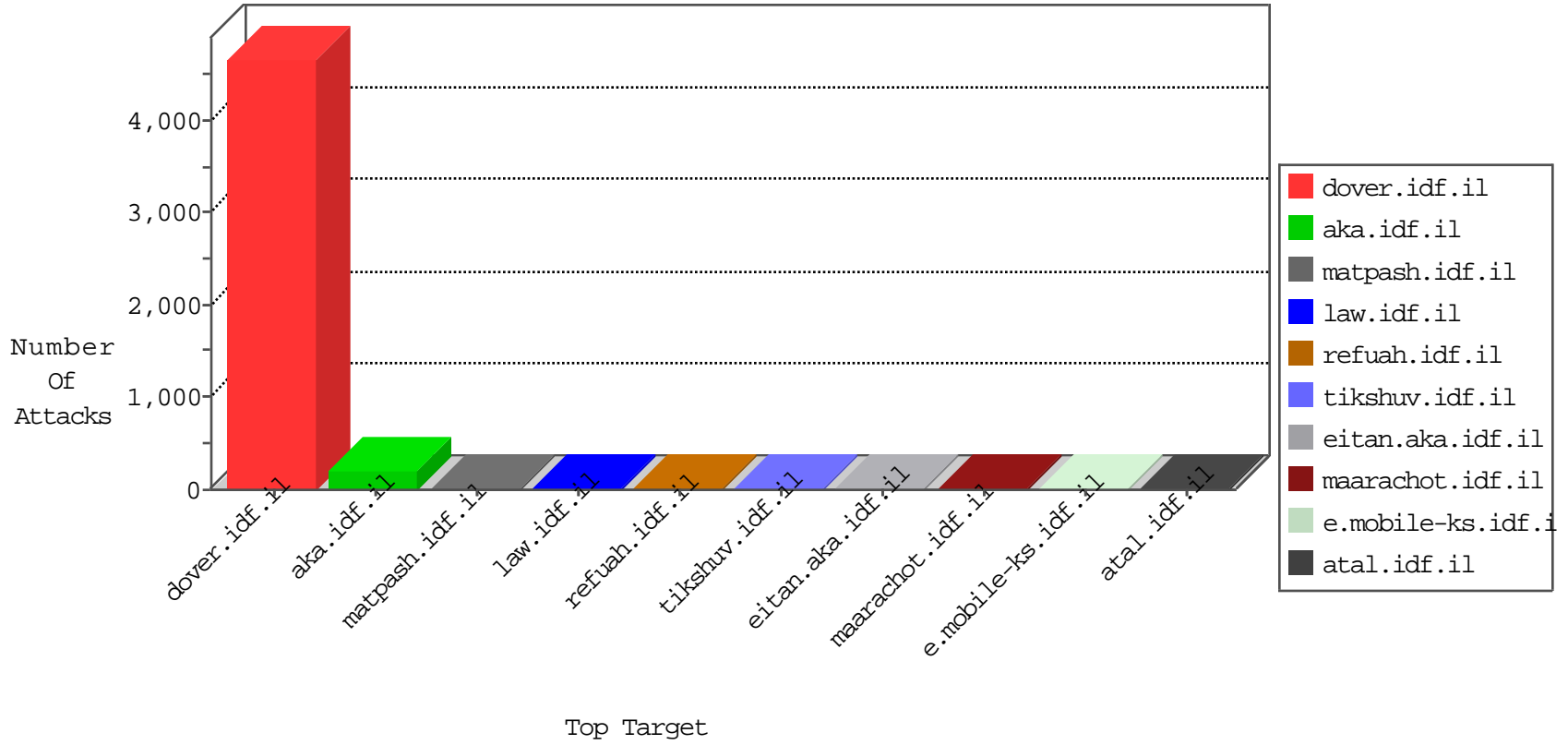


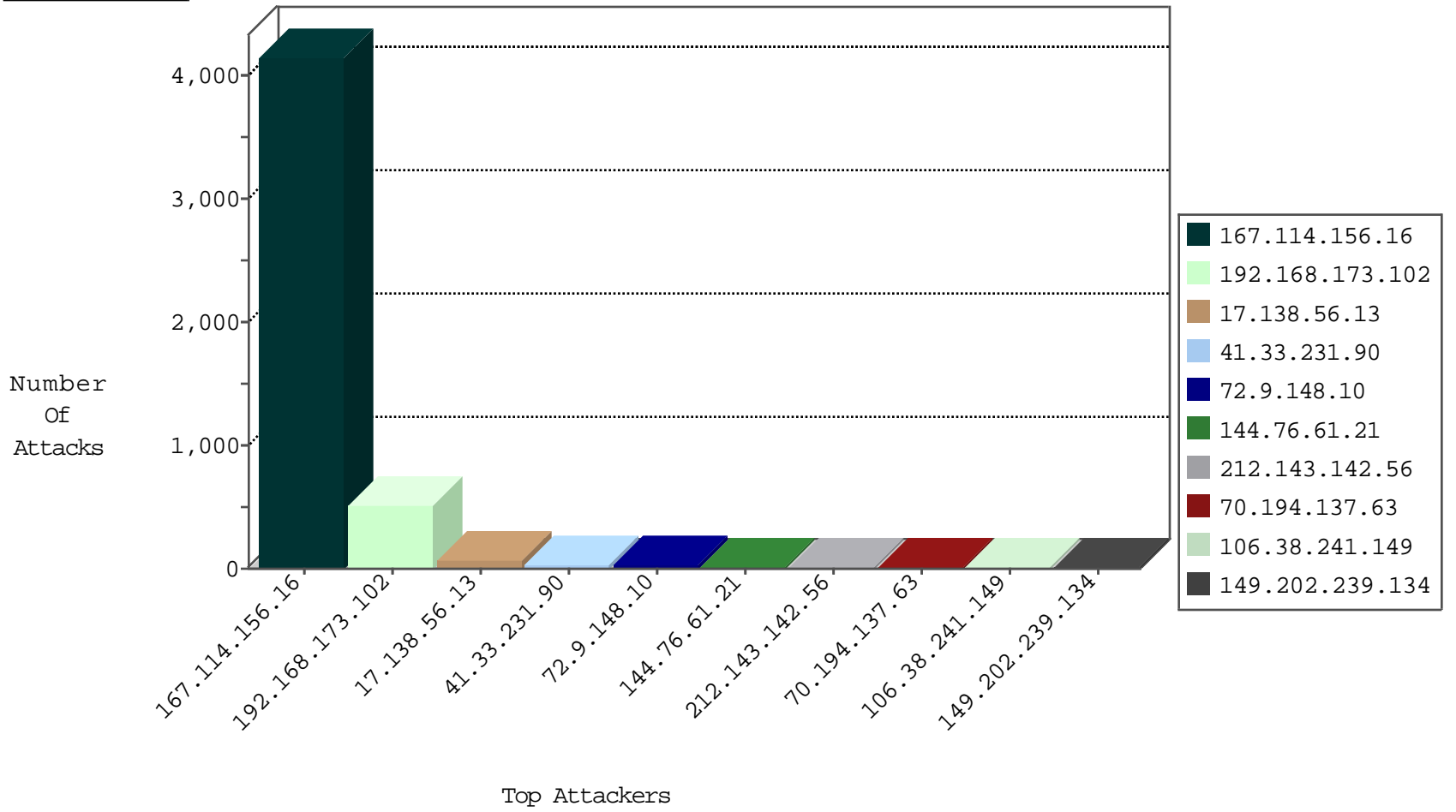
IDF Under Attack Daily Report



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	Block_Ip_Web_In	drop	4132
92.45.105.2	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
46.242.121.156	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
106.120.173.85	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
61.135.189.99	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
144.76.61.21	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
144.76.61.21	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.61.21	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.61.21	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.216.176.244	147.237.72.166	Latvia	aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.116.104.140	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.100.26.228	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
176.119.3.246	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
88.204.187.90	147.237.0.33	Kazakstan	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
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	339
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	169
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
187.132.38.134	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
70.194.137.63	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
128.199.218.181	Singapore	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
123.126.113.109	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
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
130.203.136.75	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
66.249.66.59	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
70.194.137.63	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
199.30.24.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.194	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.148.44.149	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.135.189.99	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.44	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.39.186.222	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
195.62.53.168	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.76	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.75.247.20	Germany	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
190.148.78.175	Guatemala	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.58	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.80	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.75.247.20	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
87.71.1.176	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.221.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.216	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.59.55.92	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.8	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.108	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
62.75.247.20	Germany	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
100.127.228.228		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
70.194.137.63	United States	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
46.121.221.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.228	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.23	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.90	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	5
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
169.229.3.90	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/ts.php	Block	1
74.82.47.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.142.64.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
207.46.13.140	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
174.129.237.157	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3350.jpg	Block	1
130.185.155.82	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.64.74	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
217.174.237.196	Turkmenistan	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
193.252.118.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
217.174.237.196	Turkmenistan	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
169.229.3.90	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/ts.php	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
207.46.13.105	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif	Block	1