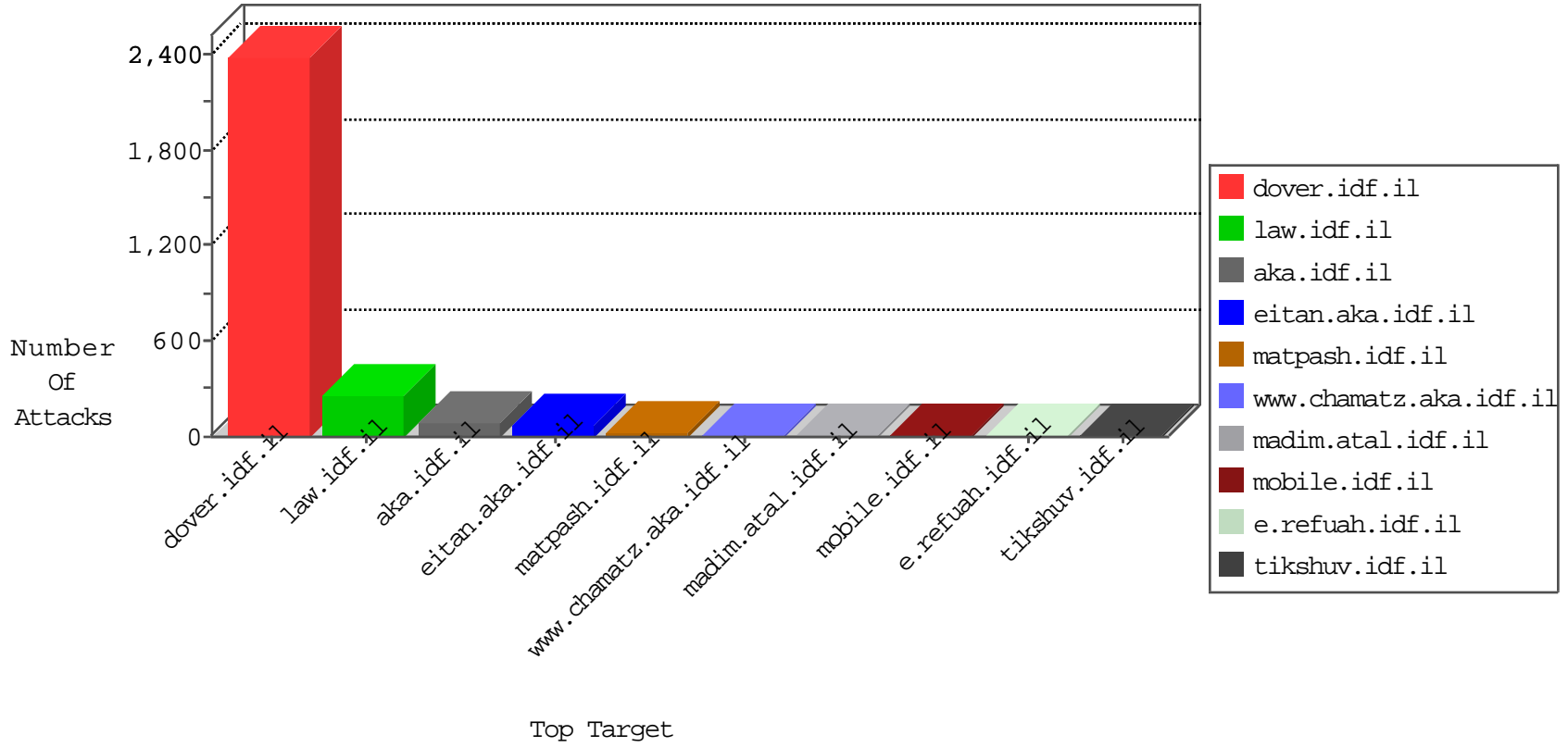


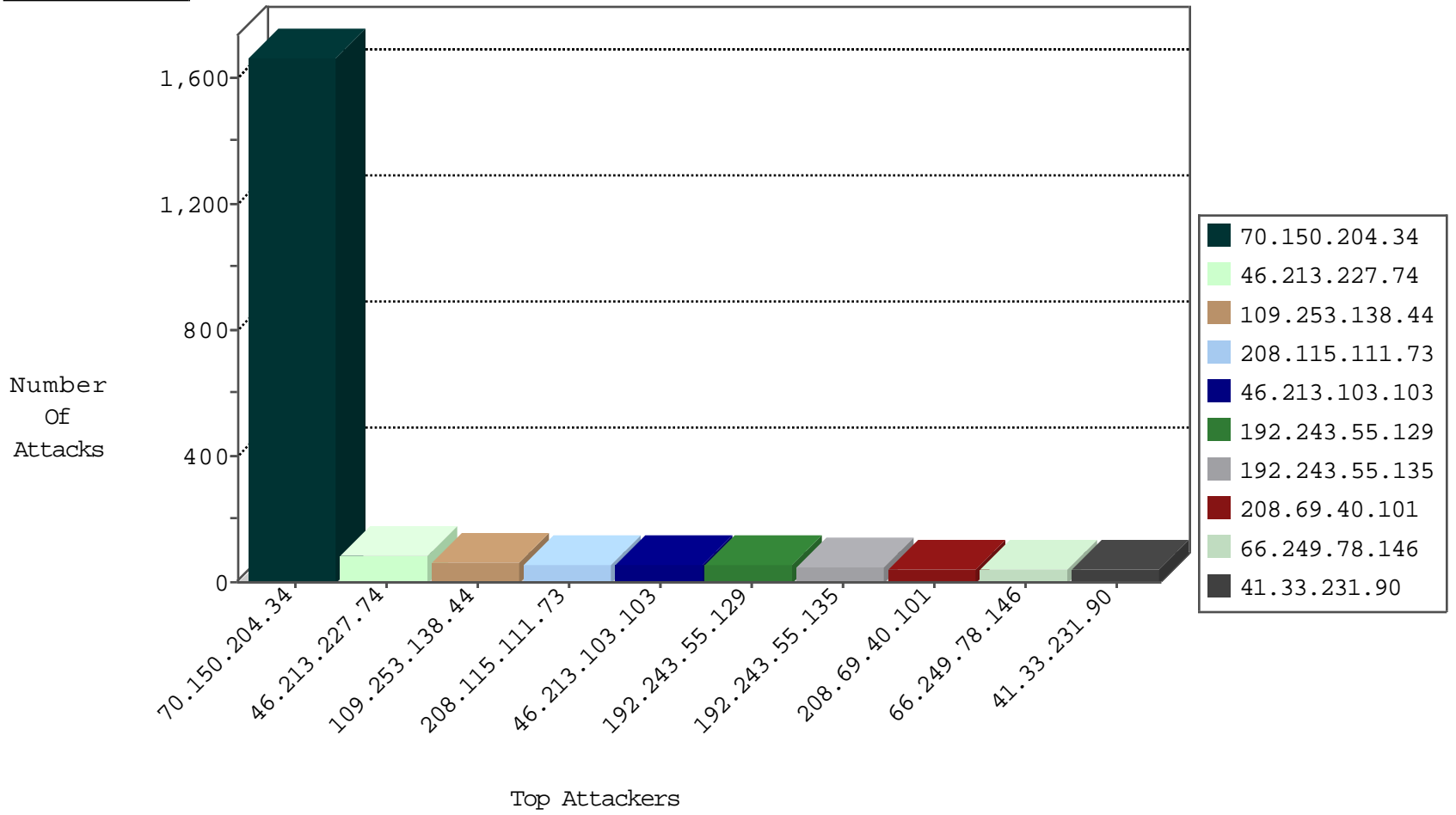
IDF Under Attack Daily Report



Top Targets



Top Attackers



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-MISC-Slowloris-DOS-Var1	dest-reset	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
94.102.52.10	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	4
66.249.69.185	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
37.8.54.218	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
141.135.125.156	147.237.8.28	Belgium	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.82.78.38	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.76	147.237.76.148	Turkey	ggcenter.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
13.82.25.17	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
109.67.49.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.82.25.17	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.150.204.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1666
109.253.138.44	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.253.134.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
46.213.227.74	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
46.213.227.74	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.213.103.103	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.213.103.103	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
46.213.227.74	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
197.15.216.31	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
162.243.104.237	United States	147.237.77.216	dover.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
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
207.46.13.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.108.132.233	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.117.207.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
209.126.117.15	United States	147.237.77.226	www.chamatz.aka.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
157.55.39.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.218.210.17	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
157.55.39.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.131.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.59	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
109.253.201.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.226.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.14	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
207.46.13.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
107.150.32.62	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/alenyby08022010.aspx	Block	1
31.154.39.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	1
192.243.55.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcbwvzahvsyxzcbwvryxjrzwlux3jpc2h1bvwxlnbkzg=&infocent eritem=true	Block	1
74.91.20.194	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
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
38.81.65.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
195.154.52.186	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/yoman.asp	Block	1
38.103.14.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
197.253.6.97	Nigeria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
157.55.39.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
68.180.229.215	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakchal.idf.il/1072-he/nakchal.aspx	Block	1
87.69.34.115	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
12.199.98.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
180.76.15.6	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1073-he/nakchal.aspx	Block	1
69.85.217.249	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
54.212.150.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1