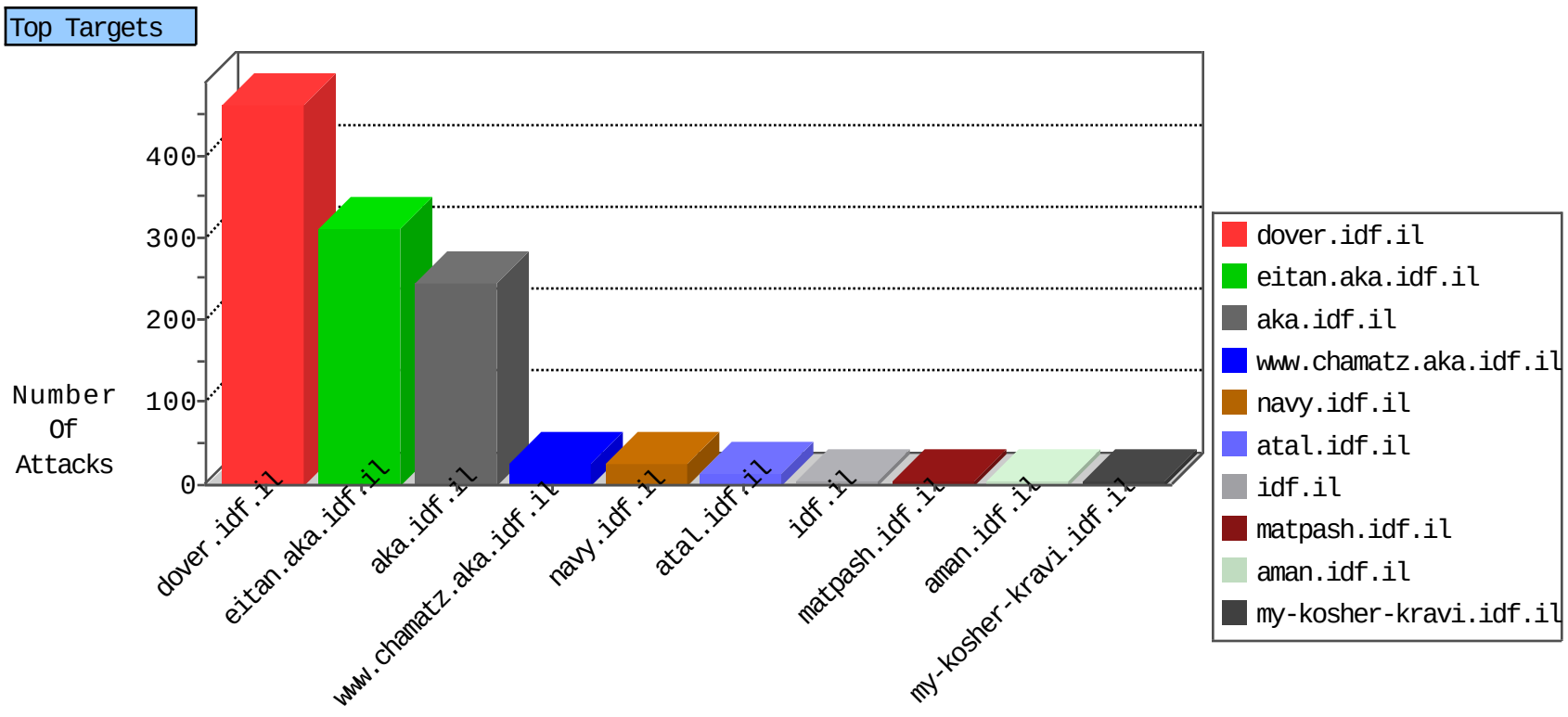
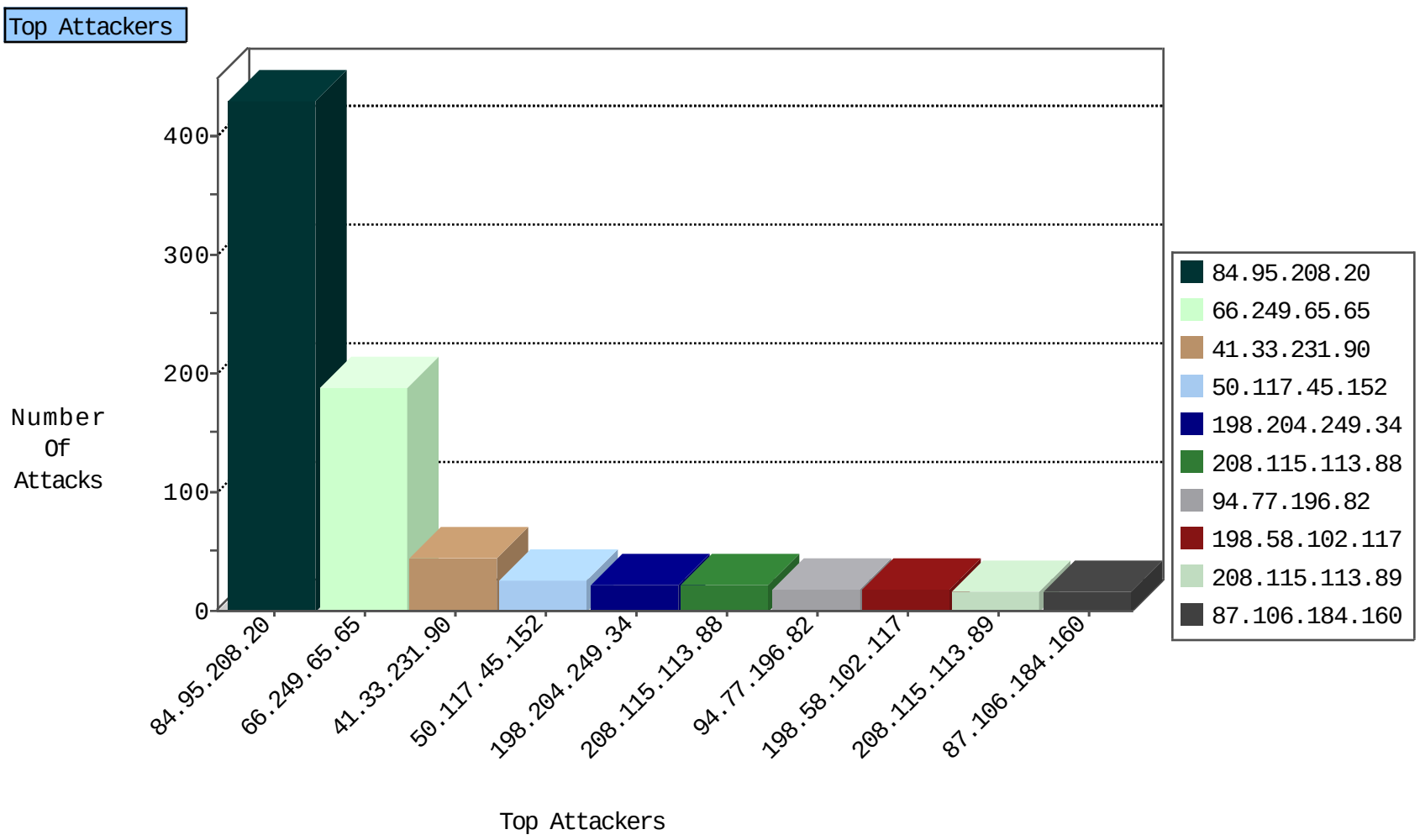
04-22-2016-03:04:09 to 04-22-2016-04:04:09

