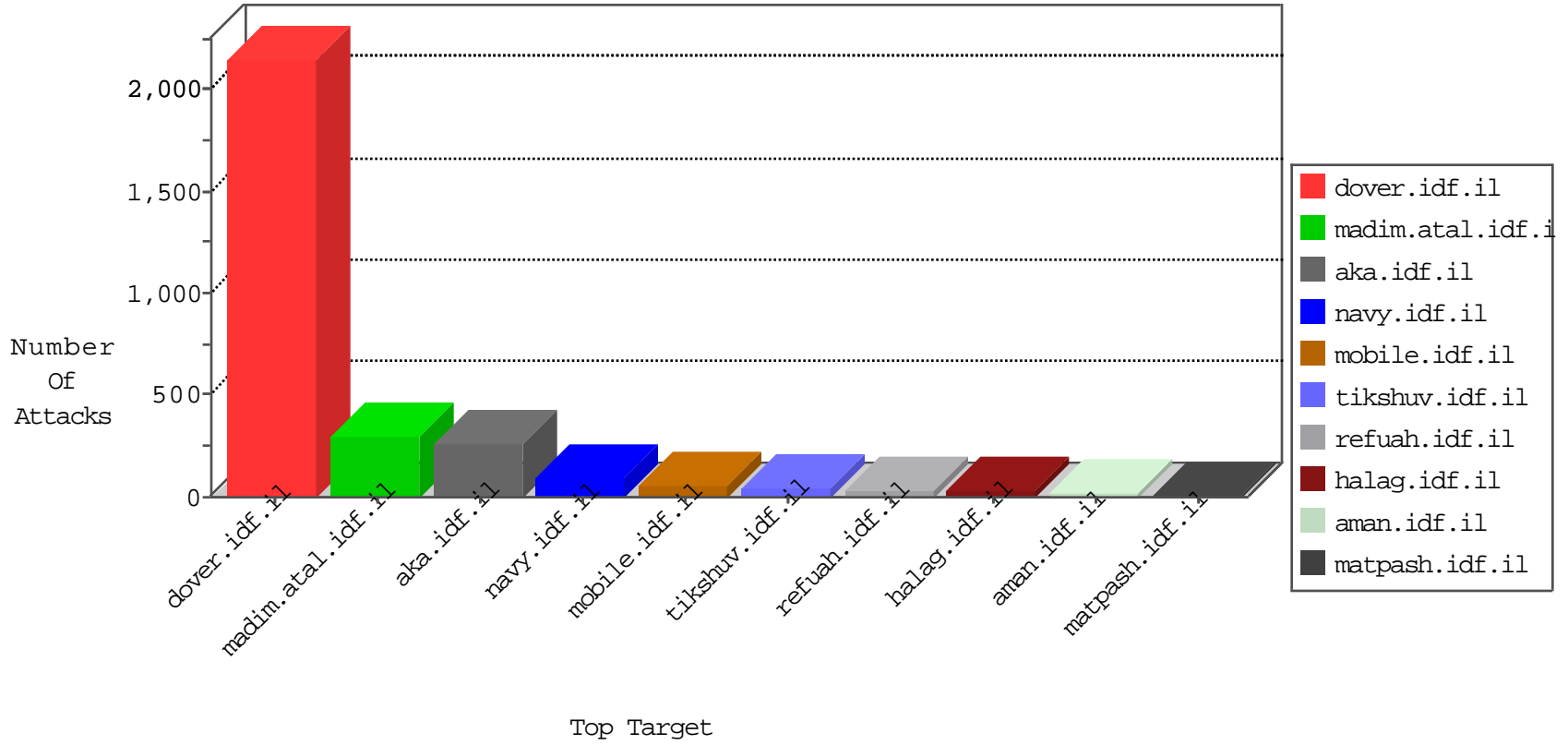


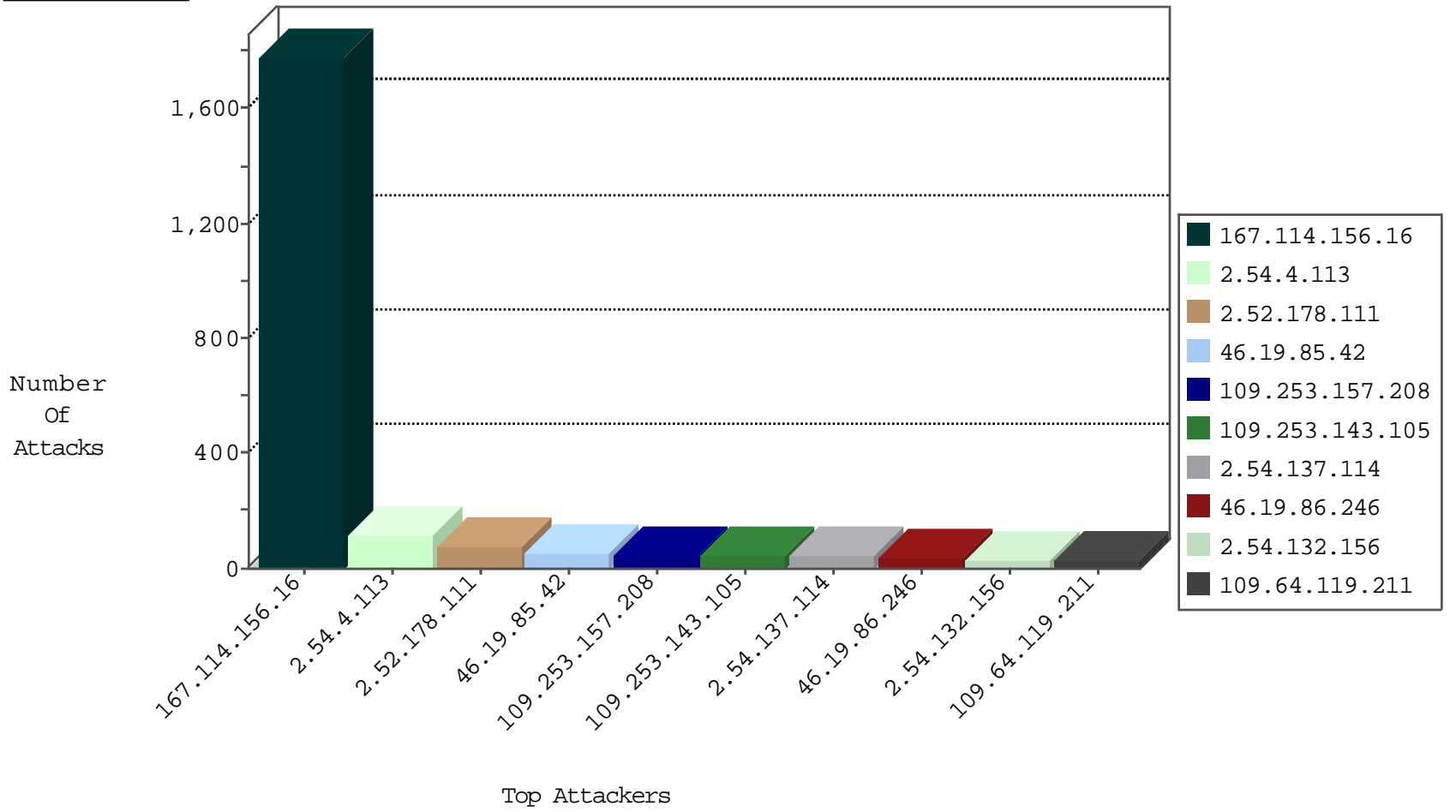
IDF Under Attack Daily Report



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	3106
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
46.19.86.246	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
2.52.177.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
46.19.86.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
46.19.85.3	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.195.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.54.147.162	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.86.170	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
2.54.5.109	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
185.5.221.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.182.38.184	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.182.38.184	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
84.111.169.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.199.241.250	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.74	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.38.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
87.68.156.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
109.253.146.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.248.252.113	Netherlands	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Block	2
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	2
94.230.93.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.120.148.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
94.230.93.182	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.219.44.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.153.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
147.235.236.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.194	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.38.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.225.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.121.136.51	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.16.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.177.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.82.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
86.108.10.32	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.15.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	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	104
2.52.178.111	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	70
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	62
109.253.143.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.64.119.211	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.85.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
46.19.85.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
185.120.125.22		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.132.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.33.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.215.157	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.27.106.12	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	5
46.19.86.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	4
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
46.19.85.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
62.219.224.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.176.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.24.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.150.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.184.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.222.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.213.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.185.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.219.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.179.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.150.203.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.181.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

