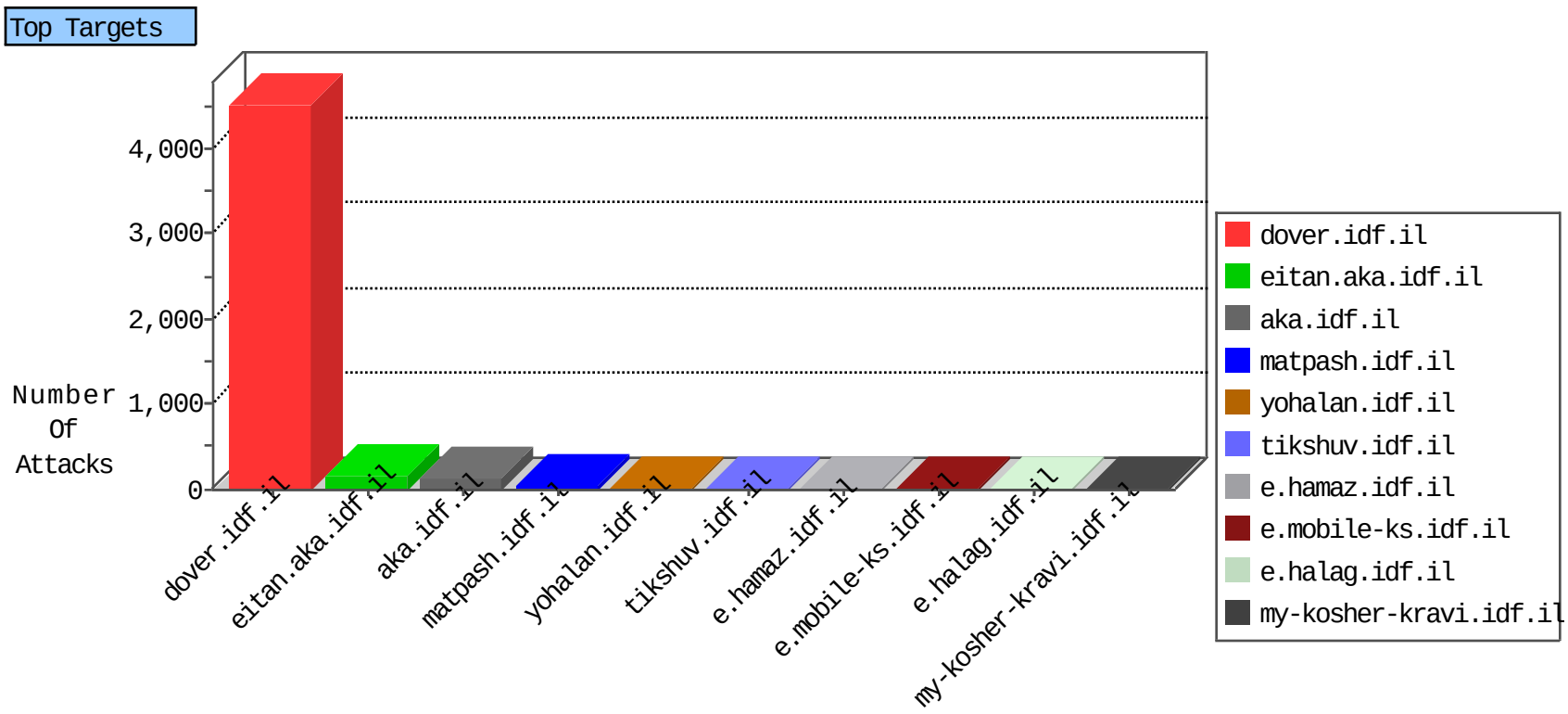
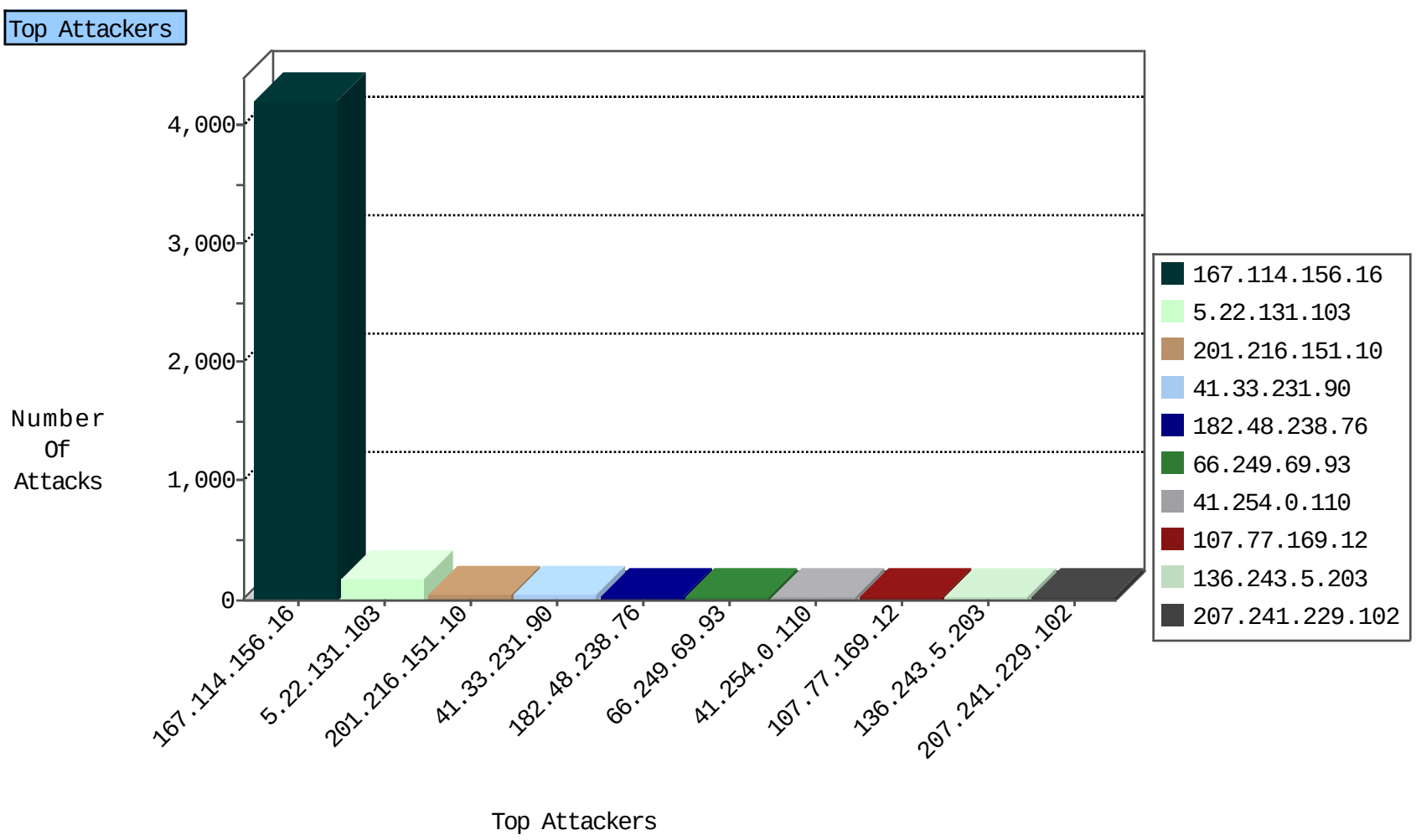
04-21-2016-05:04:00 to 04-21-2016-06:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-21-2016-05:04:00 to 04-21-2016-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4166
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2453
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1921
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1768
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
94.102.52.10	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1

