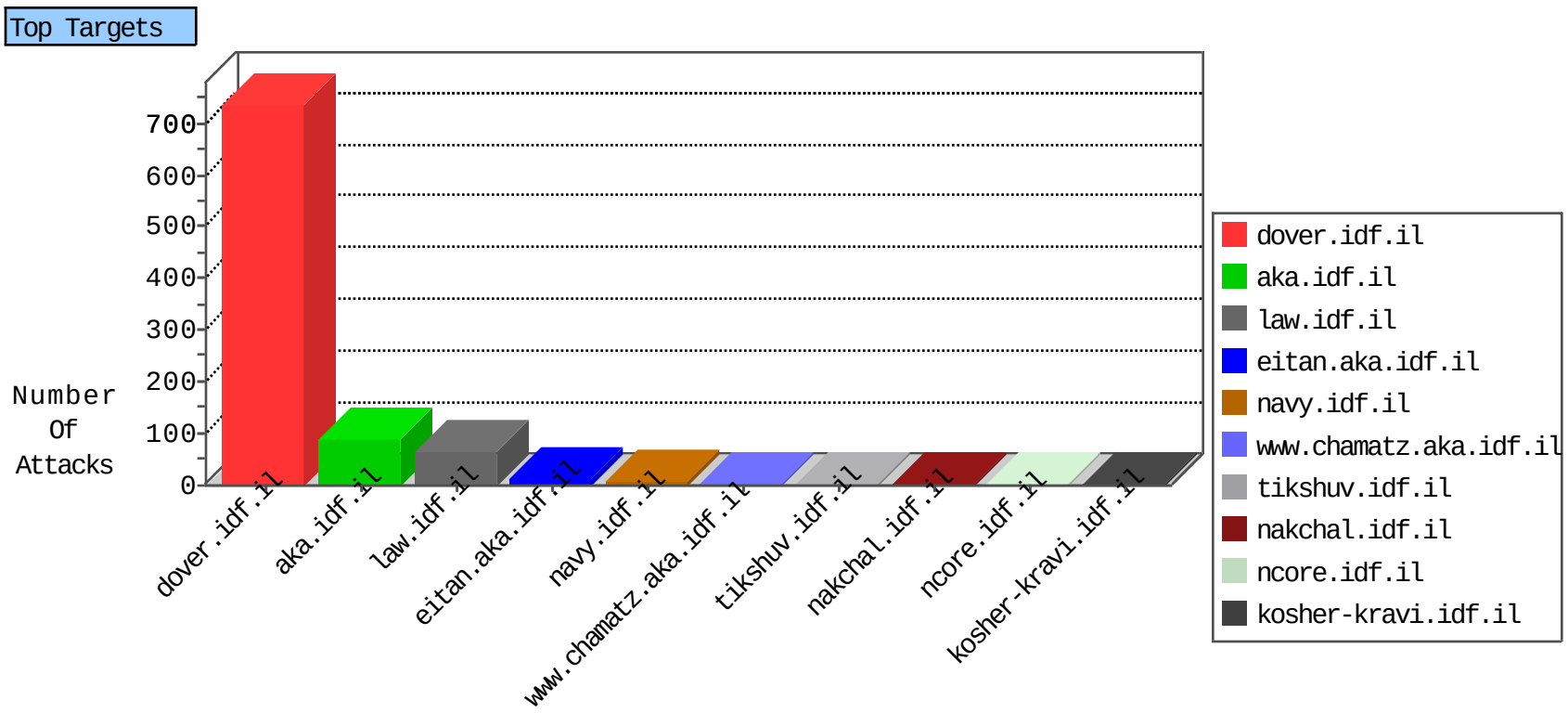
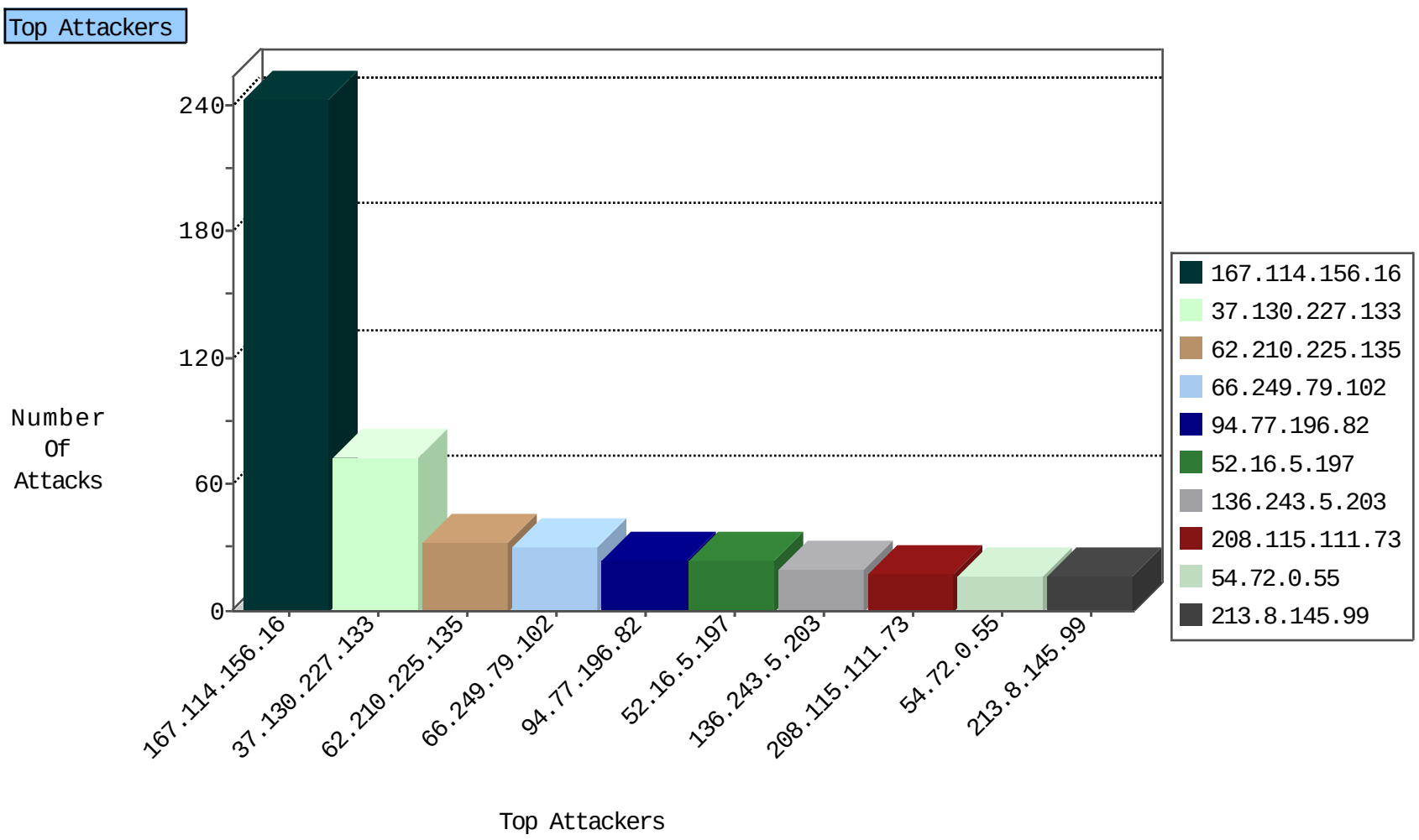
04-30-2016-04:04:04 to 04-30-2016-05:04:04

