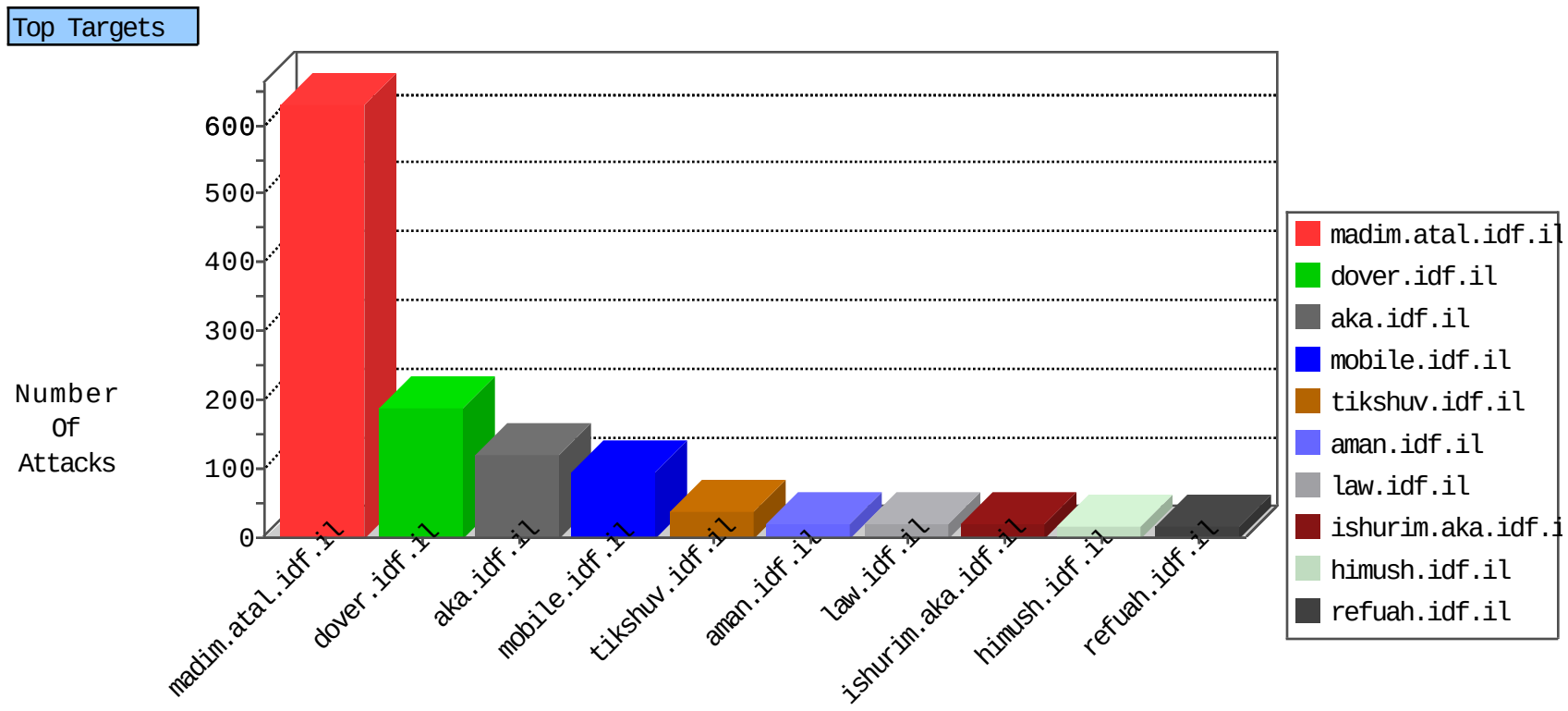
02-08-2016-07:04:07 to 02-08-2016-08:04:07

