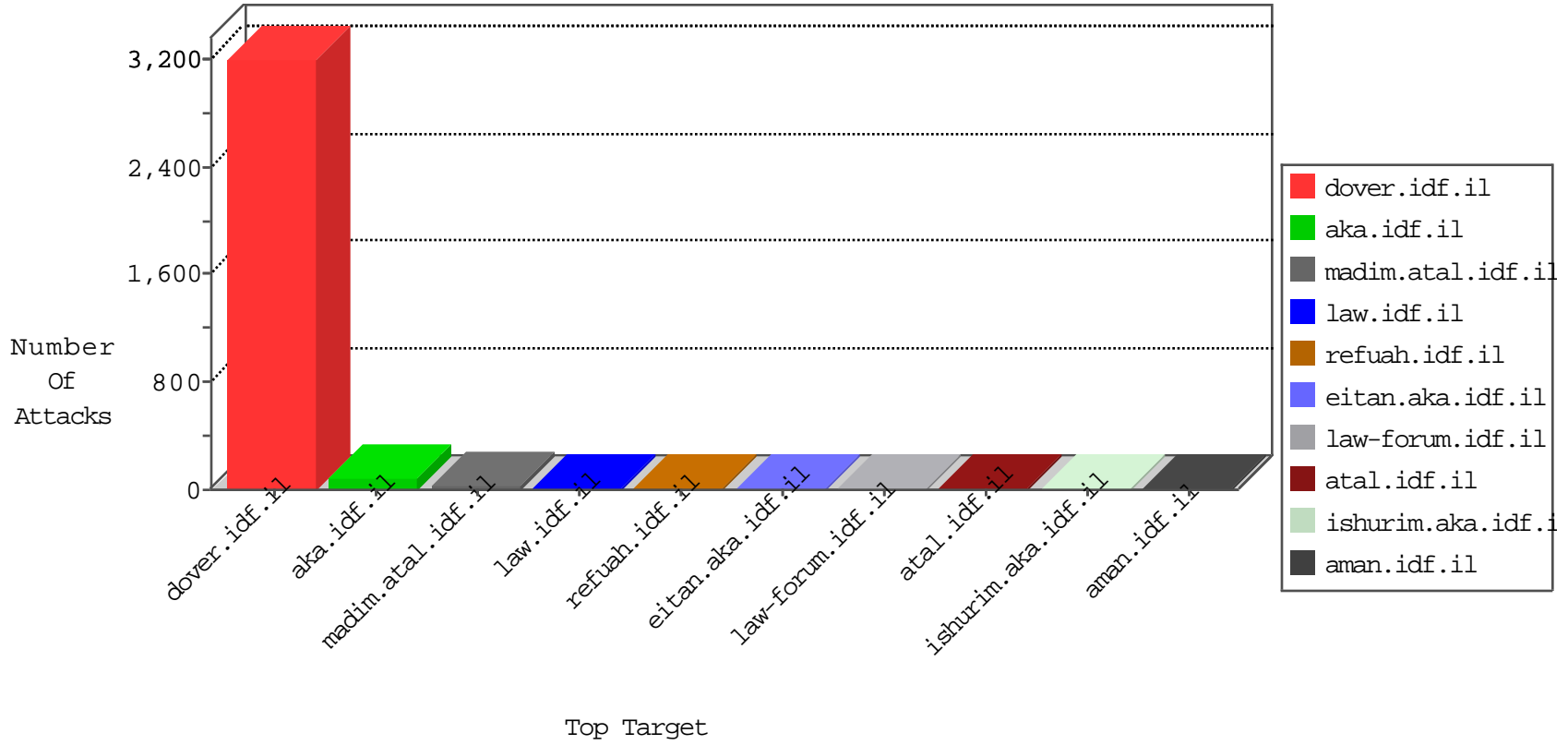


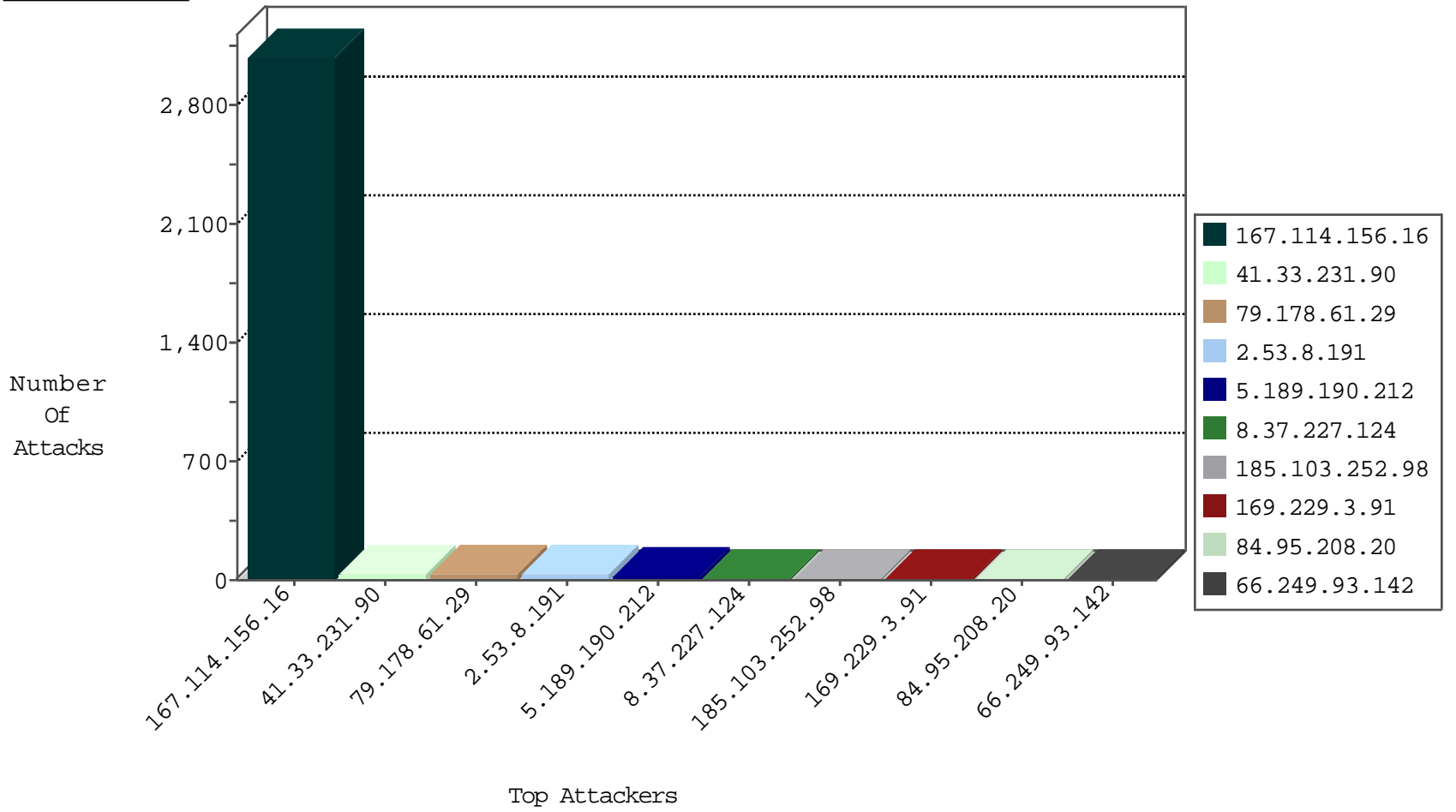
IDF Under Attack Daily Report



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_Tp_Web_In	drop	3077
8.37.227.124	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
8.37.227.124	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
184.105.139.94	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
207.243.129.34	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
107.191.40.138	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
104.255.70.247	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.118	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
104.255.70.247	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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
219.134.86.86	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.72.179.130	147.237.77.74	Romania	law.idf.il	ET SCAN NMAP -sS window 1024	1
116.109.159.90	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.148	Canada	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
222.73.115.134	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
172.87.221.214	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 4096	1
113.240.250.154	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
101.200.181.38	147.237.77.235	China	sviva.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
79.178.61.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.178.61.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
8.37.227.124	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
185.103.252.98	Russian Federation	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	7
79.178.61.29	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.142	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
2.55.152.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.103.252.98	Russian Federation	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	5
66.249.93.148	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
37.142.210.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.178.61.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.107.102.131	Hungary	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
131.253.25.202	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.14.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.50.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.66.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.133.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.118.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.61.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
185.3.146.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.178.61.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.187.248	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
79.181.179.155	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
149.78.208.190	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
216.218.206.108	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.40	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.51.38	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.158.131.217	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.108.48.253	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
159.226.95.66	China	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.30.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
106.184.3.122	Japan	147.237.76.34	yohalan.idf.il	drop		drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.65.235.154	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.3.146.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.116.200.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.182.12.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.76.148	ggcenter.aka.idf.il	drop	SAM rule	drop	1
35.0.127.52	United States	147.237.76.86	navy.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
2.53.8.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
217.132.23.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
98.246.147.184	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
146.185.129.169	Netherlands	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
104.236.55.186	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.236.55.186	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415	Block	1
157.55.39.236	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/faq.aspx	Block	1
79.181.179.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
104.236.55.186	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.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/sip_storage/files/1/2271.jpg	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
79.182.12.146	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
128.232.110.28	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	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/3/3493.jpg	Block	1
197.248.44.20	Kenya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
84.108.187.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1