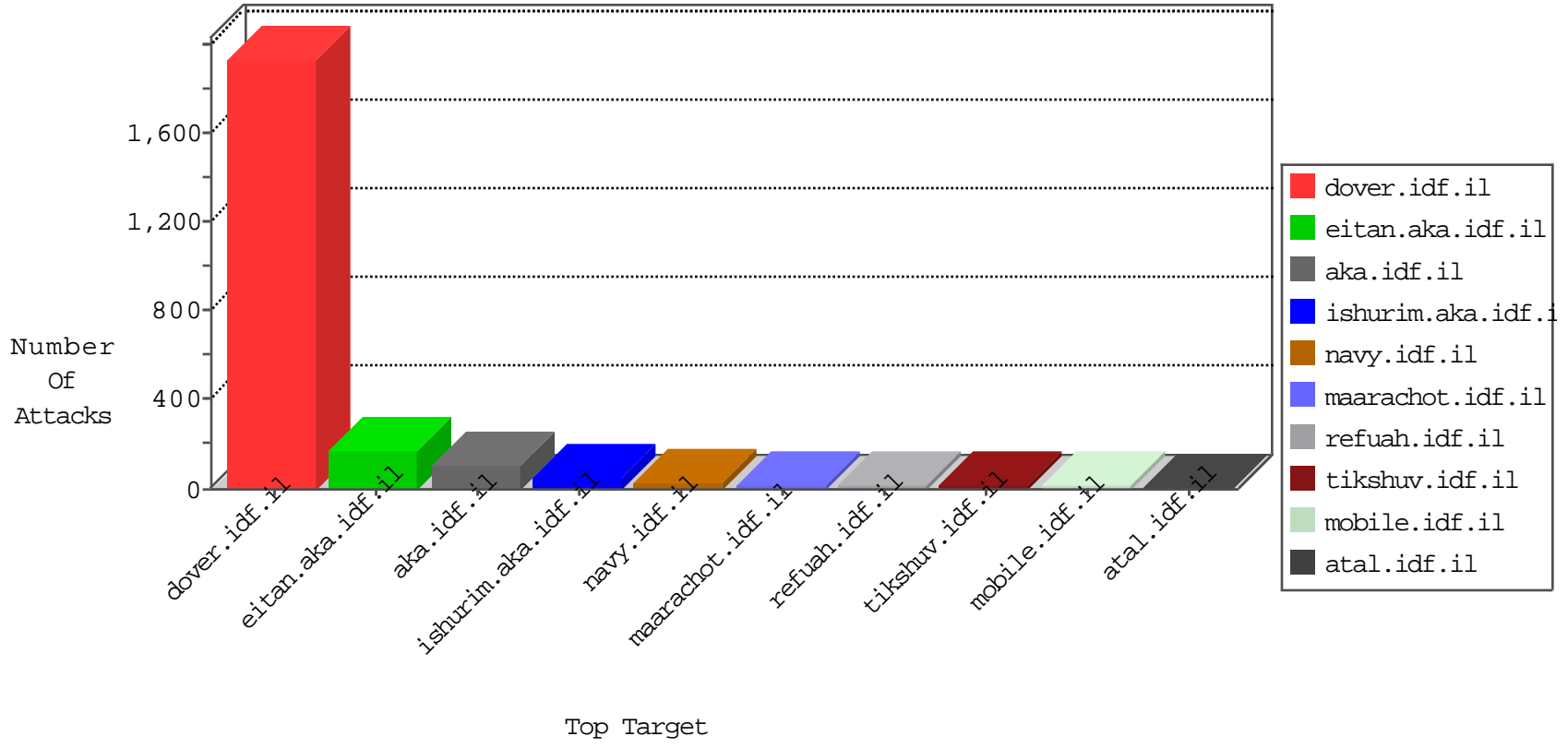


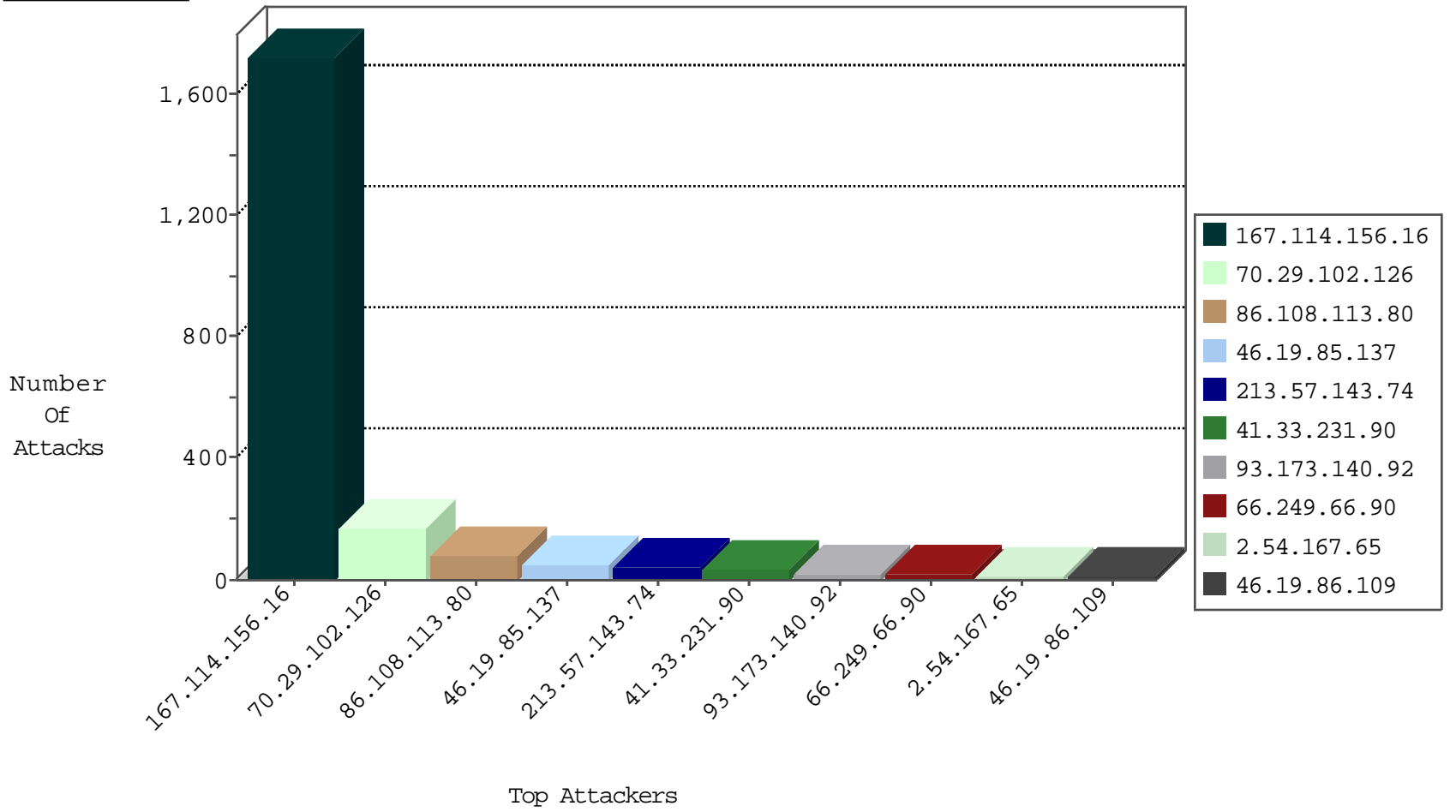
IDF Under Attack Daily Report



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	3152
115.231.222.40	China	147.237.76.198	e.ychalan.idf.il	JLM_Under_Attack_Con_Http	drop	2
208.100.26.228	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
91.246.112.170	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-17-2015-00:04:00 to 12-17-2015-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.117	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: 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
62.75.236.76	147.237.77.121	Germany	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
189.219.81.223	147.237.72.14	Mexico	dover.idf.il(ol	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.253.96.122	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.137	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
86.108.113.80	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
86.108.113.80	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
86.108.113.80	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
70.29.102.126	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
213.57.143.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
213.57.143.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
213.57.143.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
66.87.118.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.66.225.174	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.57.143.74	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
86.108.113.80	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
89.139.167.208	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
93.173.140.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
86.108.113.80	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.143.74	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
93.172.184.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
93.173.140.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.181.138.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.175	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.142.189.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
199.30.25.142	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.167.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.57.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.12.150.135	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.138.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.140.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
93.173.140.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.132.219.142	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.228.54.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.40		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.140.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
128.232.110.28	United Kingdom	147.237.76.198	e.yochalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.109	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.146.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
2.54.167.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.249	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.31.116	Israel	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.26.146.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.148.235.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.57.141.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.29.102.126	Canada	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 70.29.102.126	Block	157
176.12.148.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
82.81.24.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
84.108.96.64	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
80.246.136.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
195.154.227.118	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.176.18.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.13.102.119	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
149.78.220.184	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.220.184	Block	1
85.65.111.245	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.181.138.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
149.78.220.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/h	Block	1
93.172.184.3	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
197.36.255.153	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.117.239.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
173.252.90.120	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.188.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.20.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
131.253.35.149	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.121.246.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
70.29.102.126	Canada	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
2.54.168.196	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1