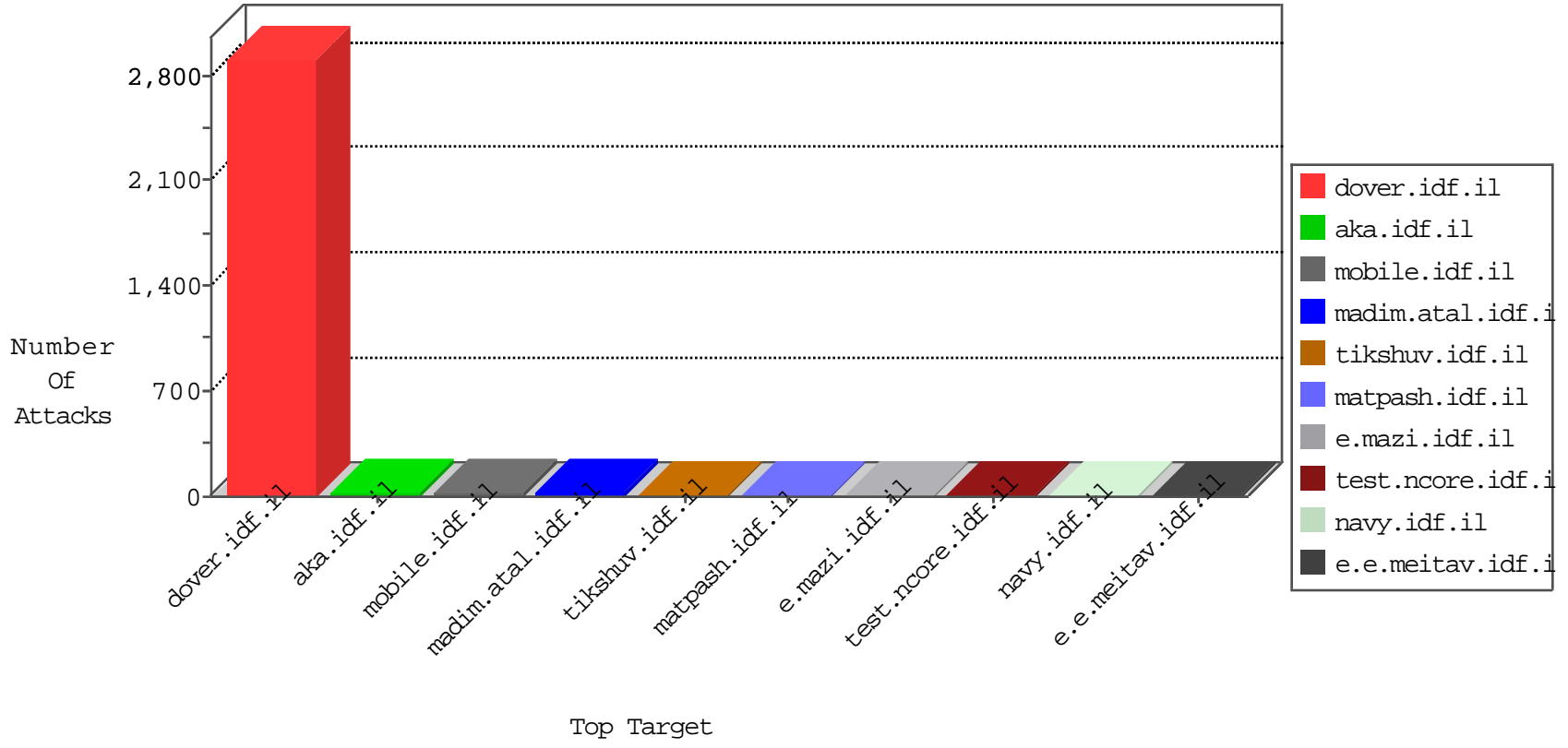


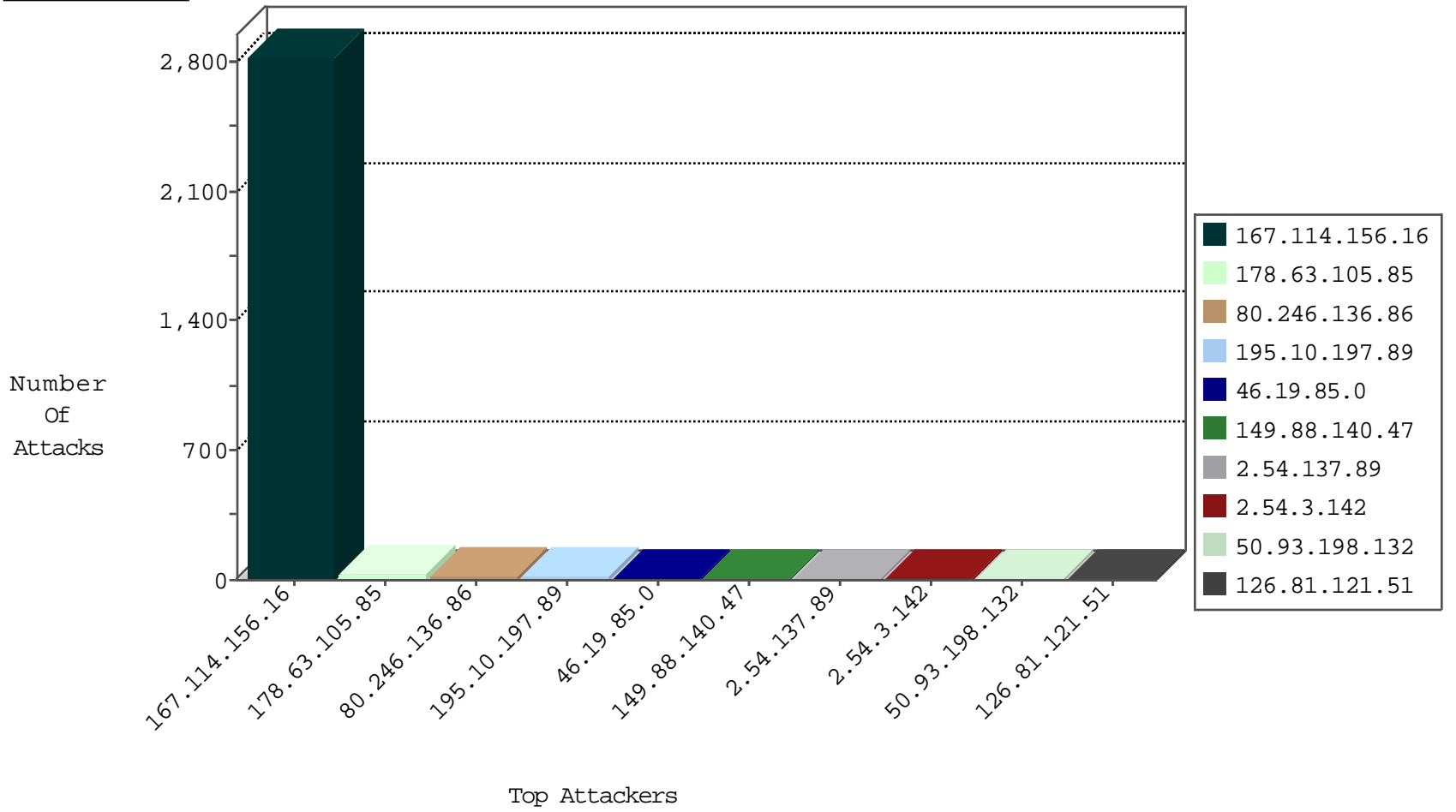
IDF Under Attack Daily Report



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	3797
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

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
42.159.232.168	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.86	Austria	navy.idf.il	ET SCAN NMAP -sS window 1024	1
65.98.40.74	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.200	Ukraine	m4u.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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	30
80.246.136.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	6
2.54.3.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.137.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
40.77.167.11	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.245.104.223	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	3
37.26.149.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.185.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
195.10.197.89	Saudi Arabia	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.10.197.89	Saudi Arabia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.61	e.oogat.idf.il	drop	SAM rule	drop	2
37.46.39.177	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.204.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.133	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.10.197.89	Saudi Arabia	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
37.46.39.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
178.63.105.85	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
216.218.206.84	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
24.114.29.54	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
207.46.13.141	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.96	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
158.58.188.211	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.84	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.44	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.149.169	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.136.86	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.102	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.47.229	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.58.188.211	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.50	United States	147.237.76.198	e.yochalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
177.237.75.75	Mexico	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.72	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.251	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.140.47	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	11
126.81.121.51	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
118.193.137.94	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 118.193.137.94	Block	3
2.54.10.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.93.198.132	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
109.253.220.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.170.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.93.198.132	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
110.82.142.18	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
37.237.154.187	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
45.37.190.123		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.65.245.127	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgquantity.aspx	Block	1
62.210.252.207	France	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
117.78.13.59	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2424.jpg	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/3467.jpg	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.32	Block	1
118.193.137.94	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-10491-en/cogat.aspx+back+to+wall+toilet+cistern&as_qdr=all&filter=0&num=100&complete=0&cr=countryil&gws_rd=ssl&hl=iw&ct=clnk	Block	1
50.93.198.132	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
199.30.24.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
110.82.142.18	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 110.82.142.18	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
41.254.9.161	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/"	Block	1
94.23.219.182	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm"	Block	1
50.93.198.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
207.46.13.35	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
110.82.142.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/pages/default.aspx/xmlrpc.php	Block	1
66.249.69.163	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	1