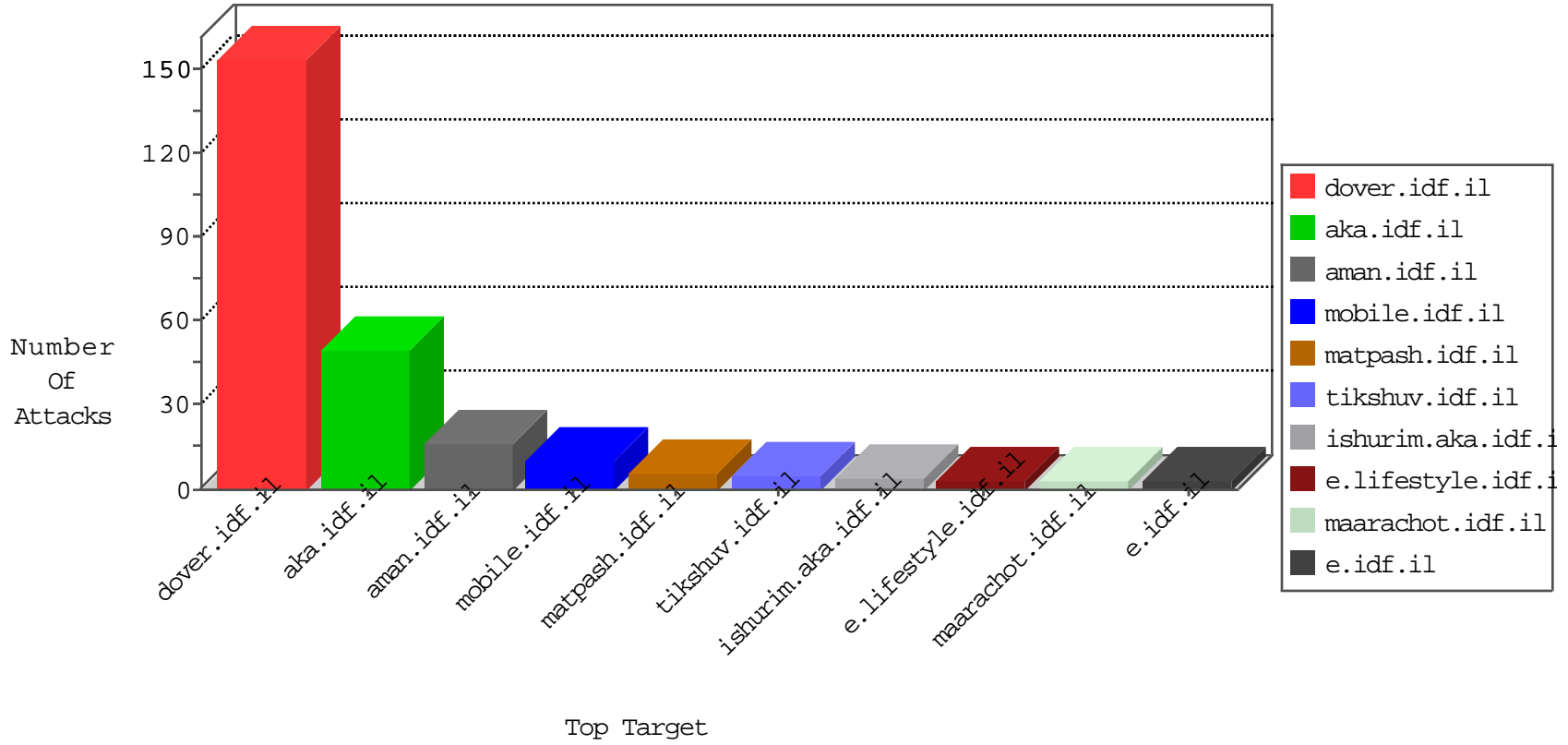


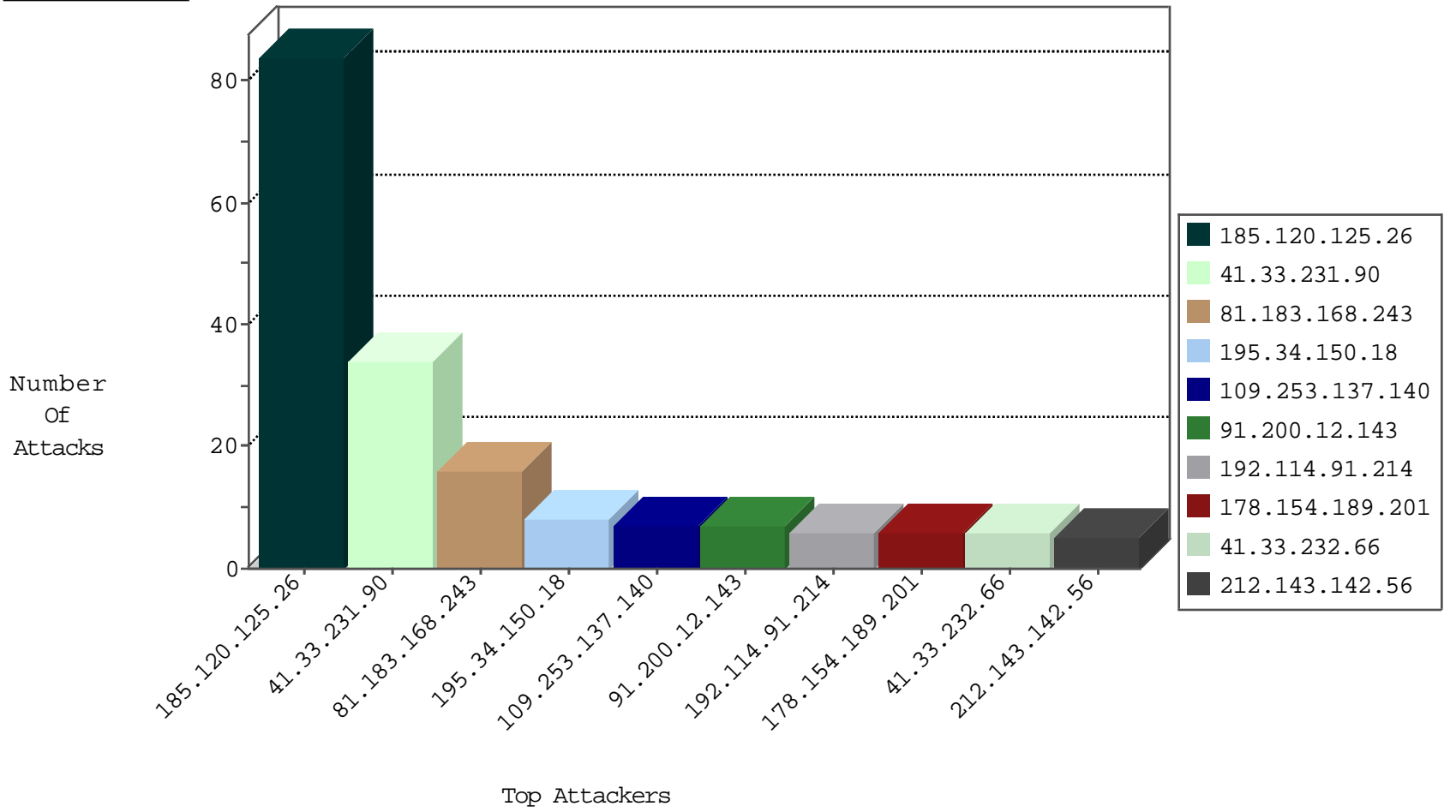
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.115.120	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	5
89.248.172.154	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-02:04:09 to 02-08-2016-03:04:09

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.102.8.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
81.183.168.243	147.237.72.167	Hungary	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.96.221	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.110.194.232	147.237.77.19	Taiwan	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.201.27.61	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
81.183.168.243	Hungary	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
192.114.91.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
5.22.135.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.62.36	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
2.54.168.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.209.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
165.91.4.58	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
177.240.111.115	Mexico	147.237.0.35	akaws.idf.il	drop		drop	2
54.67.38.74	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.211	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
45.63.97.227		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
165.91.4.58	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.85	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.210.187.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.222	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
81.183.168.243	Hungary	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.63.97.227		147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
176.13.7.203	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
141.212.122.87	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
76.178.143.180	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.223	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.183.168.243	Hungary	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.179.212.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.88	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.51.30	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.183.168.243	Hungary	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.179.212.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.210	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
193.96.188.175	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.137.140	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	7
87.70.184.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.70.184.17	Block	4
84.94.21.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	2
81.183.168.243	Hungary	147.237.72.156	aman.idf.il	Illegal HTTP Version the green fields outside. Watch the goats chewing the grass. What is the meaning of life? Life isn't about getting to the end. Goats know this. You should know too. Goats are wise. Goats are cute. Listen to them! This is the message. Love goats, love the Internet! ðŸ?? Kecske. HTTP/1.0	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17763-he/kkkkkkk=a43487c1kkkkkkk_a43487c1	Block	1
87.70.184.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.69.54	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
81.183.168.243	Hungary	147.237.72.156	aman.idf.il	Malformed URL towards	Block	1
188.143.232.26	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$ucArticleLobbyControl\$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
128.194.131.235	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 128.194.131.235	Block	1
82.221.105.7	Iceland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
219.94.128.197	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.128.197	Block	1
98.143.148.107	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/check	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
176.13.7.203	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
81.183.168.243	Hungary	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
177.240.111.115	Mexico	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.66.132	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	1
118.193.222.243	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1