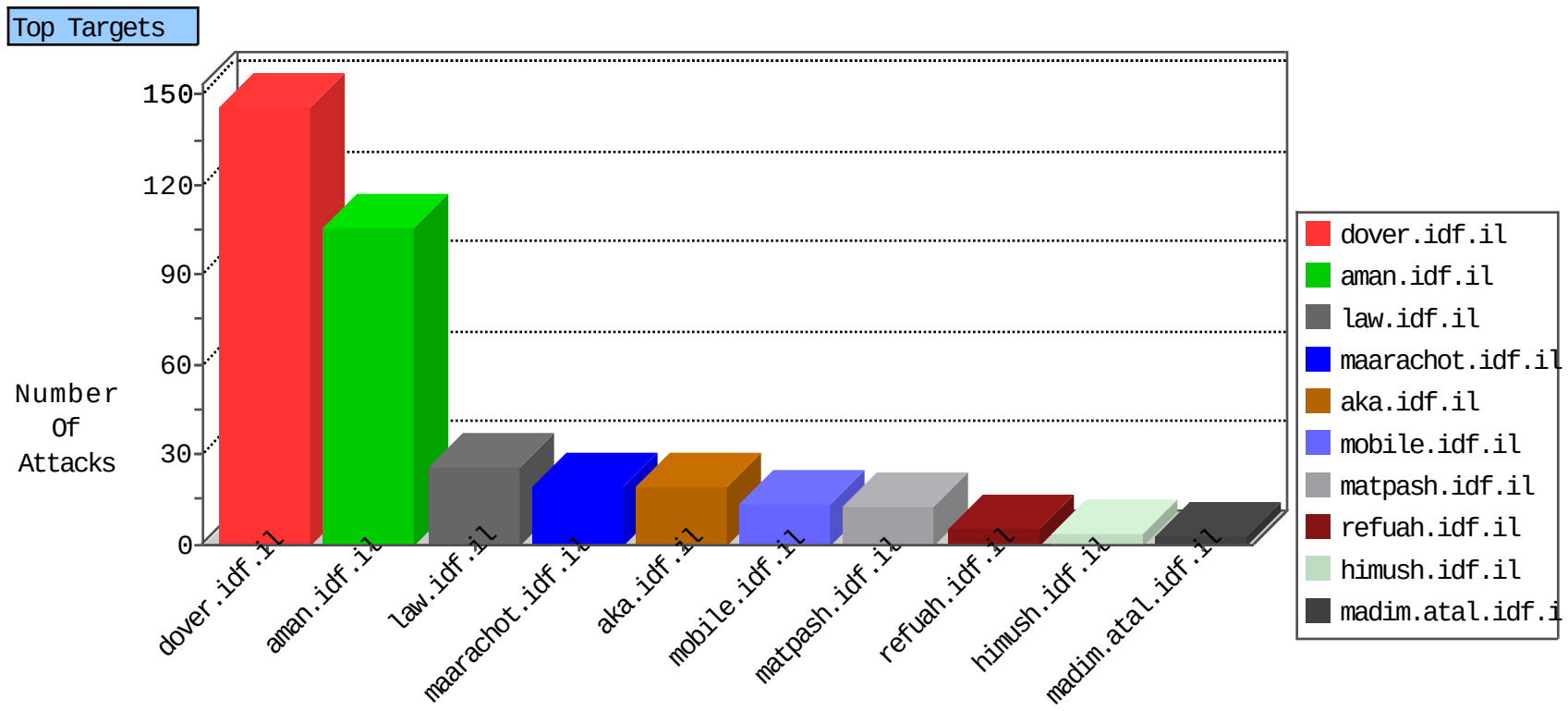
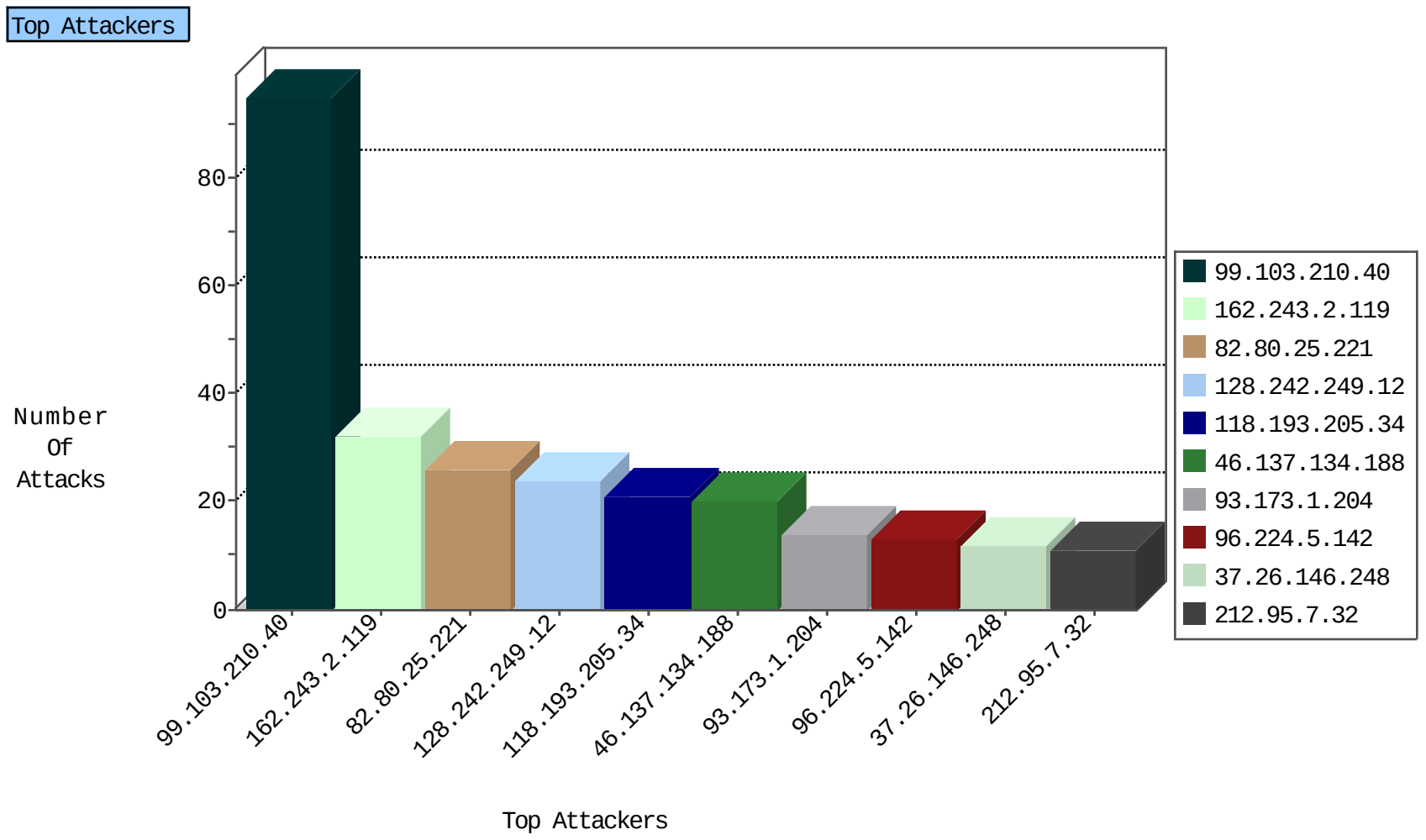
04-26-2015-05:03:01 to 04-26-2015-06:03:01

