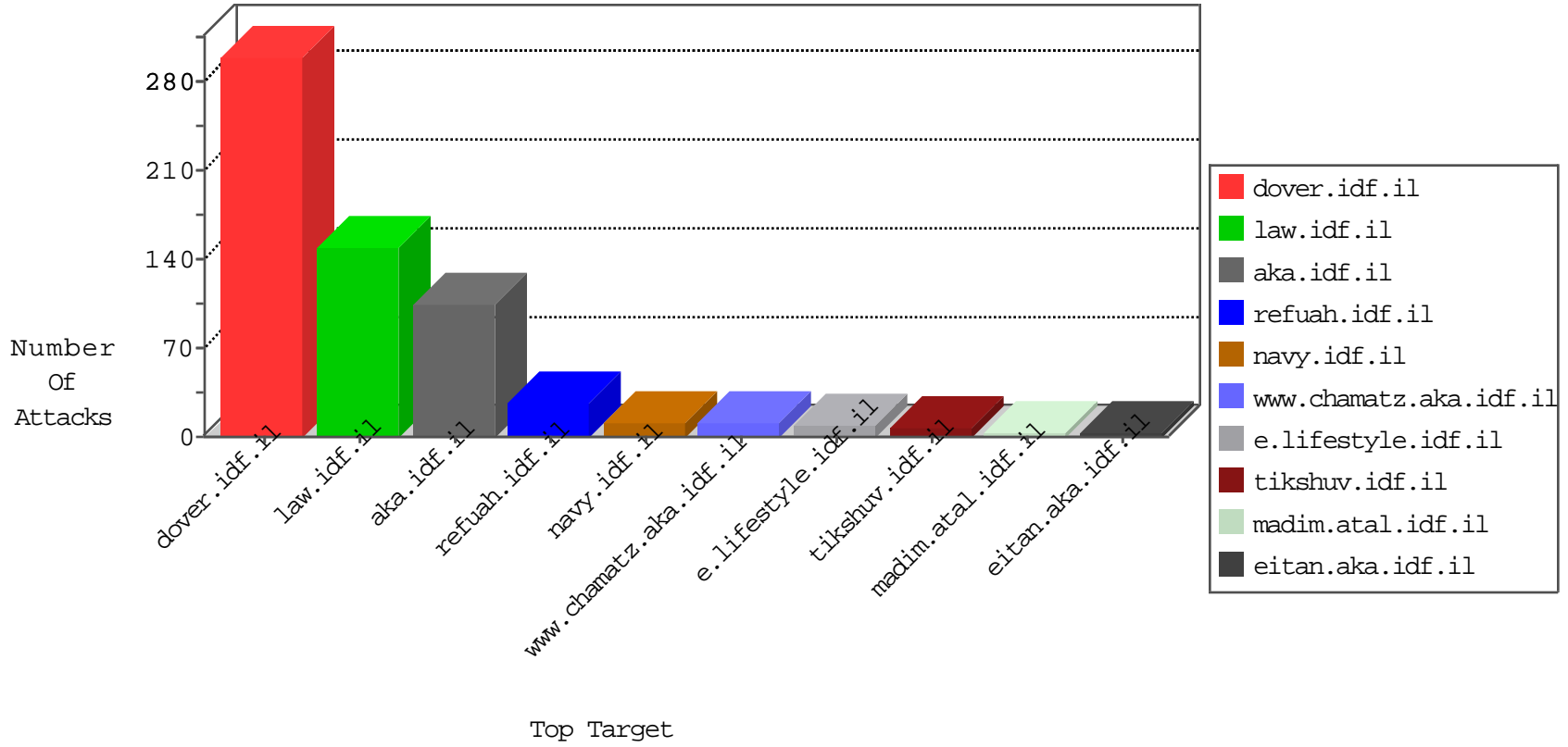


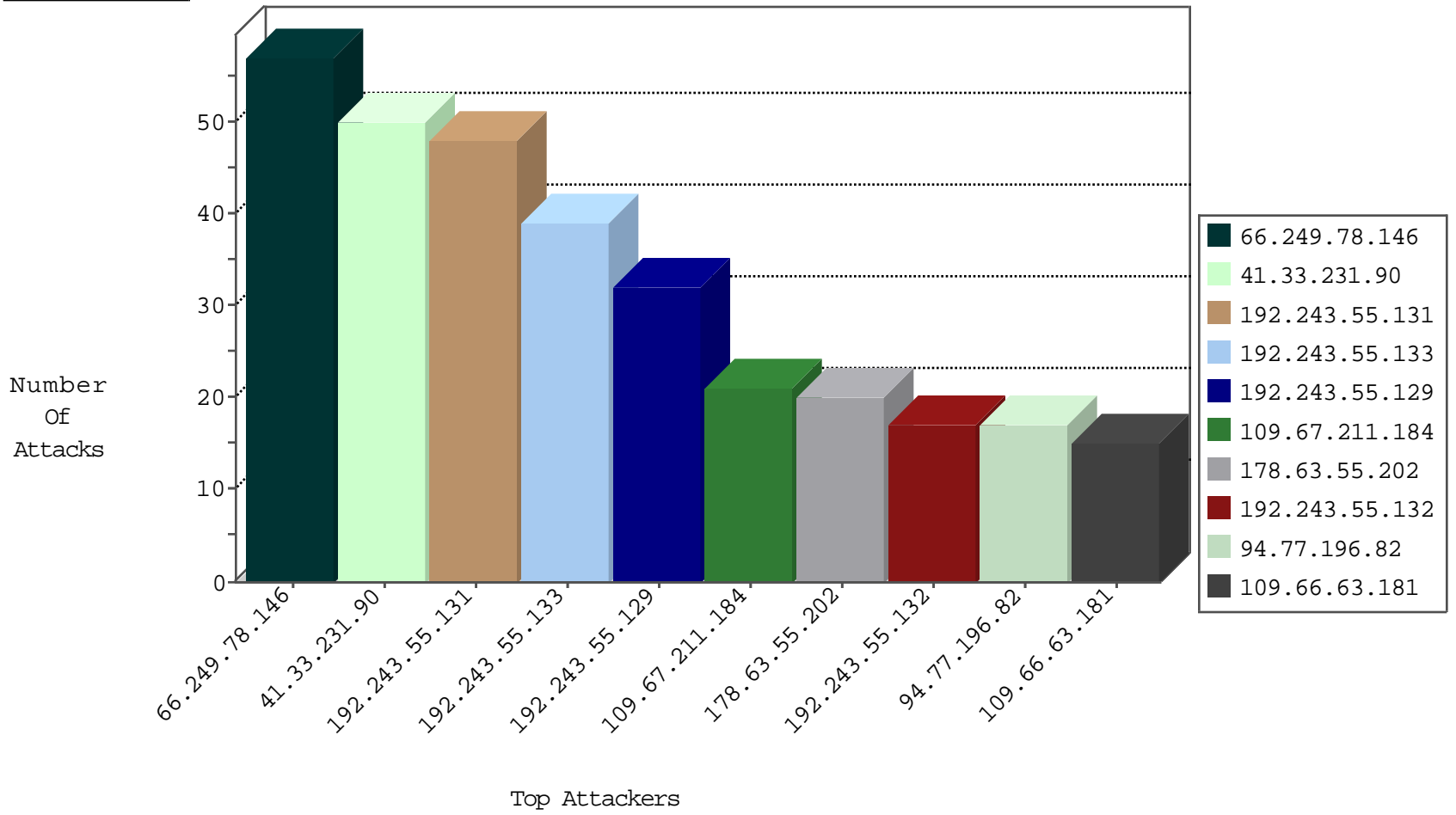
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
94.102.49.116	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
58.218.211.11	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
195.81.248.101	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
189.34.103.47	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.99	147.237.77.179	Lithuania	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.38	Lithuania	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.211.11	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
189.32.131.55	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.99	147.237.76.86	Lithuania	navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.167	Lithuania	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.67.211.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.66.63.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
209.112.251.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.116.205.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
40.77.167.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.116.205.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
149.78.84.48	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
71.232.73.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.173.179	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.246.0.243	Ireland	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
85.64.173.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.189.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
41.143.149.70	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.189.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
157.55.39.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	2
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
109.253.128.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/general.aspx	None	1
84.111.115.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
131.253.25.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ca in www.aka.idf.il/main/giyus/general.aspx	None	1
104.131.59.76	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 104.131.59.76	Block	1
51.254.215.146	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 51.254.215.146	Block	1
198.58.96.215	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/leshakot/default.asp	None	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat in www.aka.idf.il/main/giyus/general.aspx	None	1
104.131.59.76	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
51.254.215.146	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover&hellip	Block	1
37.28.152.58	Poland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;popId in www.aka.idf.il/londim/tochen/	None	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catI in www.aka.idf.il/main/giyus/general.aspx	None	1
109.67.211.184	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69059.pdf	Block	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.232	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1