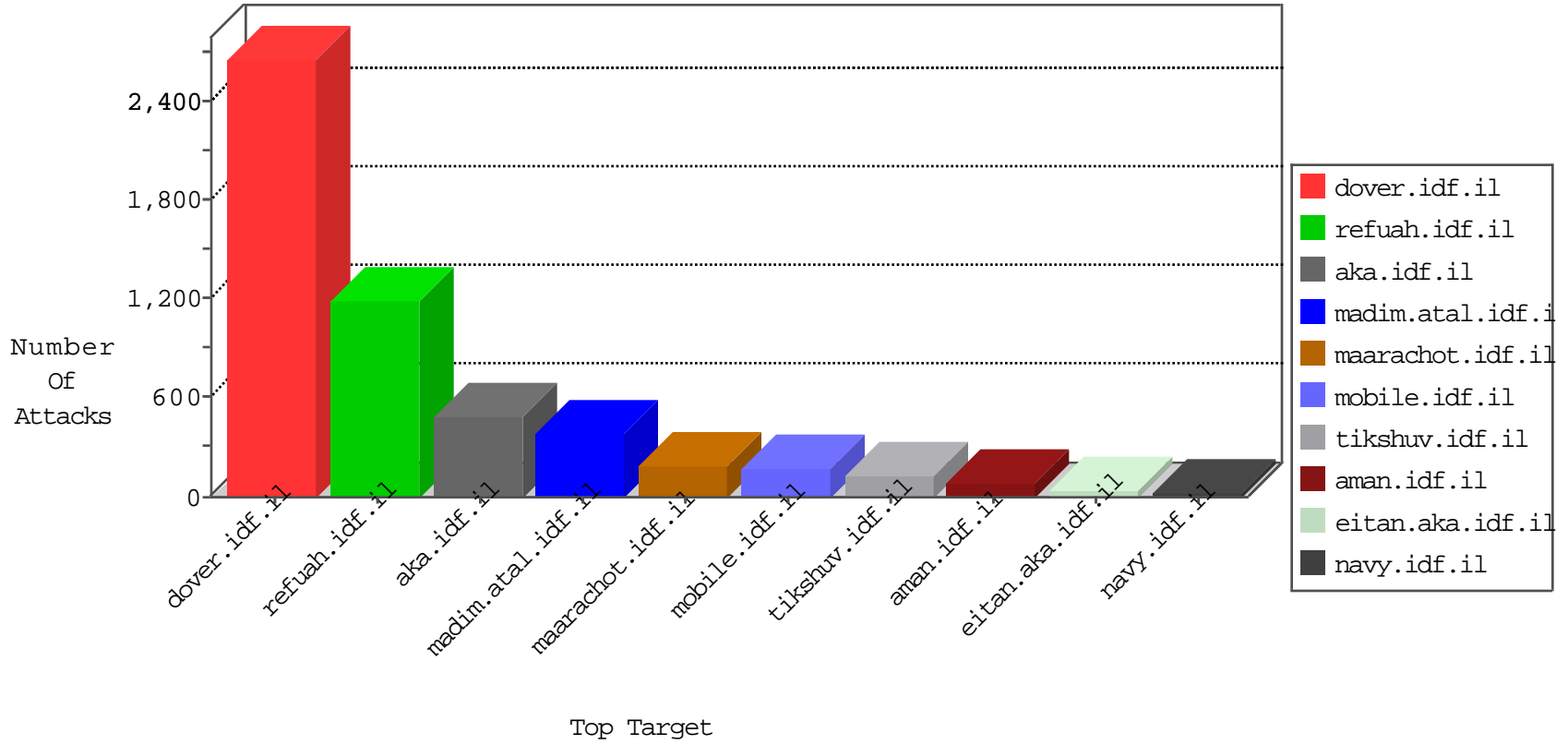


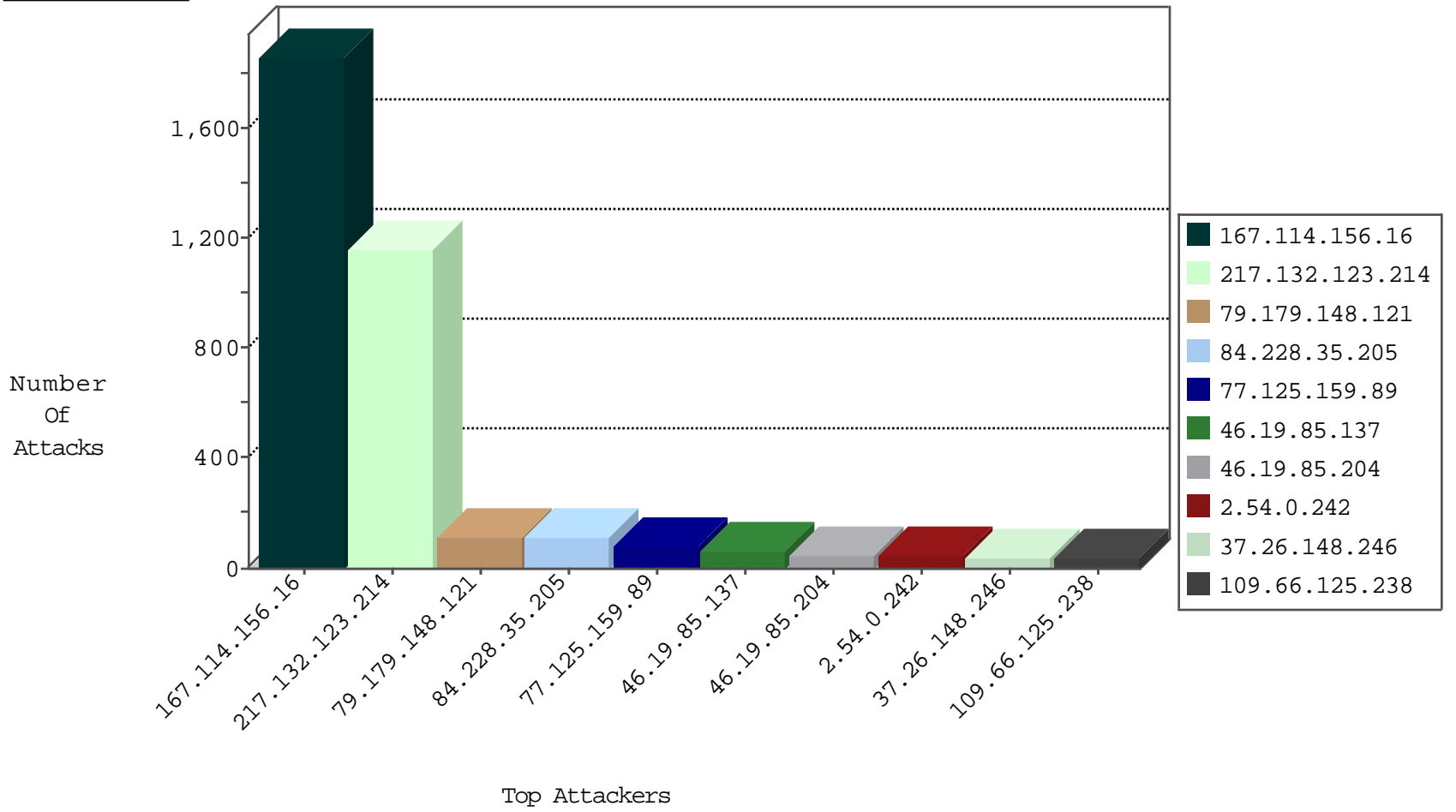
IDF Under Attack Daily Report



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	3049
79.182.55.119	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.15.236	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
79.182.55.119	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
141.212.122.203	United States	147.237.76.34	yohanan.idf.il	Block_Udp_All_Nets	drop	1

01-03-2016-18:04:01 to 01-03-2016-19:04:01

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	3

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.123.214	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1161
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.181.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
46.116.179.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
109.253.131.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
5.22.130.146	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
77.125.245.102	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.116.133.171	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.54.0.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.182.190.38	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
149.20.63.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.26.149.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.146.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.64.21.150	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
79.178.114.26	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
79.183.112.178	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
212.199.218.50	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	12
84.109.60.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.186.131.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
81.218.127.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.186.131.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.148.246	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
96.224.13.26	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
31.154.145.22	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
5.22.130.102	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.146.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
176.13.12.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.142.211.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
192.114.7.2	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.54.188.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.142.211.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
2.54.0.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.253.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.0.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.210.188.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.117.61.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.35.205	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	111
79.179.148.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	95
46.19.85.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
77.125.159.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
109.66.125.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
77.125.159.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
79.179.148.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.108.124.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.144.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.131.65	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
2.54.9.11	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
46.116.179.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
176.13.7.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.141.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.65.81.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.81.233	Block	4
82.118.24.206	Sweden	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.118.24.206	Block	4
37.26.149.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.54.57.11	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
84.108.64.31	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
192.114.5.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.146.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.183.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.61.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
87.68.37.46	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/ikunpratimishiyim.aspx	Block	3
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.157.104	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
109.67.154.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.250.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.149.131	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	2
87.69.195.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.217.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
109.64.4.103	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.48.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.48.56	Block	2
109.186.131.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.12.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.156.92	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
52.90.147.70	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/sidebar/sidebar.js	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
37.142.211.138	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.204.106.16	Netherlands	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.13.4.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1