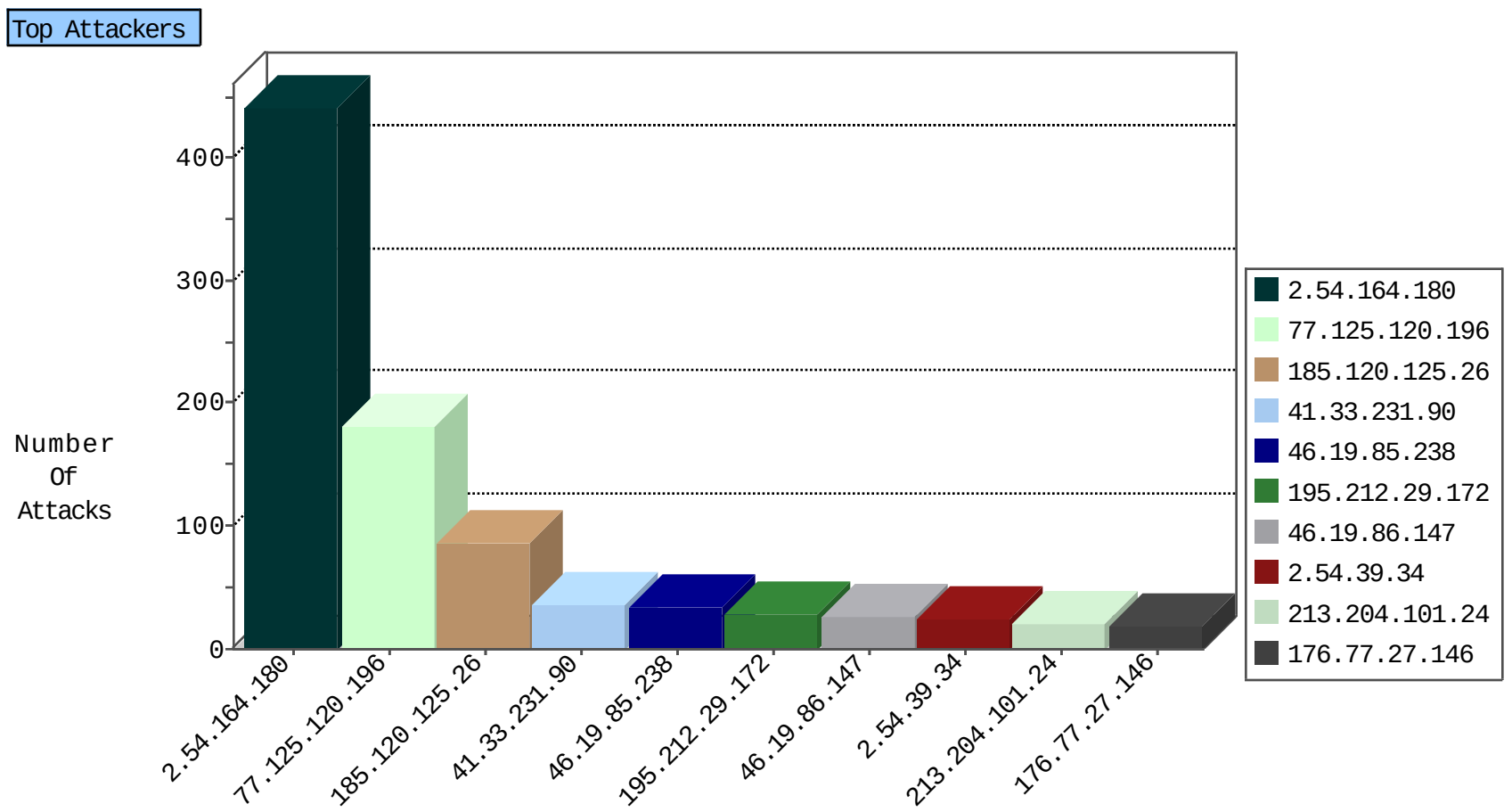
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-08-2016-07:04:07 to 02-08-2016-08:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.206.187.81	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
58.97.111.9	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
58.97.111.10	Thailand	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
107.172.23.104	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-08-2016-07:04:07 to 02-08-2016-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-08-2016-07:04:07 to 02-08-2016-08:04:07

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	3
213.204.101.24	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sS window 4096	1
78.193.2.8	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.141.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.241.253.62	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.150.44	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.172.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.170.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.224.8	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP admin.php access	1
187.246.19.99	147.237.76.38	Mexico	e.e.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-08-2016-07:04:07 to 02-08-2016-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	177
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
2.54.39.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
195.212.29.172	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	23
176.77.27.146	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	19
5.29.79.143	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.65.129.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.0	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.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
85.130.223.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.20.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.212.29.172	Europe	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.29	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
84.228.53.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.235.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.130.223.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.254.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.162.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.186.157	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.22.129.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.39.93.143	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.82.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.47.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.232.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.21.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.194.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.130.96	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.47.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.131.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.223.182.248	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.180.98.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.130.246.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-07:04:07 to 02-08-2016-08:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
77.125.120.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.164.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
77.125.120.196	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.120.196	Block	76
46.19.86.147	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	23
89.139.186.157	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	5
109.160.131.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.186.157	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
77.126.89.170	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.201.224.8	Block	2
46.19.86.147	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.147	Block	2
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
89.139.186.157	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 89.139.186.157	Block	2
46.19.86.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1158-he/dover.aspx	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
157.55.39.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.19.86.29	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
104.131.71.26	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for list.ips.gov.il/	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.78.130	Block	1
2.52.171.138	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.171.138	Block	1
216.218.206.66	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
174.67.215.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sazhar	Block	1
85.65.49.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	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
77.125.120.196	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 77.125.120.196	Block	1
188.143.232.35	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
157.55.39.48	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
46.19.85.238	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CaptchaText in mobile.idf.il/authentication/login	Block	1
193.201.224.8	Ukraine	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 193.201.224.8	Block	1

02-08-2016-07:04:07 to 02-08-2016-08:04:07