04-21-2016-05:04:00 to 04-21-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-21-2016-05:04:00 to 04-21-2016-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
169.54.244.84	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
119.206.211.18	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.195.135.82	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.180.66.29	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.131	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.139	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.84	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
13.94.239.168	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.84	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.244.84	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.248	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.54.244.84	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
203.197.205.118	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
169.54.244.84	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
95.173.184.12	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.131	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
67.211.217.131	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
169.54.244.84	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
13.94.239.168	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.244.84	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
169.54.244.84	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
169.54.244.84	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.248	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-21-2016-05:04:00 to 04-21-2016-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2681
5.22.131.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	165
201.216.151.10	Guatemala	147.237.72.166	aka.idf.il	drop	SAM rule	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
182.48.238.76	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.254.0.110	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	23
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
107.77.169.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
188.72.103.226	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
70.195.209.255	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
90.204.52.191	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
203.254.51.16	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.131.103	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
73.22.155.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.131.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
107.77.168.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
107.77.169.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.55.152.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.175	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.108.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.65	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.81.65.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.26	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.103.252.141	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.221	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.153.165.60	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

04-21-2016-05:04:00 to 04-21-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
201.216.151.10	Guatemala	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	9
95.86.122.91	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 95.86.122.91	Block	6
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	4
207.46.13.118	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	3
95.86.122.91	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.86.122.91	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
17.138.55.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20169-he/dover.aspx	Block	2
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8820-he/refuah.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.51	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
95.86.122.91	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/mobile	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1

04-21-2016-05:04:00 to 04-21-2016-06:04:00