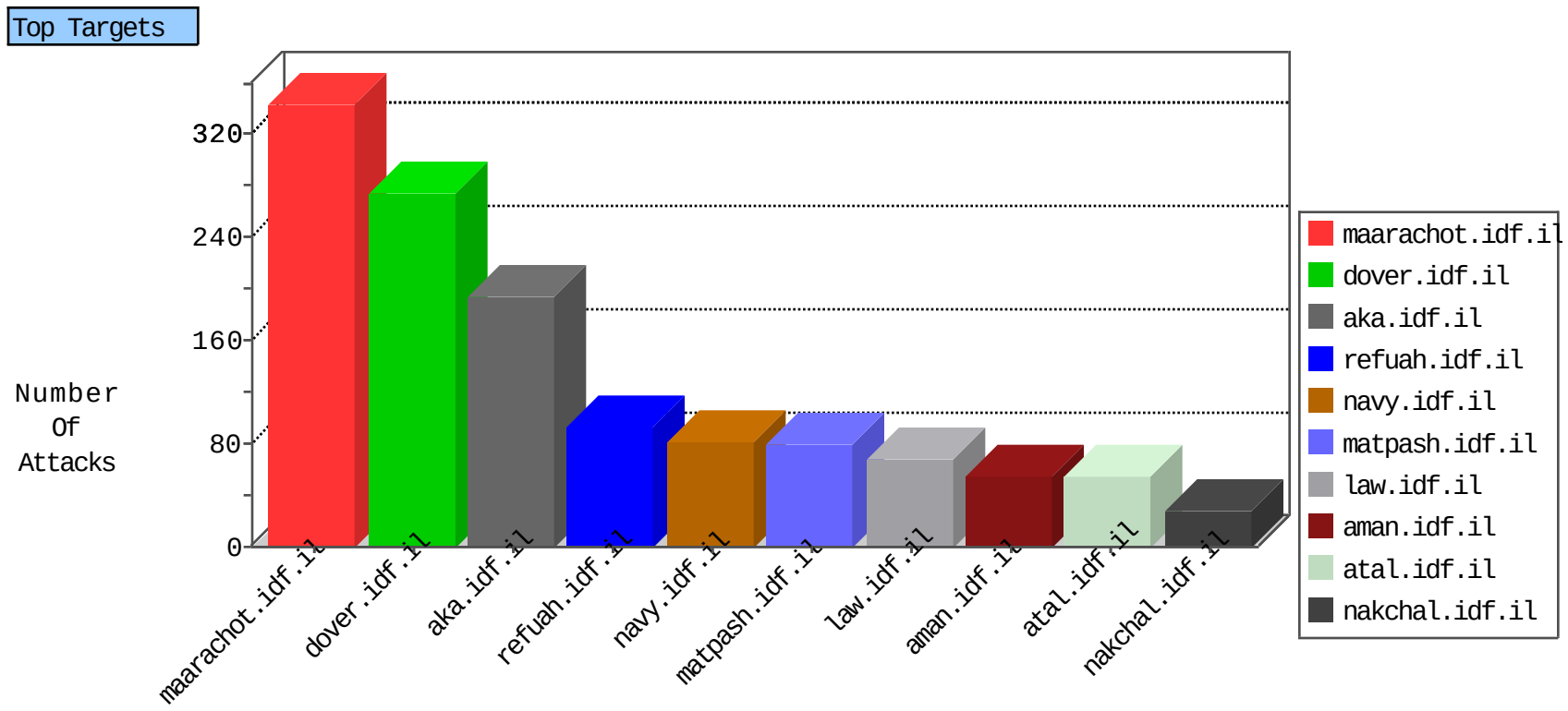
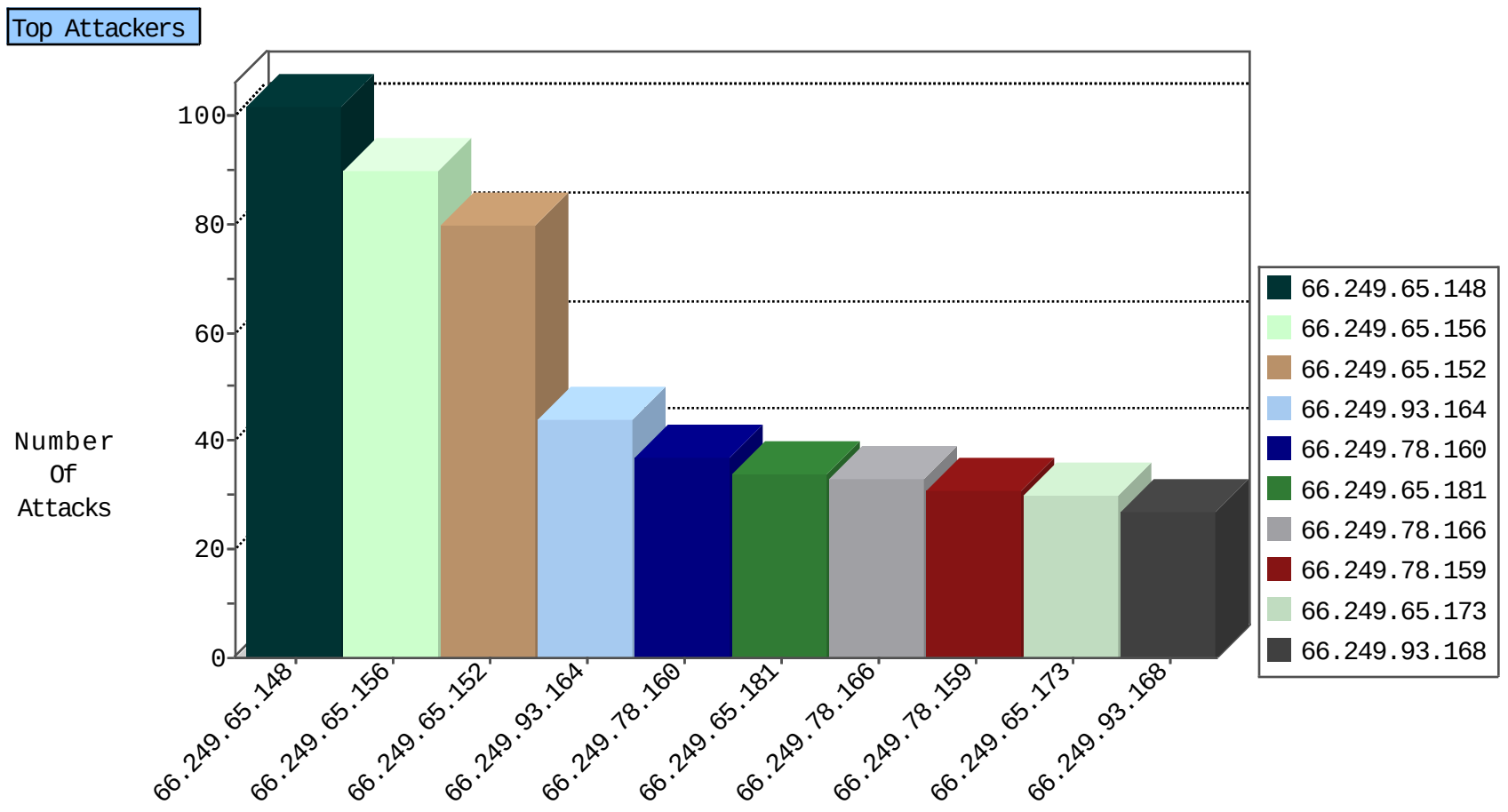
04-05-2015-05:03:07 to 04-05-2015-06:03:07

