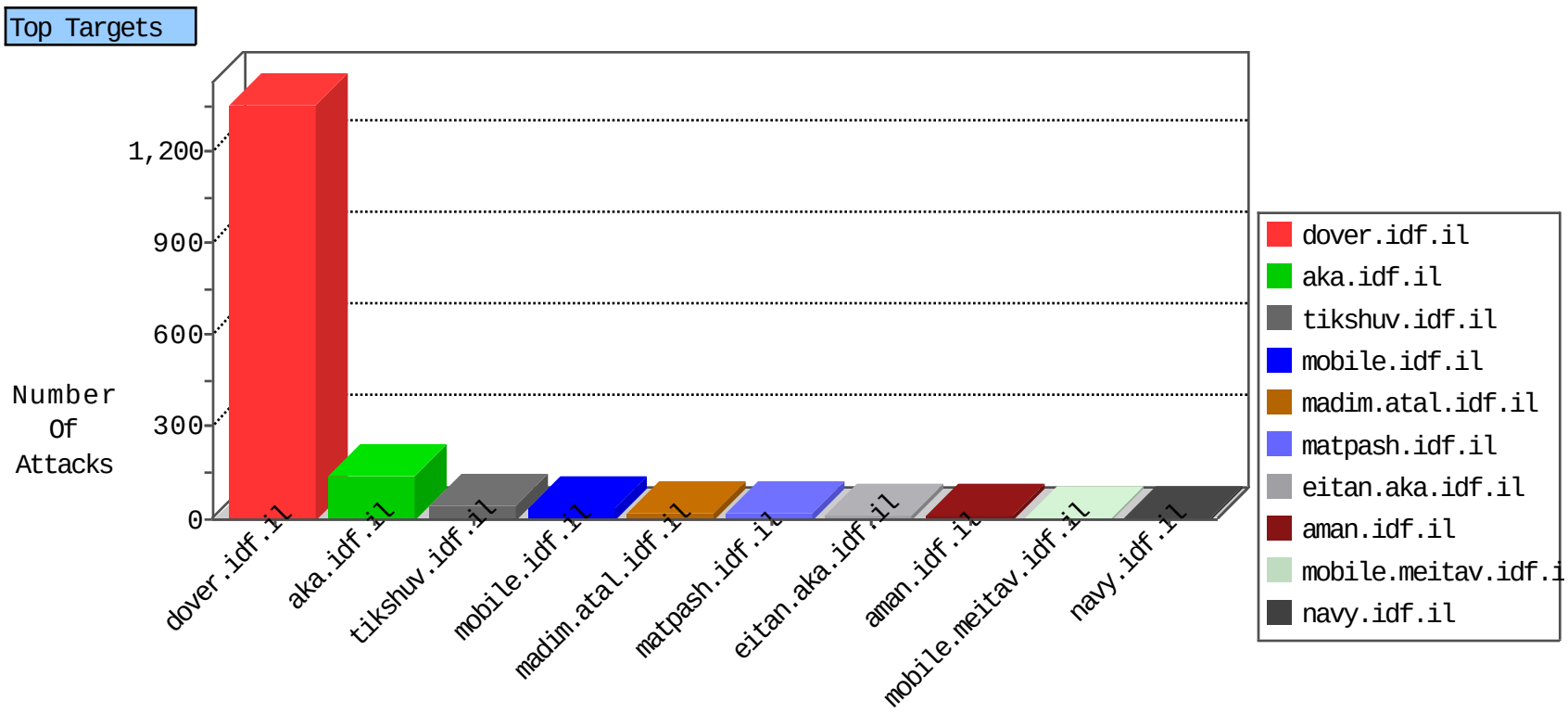
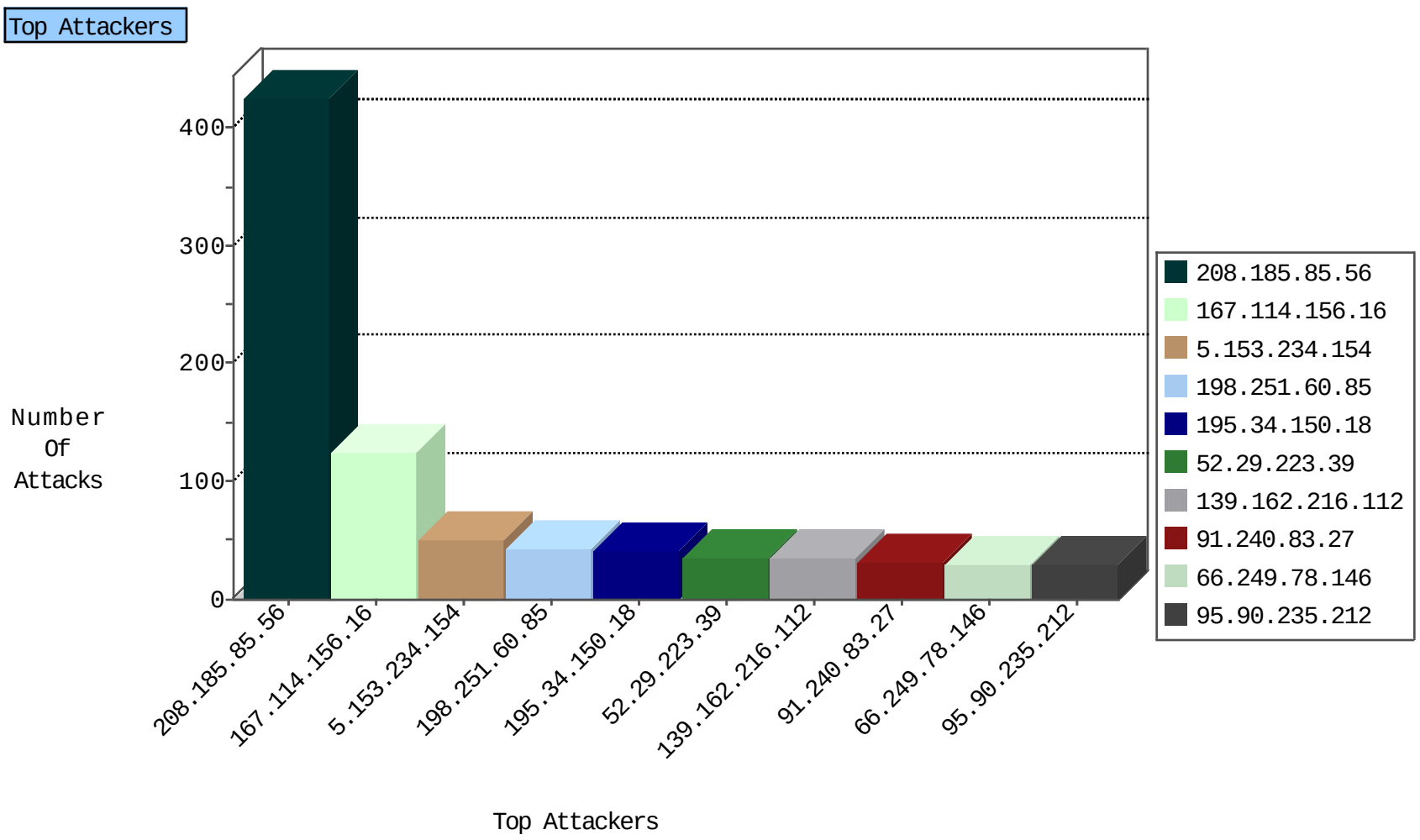
04-28-2016-23:04:07 to 04-29-2016-00:04:07

