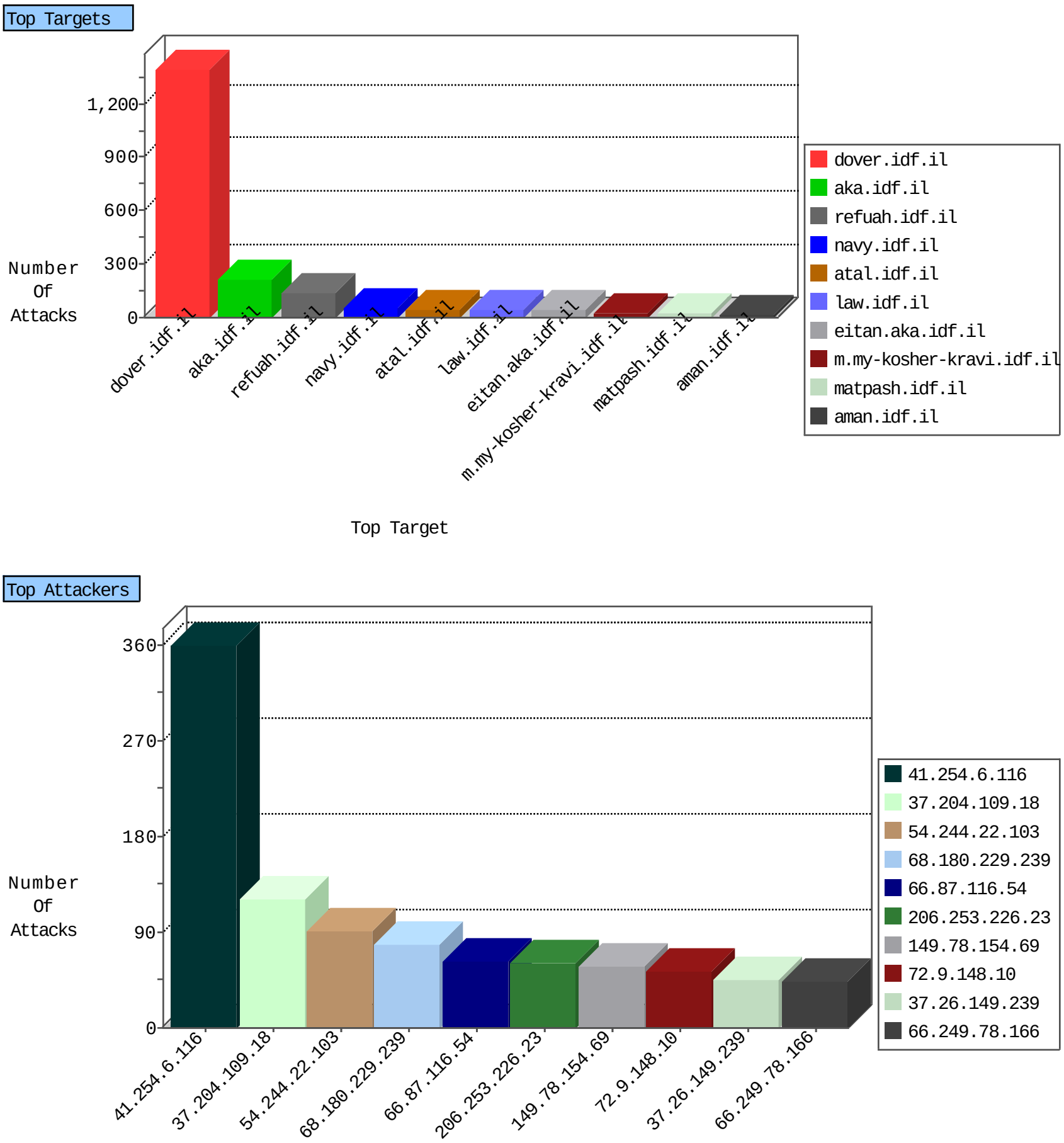
10-19-2015-05:04:02 to 10-19-2015-06:04:02

IDF Under Attack
Daily Report



10-19-2015-05:04:02 to 10-19-2015-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.157.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.204.109.18	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
73.32.238.136	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
54.235.136.3	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.204.109.18	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1

10-19-2015-05:04:02 to 10-19-2015-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-05:04:02 to 10-19-2015-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
178.89.191.77	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN Potential SSH Scan	2
222.186.160.108	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.254.138.16	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.139.194.109	147.237.76.34	Spain	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.160.108	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.254.138.16	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.197.123.148	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN NMAP -sS window 3072	1
1.235.195.234	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN NMAP -f -sS	1

10-19-2015-05:04:02 to 10-19-2015-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.254.6.116	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	360
37.204.109.18	Russian Federation	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	117
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
66.87.116.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
37.26.149.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
134.87.187.228	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.142.68.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.117.157.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
32.42.15.123	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.33.60.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.113	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
42.120.160.110	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.107.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
104.197.194.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.181.50.29	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.28.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.181.50.29	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
174.109.247.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
79.179.127.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.112	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.197.10.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

10-19-2015-05:04:02 to 10-19-2015-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	78
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
87.69.92.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	39
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
108.175.9.107	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	13
66.249.79.218	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	13
50.16.96.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	13
162.157.29.23	Canada	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	13
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	13
188.165.15.89	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	13
109.65.188.107	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding Z_$p5P%@TDp)K}Ak0sBmZjsd_*sTa in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	13
66.249.79.225	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74/robots.txt	Block	13
64.19.78.242	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	13
162.157.29.23	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 162.157.29.23	Block	13
206.253.226.23	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
109.65.188.107	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.65.188.107	None	13
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	13
162.243.38.196	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.38.196	Block	13
93.172.105.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	13
206.253.226.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	13
140.207.198.207	China	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../resources/scripts/mootools.js	Block	13
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/57978.pdf.2005	Block	13
180.76.15.17	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	13
108.175.9.107	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	13
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
206.253.226.23	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	13
157.55.39.15	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
84.108.0.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	13
182.118.54.70	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.aspx%3f_tsm_hiddenfield_	Block	13

10-19-2015-05:04:02 to 10-19-2015-06:04:02