IDF Under Attack
Daily Report





04-22-2016-03:04:09 to 04-22-2016-04:04:09

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	845
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
198.58.103.115	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.135.131	United States	147.237.76.196	e.sviva.idf.i	Block_Udp_All_Nets	drop	1

04-22-2016-03:04:09 to 04-22-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.106.184.160	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4

04-22-2016-03:04:09 to 04-22-2016-04:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.106.184.160	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	12
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
190.124.35.115	147.237.76.176	Nicaragua	test.ncore.idf.i	ET SCAN NMAP -f -sS	1
151.11.201.3	147.237.0.33	Italy	idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.0.33	Italy	idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
190.190.1.188	147.237.0.33	Argentina	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.124.35.115	147.237.76.176	Nicaragua	test.ncore.idf.i	ET SCAN NMAP -sS window 2048	1
158.255.5.147	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.0.33	Italy	idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
95.173.184.12	147.237.0.200	Turkey	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.173.215.68	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
190.124.35.115	147.237.76.176	Nicaragua	test.ncore.idf.i	ET SCAN NMAP -sS window 4096	1

04-22-2016-03:04:09 to 04-22-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	222
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	183
50.117.45.152	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
198.204.249.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
159.203.40.191	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
1.127.48.183	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
196.221.203.100	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.22.135.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.73.243	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	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
71.230.192.23	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
166.137.136.109	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
50.128.158.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
172.56.40.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
118.173.135.239	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.187.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.128.158.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.121.251.180	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.43	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
71.206.141.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.74.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
108.33.201.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
70.193.68.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.135.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
73.101.67.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-22-2016-03:04:09 to 04-22-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	103
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	20
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	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	6
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.65	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
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	2
66.220.145.244	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
64.134.97.176	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/portalmiluim/templates/inner.asp	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	1
66.220.145.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	1
65.55.210.241	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.120	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
5.39.76.158	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
79.177.145.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/miluim/templates/inner.asp	None	1
65.55.210.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.64.191	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.15	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.12	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.249.65.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

04-22-2016-03:04:09 to 04-22-2016-04:04:09