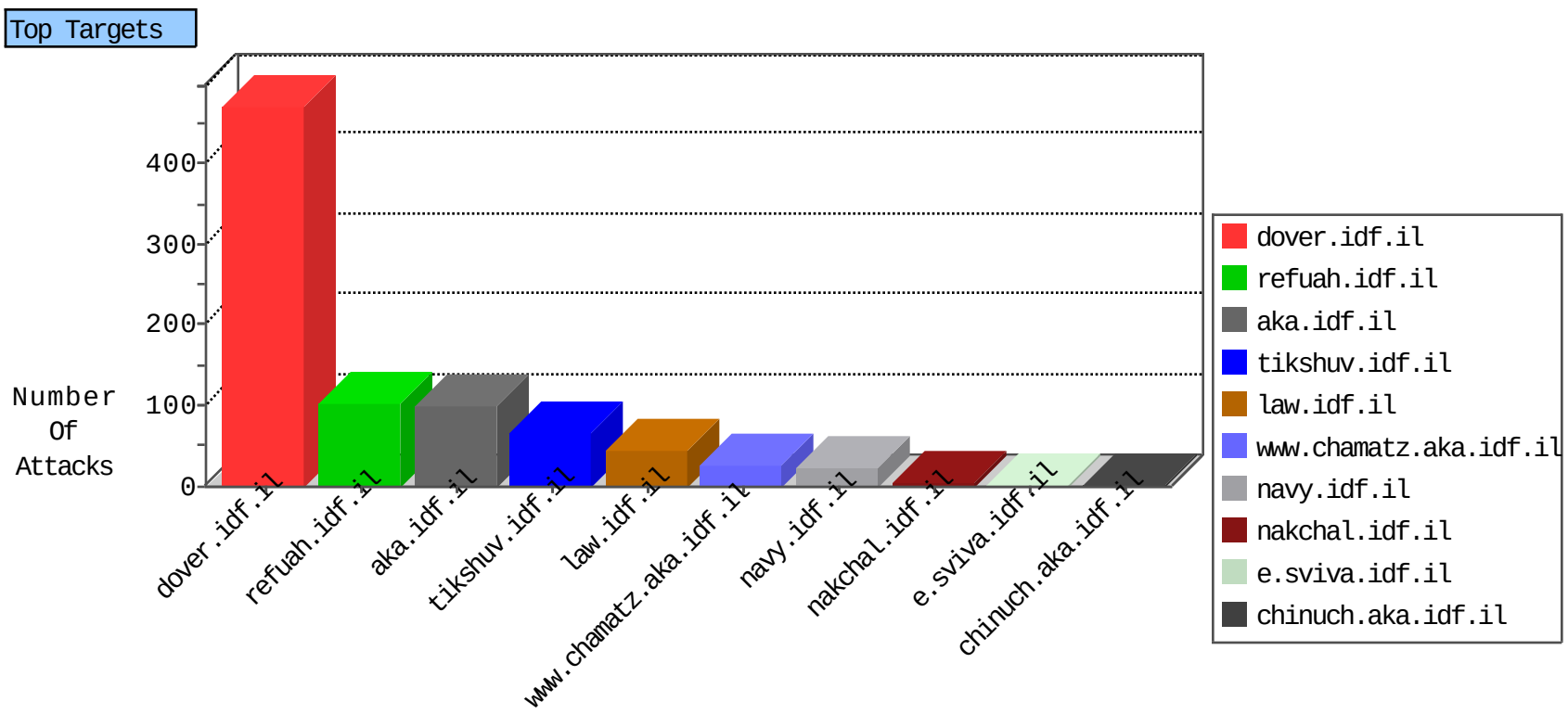
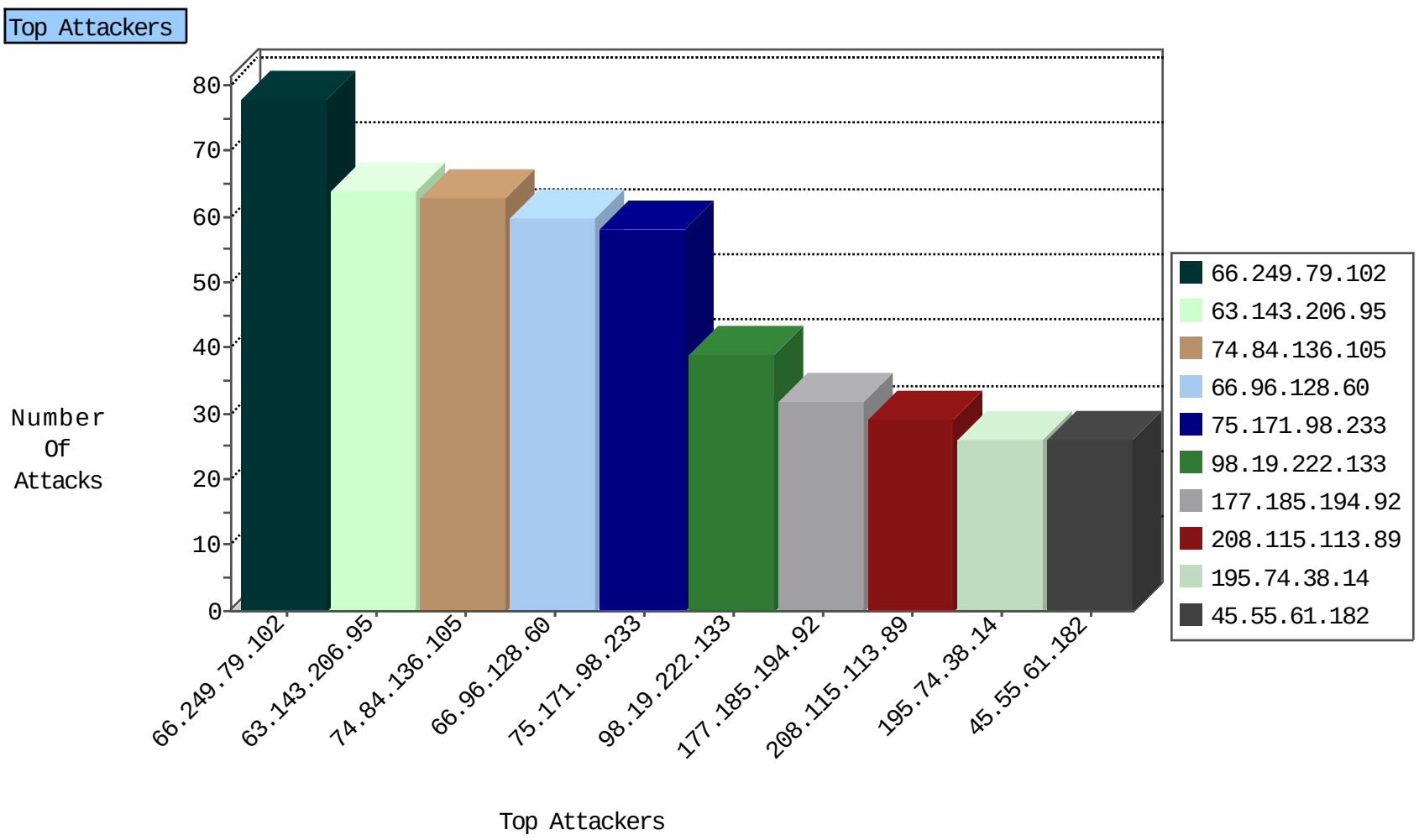
04-30-2016-05:04:01 to 04-30-2016-06:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-30-2016-05:04:01 to 04-30-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.212.75.106	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3452
123.59.59.52	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
5.206.231.84	Portugal	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
5.206.231.84	Portugal	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

