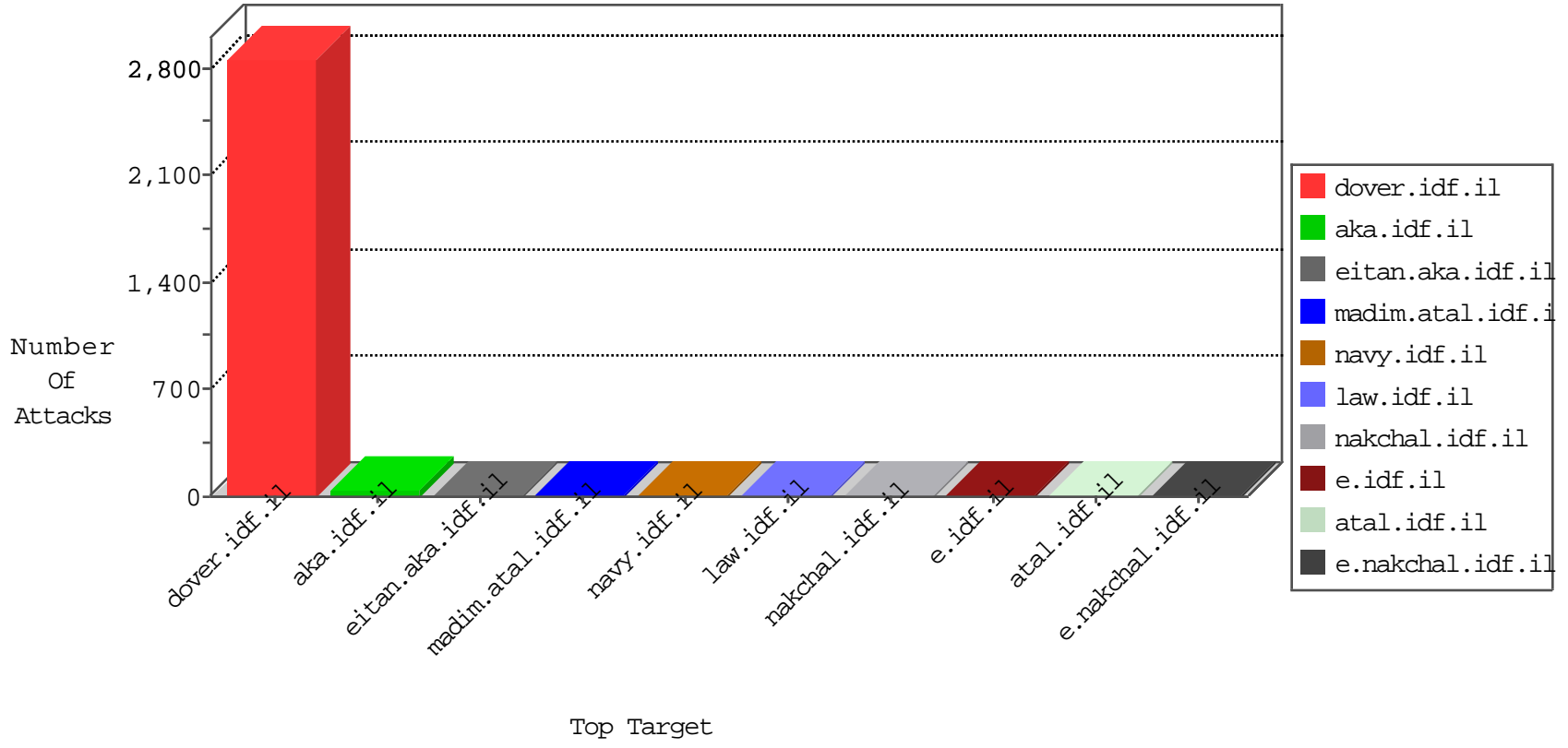


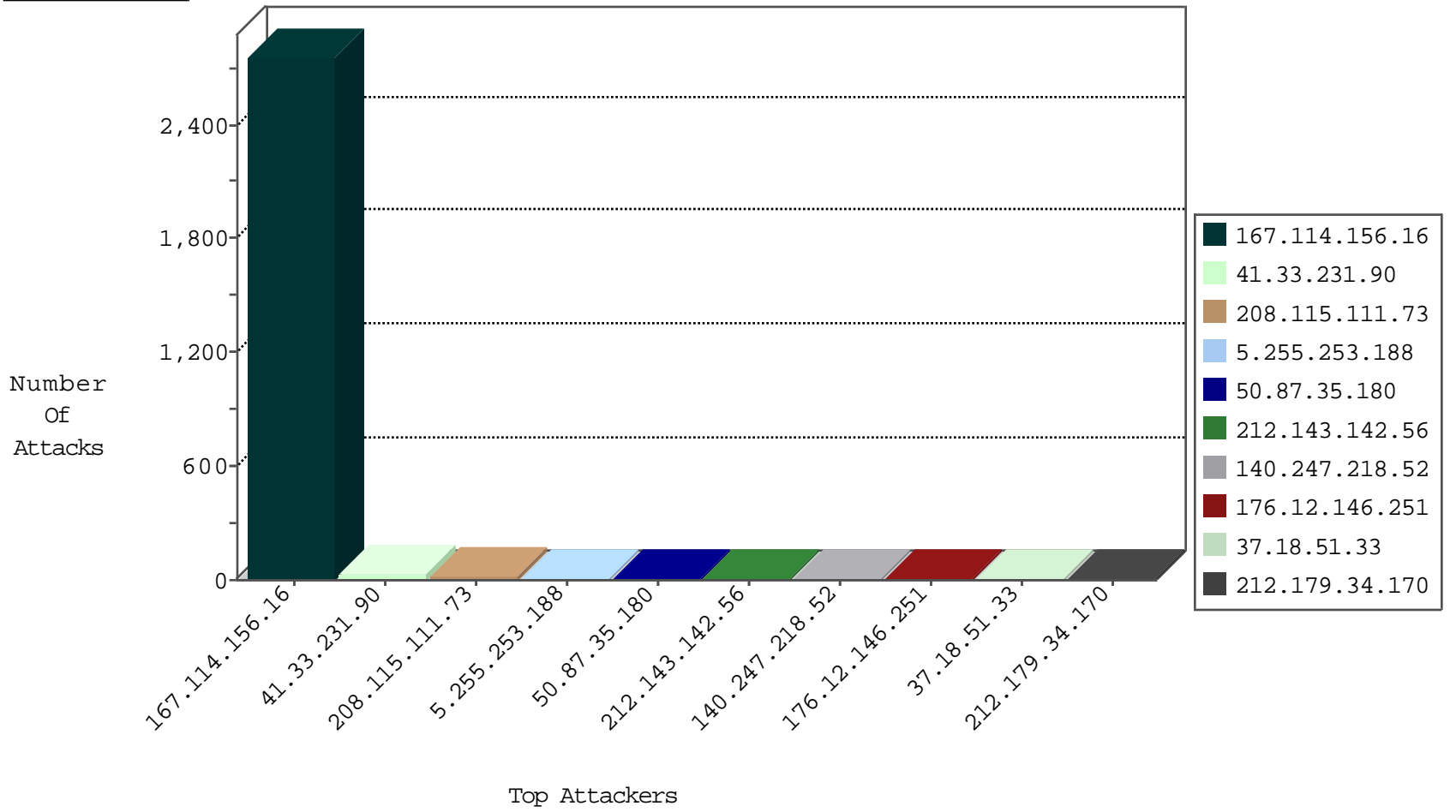
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3316
85.243.38.101	Portugal	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
202.112.51.96	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.201.224.8	Ukraine	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
151.80.31.115	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.5	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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	3
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
198.20.69.98	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
178.79.182.42	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.136.20	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
213.168.248.217	147.237.77.61	Ireland	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.76.38	Netherlands	e.e.meitav.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
140.247.218.52	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.18.51.33	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.179.34.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	3
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
2.54.168.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.138.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.122	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.24	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.88	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.87	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.122	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.115	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.62.74.74	China	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.88	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.112.51.96	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.123	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.48	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.116	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.42.42.202	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.90	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.50	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
11.11.11.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.80	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.121	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.42.42.202	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.146.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.87	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.146.251	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	5
50.87.35.180	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
45.55.55.229		147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 45.55.55.229	Block	2
77.247.30.234	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	2
199.30.16.160	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
50.87.35.180	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	2
66.249.66.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
50.87.35.180	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
193.201.224.8	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
54.153.32.246	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unknown Parameter c... in aka.idf.il/miluum/templates/inner.asp	None	1
50.87.35.180	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 50.87.35.180	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
54.153.33.145	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
45.55.55.229		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
175.44.8.19	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/trackback/	Block	1
79.180.55.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.87.35.180	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.87.35.180	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.184.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
140.247.218.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1379-he/dover.aspx	Block	1
87.68.240.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
207.46.13.16	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
140.247.218.52	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17968-he/dover.aspx<span style='font-family:tahoma	Block	1
193.201.224.8	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	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
207.46.13.176	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/home/home.asp	Block	1
40.77.167.14	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
141.212.122.129	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1