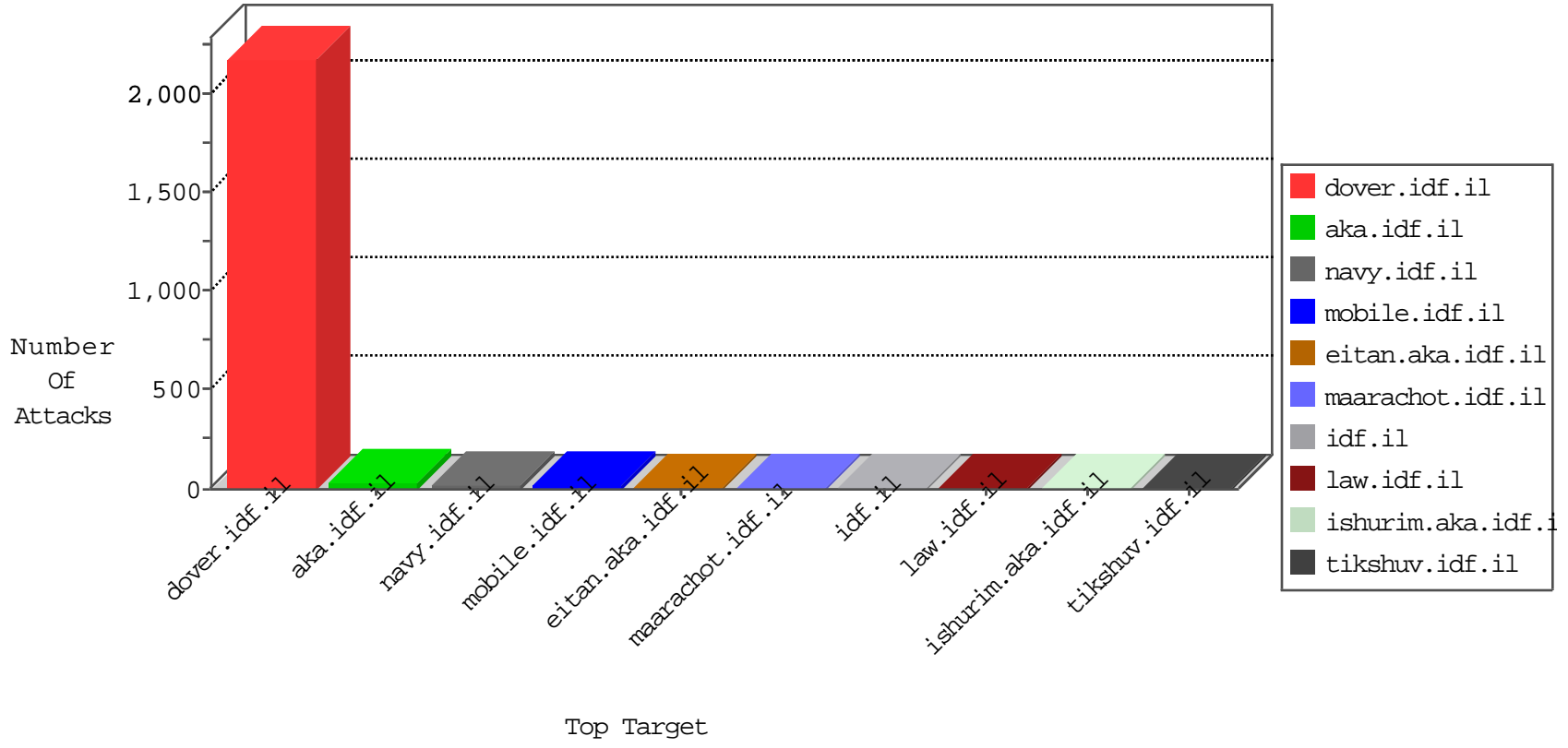


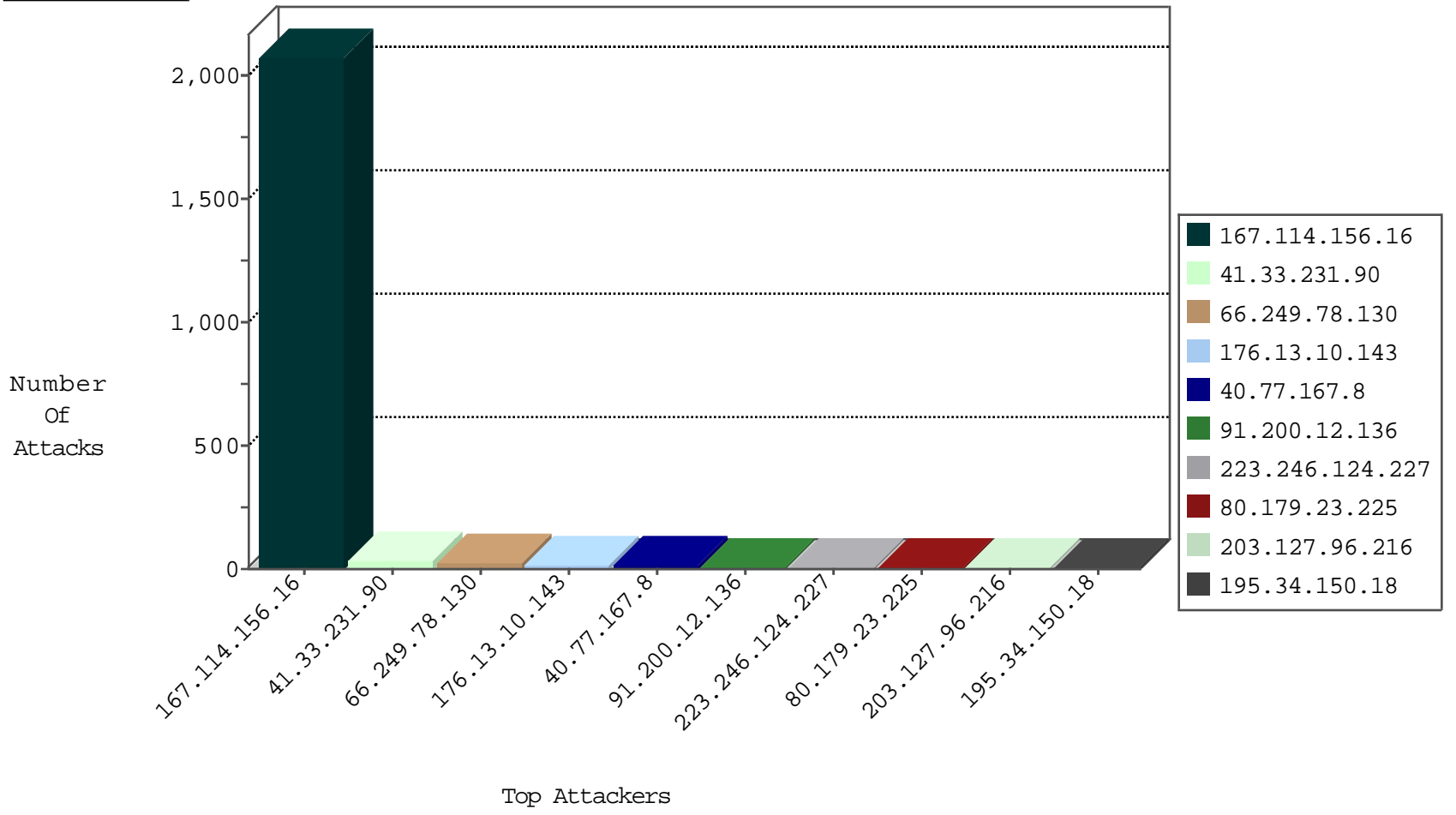
IDF Under Attack Daily Report



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	3408
66.249.65.43	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	112
115.239.228.8	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Http	drop	2
223.246.124.227	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.8	China	147.237.0.33	idf.il	Frk_Purple_Con_Limit_Http	drop	1
223.246.124.227	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
223.246.124.227	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
223.246.124.227	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
223.246.124.227	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
78.46.50.246	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	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	4
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.212.77.44	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN NMAP -sS window 1024	1
182.254.149.138	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.170	Ukraine	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
74.117.209.135	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
62.212.77.44	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
40.115.58.160	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
81.169.251.74	147.237.0.19	Germany	medim.atal.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	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
176.13.10.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
40.77.167.8	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.136	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
199.30.25.230	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
80.179.23.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.46.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
202.180.34.186	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.188	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.121.185	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.179.23.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.188	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.252	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.56.214.173	Moldova, Republic of	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.185	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.189	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.208.175.185	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.237.45.116	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.187	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.190	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.184	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.0.33	idf.il	drop		drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.187	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.121.184	United States	147.237.77.243	mobile.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
40.77.167.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.176.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
50.245.59.163	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 50.245.59.163	Block	1
157.55.39.38	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
95.180.209.142	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
5.102.173.71	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	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
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	1
50.245.59.163	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7490-he/	Block	1
157.55.39.119	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
95.180.209.142	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.246.136.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.91.90.156	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /robots.txt	Block	1
198.20.69.74	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19178-he/dover.aspx	Block	1
150.70.173.57	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
93.13.181.194	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
64.237.45.116	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	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
1.120.133.84	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
40.77.167.8	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.8	Block	1
150.70.173.57	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.172.0.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.237.45.116	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8935-he/refuah.aspx	Block	1