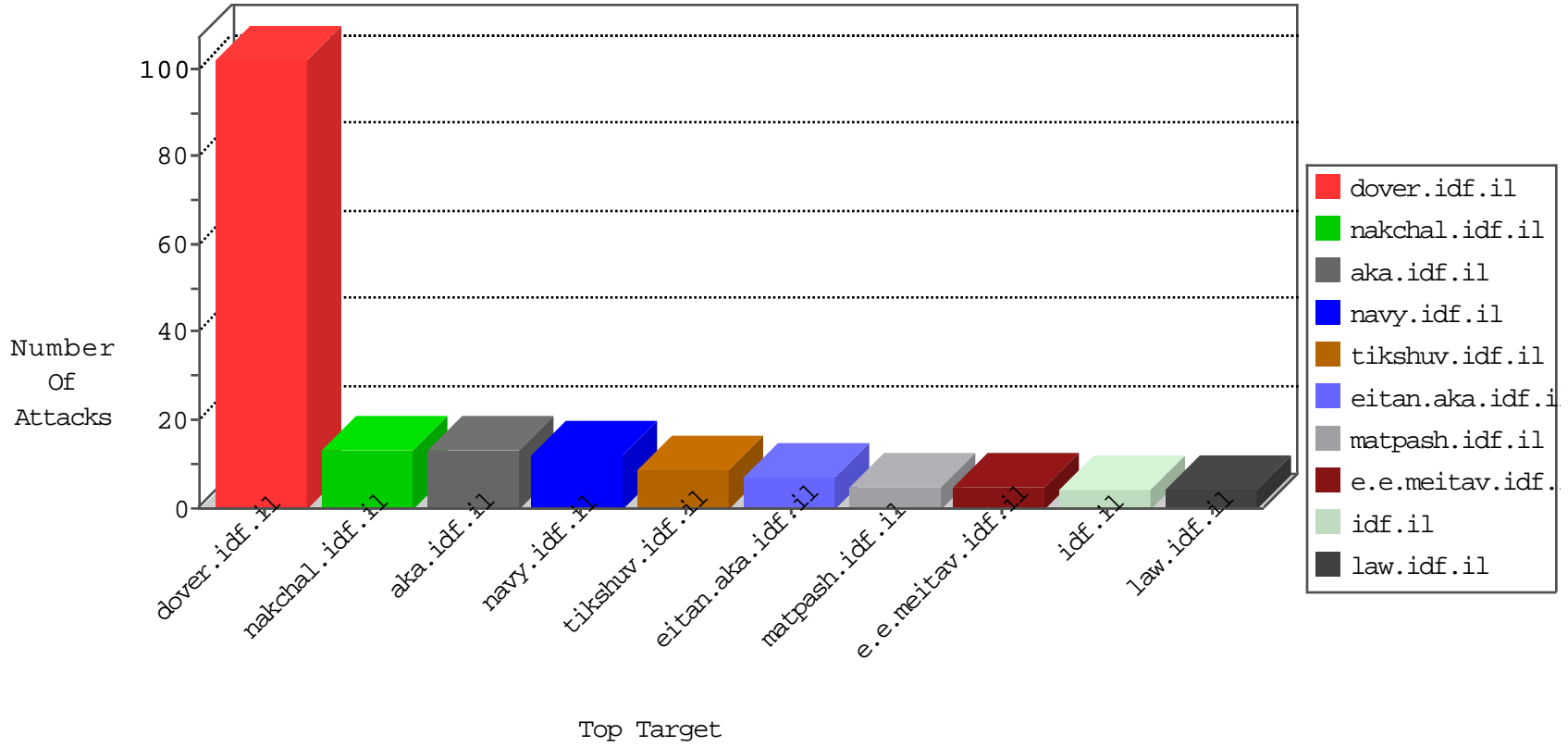


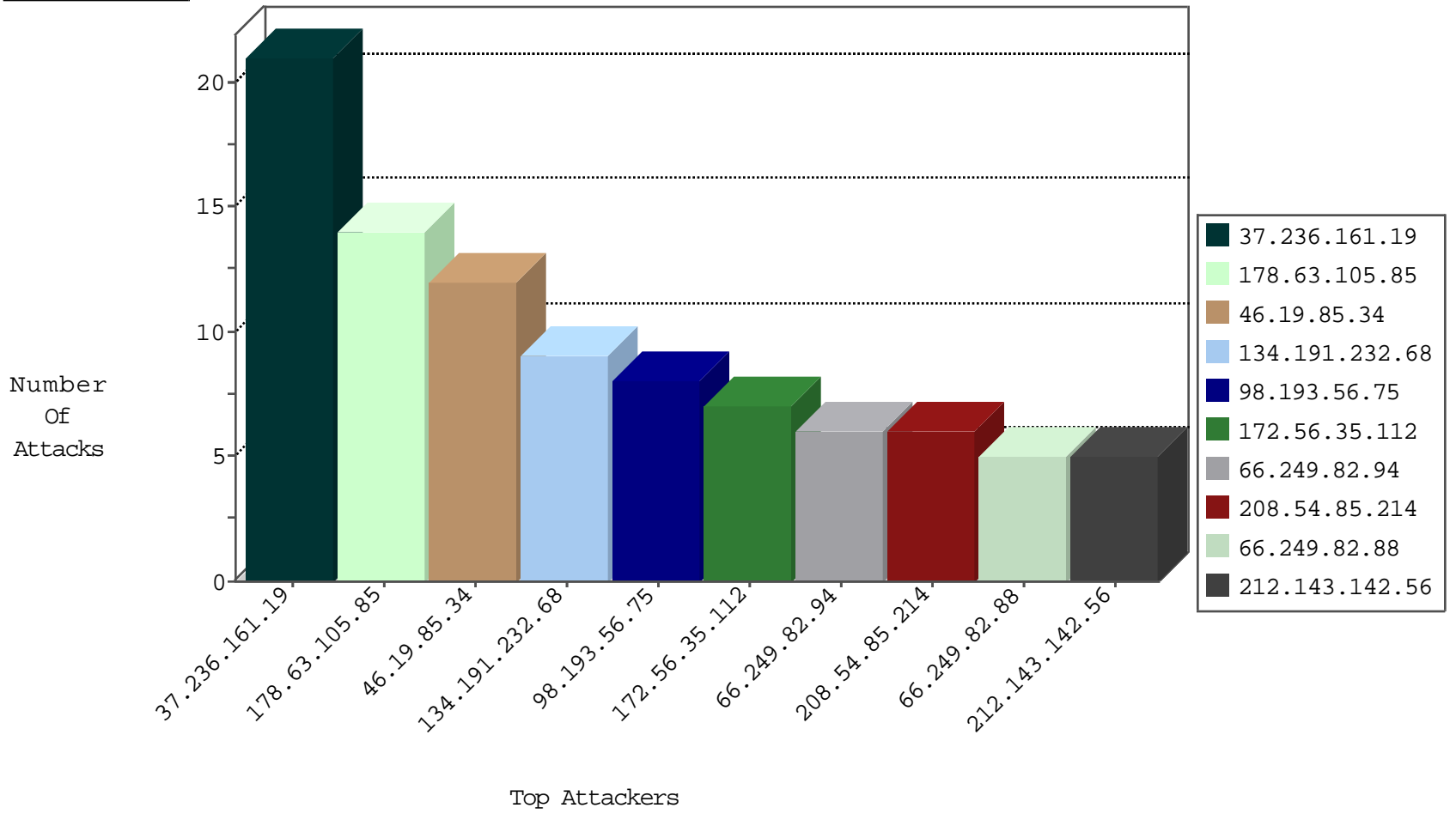
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.191.232.68	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	29
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
185.35.62.189	Switzerland	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
113.252.65.43	Hong Kong	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.50	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1

03-07-2016-04:04:08 to 03-07-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.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	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
123.59.53.156	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.163.145.38	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
5.39.222.253	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.76.148	India	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
189.110.158.12	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.122.254.212	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
95.130.13.220	147.237.76.196	France	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
219.92.25.170	147.237.76.31	Malaysia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.122.254.212	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.236.161.19	Iraq	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
98.193.56.75	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
172.56.35.112	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.54.85.214	United States	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	5
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	4
199.30.24.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.64.226.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.19.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
50.154.167.156	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
204.79.180.247	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
74.82.47.59	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.130	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.78	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.161	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.84	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.216	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.176.219.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.169	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.79	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.181.113.88	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.10	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.162	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.239	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
50.93.203.2	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.169	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.41.177.26		147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
184.105.139.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.34	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.8.46	e.chiruch.idf.il	drop	SAM rule	drop	1
37.26.149.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.166	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.244	United States	147.237.77.176	matpash.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
66.249.82.94	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.82.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
66.249.82.91	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.83.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
24.217.39.157	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
24.217.39.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	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-he/cogat.aspx	Block	1
37.26.148.228	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
94.230.93.47	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
5.34.68.131	Kazakstan	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
198.20.69.74	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
40.77.167.61	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
106.184.7.86	Japan	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	1
207.46.13.38	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
90.216.229.73	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/62953.jpg	Block	1
141.212.122.129	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /x	Block	1
66.249.83.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
90.216.229.73	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
172.56.35.112	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.83.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
94.230.93.47	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1