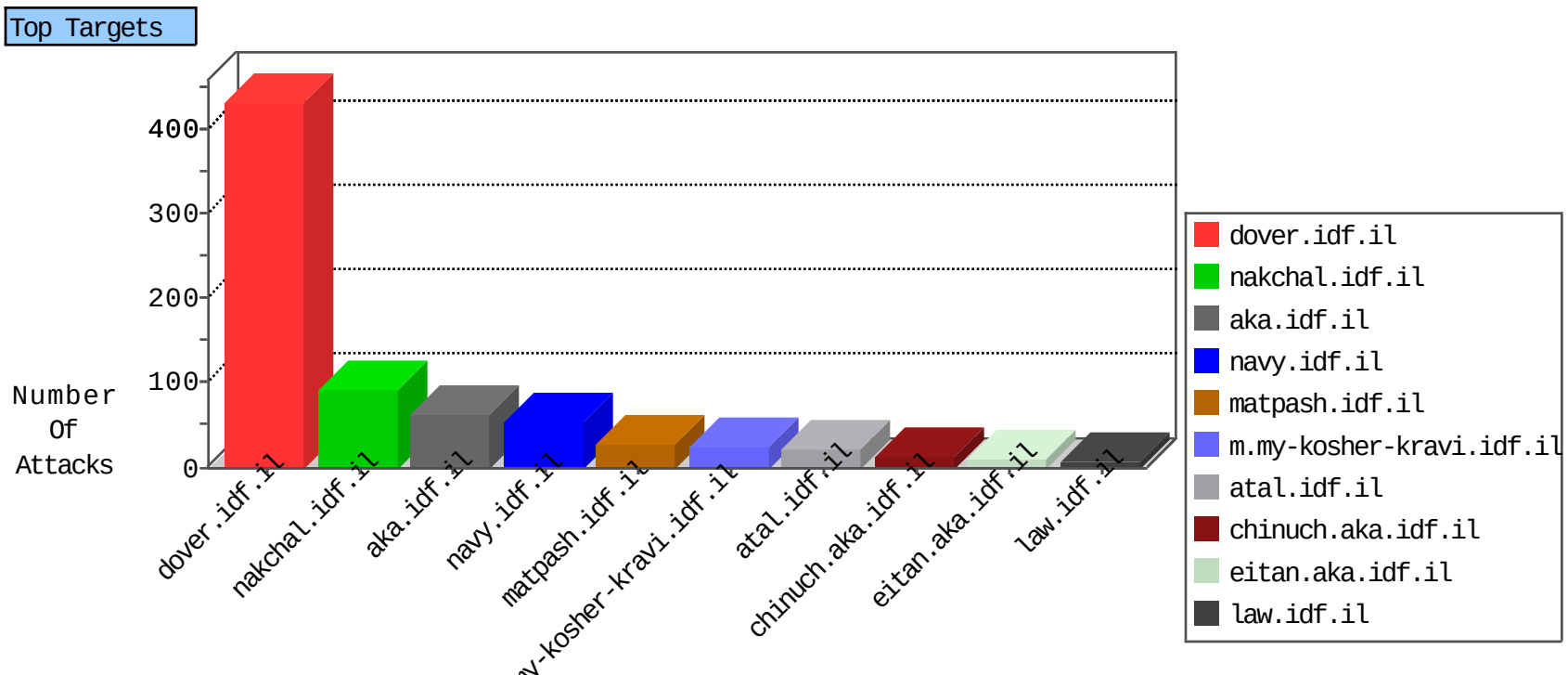
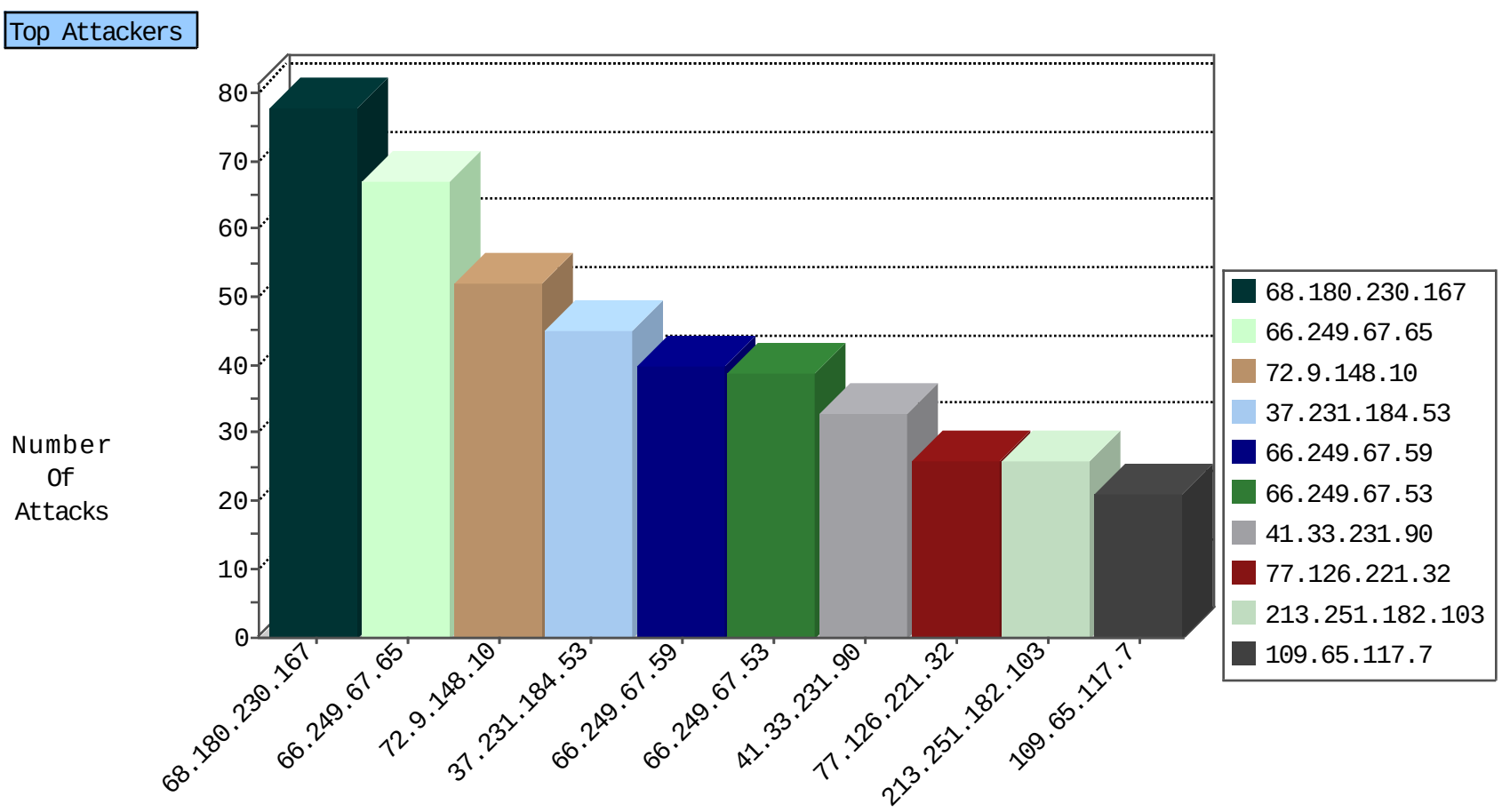
10-21-2015-02:04:07 to 10-21-2015-03:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-02:04:07 to 10-21-2015-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.108.183	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	264
89.248.172.98	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.146	Netherlands	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
93.174.93.146	Netherlands	147.237.76.147	chinuch.aka.idf.il	Invalid TCP Flags	drop	1

