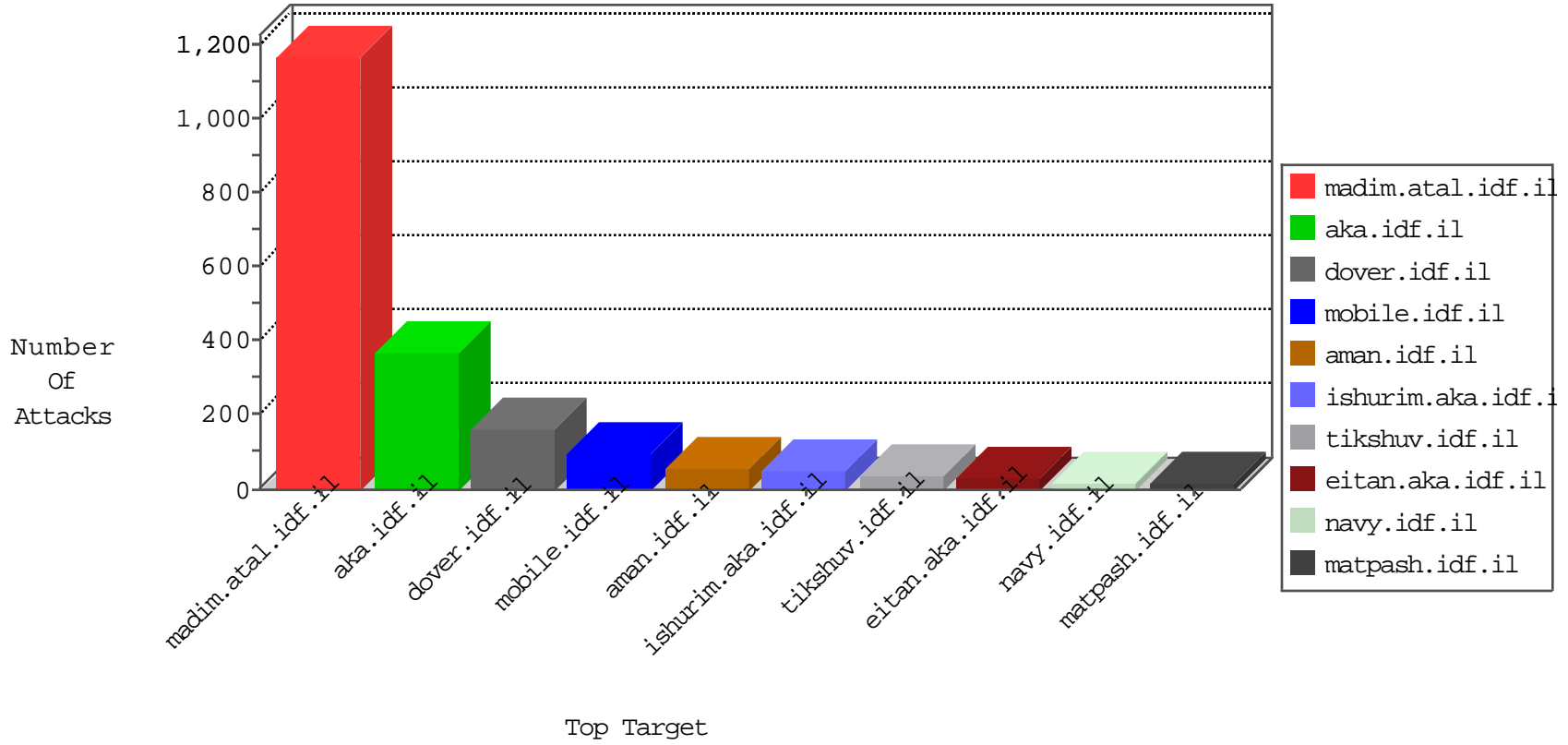


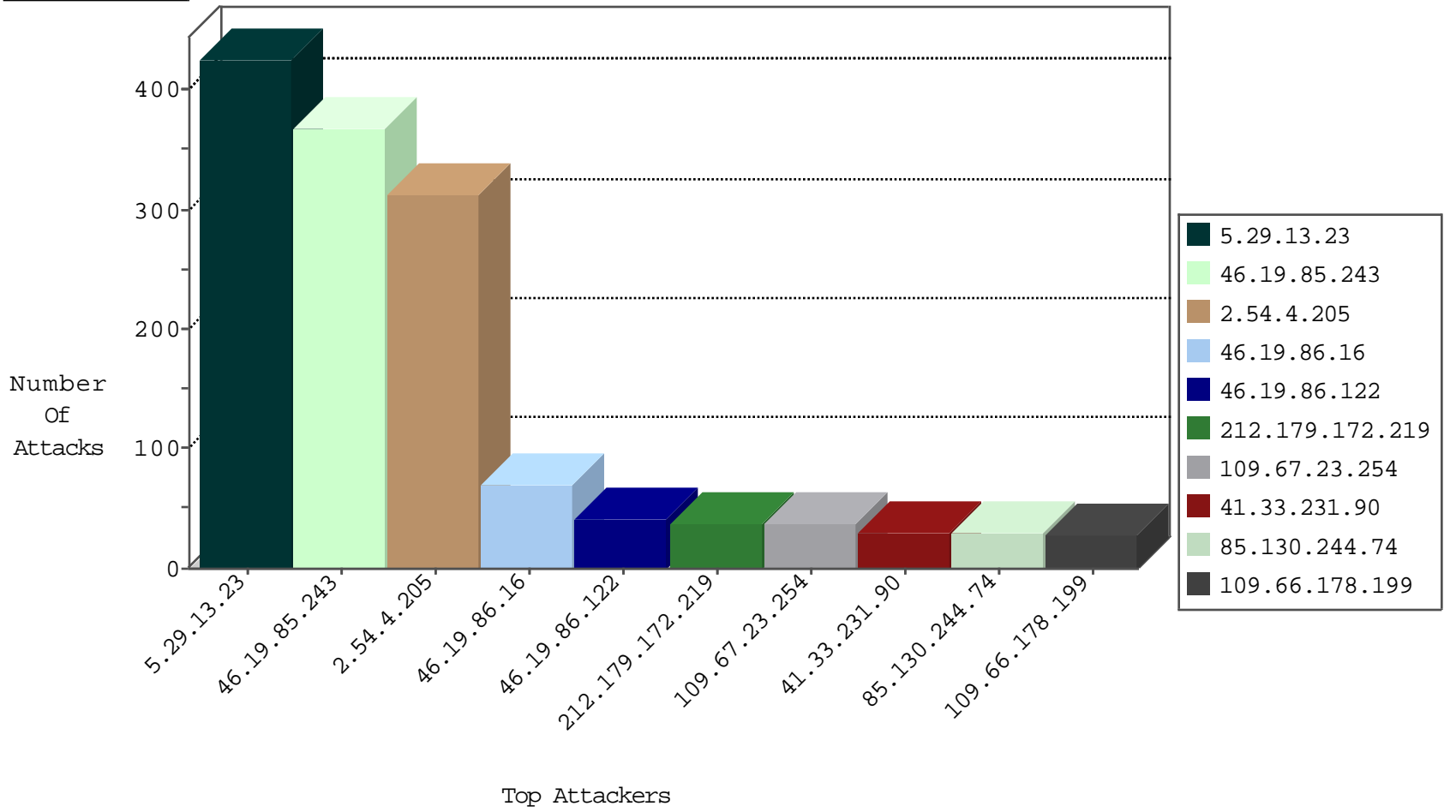
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
157.55.39.32	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
218.57.11.7	China	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
83.143.239.205	Ukraine	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.160.138	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
218.57.11.7	China	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
5.39.218.13	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.102	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
186.207.133.217	Brazil	147.237.77.176	matpash.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	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
194.63.140.74	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	2
163.47.140.140	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.72.166	Turkey	aka.idf.il	ET SCAN NMAP -sS window 4096	1
194.63.140.74	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
84.228.132.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.63.140.74	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
194.63.140.74	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.141.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.63.140.74	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
190.178.164.108	147.237.8.46	Argentina	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.63.140.74	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential SSH Scan	1
163.47.140.140	147.237.76.200	India	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
163.47.140.140	147.237.76.31	India	nakchal.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.177	Russian Federation	noore.idf.il	ET SCAN Potential SSH Scan	1
163.47.140.140	147.237.0.19	India	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
93.173.231.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
194.63.140.74	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.246.130.36	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
194.63.140.74	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
31.211.102.129	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 4096	1
194.63.140.74	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
188.126.77.138	147.237.76.199	Sweden	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
163.47.140.140	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
212.179.172.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
85.130.244.74	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.67.23.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.66.178.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.86.16	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.209.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.206	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.227.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.60.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.254.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.22.135.195	Israel	147.237.72.166	aka.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
109.253.223.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.10.189	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.58.113	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.19.116.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
77.126.18.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.71.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
188.120.154.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.117.156.169	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.41.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.242.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.205.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.130.205.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
