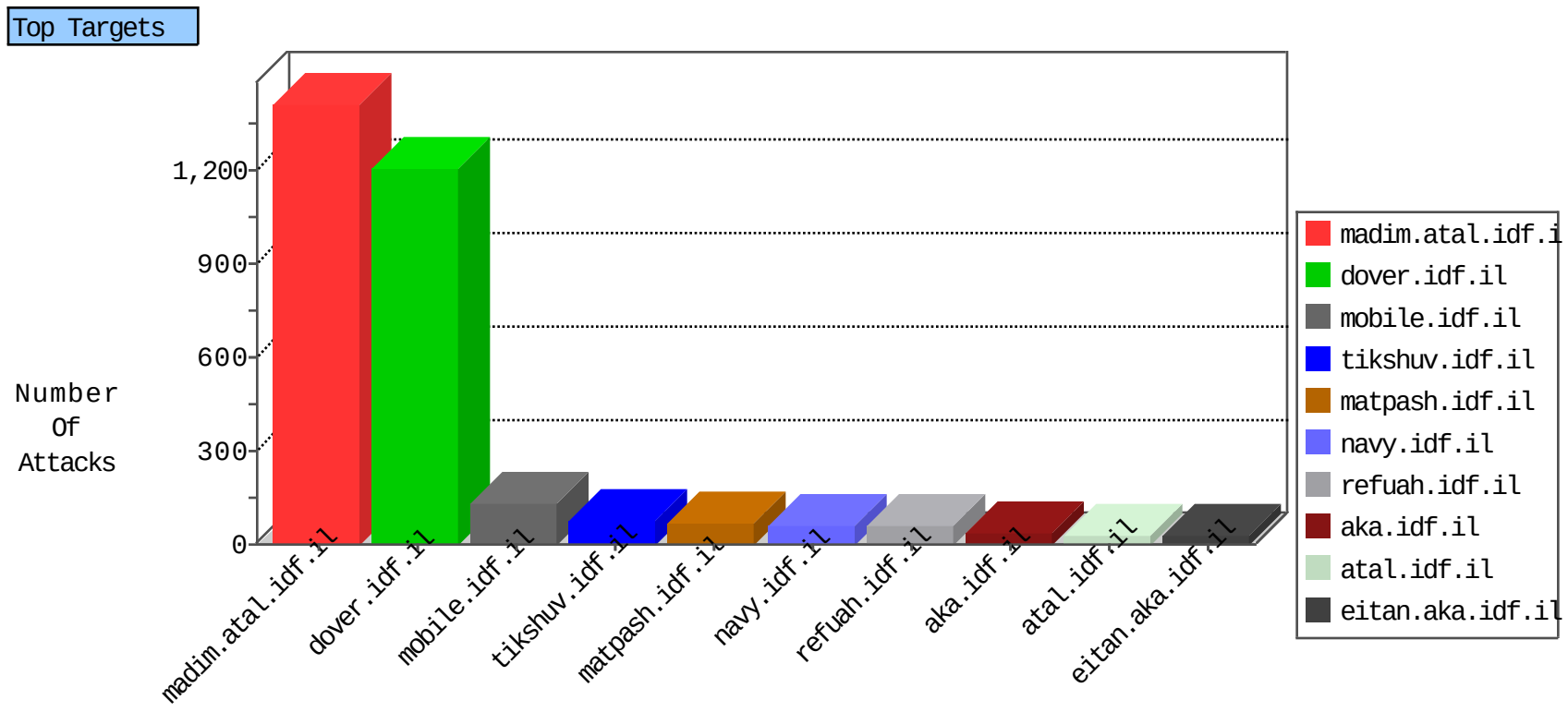
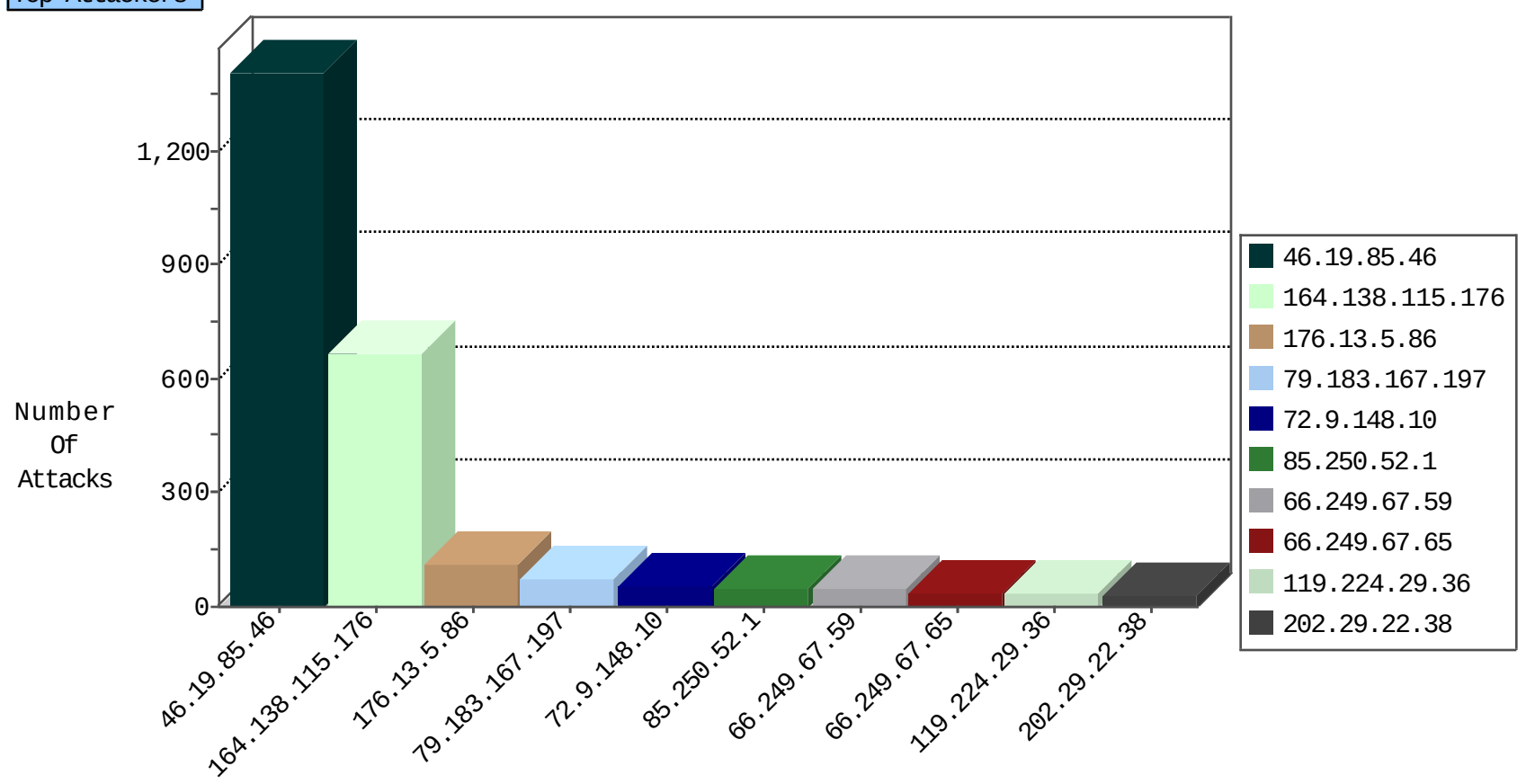
10-25-2015-01:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-01:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.29.22.38	Thailand	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
5.28.177.136	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-25-2015-01:04:05

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	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
5.8.66.90	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.32	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.240.7.206	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -f -sS	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
107.196.106.94	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.104.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
5.199.172.154	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
222.186.56.32	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.50.143.65	147.237.72.217	United Arab Emirates	e.idf.il	ET SCAN NMAP -sS window 3072	1
218.240.7.206	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.236.67	147.237.76.30	Singapore	himush.idf.il	ET SCAN NMAP -sS window 1024	1
92.241.51.98	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
46.162.116.221	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.199.172.154	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN NMAP -sS window 4096	1

10-25-2015-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
164.138.115.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	669
79.183.167.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
85.250.52.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
119.224.29.36	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
85.130.248.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.67.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	11
80.246.133.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.213.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
70.66.21.195	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.193.51.17	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
131.253.25.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.115.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
96.248.115.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
98.215.228.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.86.120.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.201.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.152.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.246.133.92	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.134.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	2
71.81.128.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.173.224.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.110.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.46.34.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.182.24.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.13.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
86.24.42.93	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
73.149.108.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.108.30.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.76.109.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.254.72.19	Italy	147.237.76.34	yohalan.idf.il	drop		drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.46	Block	1396
176.13.5.86	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.5.86	Block	70
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
176.13.5.86	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	42
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	28
50.62.57.239	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	14
188.143.232.43	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.43	Block	14
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
45.63.107.26		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	14
202.29.22.38	Thailand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	14
176.13.14.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.176.175.21	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.143.232.43	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1590-he/	Block	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	14
212.199.57.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	14
184.168.200.234	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	14
85.64.76.103	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8750-he/refuah.aspx	Block	14
157.55.39.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	14
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
184.173.183.173	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-10272-en/cogat.aspx&usg=alkjrhixl5usddtxwlhp_qizzd1bjr1n5g	Block	14
109.65.61.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	14
40.77.167.42	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17348.jpg	Block	14
69.65.3.173	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	14
46.19.86.15	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	14
188.143.232.26	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	14
41.69.194.74	Egypt	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
202.29.22.38	Thailand	147.237.77.216	dover.idf.il	PHP Attempt	Block	14