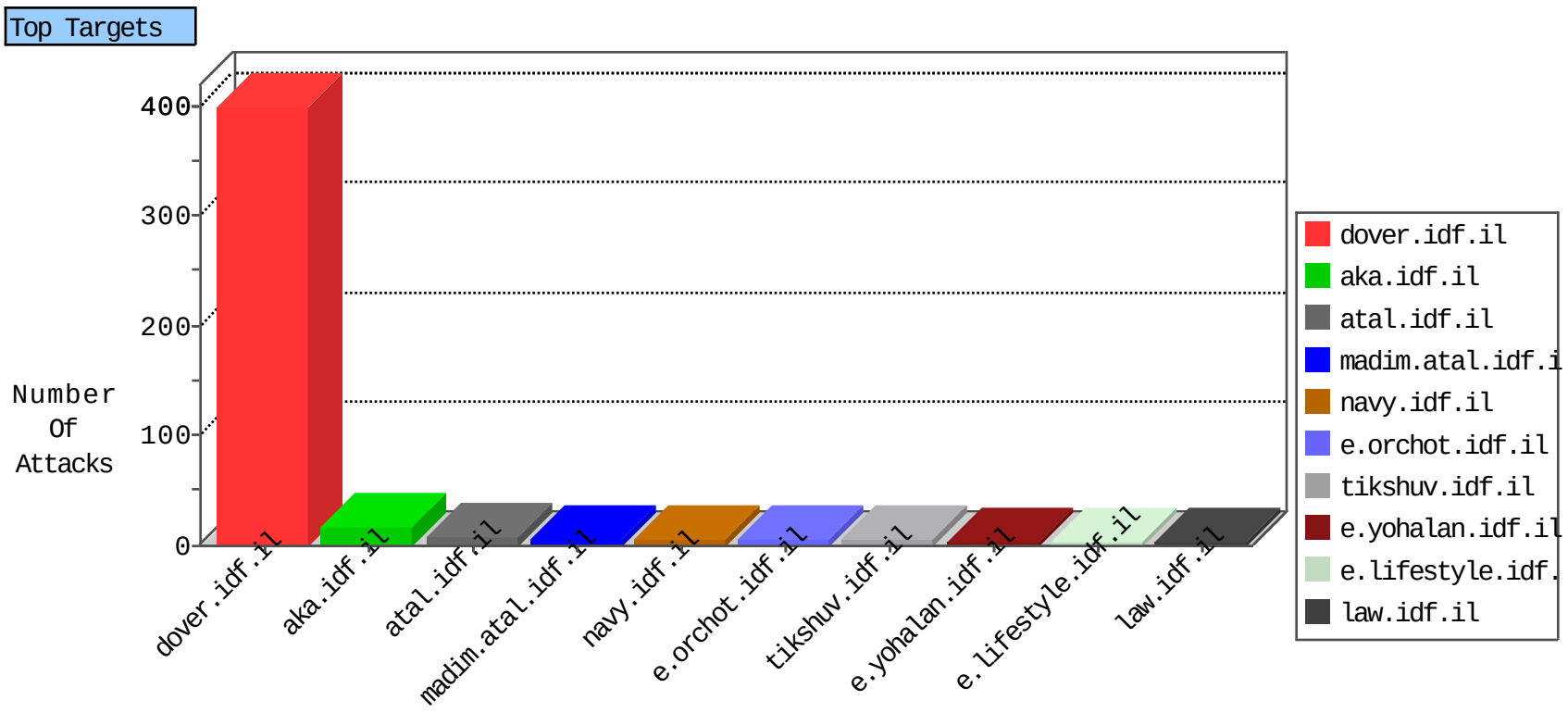
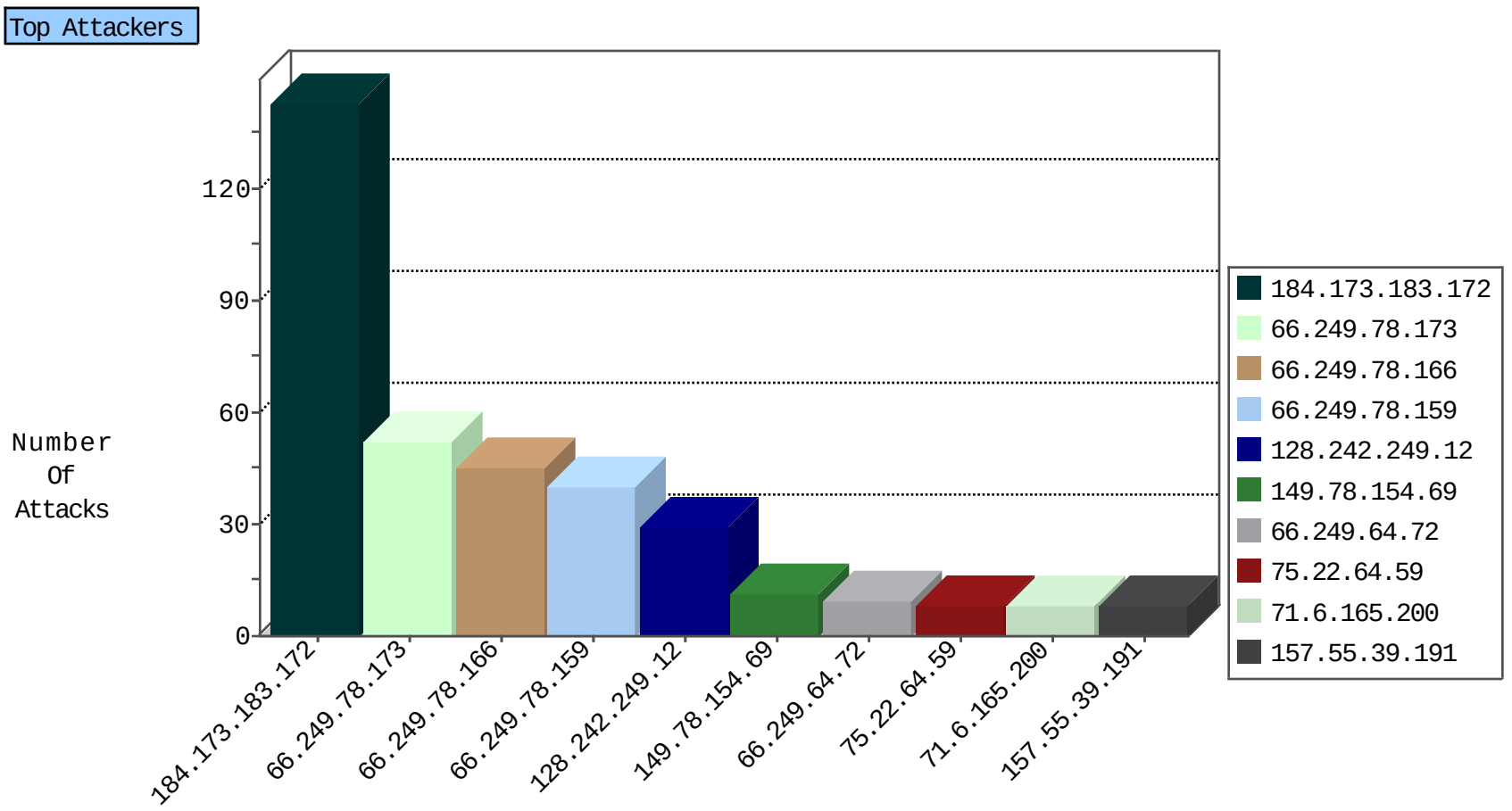
05-04-2015-04:03:03 to 05-04-2015-05:03:03

