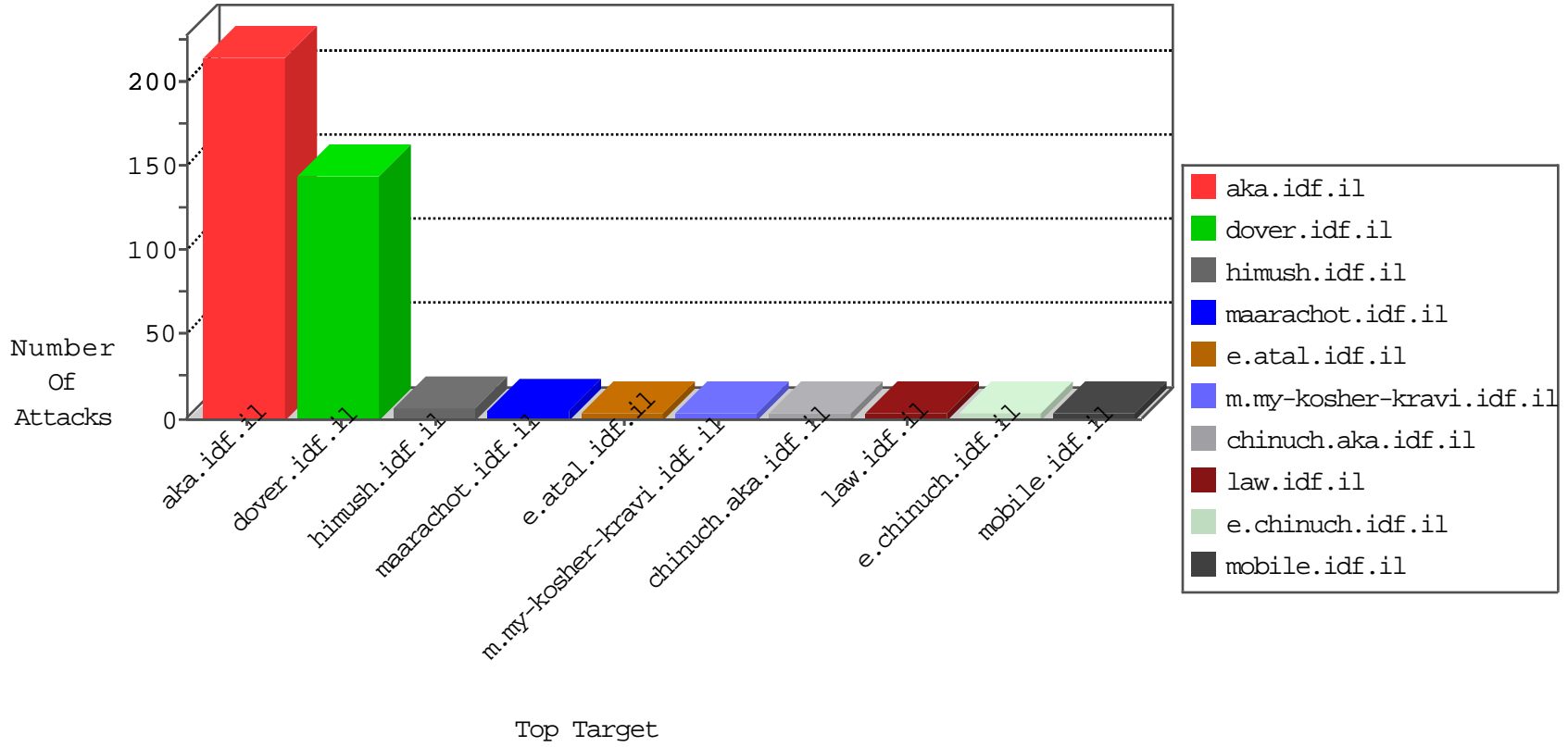


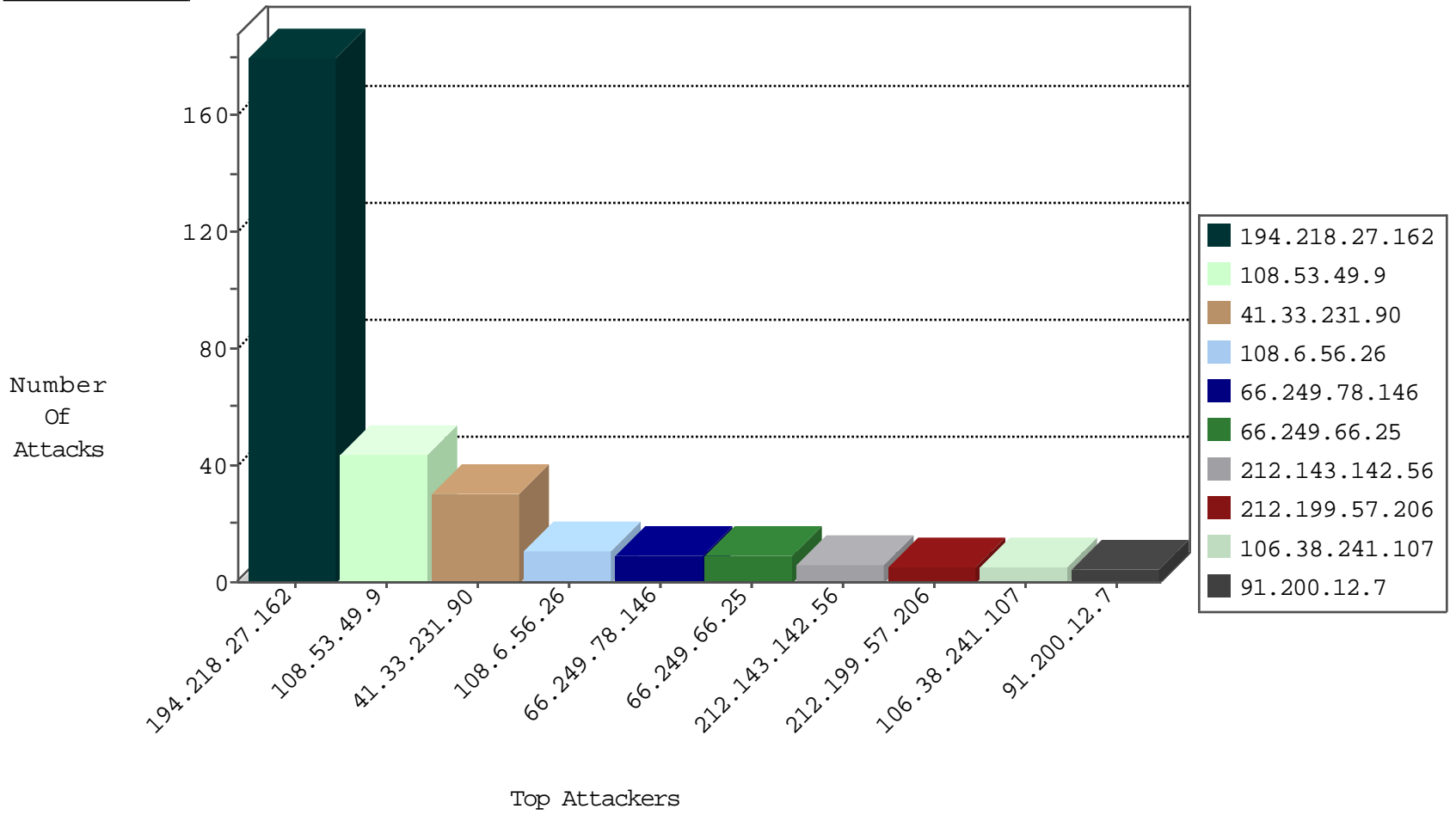
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.16	United Kingdom	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
47.88.103.153	Canada	147.237.76.42	refuah.idf.il	block-sp-trafl	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.60	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.76	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.94	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.16	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.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	3
37.26.148.221	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
221.226.31.210	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
89.163.145.155	147.237.76.30	Germany	himush.idf.il	ET SCAN NMAP -f -sS	1
221.6.32.82	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
202.71.25.29	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
159.122.254.212	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.136	147.237.76.202	Vietnam	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.167	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
221.226.31.210	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
89.163.145.155	147.237.76.30	Germany	himush.idf.il	ET SCAN NMAP -sS window 2048	1
221.6.32.82	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.77.74	Latvia	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.167	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.122.167	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
108.53.49.9	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
108.6.56.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.199.57.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.43.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.58.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.73.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.56.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
74.217.28.153	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.54.18.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
40.77.167.20	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
85.90.246.233	United Kingdom	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
47.88.103.153	Canada	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.118.60.69	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.56.12.179	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.90.246.233	United Kingdom	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
5.102.195.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.79.130.52	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.221	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.193	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.84.215	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.56.98.150		147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
182.118.20.175	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.148.221	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.194	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.90.244.30	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
47.88.103.153	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
182.118.22.213	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
75.82.147.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	7
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	3
66.249.66.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
182.118.20.172	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
66.249.78.93	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/927-he/asp.	Block	1
109.110.113.235	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
70.192.70.198	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmorret	Block	1
185.80.220.24		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/cgi-bin/php	Block	1
93.219.249.11	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
109.110.115.148	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.204.146.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.96.199	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.110.112.230	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.146	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/45741.pdf.accessed	Block	1
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.237.80	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.110.113.83	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.142.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/kkkkkkkk=bfd5eb1dkkkkkkkk_bfd5eb1d	Block	1
85.64.68.134	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.78.11	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.110.113.196	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.170	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
52.25.116.236	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1