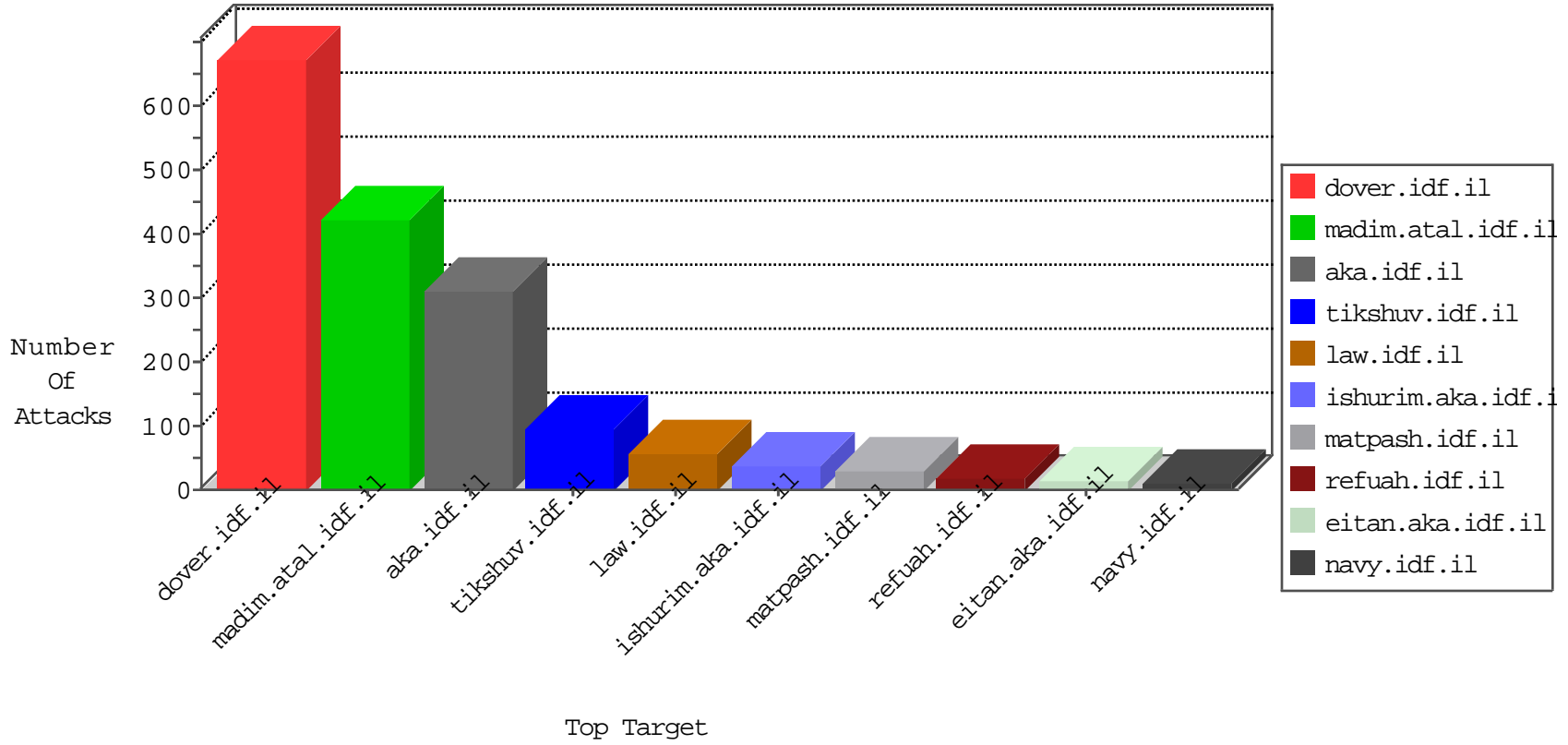


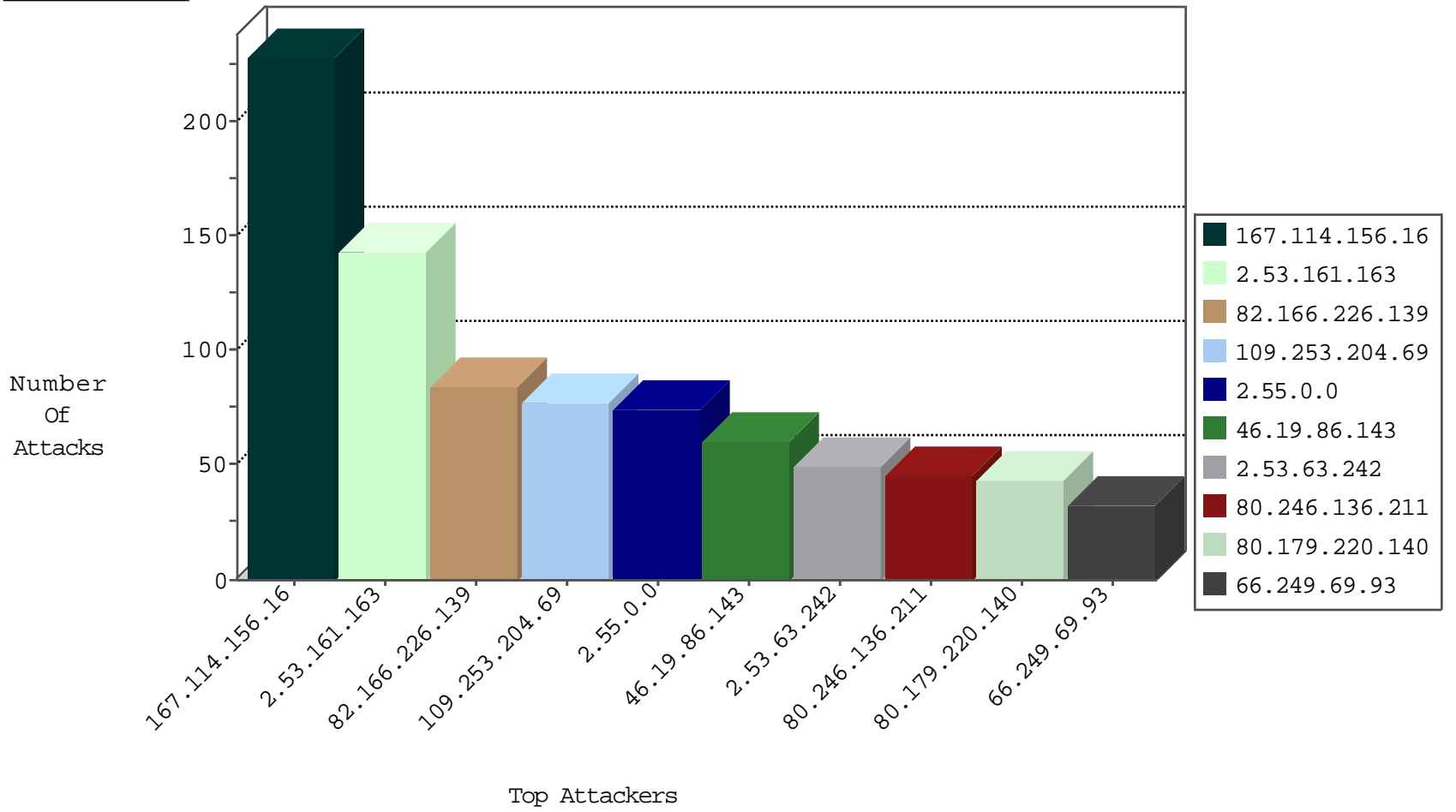
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	10527
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2810
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	673
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	12
146.185.57.8	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.103.252.96	Russian Federation	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
195.200.72.162	Sweden	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
69.137.43.13	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
85.93.89.243	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.194	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	2
79.182.126.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.177.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.22.20.155	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.84.148.3	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
193.254.206.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.178.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.54	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
2.53.3.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.100.86.128	147.237.77.216	Finland	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.219.247	147.237.77.74	Russian Federation	law.idf.il	ET SCAN Potential SSH Scan	1
94.230.86.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.165.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.242.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.84.148.3	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
192.117.135.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.10.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.54	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
146.185.219.247	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
146.185.219.247	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.197.61.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.38	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
82.166.226.139	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
2.55.0.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.26.148.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.117.136.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
196.150.198.193	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.55.129.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.209	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
209.202.5.148	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
208.54.38.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.117.135.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.125.113.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.117.135.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.176.15.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.176.15.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.114.23.18	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
40.77.167.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.67.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.41.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.179.6.139	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
17.138.55.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.168.149.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.217.75.195	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
109.253.227.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.242.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
131.253.25.206	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.242.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
193.43.246.250	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
166.137.246.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.180.175.34	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

