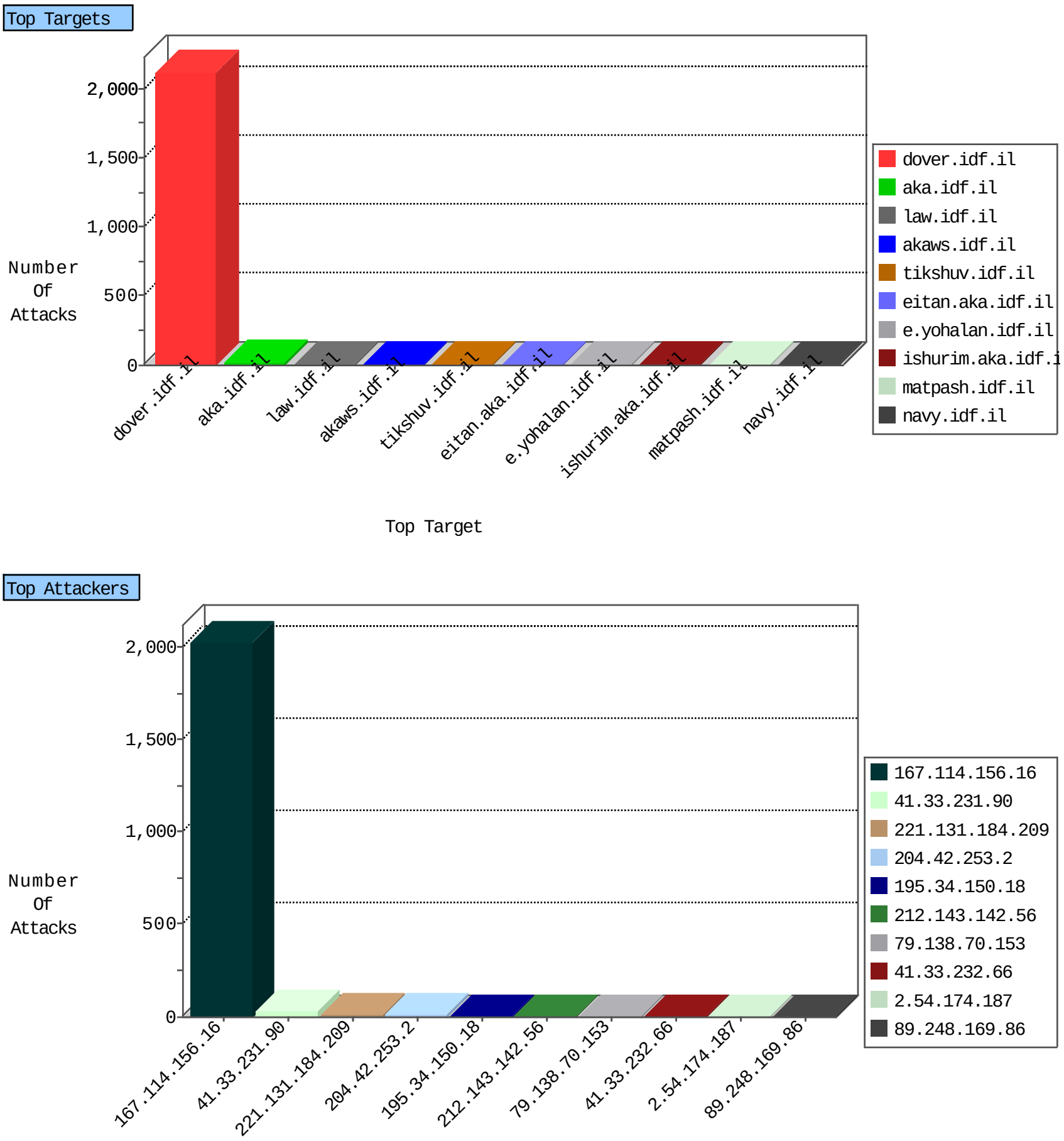
01-22-2016-03:04:07 to 01-22-2016-04:04:07

IDF Under Attack Daily Report



01-22-2016-03:04:07 to 01-22-2016-04:04:07

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	DOS-Tool-SwitchbladG	dest-reset	3075
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
200.35.95.235	Venezuela	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
85.16.189.59	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-22-2016-03:04:07 to 01-22-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-22-2016-03:04:07 to 01-22-2016-04:04:07

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
79.138.70.153	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.198	Indonesia	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
195.216.176.244	147.237.0.17	Latvia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
221.131.184.209	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
119.81.188.158	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
221.131.184.209	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.169.86	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.77.216	Sweden	dover.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.177	Sweden	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.76.198	Indonesia	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
195.216.176.244	147.237.0.35	Latvia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
221.131.184.209	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
221.131.184.209	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.169.86	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
89.248.169.86	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
221.131.184.209	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1

01-22-2016-03:04:07 to 01-22-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.109.202.213	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.174.187	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.88.158.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.228.220.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
119.81.188.158	Hong Kong	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
65.55.218.44	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
2.54.174.187	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
158.222.7.76	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
108.168.185.133	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.212	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.73	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
65.55.218.47	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
159.122.111.166	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.10.152.169	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.120.95.48	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.224	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
131.253.24.146	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.210.188.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.10.152.169	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.120.95.48	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.236	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.0.33	idf.il	drop		drop	1
74.82.47.8	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.228.220.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
119.81.188.158	Hong Kong	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
61.135.190.71	China	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.240	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-22-2016-03:04:07 to 01-22-2016-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.204.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12533-en	Block	1
40.77.167.105	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
54.205.100.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.135.158.101	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.138.65.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
40.77.167.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.86	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
178.255.215.87	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
40.77.167.63	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
216.17.99.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.65.29.39	Moldova, Republic of	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
195.62.53.168	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to /login	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.79	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.120.98.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-22-2016-03:04:07 to 01-22-2016-04:04:07