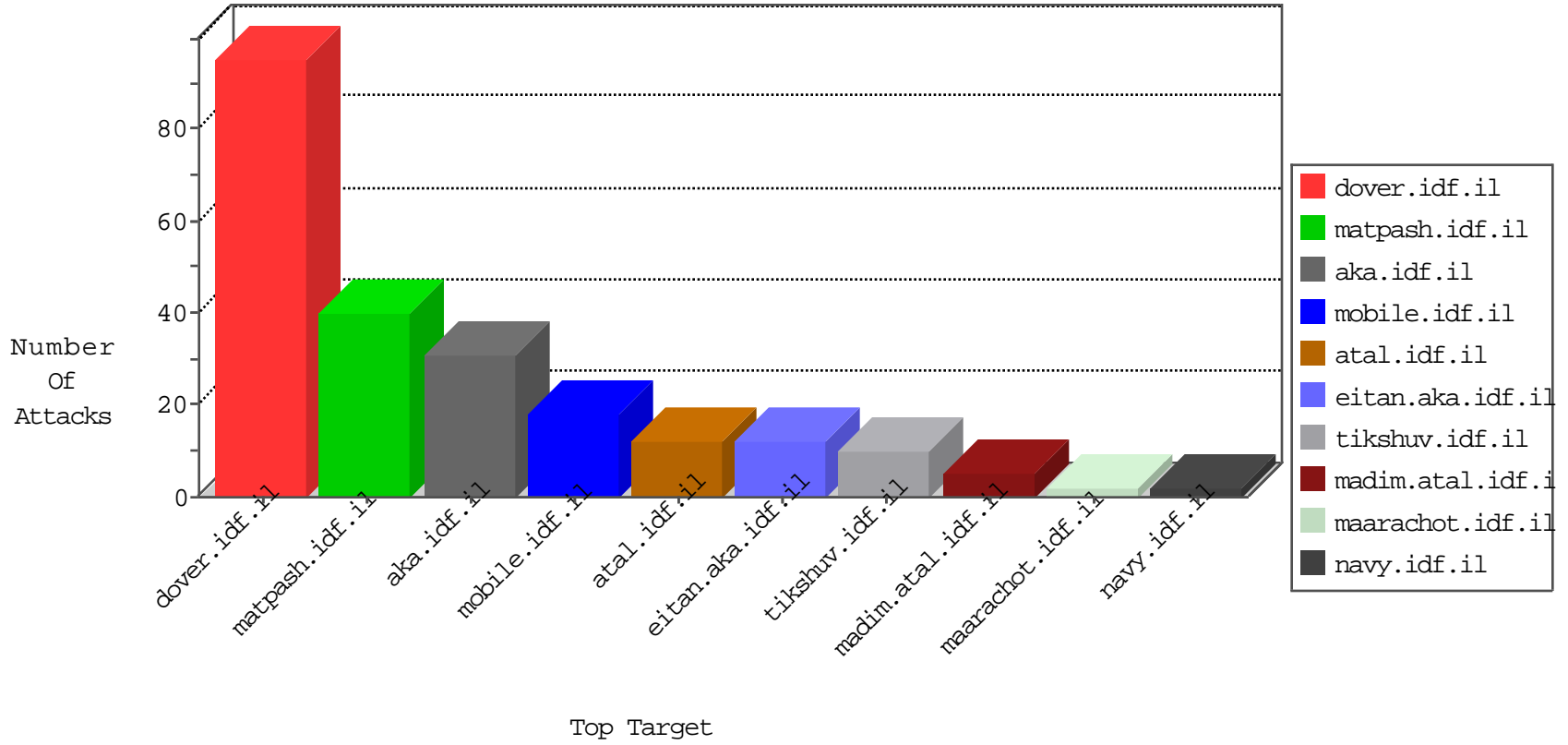


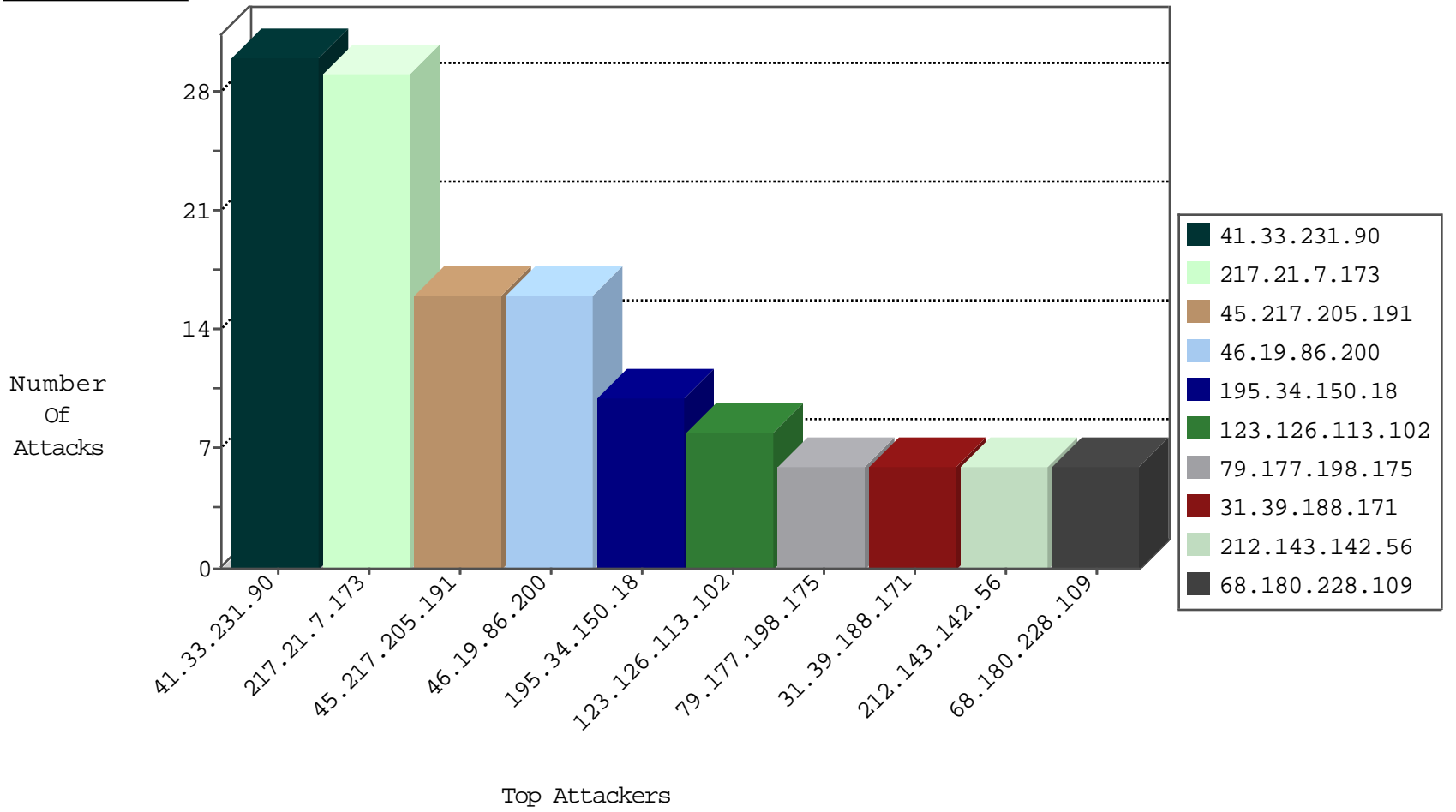
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	2
179.43.141.219	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
79.179.63.141	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.4.116.197	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.75	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.2	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
107.167.187.128	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
51.255.65.52	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.70	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	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	5
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.255.65.207	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.217.205.191	147.237.77.216	Uruguay	dover.idf.il	SERVER-WEBAPP admin.php access	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
217.21.7.173	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
46.19.86.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
79.177.198.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.39.188.171	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.249.93.45	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.214	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.41	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.93.43	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
141.8.184.30	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.223.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.25.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
123.126.113.102	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.228.15.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.39.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
85.130.211.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
85.130.211.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.25	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.117.168.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
101.162.171.141	Australia	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.109	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
46.117.168.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.29.79	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.109	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.82.200.91		147.237.76.39	mobile.meitav.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
114.112.90.54	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.182.18.41	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.230	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.134	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
88.200.214.8	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
123.125.71.25	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.217.205.191	Block	7
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.86.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
46.19.86.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
178.45.185.179	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1380-he/dover.aspx	Block	1
109.65.191.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
179.7.69.67	Peru	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109986.pdf	Block	1
157.55.39.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.82.200.91		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.69.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/106697.pdf	Block	1
45.217.205.191	Uruguay	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/login	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
31.39.188.171	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
198.20.69.74	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
157.55.39.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1