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

Top Targets



Top Attackers



05-04-2015-04:03:03 to 05-04-2015-05:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.90	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	52
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3

05-04-2015-04:03:03 to 05-04-2015-05:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	143
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	29
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.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
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

05-04-2015-04:03:03 to 05-04-2015-05:03:03

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
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
80.174.78.229	Spain	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
213.210.205.2	Saudi Arabia	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -f -sS	1
202.71.25.29	India	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
121.88.5.177	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
76.76.106.42	Canada	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
213.210.205.2	Saudi Arabia	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
207.46.13.91	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
121.88.5.177	Korea, Republic of	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
76.76.106.42	Canada	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

05-04-2015-04:03:03 to 05-04-2015-05:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
75.22.64.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
171.25.193.20	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
203.86.1.226	China	147.237.77.233	atal.idf.il	SAM rule	drop	drop	6
149.129.160.231	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
187.113.203.195	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.129.160.231	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
84.228.147.16	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.165.15.195	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
84.228.147.16	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
180.76.5.144	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.138.17.205	France	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
70.39.187.112	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
209.37.96.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.105.139.83	United States	147.237.0.33	idf.il		drop	drop	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.187.253.17	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
209.126.110.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.105.139.111	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.163.234.5	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
2.187.253.17	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.109.141.138	Switzerland	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
46.182.106.190	Netherlands	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
209.126.110.112	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
184.105.247.216	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
199.119.124.44	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

05-04-2015-04:03:03 to 05-04-2015-05:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	31
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	26
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	19
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	8
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	4
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	4
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.229.164.111	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.95	France	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/994-9697-he/refuah.aspx	Block	1
46.229.164.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.114	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid\u003d59336 in www.aka.idf.il/main/giyus/general.aspx	None	1
188.165.15.110	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/january/16b.stm	Block	1
66.249.78.44	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
68.180.228.123	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

05-04-2015-04:03:03 to 05-04-2015-05:03:03