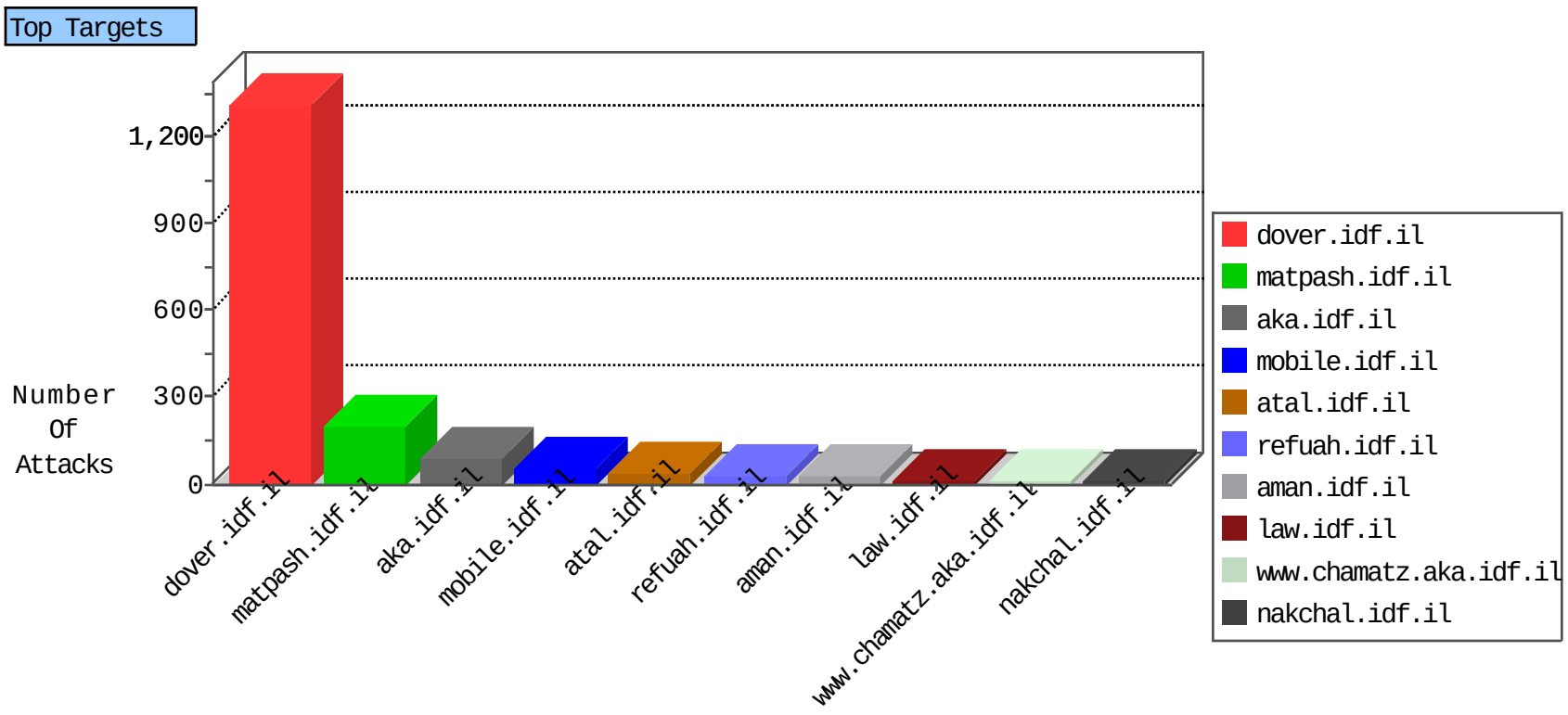
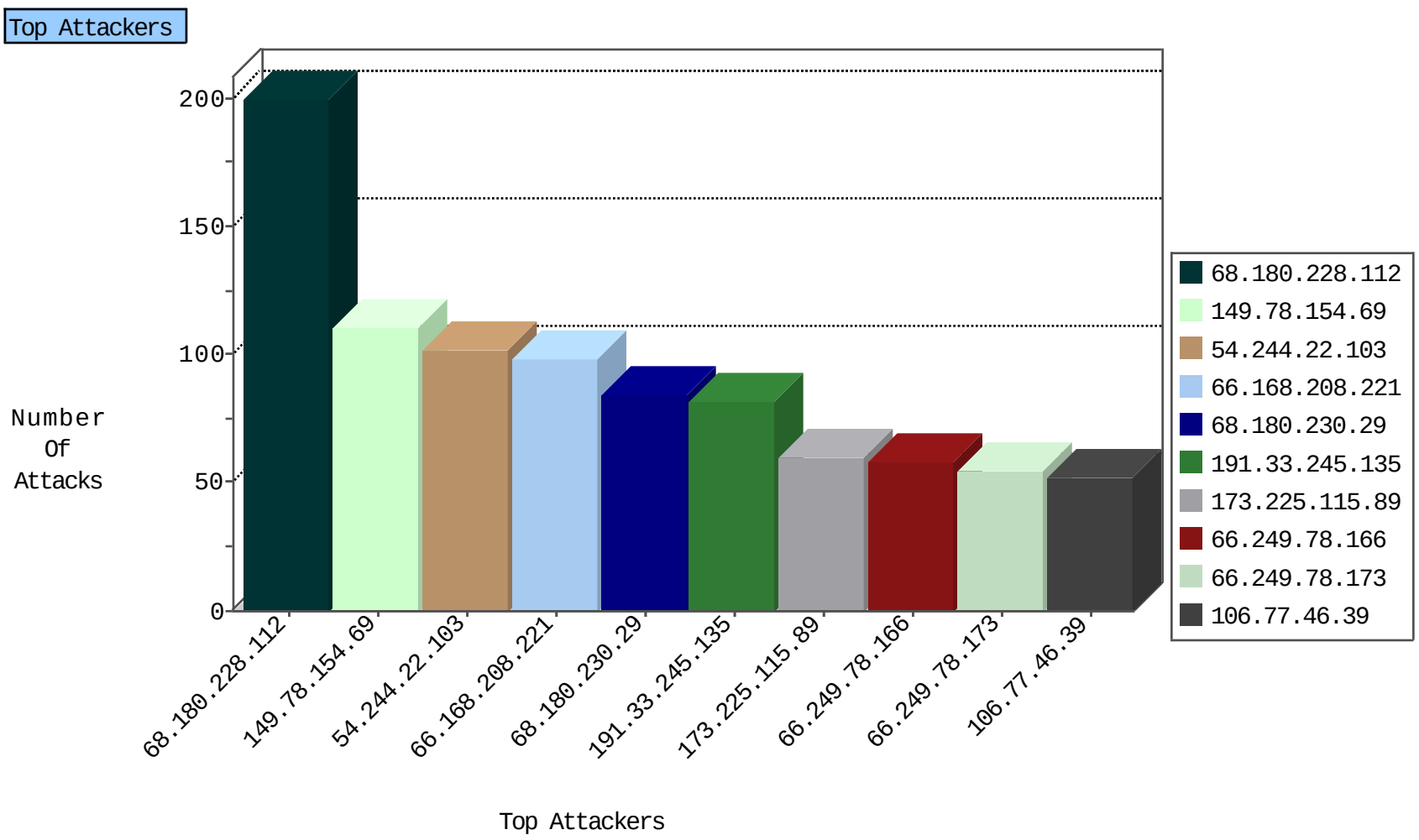
10-28-2015-05:04:06 to 10-28-2015-06:04:06