04-30-2016-05:04:01 to 04-30-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
195.74.38.14	Sweden	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.96.128.60	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
74.84.136.105	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
195.74.38.14	Sweden	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.96.128.60	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.84.136.105	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.194.92	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.84.136.105	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.92	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

04-30-2016-05:04:01 to 04-30-2016-06:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.84.136.105	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	47
66.96.128.60	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	36
98.19.222.133	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	28
177.185.194.92	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	24
195.74.38.14	147.237.77.226	Sweden	www.chamatz.aka.idf.il	SQL Injection - Select From	14
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.199.48.57	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
203.86.29.220	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
40.76.60.52	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
193.201.227.63	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
112.184.135.220	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.199.48.57	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
40.76.60.52	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
195.154.54.169	147.237.76.202	France	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.63	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-30-2016-05:04:01 to 04-30-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
63.143.206.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
75.171.98.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
45.55.61.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
162.243.97.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
125.215.199.5	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.96.128.60	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.212.123.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
139.162.216.112	United States	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
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.132.59.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.7.249.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
192.0.114.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.228.204.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.19	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	3
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.119.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.220.158.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.95.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.70.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
118.193.208.231	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.106.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
63.143.206.95	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
203.20.167.12	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.63.188.200	United States	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

04-30-2016-05:04:01 to 04-30-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 88.198.48.46	Block	2
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
118.193.208.231	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.79.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
54.188.170.125	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/homepage.aspx	Block	1
66.249.79.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
88.198.48.46	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
54.212.76.205	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415-10815-he/kkkkkkk=e248d0a6kkkkkkk_e248d0a6	Block	1
83.218.138.87	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
109.65.222.105	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
118.193.208.231	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.182	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1
207.46.13.50	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-7860-he	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/apple-app-site-association	Block	1

04-30-2016-05:04:01 to 04-30-2016-06:04:01