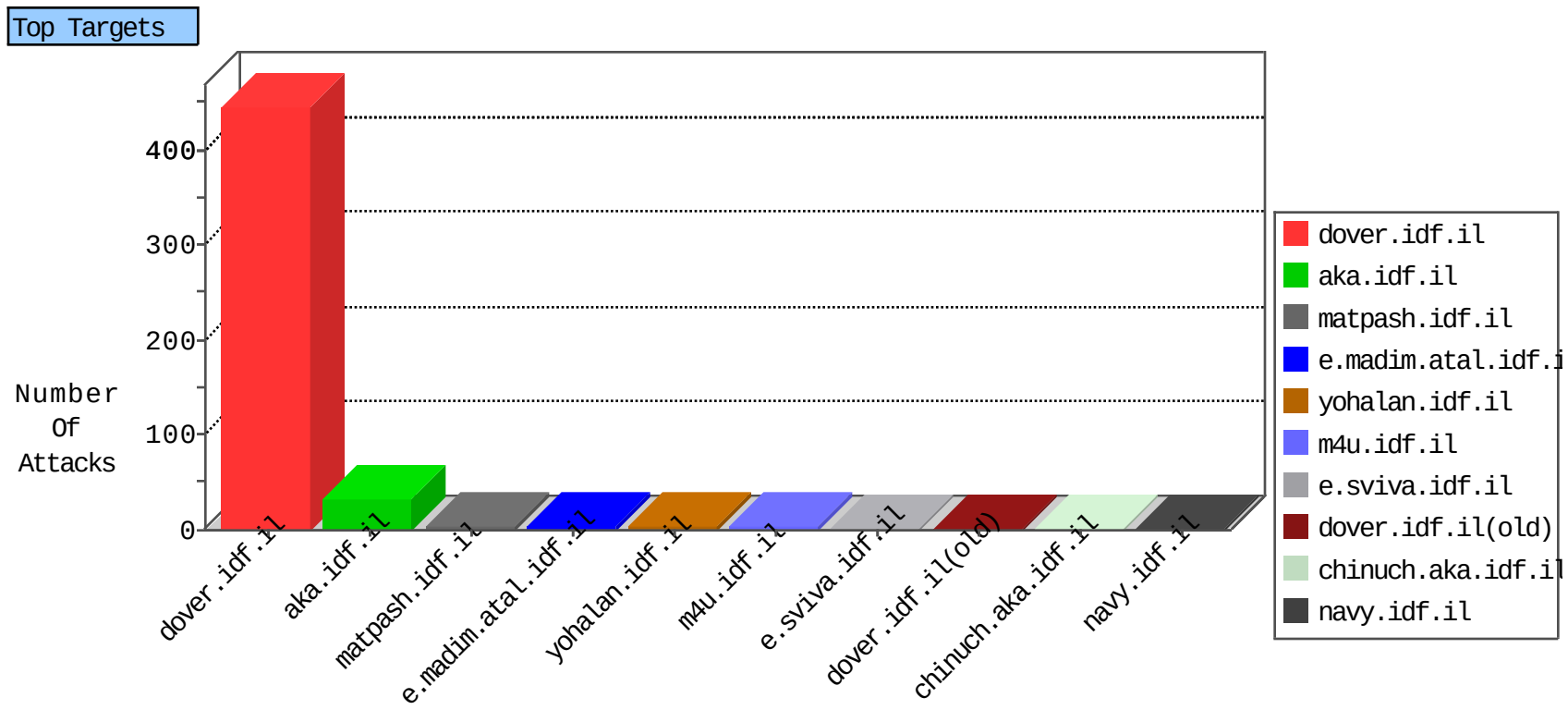
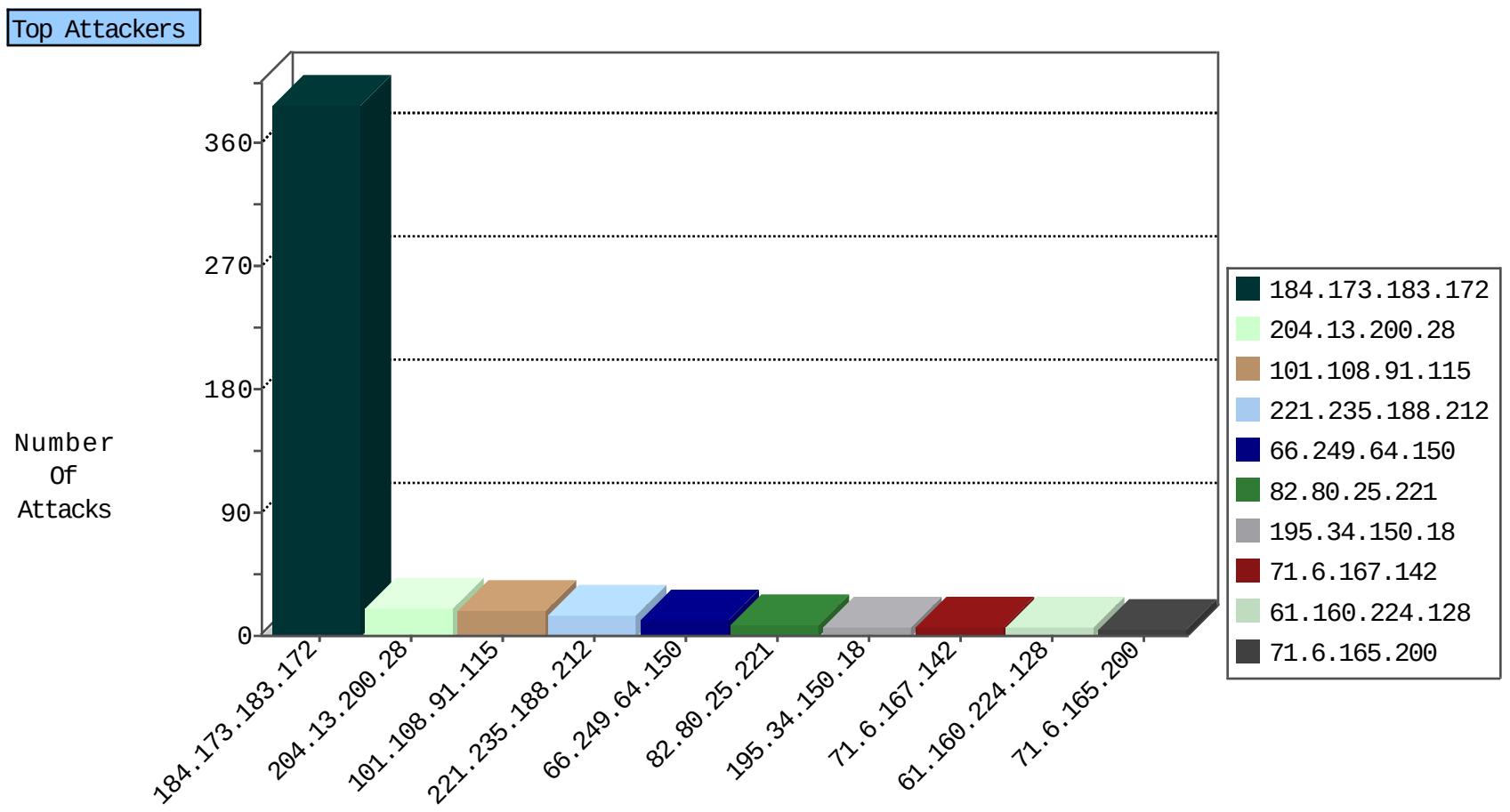
04-01-2015-04:03:07 to 04-01-2015-05:03:07

