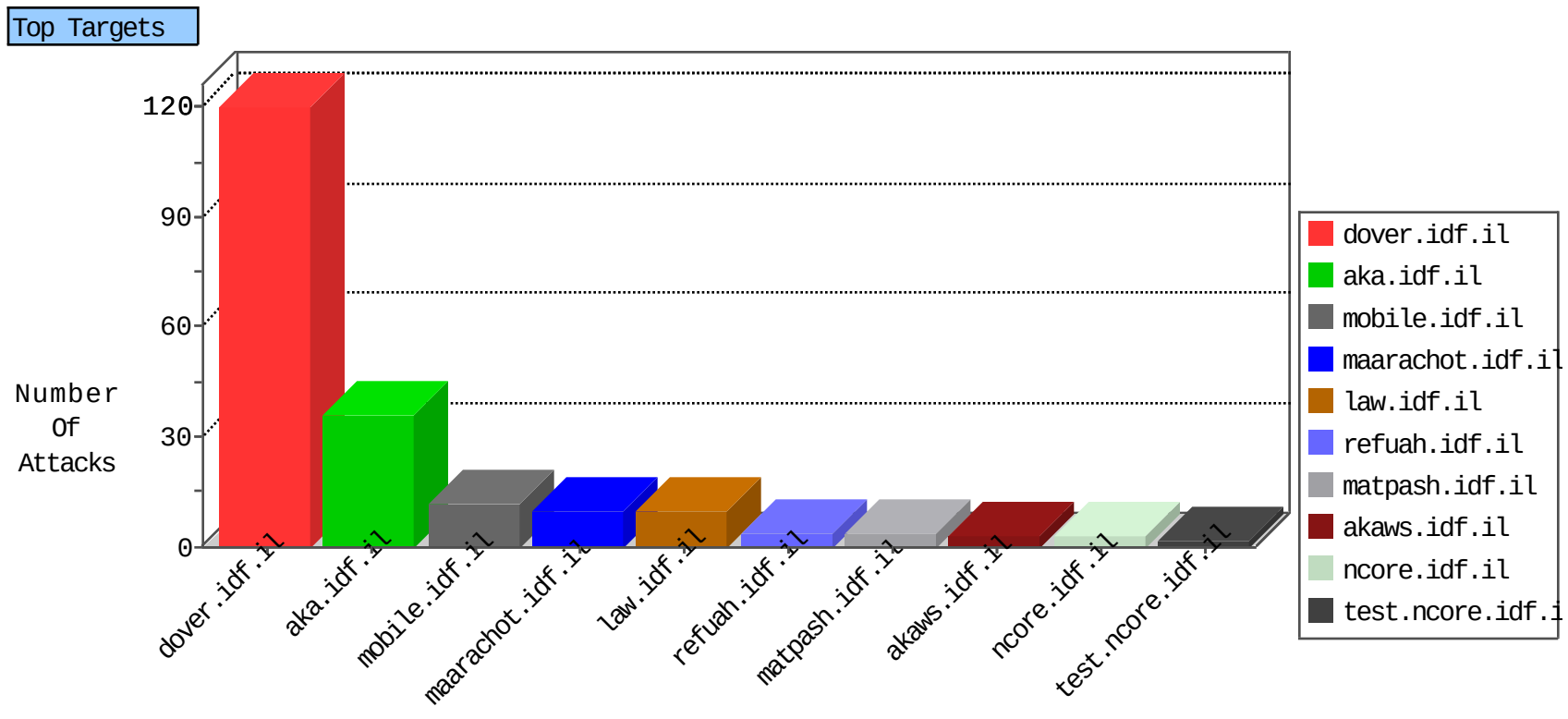
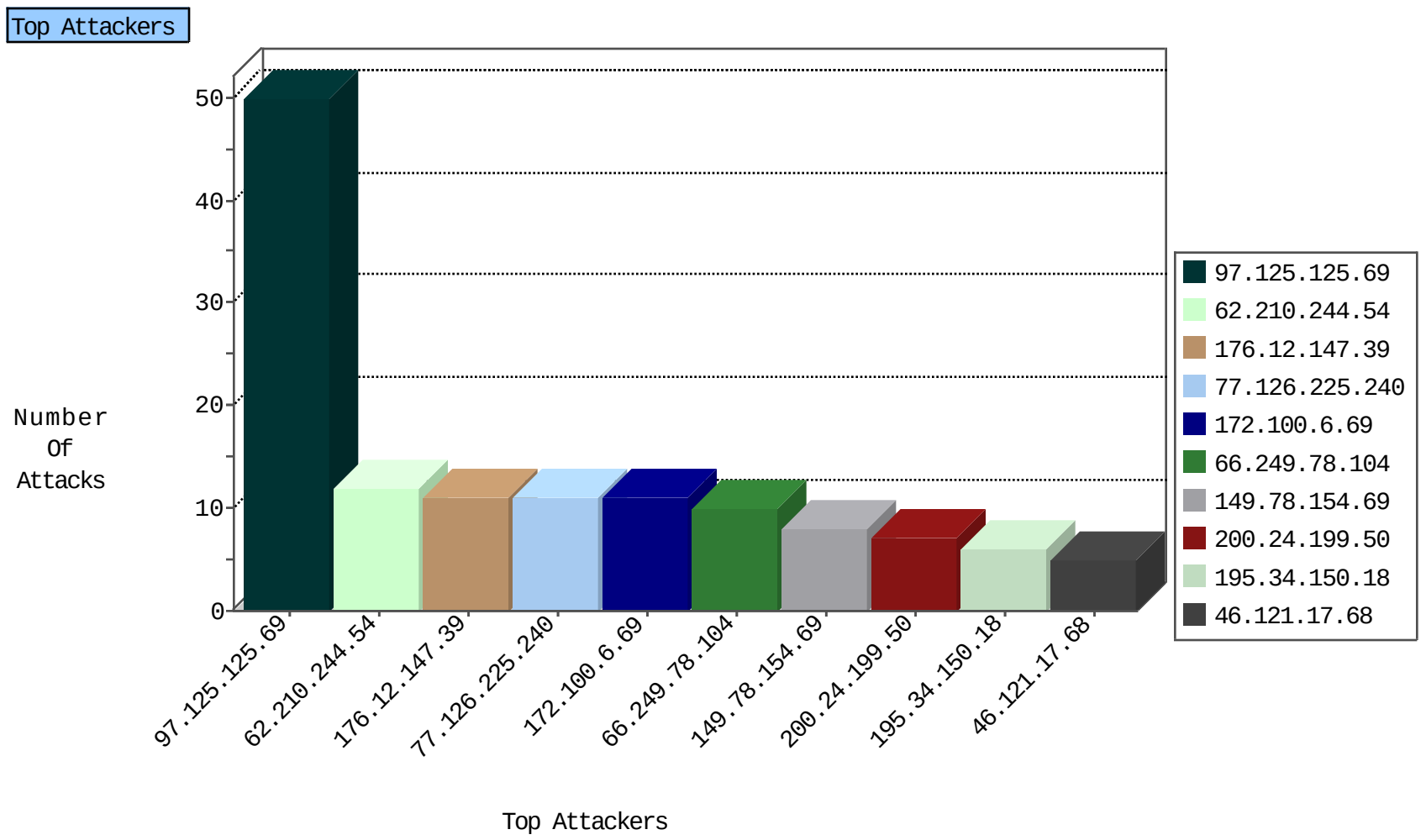
04-27-2015-05:03:07 to 04-27-2015-06:03:07