74.111.238.237	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.115.248.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.76.98.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.1.108	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.186.86	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.9.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.32.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.16	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
178.154.189.21	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.124.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.165.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.11.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-15-2016-21:04:09 to 02-15-2016-22:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.108.194.197	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
188.120.148.71	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.13.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	197
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
2.54.4.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	150
2.54.4.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	131
5.29.13.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
5.29.13.23	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 5.29.13.23	Block	49
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
5.29.13.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	38
2.54.4.205	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.4.205	Block	25
89.138.169.63	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
109.67.112.79	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	18
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	17
84.108.47.67	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.108.47.67	Block	7
109.67.23.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
2.54.4.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	6
46.117.243.181	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.117.243.181	Block	6
131.253.25.251	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
84.108.47.67	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
188.120.154.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.88.67.174	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
79.176.128.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.213.182.43	Russian Federation	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 95.213.182.43	Block	3
80.178.157.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.168.240.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.111.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.228.154.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.116.29.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
84.94.179.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
2.54.4.205	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
95.213.182.43	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
84.228.199.27	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.199.27	Block	1
165.139.227.1	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
89.139.165.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cpMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyius/atuda/asmachta.aspx	None	1
46.116.63.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/controls/atuda/Å	Block	1
46.19.85.220	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
157.55.39.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
54.147.176.220	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
46.31.103.30	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.228.199.27	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.199.27	Block	1
5.29.70.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
165.139.227.1	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.160.177.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.69.32.225	Italy	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1500-en	Block	1