IDF Under Attack Daily Report





04-30-2016-04:04:04 to 04-30-2016-05:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	12221
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1500
156.212.75.106	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	45
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
120.132.50.135	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
204.42.253.132	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
5.206.231.84	Portugal	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

04-30-2016-04:04:04 to 04-30-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.63.228.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.74.38.14	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
62.210.225.135	France	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
202.124.109.87	New Zealand	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
92.222.5.193	France	147.237.0.34	tikshuv.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
93.90.147.81	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

04-30-2016-04:04:04 to 04-30-2016-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	24
213.8.145.99	147.237.72.166	Israel	aka.idf.il	SQL Injection - Select From	12
93.90.147.81	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	6
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.74.38.14	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.72.166	New Zealand	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
188.214.249.146	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.47.12.162	147.237.76.200	China	eitan.aka.idf.i	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
89.216.119.94	147.237.77.243		mobile.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
60.31.144.3	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.47.12.162	147.237.76.198	China	e.yohalan.idf.i	ET SCAN Potential SSH Scan	1
98.19.222.133	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
89.216.119.94	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.8.24	Netherlands	e.lifestyle.idf	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -f -sS	1

04-30-2016-04:04:04 to 04-30-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.180.62.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.99.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.100.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.101.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.154.81.29	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.99.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.0.117.242	United States	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	7
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	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
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.0.112.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
208.54.80.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.84.255.125	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.86.145.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
86.246.144.108	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
12.11.110.8	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.150.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.226.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.6.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.173	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-30-2016-04:04:04 to 04-30-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
188.120.133.23	Israel	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	2
157.55.39.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
37.115.184.150	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
45.58.42.175	United States	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	1
188.214.249.146	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.214.249.146	Block	1
180.76.15.25	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
45.58.42.175	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
188.214.249.146	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
188.120.133.23	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.120.133.23	Block	1
45.58.42.175	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/administrator/index.php	Block	1
195.154.81.29	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
93.173.9.171	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/mobile	Block	1
5.29.15.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
66.249.66.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.120.133.23	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18630-he/dover.aspx¸'"½¸¿¸¯¸'©'½¸¿¸¯¸'¯¸¿¸½,	Block	1

04-30-2016-04:04:04 to 04-30-2016-05:04:04