IDF Under Attack
04-27-2015-05:03:07

Top Targets



Top Attackers



04-27-2015-05:03:07 to 04-27-2015-06:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	380
62.210.244.54	France	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

04-27-2015-05:03:07 to 04-27-2015-06:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
91.200.12.18	Ukraine	147.237.77.74	law.idf.il	C1000196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1

04-27-2015-05:03:07 to 04-27-2015-06:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
101.226.2.99	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.59	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.128	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.59	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.13.137.206	Russian Federation	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
88.249.106.23	Turkey	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.59	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.128	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.59	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.128	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
185.13.137.206	Russian Federation	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

04-27-2015-05:03:07 to 04-27-2015-06:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
97.125.125.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
172.100.6.69		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
176.12.147.39	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
200.24.199.50	Ecuador	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.121.17.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
203.116.187.1	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
174.124.201.215	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
184.153.75.12	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
76.232.180.94	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
77.125.119.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.181.208.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
121.204.189.122	China	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1

04-27-2015-05:03:07 to 04-27-2015-06:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.126.225.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	11
91.200.12.18	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	4
24.188.199.124	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
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
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	2
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
184.105.247.196	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
85.64.210.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1528-12858-h	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/chenofficers.asp	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter sideS*roll in www.aka.idf.il/giyus/kadatz/	None	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.48	Block	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
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/shalishut/site/gallery.aspx	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/asp/wars.asp	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/address.stm	Block	1
109.66.53.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.78.80	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
176.12.143.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.119.113.155	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
119.127.90.197	China	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//shared/usercontrols/headerupper/	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.32	Block	1
176.12.147.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored7.stm	Block	1
54.91.152.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
121.204.189.122	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1

04-27-2015-05:03:07 to 04-27-2015-06:03:07