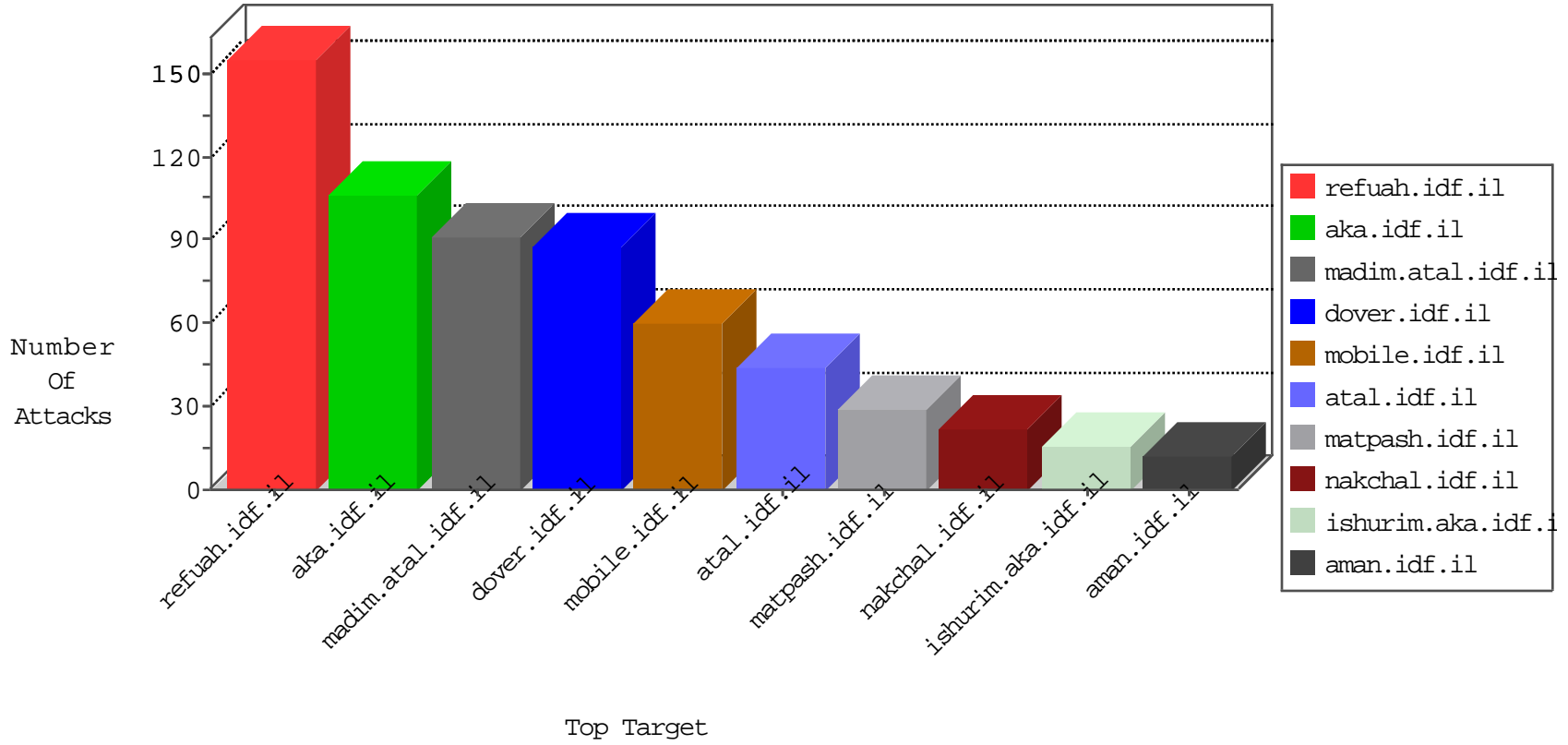


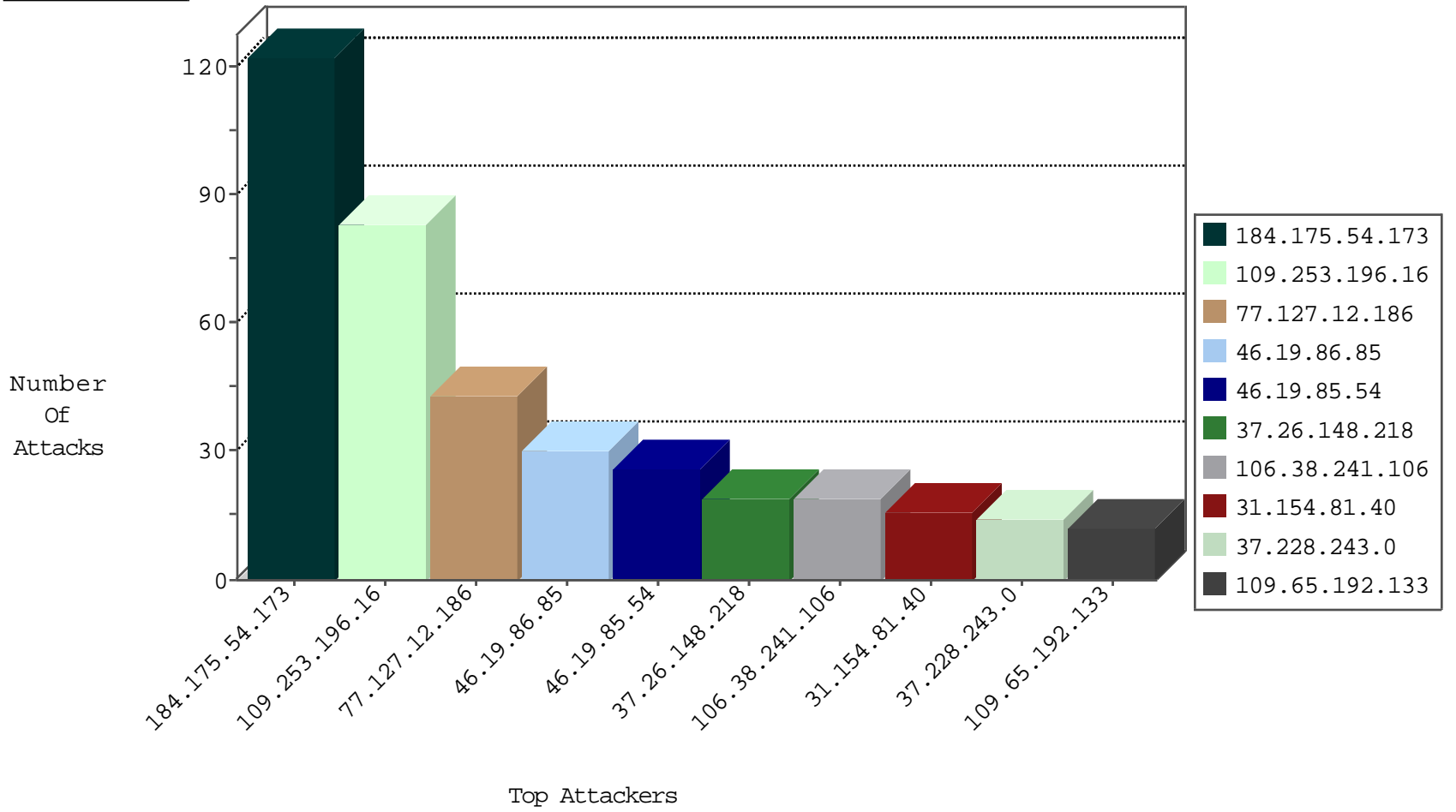
# IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	14
106.38.241.106	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.172.91.21	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
163.172.115.5	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
89.39.1.65	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.93.216	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
50.116.123.33	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
14.182.16.146	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.140.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.115.5	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.115.5	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
89.39.1.65	147.237.72.167	Romania	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
58.186.44.220	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.175.54.173	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	122
77.127.12.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
46.19.86.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
197.116.222.233	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
164.138.119.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.192.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.85.54	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.54	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.108.100.81	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
185.32.179.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.76.96.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.148.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.65.10	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.67.149.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.146.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
197.165.232.235	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.177.223.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.228.243.0	Ireland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.138.125.65	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
176.13.18.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.36.146.226	Oman	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
217.132.100.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.228.243.0	Ireland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
109.65.192.133	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.148.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.22.134.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.228.243.0	Ireland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
37.26.148.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.102.9.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.228.243.0	Ireland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.228.243.0	Ireland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.117.184.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.109.235.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.217.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.162.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.89	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
92.222.245.134	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.148.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.233.103.237	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.218	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.178.192.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.93	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.226.162.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.196.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	83
31.154.81.40	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 31.154.81.40	Block	14
46.121.142.226	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
46.19.86.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.197.128.154	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
169.229.3.91	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.127.12.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.121.142.226	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	1
207.46.13.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.69.241.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8759-he/refuah.aspx	Block	1
31.154.81.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
176.228.190.238	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
77.139.74.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
66.102.6.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
212.76.96.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/	Block	1
176.228.190.238	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.228.190.238	Block	1
77.139.101.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash2017/lobby.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/65012.doc	Block	1
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
95.86.117.67	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.124.55.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.27.105.136	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
81.7.17.2	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.248.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authentication.service.asmx/getauthuser	Block	1
77.125.61.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.142.226	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 46.121.142.226	Block	1
87.69.122.129	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9724-he/refuah.aspx	Block	1