IDF Under Attack
04-01-2015-04:03:07

Top Targets



Top Attackers



04-01-2015-04:03:07 to 04-01-2015-05:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	282
219.90.235.45	Australia	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.44	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

04-01-2015-04:03:07 to 04-01-2015-05:03:07

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	388
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
24.185.1.223	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
109.201.152.225	Netherlands	147.237.8.27	e.madim.atal.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	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
109.201.152.225	Netherlands	147.237.76.198	e.yohalan.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
71.6.167.142	United States	147.237.77.235	sviva.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
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-04:03:07 to 04-01-2015-05:03:07

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	6
61.160.224.128	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
208.124.237.146	Canada	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.196.147.122	Germany	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-04:03:07 to 04-01-2015-05:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
101.108.91.115	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.183	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.183	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
141.212.122.63	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
90.63.151.249	France	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
37.16.72.139	France	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.119	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
184.105.247.235	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
71.6.216.36	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.61	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
198.20.69.74	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
71.6.216.50	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.62	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
216.218.206.83	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
71.6.216.62	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-01-2015-04:03:07 to 04-01-2015-05:03:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
90.63.151.249	France	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.69.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
180.76.4.135	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalanfaq/faq.asp	Block	1
2.54.40.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
90.63.151.249	France	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.75.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
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	1
2.54.40.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00_ctl00_ScriptManager1_HiddenField in aka.idf.il/main/sachar/	None	1
93.172.169.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/te emplates/inner.asp	Block	1
79.182.207.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
52.4.217.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/nifg.stm.	Block	1
125.209.235.171	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
79.182.207.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl65 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.150	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/common/includes/bignewswnd.asp	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1

04-01-2015-04:03:07 to 04-01-2015-05:03:07