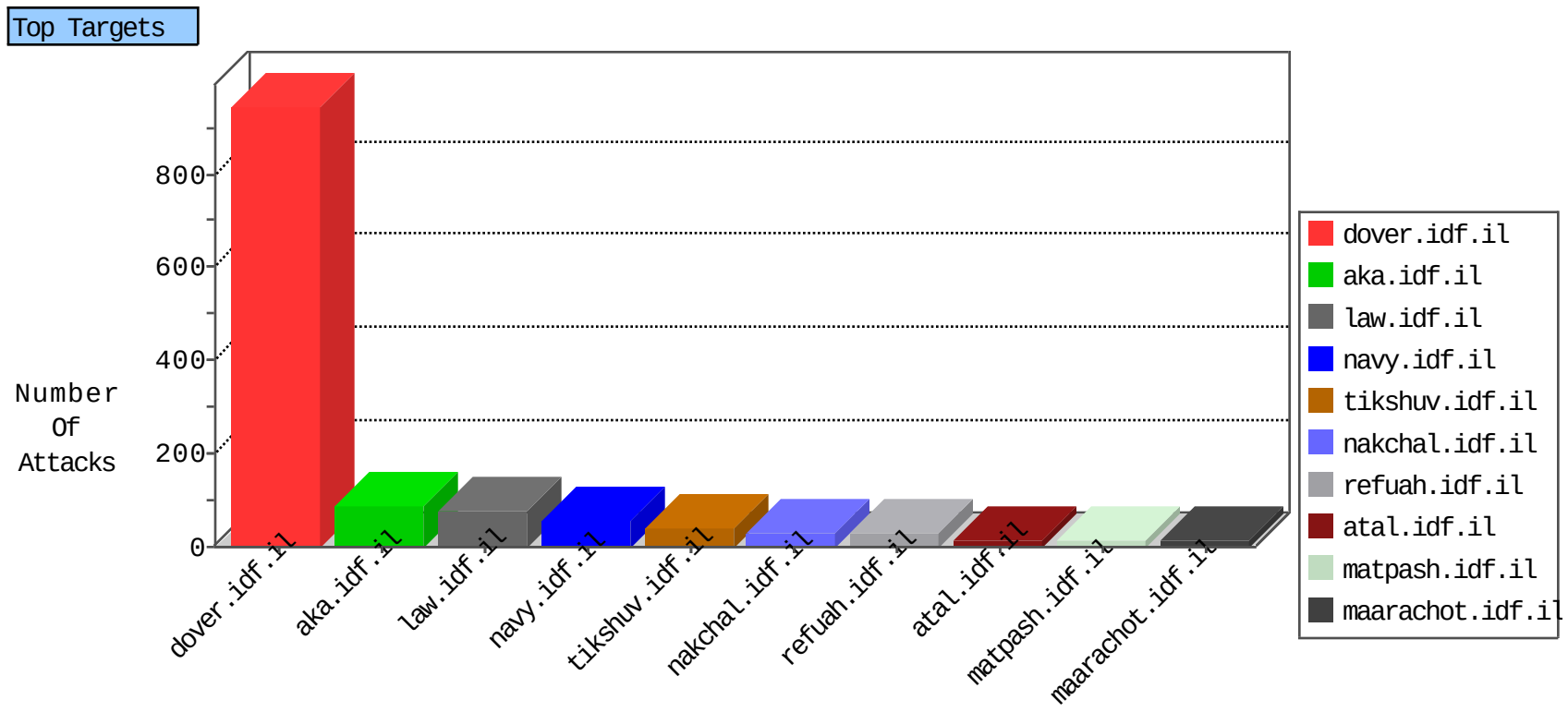
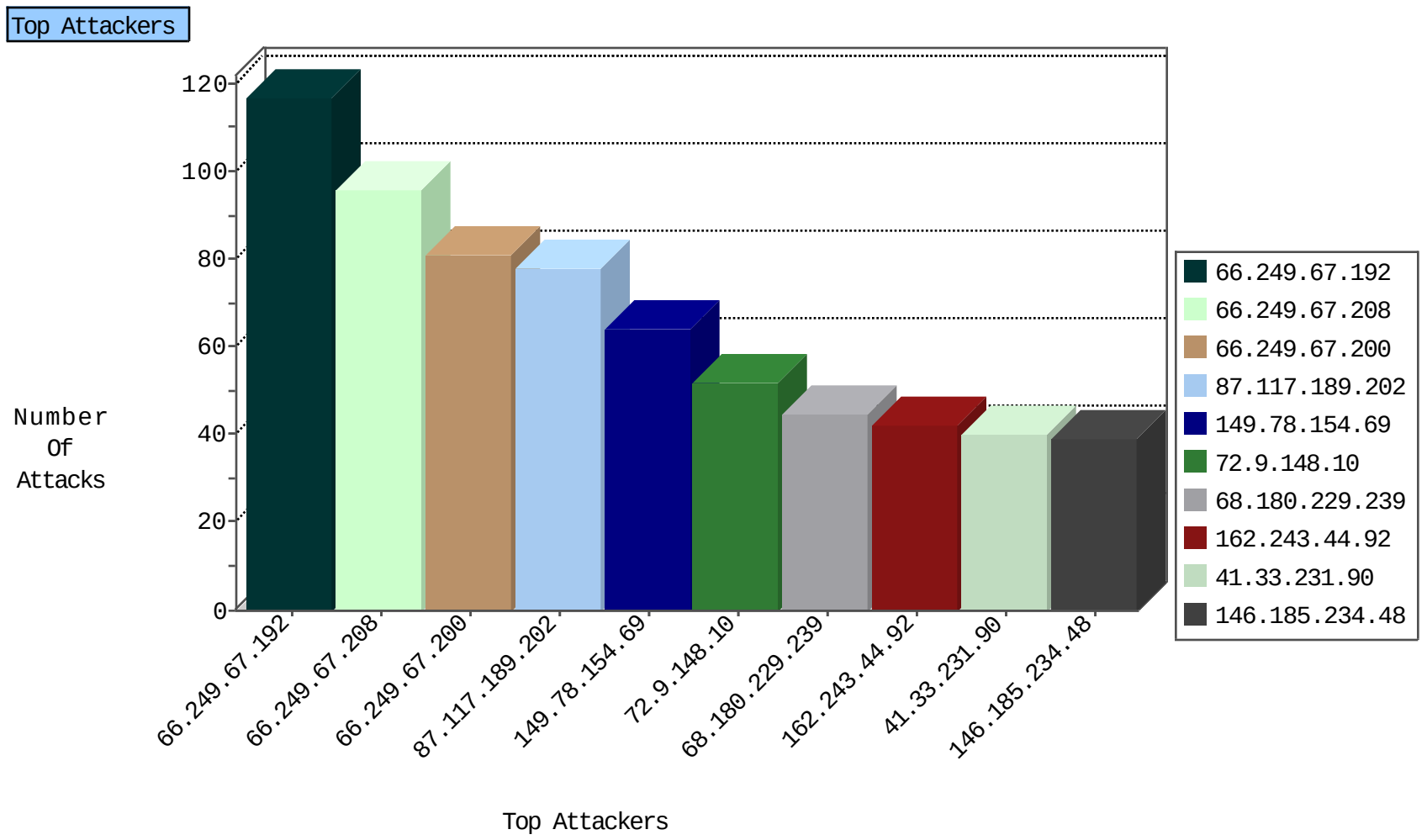
10-21-2015-05:04:08 to 10-21-2015-06:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-05:04:08 to 10-21-2015-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.192	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4094
202.126.217.136	Hong Kong	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	5
79.182.5.230	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.93.146	Netherlands	147.237.76.30	himush.idf.il	Invalid TCP Flags	drop	1
89.248.172.98	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
50.7.207.42	Czech Republic	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.146	Netherlands	147.237.0.33	idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.146	Netherlands	147.237.8.24	e.lifestyle.idf.	Invalid TCP Flags	drop	1

