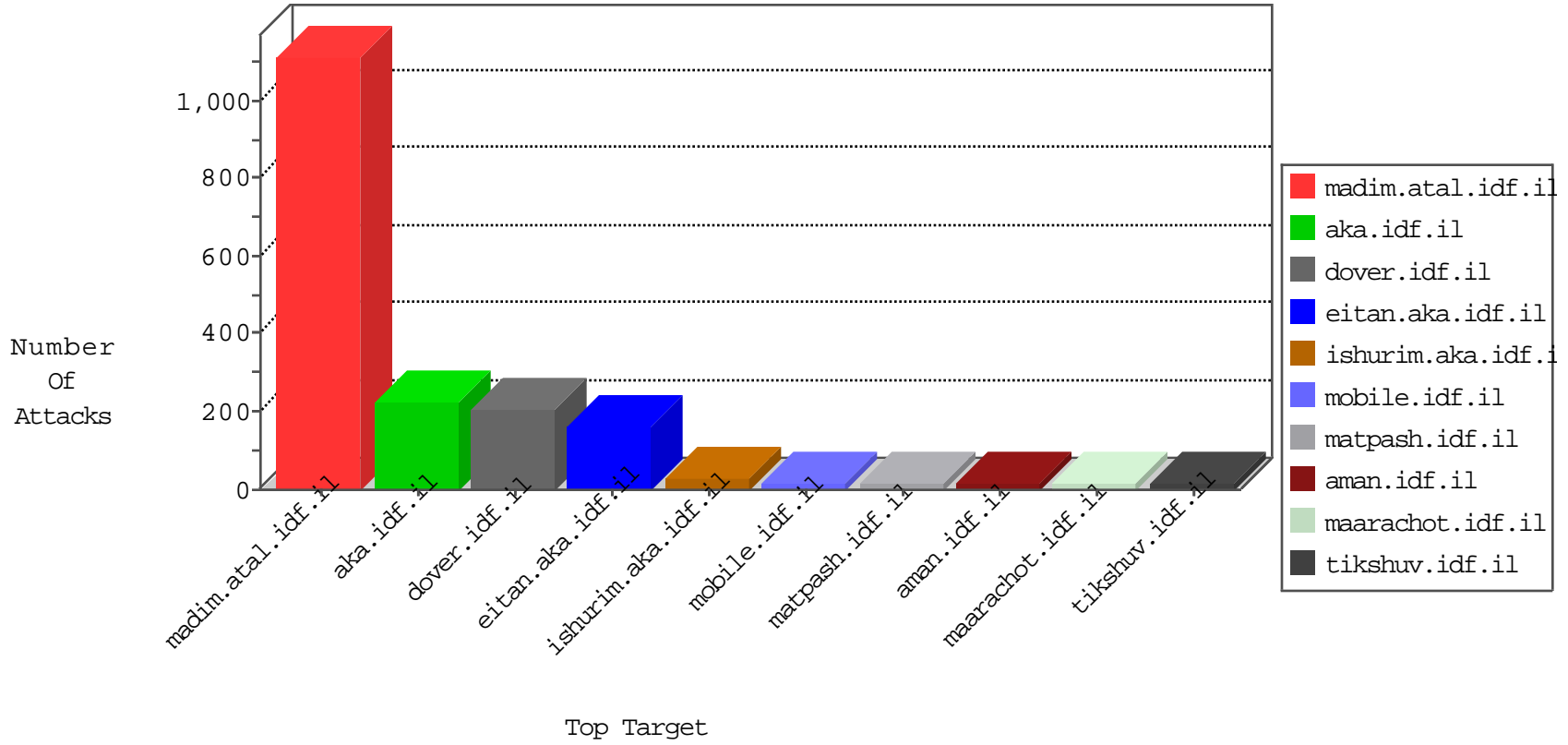


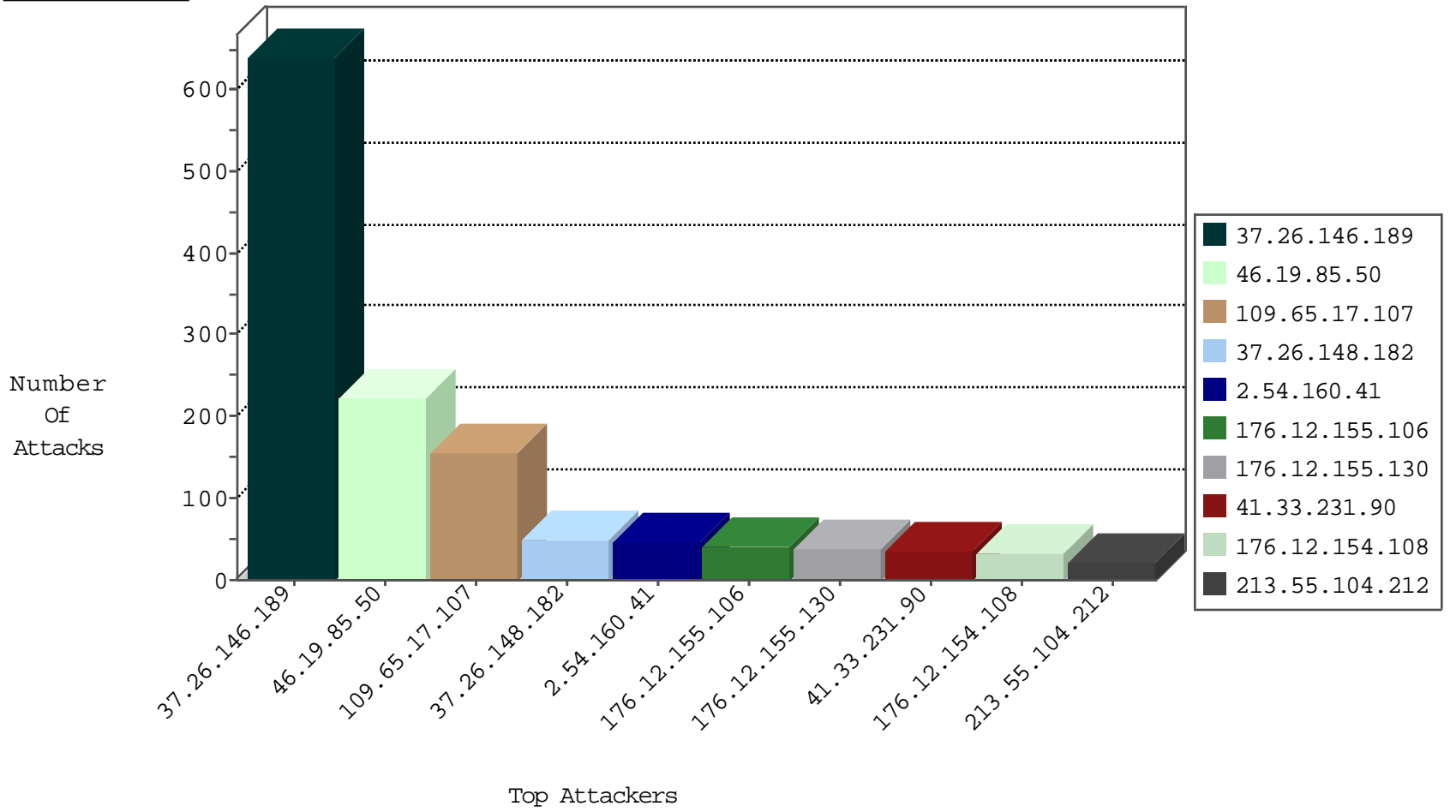
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
116.126.120.206	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
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

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.86.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.72.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
17.78.98.80	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.37.128.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.106.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.234.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.149.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.118.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.62.52.41	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.63	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.123	147.237.76.177	Moldova, Republic of	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.154.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.129.113	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
109.65.17.107	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.55.104.212	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.54.160.41	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	16
85.64.129.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
52.5.69.31	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.10.177	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.160.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.160.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.160.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.52.145.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.116	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.29.214.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.173.9.10	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.178.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.116	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.69.88	United States	147.237.0.19	madim.atal.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	5
2.54.160.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
46.19.85.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
65.55.210.88	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.132.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
52.0.86.232	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
81.218.70.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.246.136.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.132.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.32.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.154.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.141.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.229.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.76.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.186	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
54.85.198.156	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.3.146.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.155.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.188.90	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
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	356
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.146.189	Block	181
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.50	Block	111
37.26.146.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.12.155.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.12.155.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
176.12.154.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.139.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
185.32.179.147	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.46.38.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.74.105.107	Block	12
176.12.155.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
80.246.139.146	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
46.19.85.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.140.31	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
219.94.192.47	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.192.47	Block	4
193.37.128.3	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 193.37.128.3	Block	3
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.144.70.32	Germany	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
2.52.50.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.44.204	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
2.54.183.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.139.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/modiin/default.aspx	Block	3
80.246.139.86	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
2.52.20.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
52.0.86.232	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/news	Block	2
176.12.154.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.240.21	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
84.109.176.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.178.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.52.178.107	Block	2
62.219.44.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
157.55.39.210	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	1
205.177.226.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21950-he/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
2.52.178.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guis	Block	1
46.19.86.201	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
41.237.123.131	Egypt	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
109.64.195.17	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
219.94.192.47	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/106052.pdf	Block	1
193.37.128.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
176.12.154.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.144.70.32	Germany	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	1
40.77.167.33	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/results.asp	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-he/cogat.aspx	Block	1