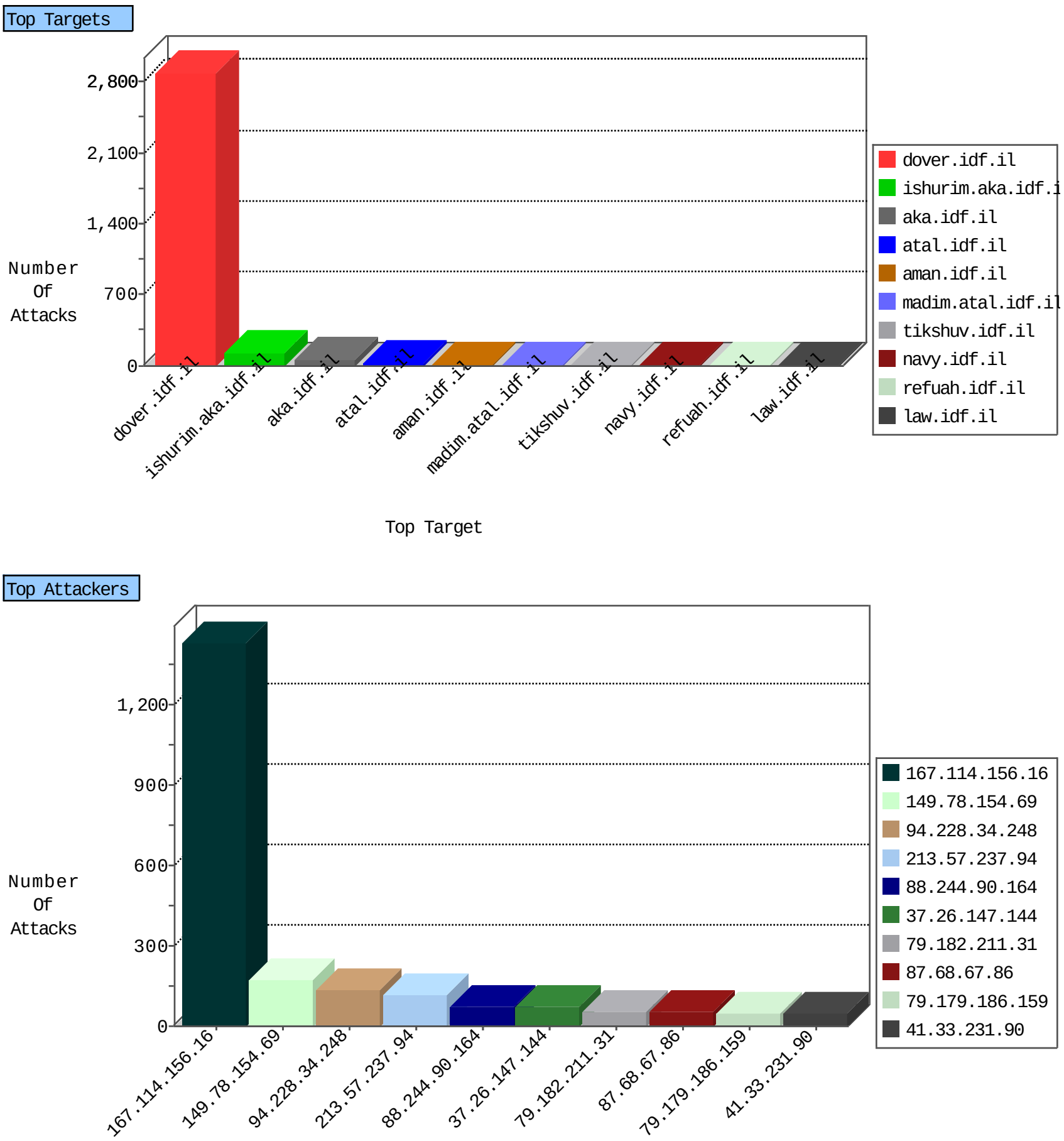
11-09-2015-01:04:08 to 11-09-2015-02:04:08

IDF Under Attack
Daily Report



11-09-2015-01:04:08 to 11-09-2015-02:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2382
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	619
84.111.28.61	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.12.139.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
24.190.3.234	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.186.90	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-09-2015-01:04:08 to 11-09-2015-02:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-09-2015-01:04:08 to 11-09-2015-02:04:08

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
119.90.138.60	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
31.6.71.154	147.237.77.74	Poland	law.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.138.60	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
84.21.203.130	147.237.8.45	Bulgaria	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

11-09-2015-01:04:08 to 11-09-2015-02:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	170
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
88.244.90.164	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
37.26.147.144	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.182.211.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
79.179.186.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
85.64.53.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
87.68.67.86	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
84.94.74.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
64.233.172.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
87.68.67.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
116.14.50.100	Singapore	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		drop	10
185.120.126.59		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
24.190.3.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
146.185.56.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.125.1.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.172.160.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.180.217.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
86.179.77.218	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.111.28.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.76	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
77.100.43.102	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.66.147.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.146.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
74.64.108.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

11-09-2015-01:04:08 to 11-09-2015-02:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.237.94	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.237.94	Block	108
46.19.85.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	4
2.54.182.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.67.86	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
188.165.15.204	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
213.57.237.94	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.93.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.210	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.93.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
62.210.247.93	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
84.94.22.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.169.251	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8818-he/refuah.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.54.182.135	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1447021863,"https://www.google.co.il/"], Observed ["","",1447025335,"https://www.google.co.il/"]	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

11-09-2015-01:04:08 to 11-09-2015-02:04:08