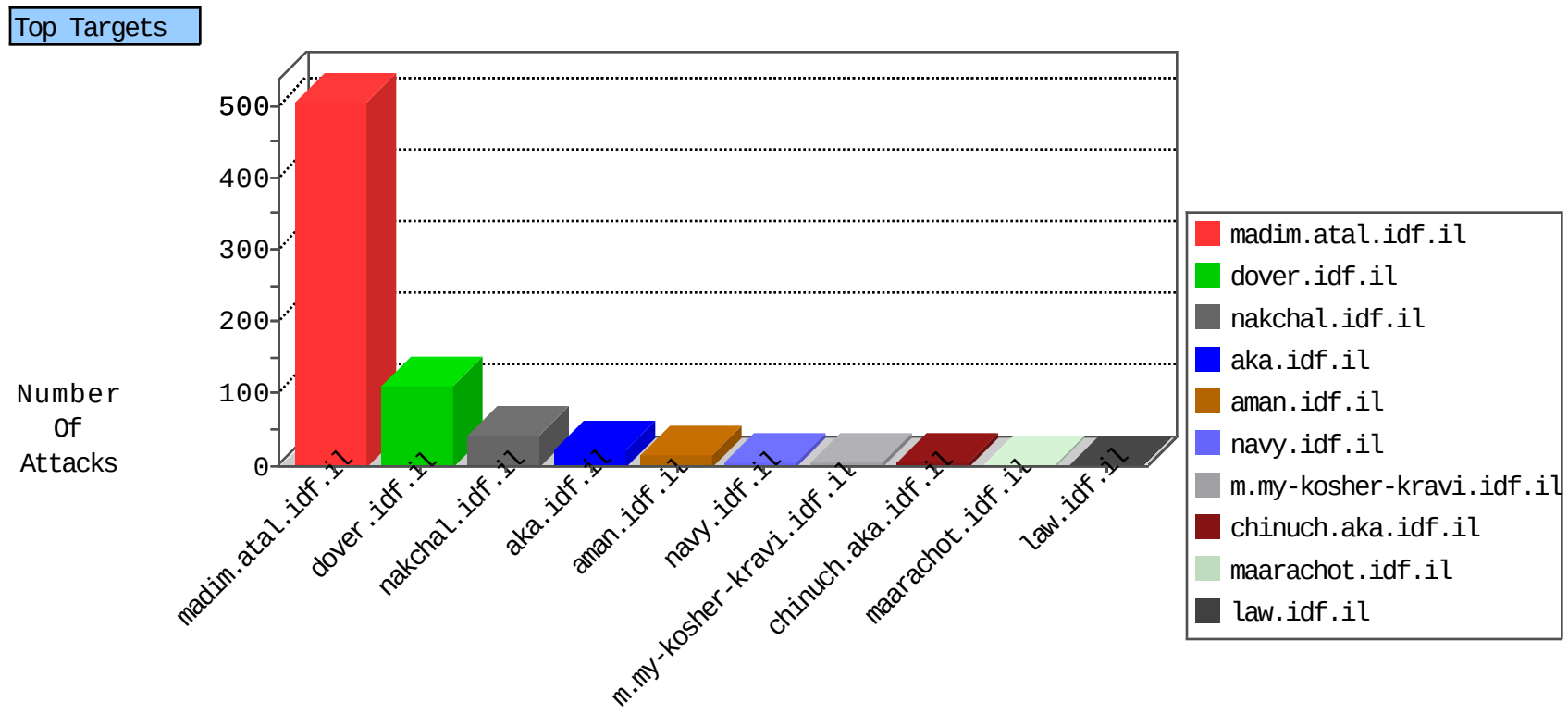
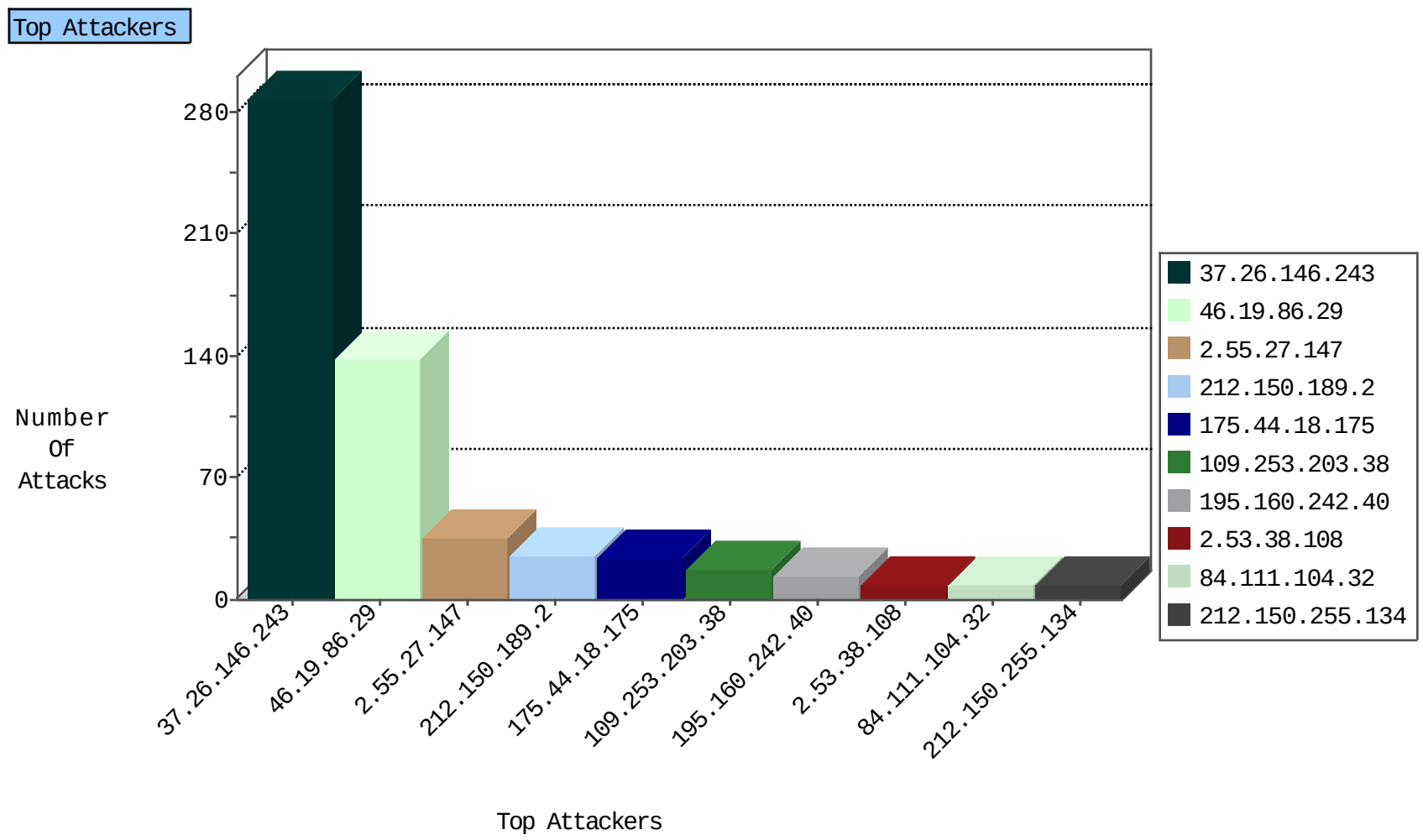
08-17-2016-13:04:00 to 08-17-2016-14:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-13:04:00 to 08-17-2016-14:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.160.152	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
114.79.23.5	Indonesia	147.237.76.31	nakchal.idf.il	Black List	drop	3
123.151.149.222	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
192.243.55.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.171.2	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
222.186.39.75	China	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-17-2016-13:04:00 to 08-17-2016-14:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.139.95.146	China	147.237.77.216	dover.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	8
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
94.154.239.69	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.17	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-17-2016-13:04:00 to 08-17-2016-14:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.27.106.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.162.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
113.108.10.31	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -f -sS	1
109.66.57.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.34.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.154.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
77.138.176.196	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
191.96.249.42	147.237.77.205	Chile	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
185.118.65.230	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.103.161.153	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
132.73.196.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
113.108.10.31	147.237.77.176	China	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.132.150.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.159.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.189.2	147.237.76.31	Israel	nakchal.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	1
81.218.29.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.232.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.34.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.118.65.230	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.118.65.230	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

08-17-2016-13:04:00 to 08-17-2016-14:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.143.174.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
112.208.217.177	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.106.82.117	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.9.78	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.222.33	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
186.213.177.135	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.224.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.156.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.9.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
80.246.130.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.198.235	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.245	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