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

Top Targets



Top Attackers



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	98
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	90
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	80
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	44
66.249.78.160	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	37
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	34
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	33
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	31
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	27
66.249.65.191	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	27
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.78.137	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	25
66.249.78.153	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	25
66.249.78.144	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	24
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	23
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	22
66.249.78.130	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.78.2	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	20
66.249.78.254	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	19
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	18
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.65.187	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.9	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.79.71	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	15
66.249.79.42	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.79.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.79.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	14
66.249.79.63	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	14
66.249.75.39	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.134	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.90.82	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.64.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.65.195	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	9
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	8
66.249.64.8	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.79.140	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.79.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.75.31	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.79.132	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.69.83	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.148	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.64.45	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
66.249.64.117	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.80.83	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	25
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
93.115.82.54	Anonymous Proxy	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
147.226.238.247	United States	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
89.139.182.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1

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

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
61.160.224.128	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
211.144.94.227	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
211.144.94.227	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
31.192.105.59	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.144.94.227	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.192.105.59	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
211.144.94.227	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.140.170	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.143.144	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	10
17.142.152.85	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
23.28.137.23	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.4	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
220.181.108.145	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
220.181.108.152	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
220.181.108.174	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
17.142.152.111	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
82.102.141.255	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
82.102.141.255	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
176.12.147.192	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.72	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
82.102.141.255	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
176.12.147.192	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
92.19.110.120	United Kingdom	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	1
193.106.206.10	Israel	147.237.72.156	aman.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
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
93.172.56.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.255	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
93.172.56.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
5.29.49.127	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.49.127	Block	1
202.46.49.138	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	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
107.208.97.151	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.29.49.127	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/registrationwizard/register.aspx	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1219-2.stm	Block	1
32.209.208.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
72.181.140.122	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20038-he/dover.aspx<span style='color:red	Block	1
37.26.146.175	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1