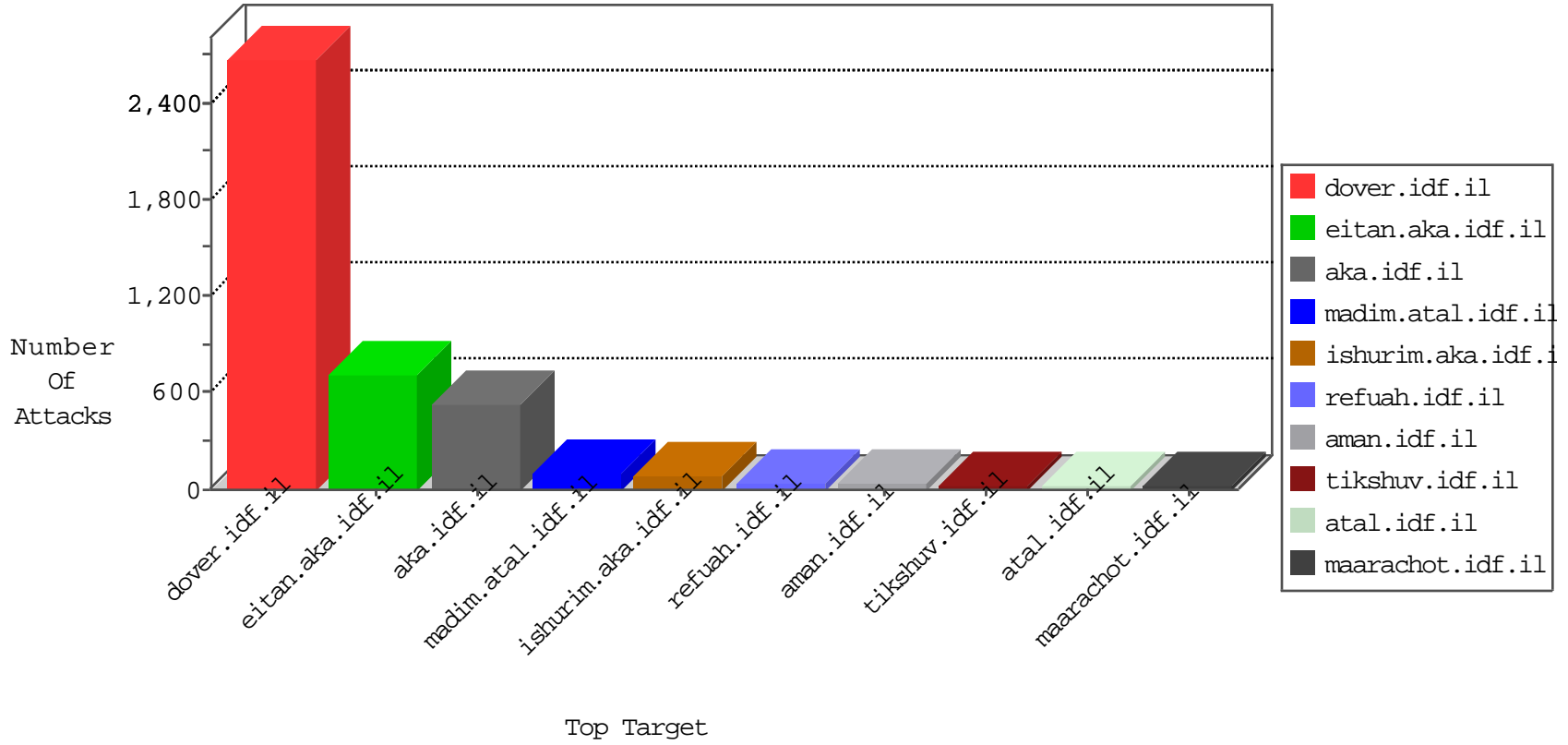


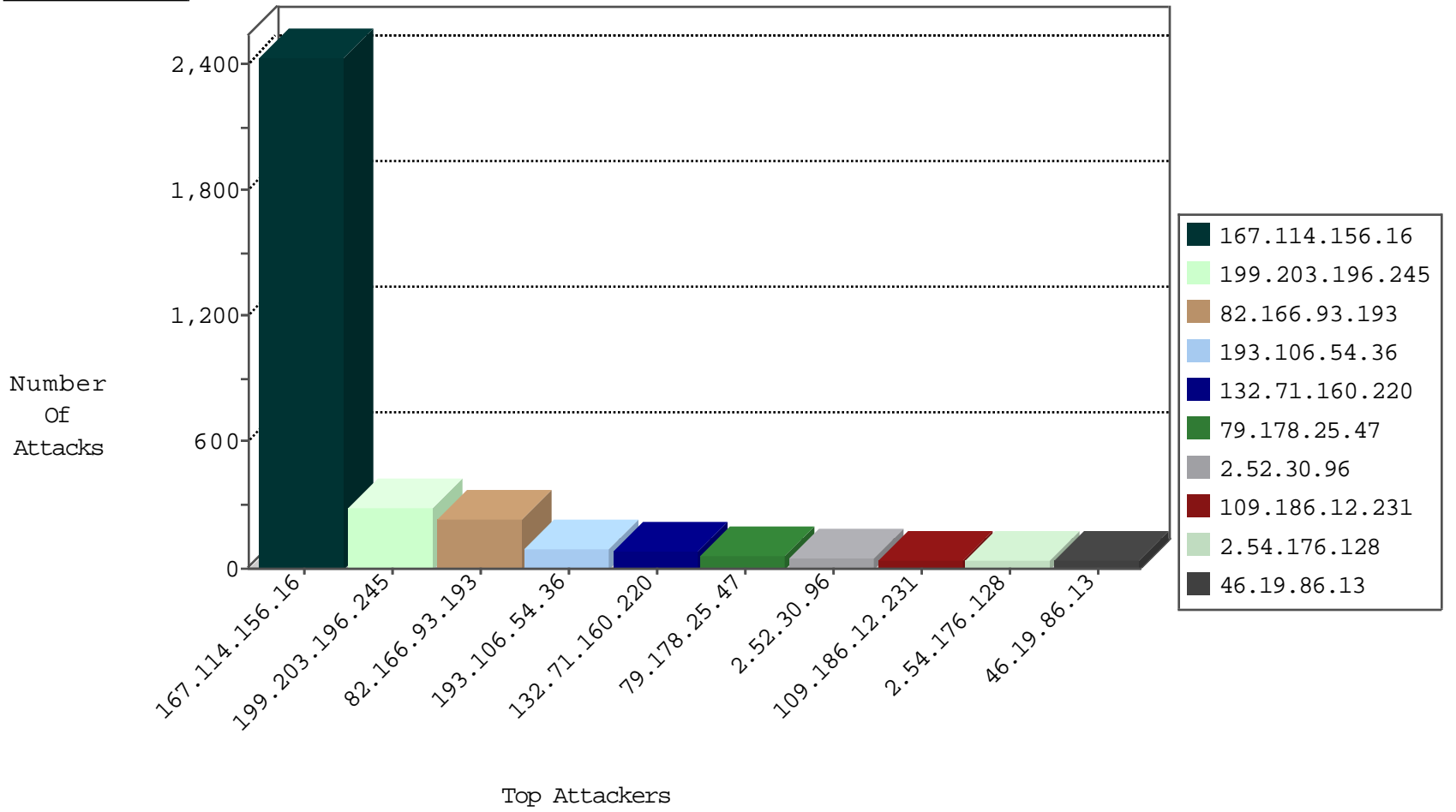
IDF Under Attack Daily Report



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	3325
115.239.228.8	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
192.3.170.124	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-trafl	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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.120.71.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.254.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.32	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.61.109.189	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
176.106.226.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.150.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.29.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.61.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
192.114.87.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.61.109.189	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
159.147.148.28	147.237.72.156	Spain	aman.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.235.88	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
199.203.196.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	164
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
46.19.86.201	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	26
100.100.53.191		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
79.178.25.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
2.54.87.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
80.178.198.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
158.85.253.245	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.178.25.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
62.207.60.229	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
213.57.134.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
213.57.134.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.186.12.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
100.100.12.245		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.186.12.231	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.52.34.223	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
193.106.54.36	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.52.30.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.120.44.246	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
79.178.25.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
100.100.123.64		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.14.94	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.26.146.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
132.71.160.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.64.152.227	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
82.166.93.193	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
96.232.99.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
100.100.90.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.178.25.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
100.100.85.90		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.25.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.127.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.210.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.101.218.101	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.116.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.100.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.12.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.210.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.62.61		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.127.52.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.155.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.18.84	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6

