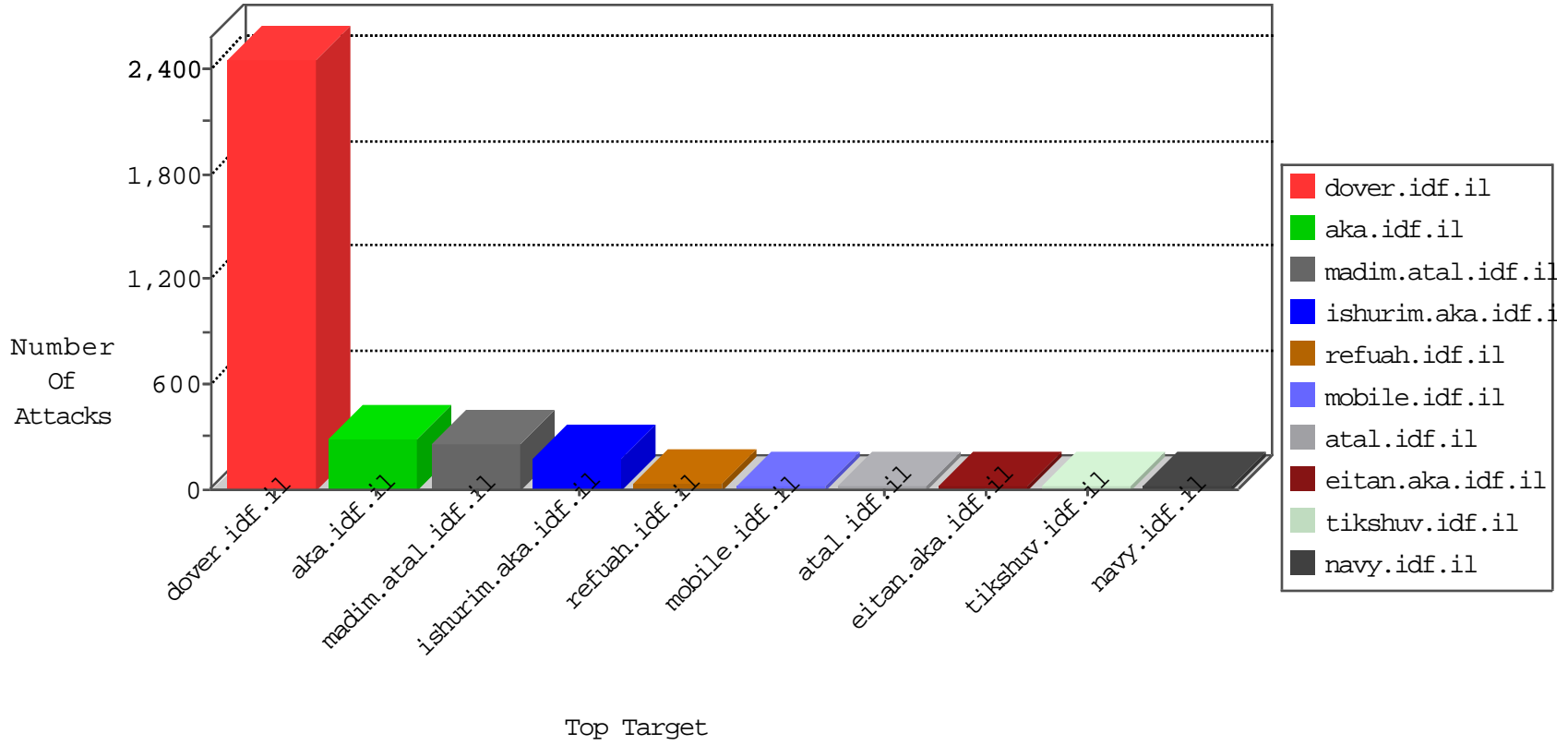


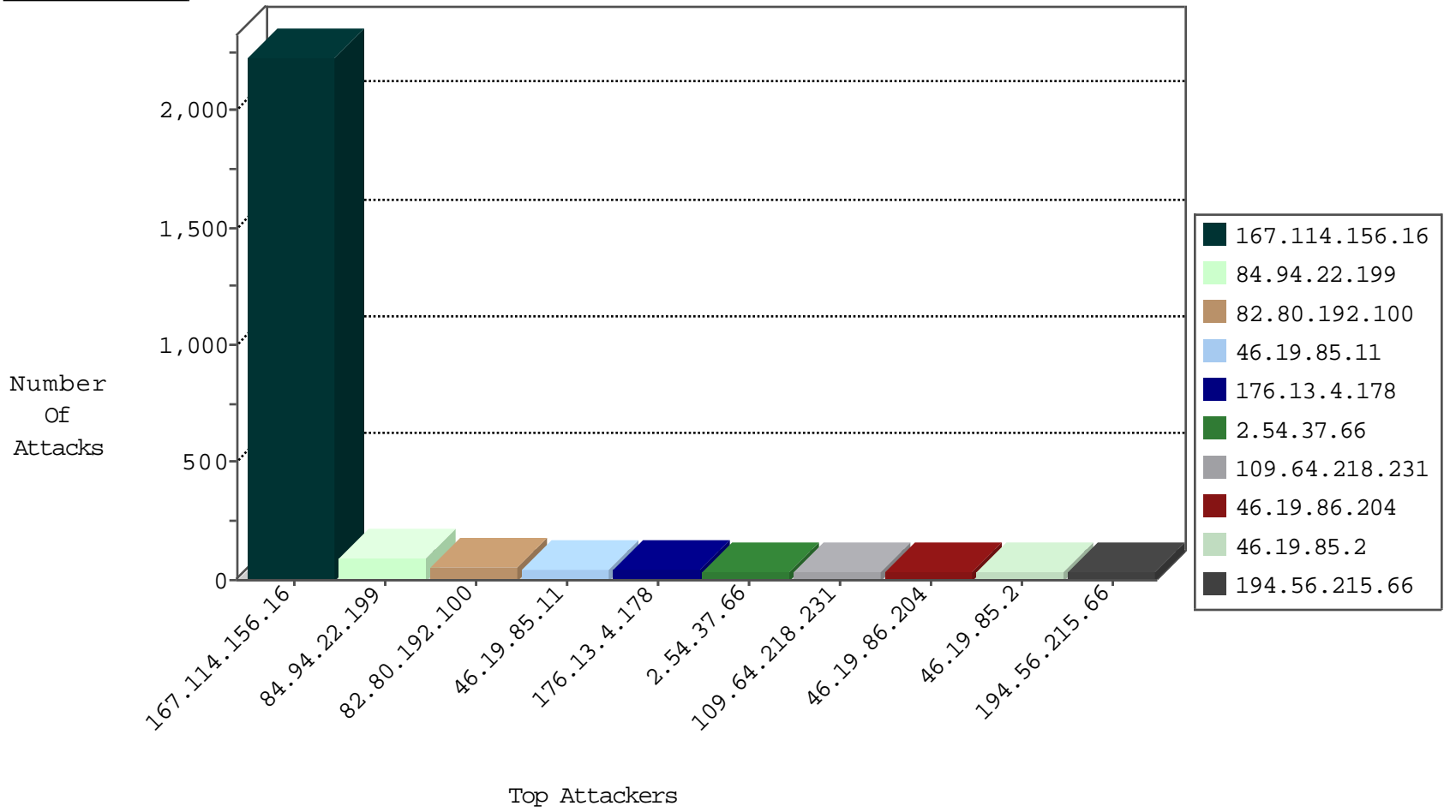
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3142
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
58.221.42.91	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
204.42.253.130	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
203.198.119.98	Hong Kong	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
82.80.177.111	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: 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	2
46.19.86.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.13.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
182.75.6.126	147.237.77.61	India	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.11.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.150.174.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
109.226.28.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.77.176	Brazil	matpash.idf.il	ET SCAN Potential SSH Scan	1
85.250.65.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.181.27.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
182.75.6.126	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.8.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.53.12	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
187.84.162.97	147.237.77.178	Brazil	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
95.35.16.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
84.228.42.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.84.162.97	147.237.76.86	Brazil	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
46.19.86.204	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
194.56.215.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
213.57.137.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
109.64.218.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
109.160.131.170	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
85.64.150.30	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.75.201	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
65.55.218.58	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.64.218.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.64.218.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
84.110.210.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
194.56.215.66	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.255	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
217.132.1.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.200.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.183.224.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.146.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.118.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.18.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.190	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.175	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.10.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.255	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.10.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.130	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
122.3.142.91	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.175	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.150.30	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
