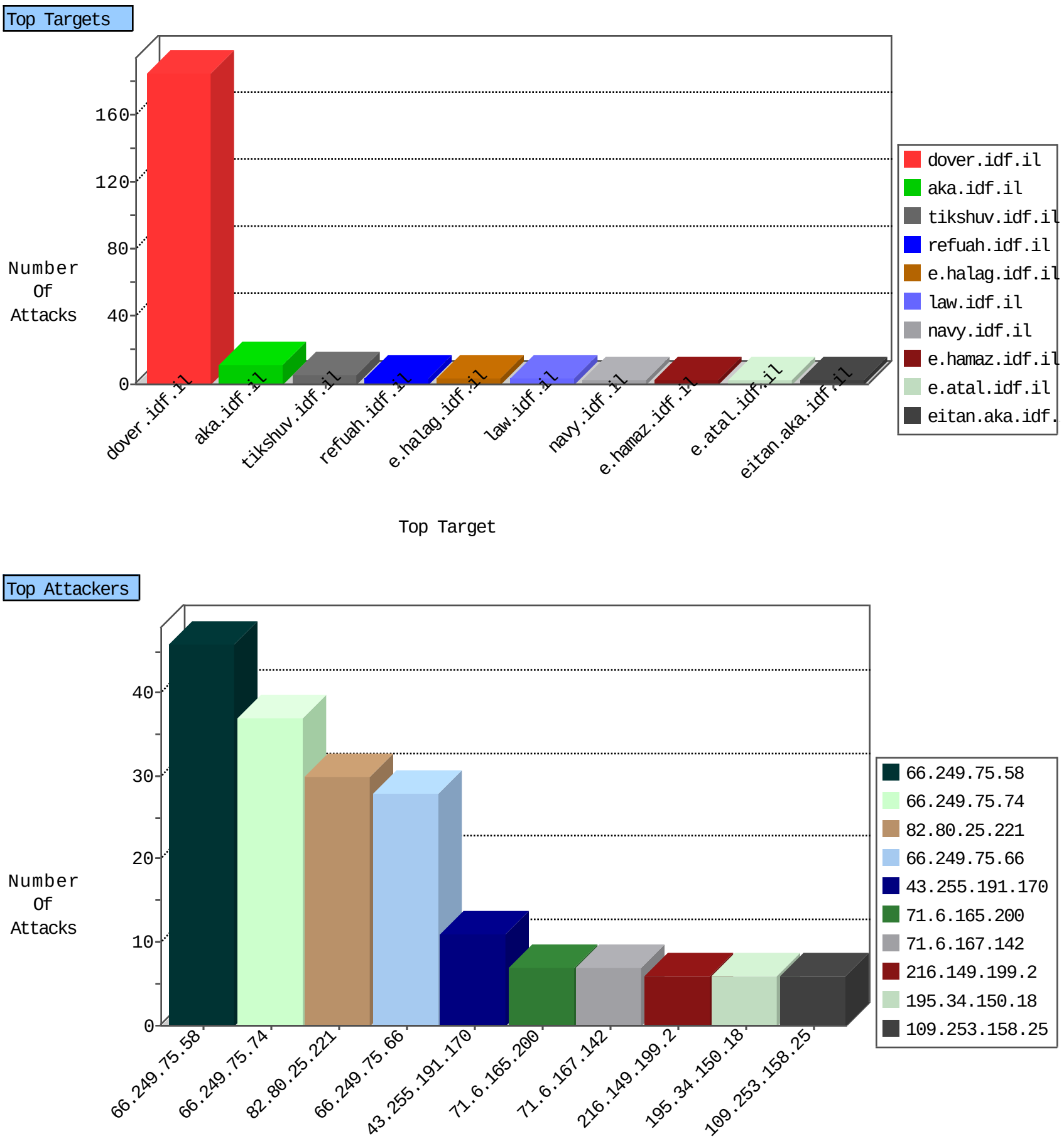
04-02-2015-06:03:05 to 04-02-2015-07:03:05

IDF Under Attack
04-02-2015-06:03:05

Top Targets



Top Attackers

04-02-2015-06:03:05 to 04-02-2015-07:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
198.48.92.104	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-02-2015-06:03:05 to 04-02-2015-07:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.91.181.154	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.65.117.8	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	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.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
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1

04-02-2015-06:03:05 to 04-02-2015-07:03:05

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
66.249.67.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
87.236.215.124	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
169.54.237.52	Switzerland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
128.61.240.66	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.227	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.170	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1

04-02-2015-06:03:05 to 04-02-2015-07:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	30
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.158.25	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
216.149.199.2	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
24.35.204.133	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
146.185.239.104	Russian Federation	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
24.35.204.133	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
218.22.211.69	China	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
184.105.247.207	United States	147.237.8.24	e.lifestyle.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.8.28	e.mobile-ks.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.222	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.253.144.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-02-2015-06:03:05 to 04-02-2015-07:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.157	Block	3
79.178.109.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	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
87.68.253.95	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/')	Block	1
5.77.53.149	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
95.86.116.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
72.192.254.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
198.170.241.46	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
89.42.216.25	Romania	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
66.249.75.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/french/default.stm	Block	1
31.168.217.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
101.22.191.97	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx/trackback/	Block	1
74.82.47.3	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
62.249.198.2	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
93.157.100.74	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
66.249.78.11	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
31.168.217.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
109.65.140.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/58457.pd	Block	1
94.159.152.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/january/26.stm	Block	1
31.168.217.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
109.186.191.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.72.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	1
94.159.152.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.y in aka.idf.il/main/sachar/	None	1
54.145.182.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/mazen.stm	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1

04-02-2015-06:03:05 to 04-02-2015-07:03:05