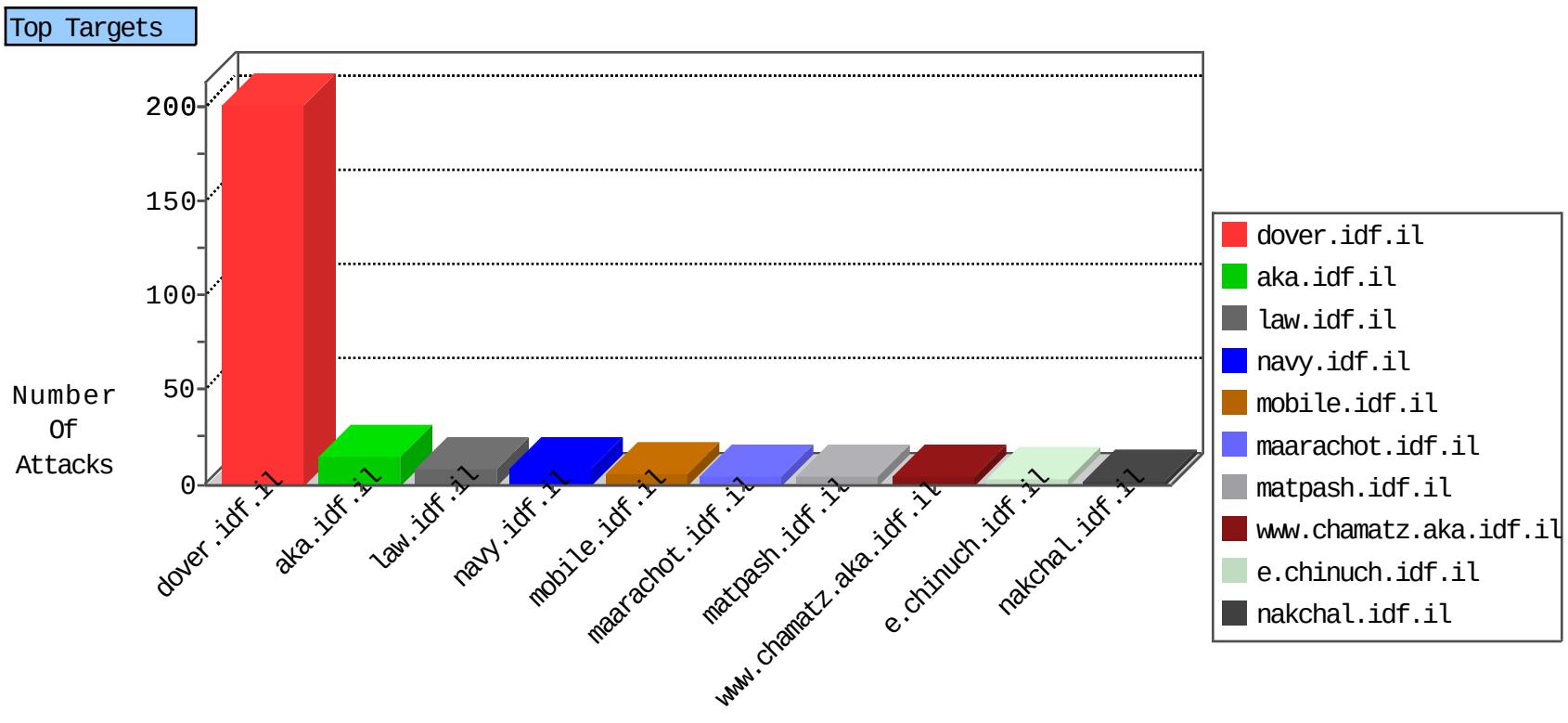
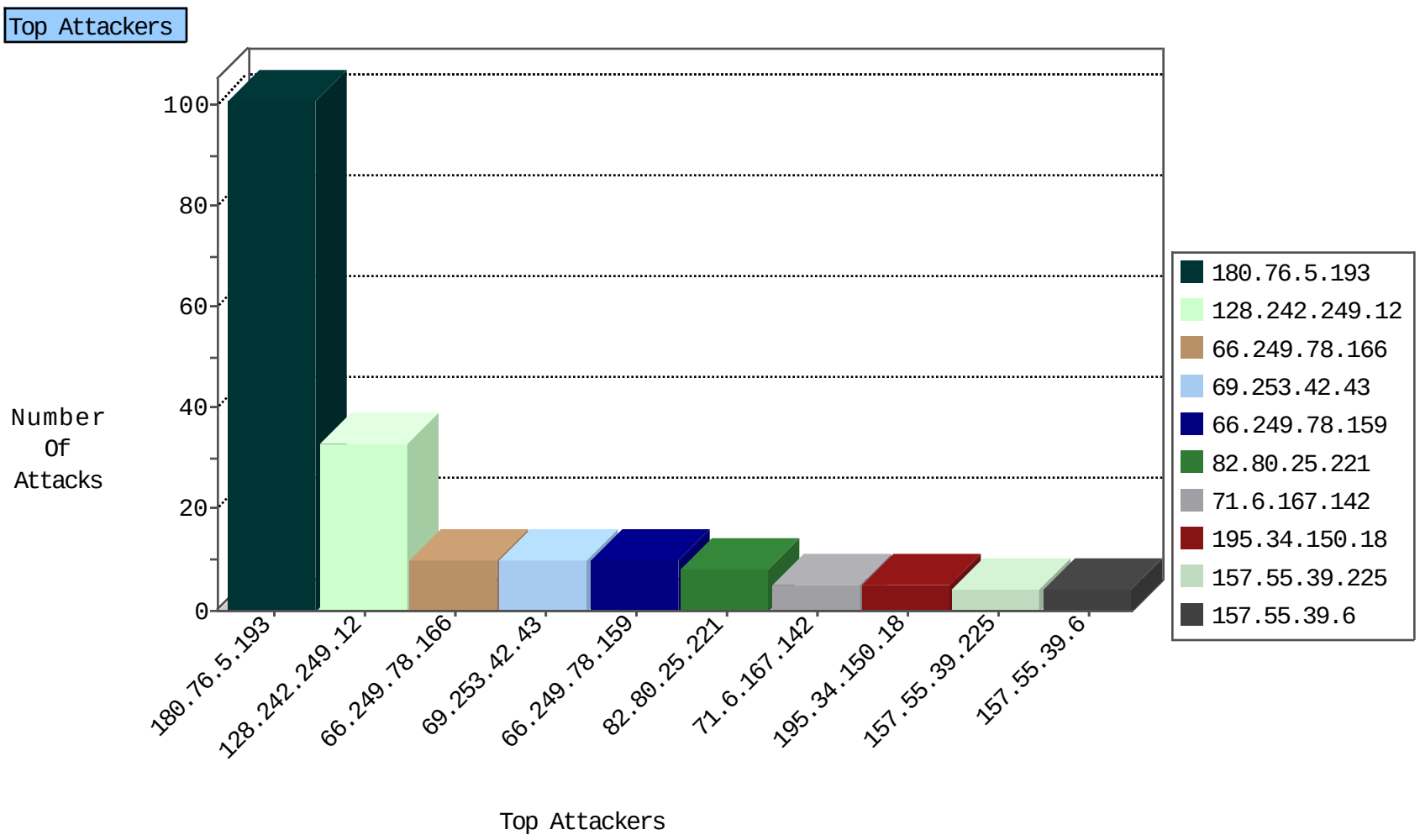
04-26-2015-04:03:05 to 04-26-2015-05:03:05