10-21-2015-02:04:07 to 10-21-2015-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-02:04:07 to 10-21-2015-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
93.174.89.142	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
5.8.60.88	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
174.128.228.82	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
174.128.228.82	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
101.1.17.53	147.237.72.14	Hong Kong	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
93.174.89.142	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.89.142	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
174.128.228.82	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
162.248.10.134	147.237.76.202	Canada	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
113.59.33.61	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.89.142	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-21-2015-02:04:07 to 10-21-2015-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.231.184.53	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
109.65.117.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
184.171.239.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
186.188.226.123	Panama	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.78.99		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
70.118.229.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
131.253.25.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
197.36.162.91	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.75.211.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.90.8	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
79.183.101.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.184	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
207.46.13.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
71.137.242.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.202	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.55.210.20	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.75.102.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
98.114.138.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
86.85.174.241	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.141	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
89.138.79.137	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
216.4.56.184	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.165.15.89	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.111.30.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.237	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.66.200.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.102.234.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.140.178.250	Russian Federation	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.221	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
72.235.50.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
198.20.69.74	United States	147.237.0.19	madim.atal.idf.i	drop	SAM rule	drop	1
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.12.143.60	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

10-21-2015-02:04:07 to 10-21-2015-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	78
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	52
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	39
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	26
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	26
77.126.221.32	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 77.126.221.32	None	13
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
207.46.13.40	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	13
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
66.249.67.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	13
84.229.197.198	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
220.181.108.84	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	13
157.55.39.212	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
77.126.221.32	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	13
192.99.12.99	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13

10-21-2015-02:04:07 to 10-21-2015-03:04:07