176.13.240.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
87.138.96.95	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.215.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
54.174.78.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
109.253.143.82	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.47	United States	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.144.138	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-17-2016-13:04:00 to 08-17-2016-14:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	288
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
2.55.27.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.203.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
175.44.18.175	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.44.18.175	Block	17
212.150.189.2	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	15
2.53.38.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
87.68.24.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
212.150.189.2	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.150.189.2	Block	8
84.111.104.32	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
175.44.18.175	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
212.150.255.134	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
87.69.37.33	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.253.156.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.249.49	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
131.253.25.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
37.26.146.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.150.255.134	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	3
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
209.6.26.131	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
79.179.185.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
80.246.133.144	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
66.249.64.163	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.64.163	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Method	Block	1
84.111.104.32	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
212.150.189.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1
77.138.127.16	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version sdch	Block	1
87.70.247.126	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
80.246.136.166	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.40	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/modiin/maslul.aspx	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.i	NULL Character in Method	Block	1
46.121.136.43	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
85.64.162.126	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.76.15.10	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
77.139.80.115	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Malformed URL deflate,	Block	1
87.70.247.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
84.108.24.187	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
212.143.174.37	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.121.136.43	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
5.29.165.67	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

08-17-2016-13:04:00 to 08-17-2016-14:04:00