188.120.148.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.135.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.66	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.131.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.138.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.128.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.200.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.22.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 82.80.192.100	Block	56
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
176.13.4.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
2.54.37.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
84.94.22.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.94.22.199	Block	25
2.52.8.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.52.8.154	Block	15
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.136.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
199.203.179.99	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
84.95.84.211	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
107.167.99.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	4
212.199.224.24	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	4
80.246.139.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.169	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
52.33.66.29	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.33.66.29	Block	2
176.13.11.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
23.228.68.62	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.158.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.194.245.152	Ireland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
176.13.10.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.146.104.247	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
50.31.26.42	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
150.70.173.54	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
2.54.51.72	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.193.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
62.219.228.13	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.22.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.186.25	Israel	147.237.0.19	madim.atal.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.186.25	Block	1
84.111.48.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.137.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.255	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
141.212.122.80	United States	147.237.76.39	mobile.meitav.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
2.52.190.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.80.192.100	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many 404: Response Code per Session	Block	1
212.199.224.24	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/1535.png	Block	1
46.19.86.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$questionUpdate0 in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
109.160.160.181	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
79.177.137.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
197.32.242.234	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
54.194.245.152	Ireland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
37.142.68.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
103.14.202.124	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
50.87.119.203	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
150.70.173.59	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
2.54.128.223	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1