IDF Under Attack
Daily Report





10-28-2015-05:04:06 to 10-28-2015-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.34.48	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
68.116.5.134	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	2
66.168.62.225	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1

10-28-2015-05:04:06 to 10-28-2015-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.228.158	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	2

10-28-2015-05:04:06 to 10-28-2015-06:04:06

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
193.105.134.220	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.66.78	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.179	Sweden	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
169.57.5.20	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
31.211.102.129	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1

10-28-2015-05:04:06 to 10-28-2015-06:04:06

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	111
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
191.33.245.135	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
173.225.115.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
106.77.46.39	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
46.19.86.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
191.145.188.204	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
92.229.17.127	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.9.46		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
71.222.14.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
92.229.17.127	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.26.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
112.143.19.243	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.199.182.150	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	First packet isn't SYN	drop	10
84.229.30.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
107.77.89.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
70.52.230.237	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
96.19.209.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
216.13.56.3	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
65.55.210.85	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
79.182.122.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
131.253.25.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.8.6.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
75.82.50.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.51.65.57	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
176.12.149.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.229.156.214	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
99.167.198.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.22.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

10-28-2015-05:04:06 to 10-28-2015-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.168.208.221	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.168.208.221	Block	84
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	42
112.143.19.243	Thailand	147.237.77.216	dover.idf.il	Parameter Type Violation id in www.idf.il/1294-en/dover.aspx	Block	28
77.237.138.51	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17841-en/dover.aspx maj. gen. gadi eizenkot appointed deputy to chief of general staff	Block	14
46.121.228.158	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	14
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18063-he/dover.aspx	Block	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	14
45.63.49.95		147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	14
79.180.146.218	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
66.249.79.104	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
216.218.206.67	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	14
45.63.49.95		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
99.167.198.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	14
66.249.79.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
66.168.208.221	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/3699.pdf++972+import+export@.com+il&as_qdr=all&filter=0&num=100&complete=0&cr=countryil&gws_rd=ssl&hl=iw&&ct=clnk	Block	14
157.55.39.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/transportation.asp	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
45.63.49.95		147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	14
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1151-he/chinuch.aspx	Block	14
176.13.22.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
73.169.170.207	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/page/28/	Block	14
46.121.214.39	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	14
122.13.132.199	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	14
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
184.105.247.196	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	14

10-28-2015-05:04:06 to 10-28-2015-06:04:06