IDF Under Attack
04-26-2015-05:03:01

Top Targets



Top Attackers



04-26-2015-05:03:01 to 04-26-2015-06:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
99.103.210.40	United States	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	886
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	327
220.181.108.167	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	232
99.103.210.40	United States	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	10
99.103.210.40	United States	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1
192.3.202.58	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

04-26-2015-05:03:01 to 04-26-2015-06:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.121	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-05:03:01 to 04-26-2015-06:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	26
99.103.210.40	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.90	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
216.178.244.160	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
99.103.210.40	United States	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
91.224.132.118	Russian Federation	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2015-05:03:01 to 04-26-2015-06:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
99.103.210.40	United States	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	34
162.243.2.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
118.193.205.34	China	147.237.77.74	law.idf.il	SAM rule	drop	drop	21
37.26.146.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
212.95.7.32	Austria	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
187.212.16.84	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.43.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
100.37.230.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.200.83.43	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.199.203.98	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
216.218.206.80	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
198.200.83.43	Canada	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
98.210.231.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.172.89	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-26-2015-05:03:01 to 04-26-2015-06:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
93.173.1.204	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.173.1.204	Block	12
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
198.50.143.190	Canada	147.237.77.74	law.idf.il	PHP Attempt	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
93.173.1.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
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	2
184.105.247.196	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
96.224.5.142	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
87.237.122.79	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.67.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.66	Block	1
186.84.185.231	Colombia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
98.206.23.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/civilian.stm	Block	1
54.163.100.58	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
92.53.114.87	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.67.90	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
99.103.210.40	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /	Block	1
54.163.100.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
176.12.148.191	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
119.176.87.81	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-15093-en/dover.as	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.216.170.29	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
180.76.4.171	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.78.89	None	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
66.249.64.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1

04-26-2015-05:03:01 to 04-26-2015-06:03:01