10-21-2015-05:04:08 to 10-21-2015-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-05:04:08 to 10-21-2015-06:04:08

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	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.67.200	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.201	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.107.16.206	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
78.188.236.24	147.237.76.34	Turkey	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.128.228.82	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
108.61.220.143	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.172.201	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.201	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
190.128.136.222	147.237.76.197	Paraguay	e.himush.idf.il	ET SCAN Potential SSH Scan	1
139.162.215.8	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.201	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

10-21-2015-05:04:08 to 10-21-2015-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
162.243.44.92	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
79.182.5.230	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	26
67.84.27.125	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
78.53.241.213	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
5.22.129.148	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
176.12.151.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
189.139.137.13	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
78.53.241.213	Germany	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
17.142.152.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
190.218.46.242	Panama	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
117.221.212.103	India	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
80.246.130.60	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.249.67.192	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
151.80.31.115	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	SAM rule	drop	7
17.142.152.86	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
109.66.200.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
71.190.255.85	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
157.55.39.237	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
100.8.103.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
17.142.145.3	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
66.249.67.208	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
17.142.152.72	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
157.55.39.255	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
17.142.156.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
157.55.39.255	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
200.3.185.129	Argentina	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
174.1.75.151	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	4
17.142.152.110	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
207.46.13.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
66.249.67.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
71.232.180.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
100.100.87.247		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3
157.55.39.26	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	3

10-21-2015-05:04:08 to 10-21-2015-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	78
87.117.189.202	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 87.117.189.202	Block	65
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
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	52
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	52
68.180.229.239	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	39
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born	Block	26
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	26
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
182.118.53.125	China	147.237.76.31	nakchal.idf.il	URL is Above Root Directory nakhal.idf.il/../shared/clientscripts/jquery/expand.js	Block	13
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
87.117.189.202	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/faq/faq.aspxsb_item_lev1	Block	13
182.118.60.138	China	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../shared/clientscripts/sa_swfobject.js	Block	13
77.237.138.51	Czech Republic	147.237.77.170	maarachot.idf.i	Unauthorized URL Access to /	Block	13
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/mazi.idf.il	Block	13
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	13
79.180.143.80	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
66.249.67.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	13
207.46.13.82	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	13
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
157.55.39.198	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	13
70.192.139.76	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
207.46.13.163	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/patzar/klali/default.asp	None	13
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13

10-21-2015-05:04:08 to 10-21-2015-06:04:08