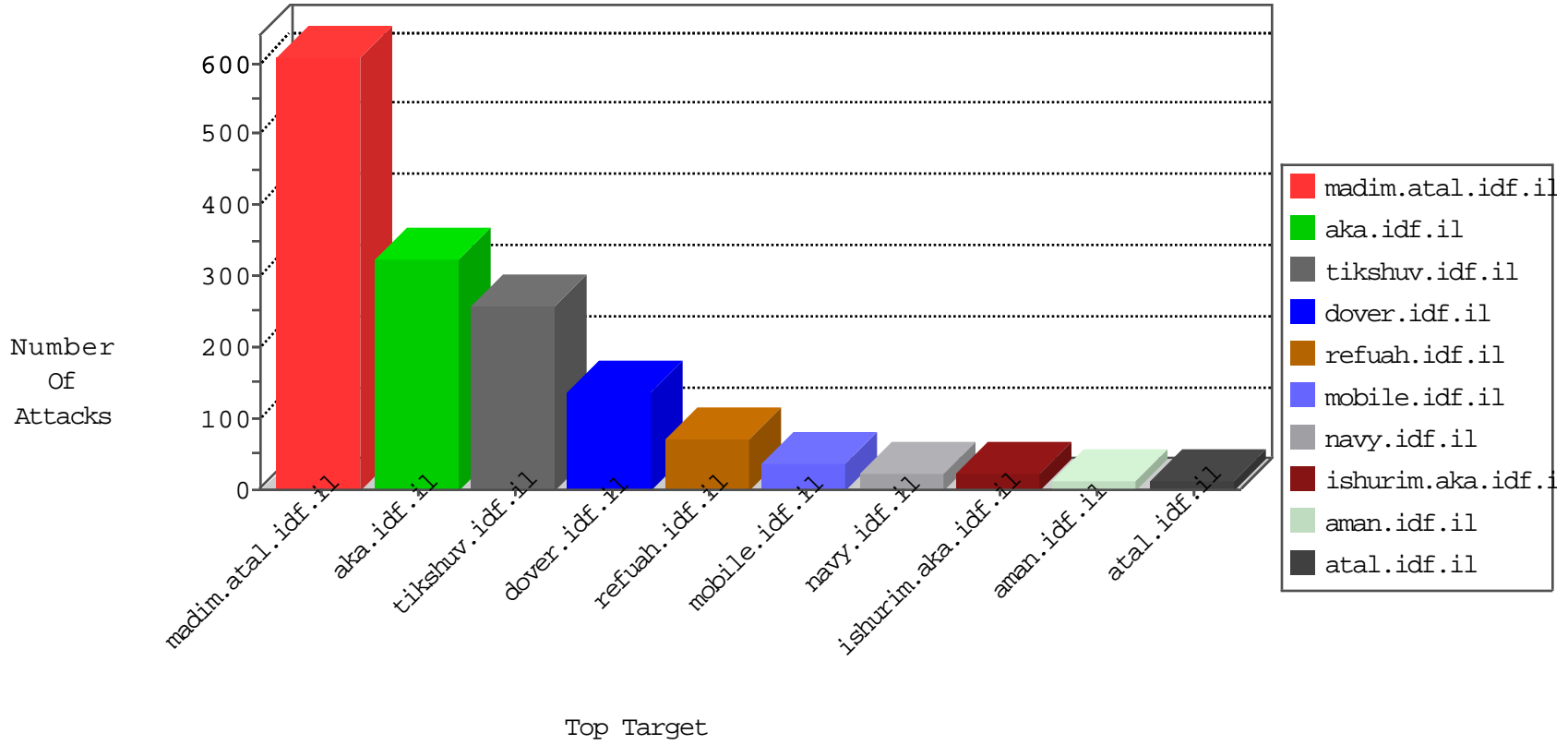


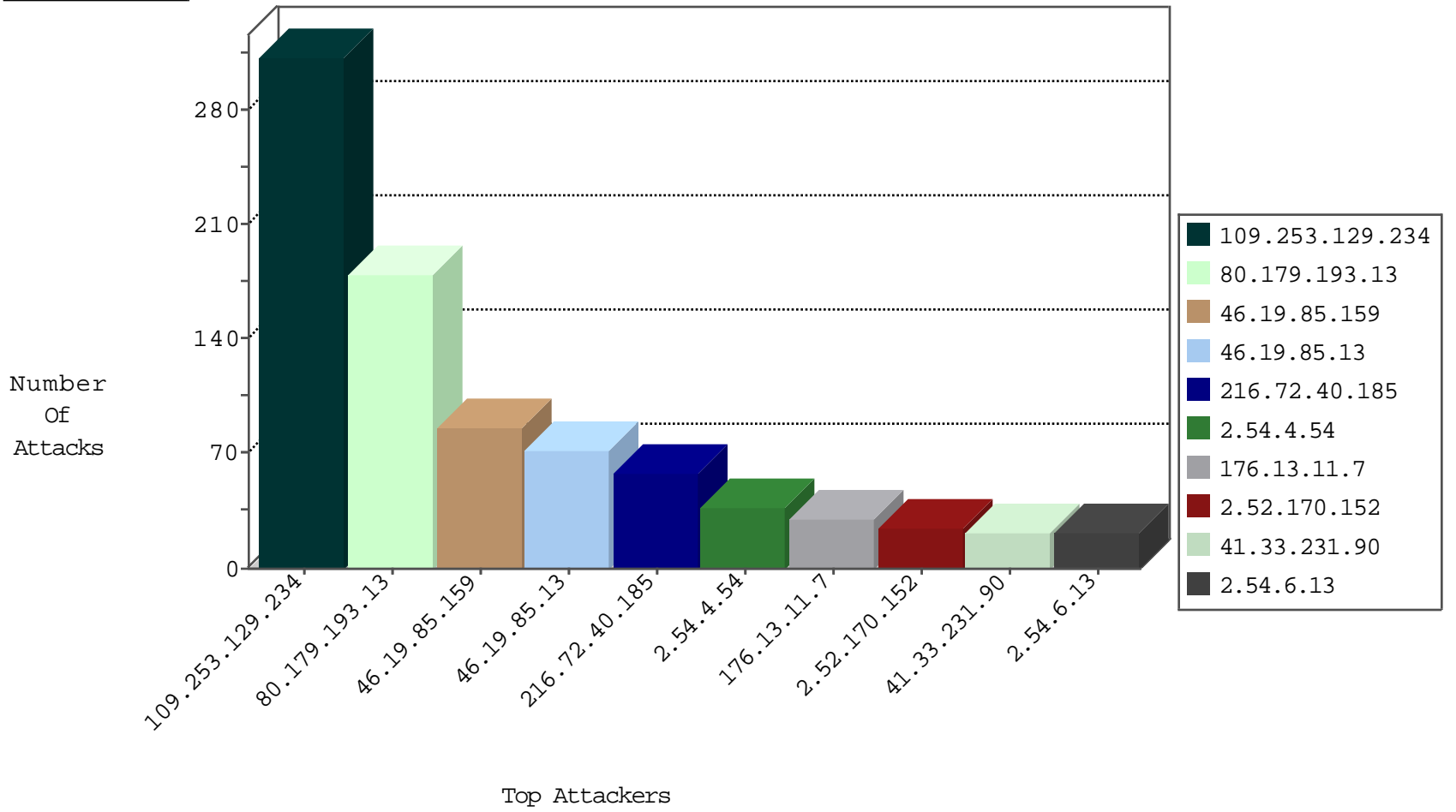
# IDF Under Attack Daily Report



### Top Targets



### Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.247	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	16
104.131.226.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
88.249.87.51	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
23.228.101.234	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
51.36.14.46	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
88.249.87.51	Turkey	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
23.228.101.234	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
88.249.87.51	Turkey	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
80.70.128.129	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
37.26.148.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

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
31.168.172.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
94.102.51.30	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
79.181.147.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.112.81.67	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
12.14.13.130	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.112.81.67	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.8.14	Switzerland	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.98.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.148.120	147.237.72.166	Israel	aka.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
37.26.149.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.161.185.85	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.80.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.112.81.67	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
2.54.178.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.65.31.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
46.19.85.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.4.90	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.6.13	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.180.151.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
188.161.185.85	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.116.218.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.36	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.169.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.115.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.235.103.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
192.114.1.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.183.190.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.64.171.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.218.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.11.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.38.205	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.170.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.170.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
62.90.152.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.52.170.152	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.170.152	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.170.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.48.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.78.218	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.166.29	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.6.13	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.114.1.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.6.13	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.253.128.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.147.176.220	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.173.