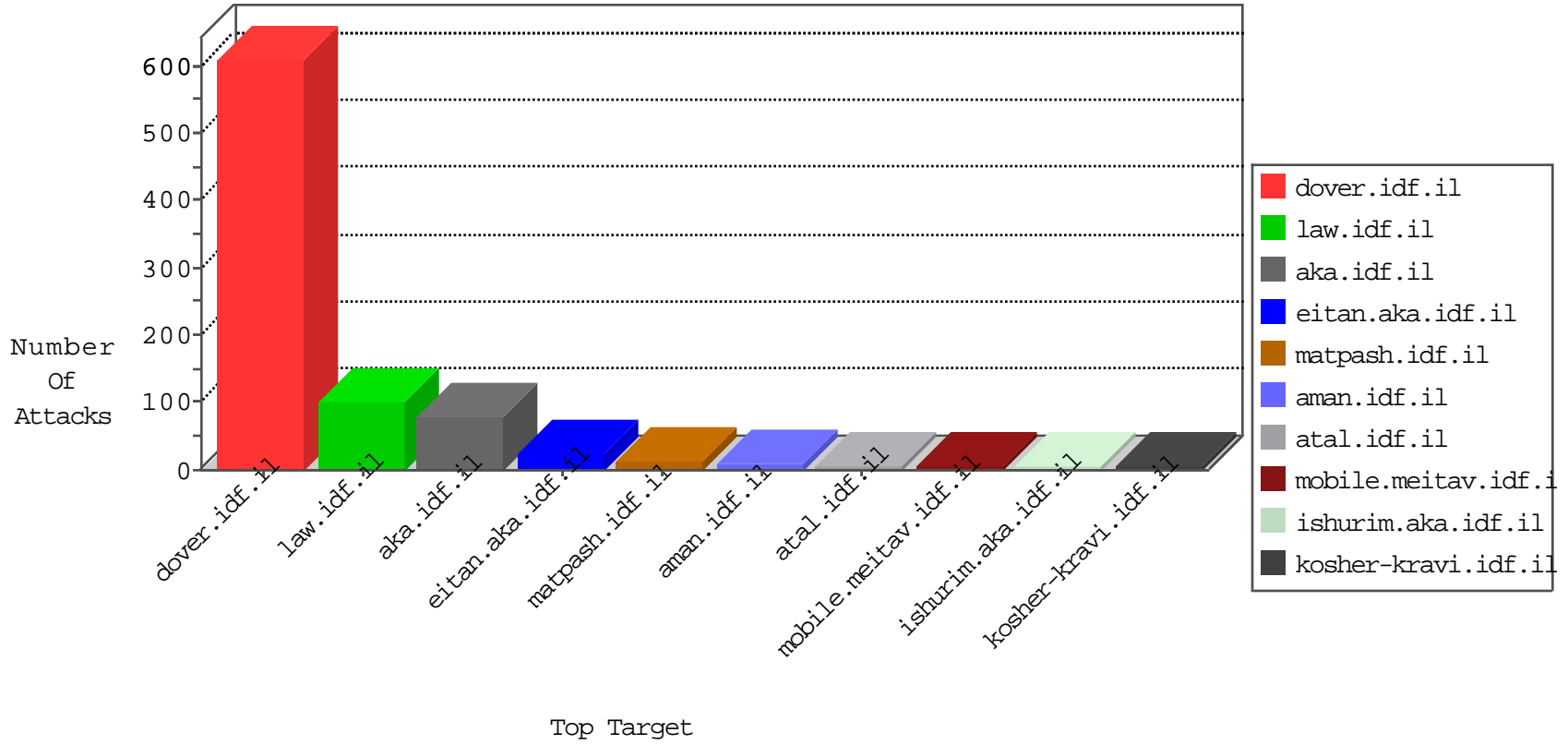


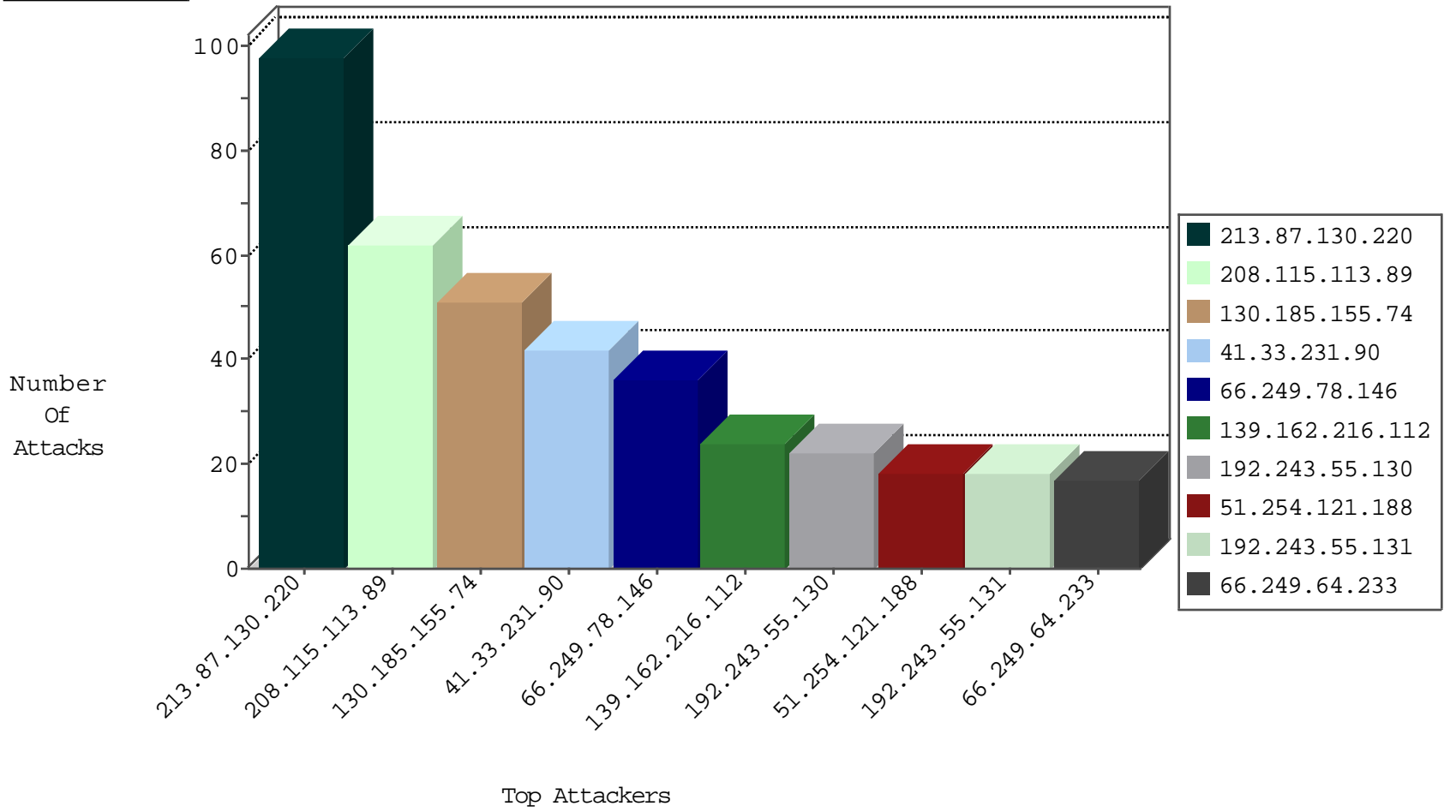
IDF Under Attack Daily Report



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	TCP handshake violation, first packet not syn	drop	430
31.154.49.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
168.243.25.9	El Salvador	147.237.0.200	m4u.idf.il	I4 Source or Dest Port Zero	drop	3
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.i	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.102.52.10	Netherlands	147.237.76.202	e.halag.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
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.82.78.38	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
173.65.154.27	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.0.15	Italy	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.88.102	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
41.89.94.12	147.237.0.15	Kenya	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
13.94.233.163	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
182.191.70.10	147.237.0.33	Pakistan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
122.54.215.145	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.87.130.220	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
51.254.121.188	France	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
50.177.133.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.9.131.69	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.5.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.172.193.32	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
157.55.39.230	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
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	9
41.33.231.90	Egypt	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
77.163.8.164	Netherlands	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
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
70.169.16.74	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
79.181.206.129	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.90.106	Israel	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
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
86.142.221.226	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.42.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.39.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
173.70.42.16	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.126.252.12	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.131	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.9.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
185.81.141.139	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	2
77.46.185.84		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
40.77.167.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.150.46.34	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
163.172.13.21	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176/	Block	1
77.75.78.172	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/34/	Block	1
207.241.237.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
109.67.30.166	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/general/mobile	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
165.234.100.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$ucArticleLobbyControl\$txtSearch in www.idf.il/1393-en/dover.aspx	Block	1
94.180.21.153	Russian Federation	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
109.167.200.251	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
180.76.15.151	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
94.180.21.153	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
128.0.208.2	Greece	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.46.185.84		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
40.77.167.12	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
185.81.141.139	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.81.141.139	Block	1
107.150.32.61	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
141.212.122.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1