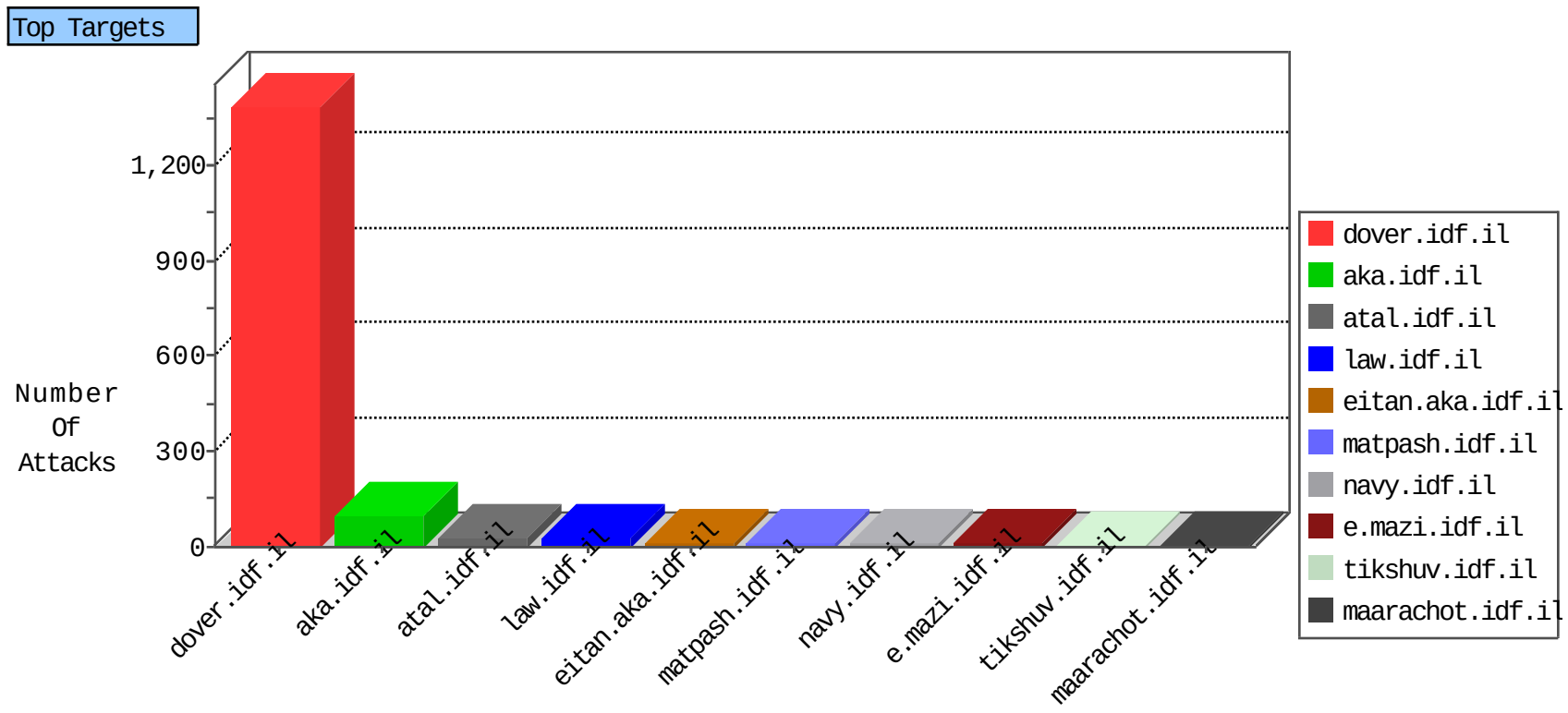
05-02-2016-02:04:01 to 05-02-2016-03:04:01