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.114.1.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.172.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.195.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.28.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.176.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.57.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.35.76.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.16.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.173.195	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	3
31.168.240.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.200.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-12:04:10 to 02-08-2016-13:04:10

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.18.87	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
80.179.193.13	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
109.253.129.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	171
109.253.129.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
46.19.85.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
2.54.4.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.11.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
176.13.10.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.26.147.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.117.23.174	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
37.26.149.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.143.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.148.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.148.123	Block	3
176.13.9.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.53.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.55.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.157.226	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.187.168.249	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
176.13.0.135	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
2.54.55.121	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.228.141.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
128.232.110.28	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.26.149.193	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captcha Text in aka.idf.il/main/gyus/default.aspx	None	1
95.86.98.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
80.246.133.68	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
176.13.4.90	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.67.148.123	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/	Block	1
37.26.146.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
82.166.146.81	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1
179.179.60.118	Brazil	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20027-he/dover.aspx	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
2.54.25.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.98.94	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsuneymofet.aspx	None	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 81.218.53.114	Block	1
217.194.207.24	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 217.194.207.24 (Open Mode)	None	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
82.166.193.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
66.249.66.87	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/894-he	Block	1
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
95.86.116.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple _vti_ from 81.218.53.114	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method L,he;q=0.8,en-US;q=0.6,en;q=0.4 in URL	Block	1