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





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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3651
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	230
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.32.179.178	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	101
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	33
69.253.42.43	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
201.13.190.33	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
192.116.177.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	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
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1

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

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
46.162.116.49	Sweden	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
46.162.116.49	Sweden	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
188.95.158.103	Ukraine	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
98.143.148.107	United States	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
208.39.68.33	United States	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
46.162.116.49	Sweden	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
188.95.158.103	Ukraine	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
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
69.253.42.43	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
73.46.78.64	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.100	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.183.142.138	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
108.7.14.161	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
123.125.71.69	China	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1

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	3
157.55.39.225	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.225	Block	3
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	2
5.9.151.67	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	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
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	1
66.249.67.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
157.55.39.52	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.111	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
76.14.119.222	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/barak/reshef.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20162-he/kkkkkkk=0ff22d83kkkkkkk_0ff22d83	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-6353-he/	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/search/results.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unknown Parameter b6e681f8 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
1.169.10.7	Taiwan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.52	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 157.55.39.52	Block	1
95.173.190.6	Turkey	147.237.72.167	ishurim.aka.idf.il	Illegal HTTP Version	Block	1
180.76.4.210	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
157.55.39.112	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/x©x§x•x¤x™xª 3	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	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
69.30.240.46	United States	147.237.77.234	halag.idf.il	Illegal HTTP Version	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
157.55.39.52	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	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	Unauthorized URL Access to www.idf.il/newsite/images/0108	Block	1
180.76.6.63	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/1205-ar/cogat.aspx	Block	1
157.55.39.166	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.166	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
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
207.46.13.111	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.225	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
184.105.247.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
157.55.39.166	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.67.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/yoman/	Block	1
207.46.13.111	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 207.46.13.111	Block	1
76.14.119.222	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
172.245.71.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15645-en/dover.aspx/rk=0/rs=lwrilaaq2chpcmod9um7psisa5w-	Block	1