IDF Under Attack
Daily Report





04-28-2016-23:04:07 to 04-29-2016-00:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	6118
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1555
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

04-28-2016-23:04:07 to 04-29-2016-00:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.32.206.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	3798: HTTP: SQL Injection (Boolean Identity)	Block	1
5.34.160.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12618: HTTP: WebCruiser Vulnerability Scanner	Block	1

04-28-2016-23:04:07 to 04-29-2016-00:04:07

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
174.37.194.144	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sA (2)	2
109.67.148.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.3	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.0.16	Austria	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.131	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
197.48.234.170	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.86	147.237.77.176	Lithuania	matpash.idf.il	ET SCAN Potential SSH Scan	1
66.176.28.101	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
111.68.104.195	147.237.8.24	Pakistan	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.3	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.3	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
89.248.167.131	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.167.131	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.86	147.237.76.30	Lithuania	himush.idf.il	ET SCAN Potential SSH Scan	1
49.142.231.184	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1

04-28-2016-23:04:07 to 04-29-2016-00:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
208.185.85.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	426
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
198.251.60.85	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
91.240.83.27	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
95.90.235.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.178.83.201	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
149.78.160.203	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
207.46.13.2	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
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
187.207.55.139	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.13.45.167	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.190.149.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.184.203.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.202.26.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.185.248.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.188.213.250	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
8.39.217.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
105.155.143.138	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.64.147.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
92.40.249.56	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.1.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
91.87.217.70	Belgium	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

04-28-2016-23:04:07 to 04-29-2016-00:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.74.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
199.30.24.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.32.206.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.32.206.191	Block	2
199.30.25.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.64.147.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.87.217.70	Belgium	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.141	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
96.224.0.54	United States	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
75.141.65.80	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
141.212.122.161	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
84.108.120.146	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
96.224.0.54	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-6859-en/	Block	1
75.141.65.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.32.206.191	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
105.155.143.138	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
80.246.133.91	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
64.71.32.25	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
85.64.175.26	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.65.206.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
164.132.161.44	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1100-he/nakhal.aspx	Block	1
46.28.138.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
141.212.122.161	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
84.108.50.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

04-28-2016-23:04:07 to 04-29-2016-00:04:07