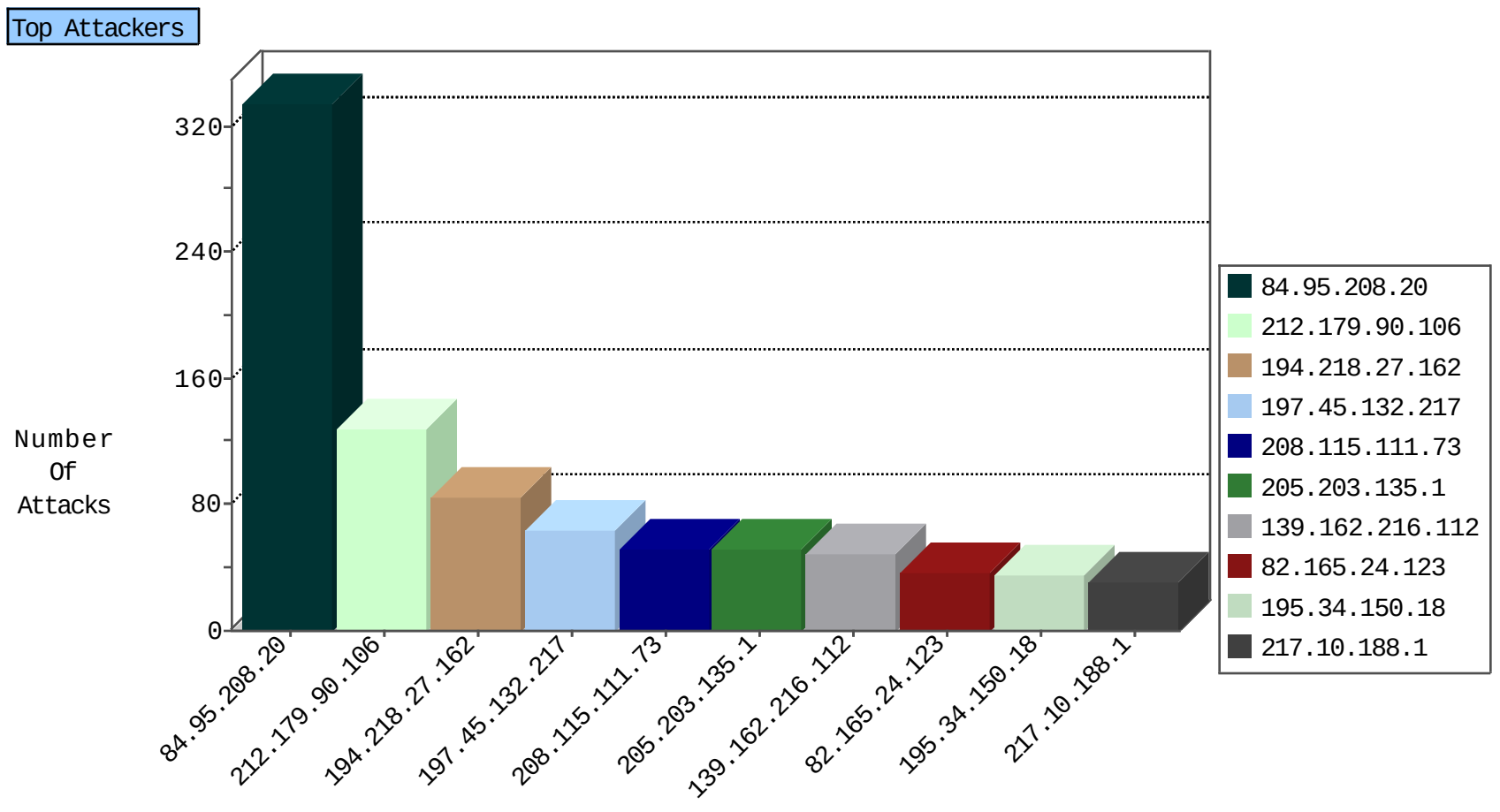
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-02-2016-02:04:01 to 05-02-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.160.60.93	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	13
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
197.160.60.93	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
94.102.52.10	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.110	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

05-02-2016-02:04:01 to 05-02-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.165.24.123	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
204.12.168.26	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.165.24.123	Germany	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
140.117.150.103	Taiwan	147.237.76.147	chinuch.aka.idf.i	22280: HTTP: Joomla Object Injection Vulnerability	Block	2
197.160.60.93	Egypt	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
177.53.141.186	Brazil	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1

05-02-2016-02:04:01 to 05-02-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.165.24.123	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	14
82.165.24.123	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	6
204.12.168.26	147.237.77.74	United States	law.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
66.249.64.153	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sA (2)	2
66.102.8.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
212.98.189.183	147.237.8.28	Belarus	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.73.83.242	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.73.83.242	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
46.228.207.18	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
46.228.207.18	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.217.27.204	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.98.189.183	147.237.8.28	Belarus	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.73.83.242	147.237.76.196	Brazil	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
174.37.194.144	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.114.230.220	147.237.77.170	France	maarachot.idf.il	SERVER-WEBAPP admin.php access	1
104.219.238.10	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

05-02-2016-02:04:01 to 05-02-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	323
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
162.210.196.97	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
217.10.188.1	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.83.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
203.133.169.205	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
45.216.74.248	Morocco	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.115.61.75	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.203.240.108	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.55.61.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.107.231.92	Albania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
8.37.235.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.205.8.236	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.91.107.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.144.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.10.188.1	Satellite Provider	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
104.179.115.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

05-02-2016-02:04:01 to 05-02-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
148.102.19.181	Peru	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
190.234.106.56	Peru	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
82.80.230.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

05-02-2016-02:04:01 to 05-02-2016-03:04:01