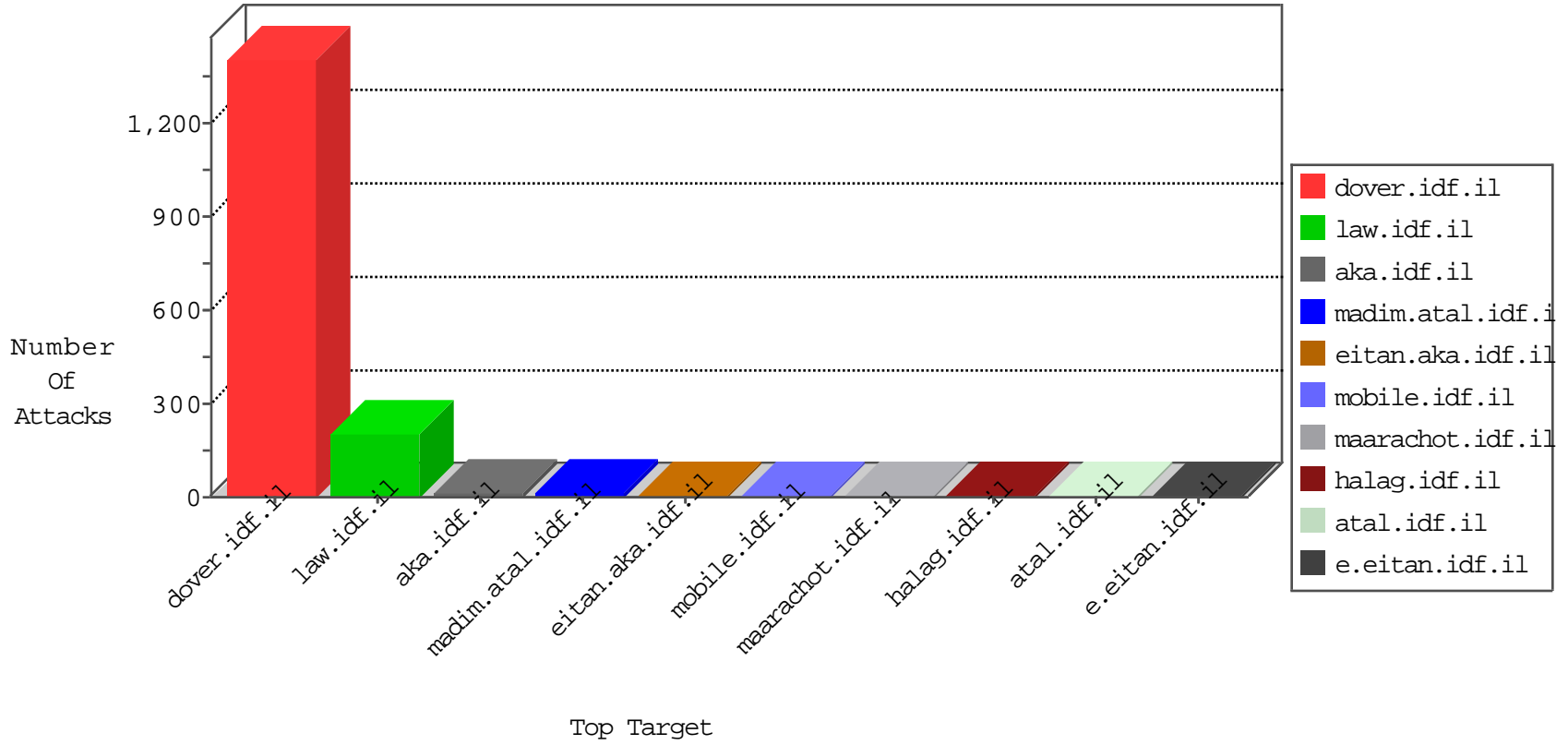


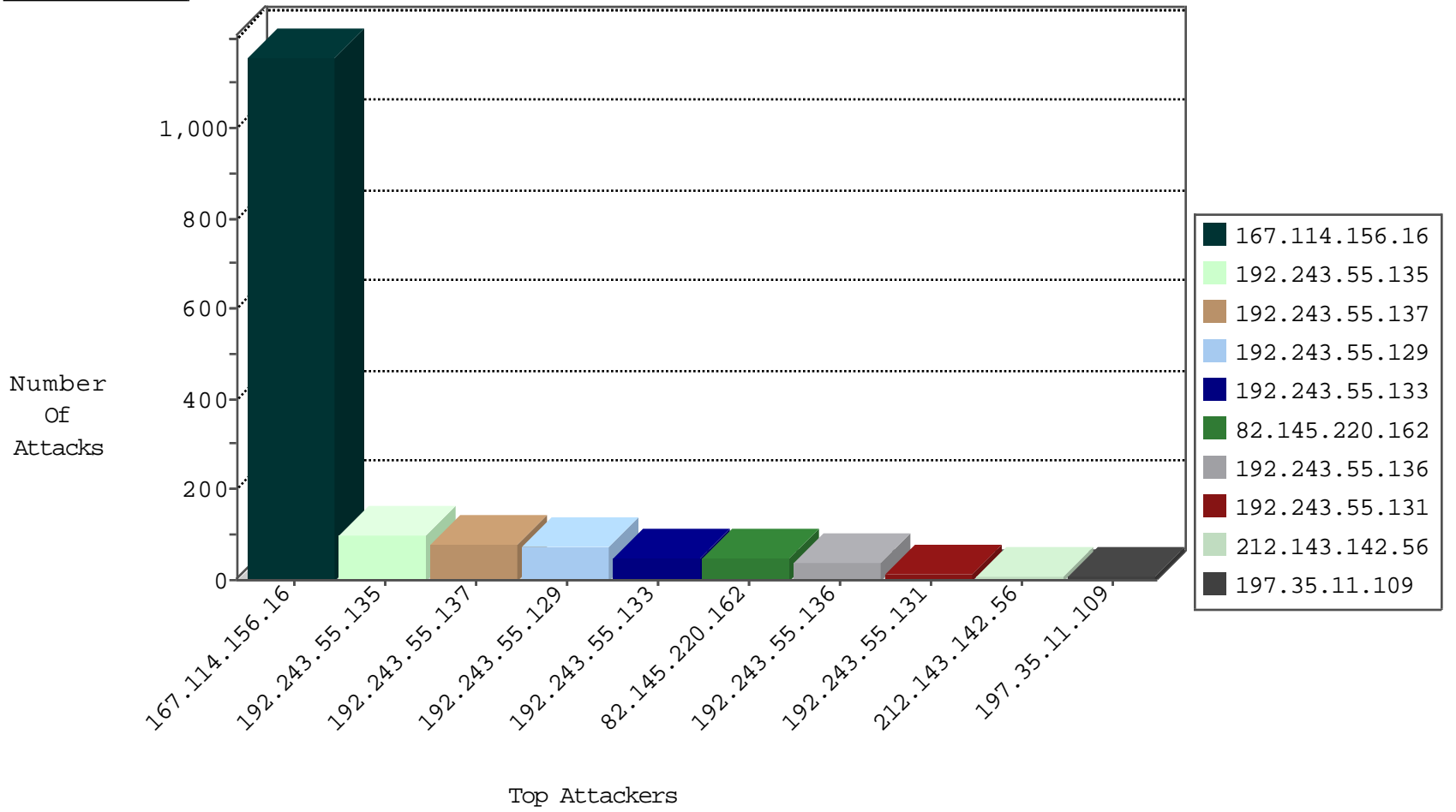
IDF Under Attack Daily Report



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	3980
82.145.220.162	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	47
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
94.102.49.206	Netherlands	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
5.189.172.102	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
125.65.46.143	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
192.243.55.135	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
5.189.172.102	Germany	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	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
66.249.65.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.76.199	Austria	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.192.138	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
50.102.242.22	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.70.114	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.137	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.66.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
197.48.61.233	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.138	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.204	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	2
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.21	United States	147.237.72.166	aka.idf.il	Unknown Parameter 0559c450 in www.aka.idf.il/main/home/default.aspx	None	1
125.65.46.143	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idhsustainabletrade.com/wp-admin/admin-ajax.php	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.186	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1093-7963-he.aspx.	Block	1
65.55.210.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.252.90.243	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/106616.pdf	Block	1
199.30.25.0	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/105946.pdf	Block	1
65.55.210.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.16.186	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.64.58	Block	1
23.242.161.57	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
217.69.133.245	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
199.30.24.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1