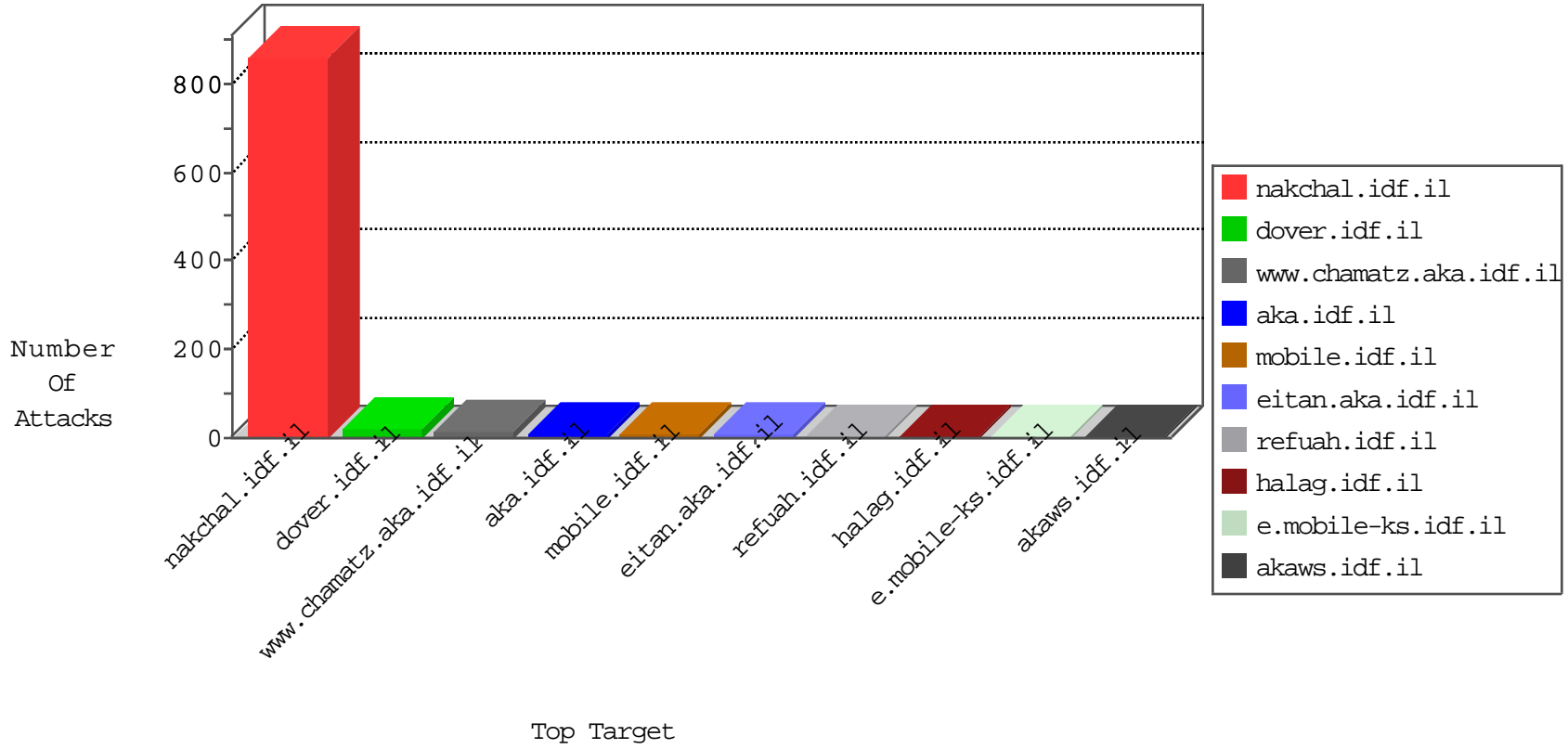


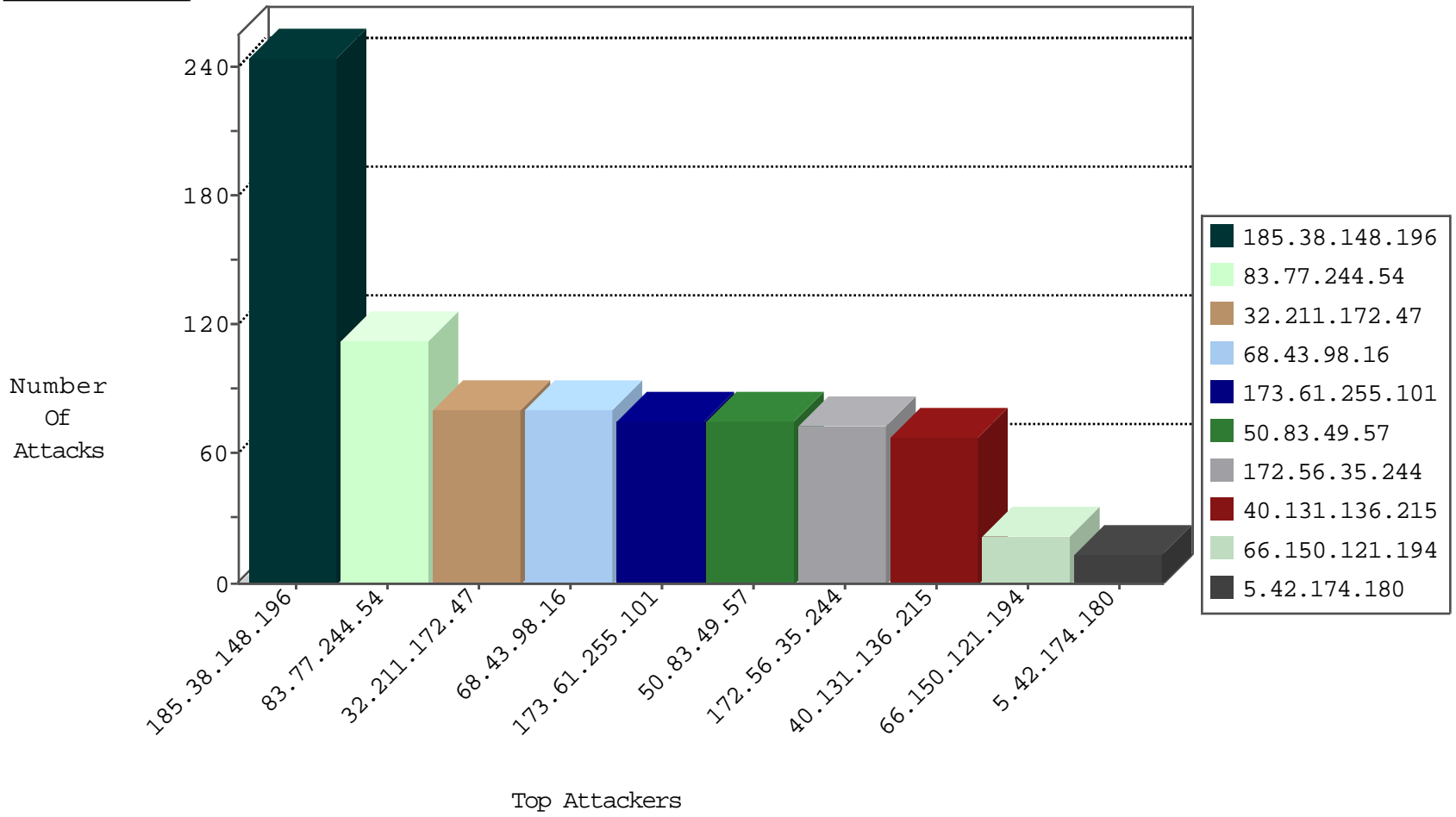
# IDF Under Attack Daily Report



## 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	147.237.76.176	test.ncore.idf.il	Black List	drop	1

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
93.171.33.219	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 3072	1
42.247.4.164	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 4096	1
42.247.4.164	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
42.247.4.164	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.234	Indonesia	halag.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.242	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
139.59.28.44	147.237.76.44	Singapore	e.refuah.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
185.38.148.196	United Kingdom	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	234
32.211.172.47	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
68.43.98.16	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
173.61.255.101	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	76
50.83.49.57	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	75
172.56.35.244	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
40.131.136.215	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	68
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	26
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	25
66.150.121.194	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
46.19.86.131	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
172.56.13.227	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.4.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.38.148.196	United Kingdom	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
131.253.25.206	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.42.174.180	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
185.38.148.196	United Kingdom	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
5.42.174.180	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
5.42.174.180	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.38.148.196	United Kingdom	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
66.150.121.194	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
199.30.24.61	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.42.174.180	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.139.89	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
5.42.174.180	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
162.245.1.125	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
172.56.139.89	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
137.226.113.7	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.32.179.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.111.13.47	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.56.139.89	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
162.245.1.125	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.31.224.21	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.16	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.72.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.245.1.125	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
137.226.113.7	Germany	147.237.0.35	akaws.idf.il	drop		drop	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
176.31.224.21	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1

09-28-2016-02:04:03 to 09-28-2016-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.149	Israel	147.237.76.200	eitan.aka.idf.	Unknown Parameter lang in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
31.154.81.9	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1767	Block	1
31.154.81.9	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
77.138.66.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar/login/	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
89.248.172.16	Netherlands	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	1

09-28-2016-02:04:03 to 09-28-2016-03:04:03