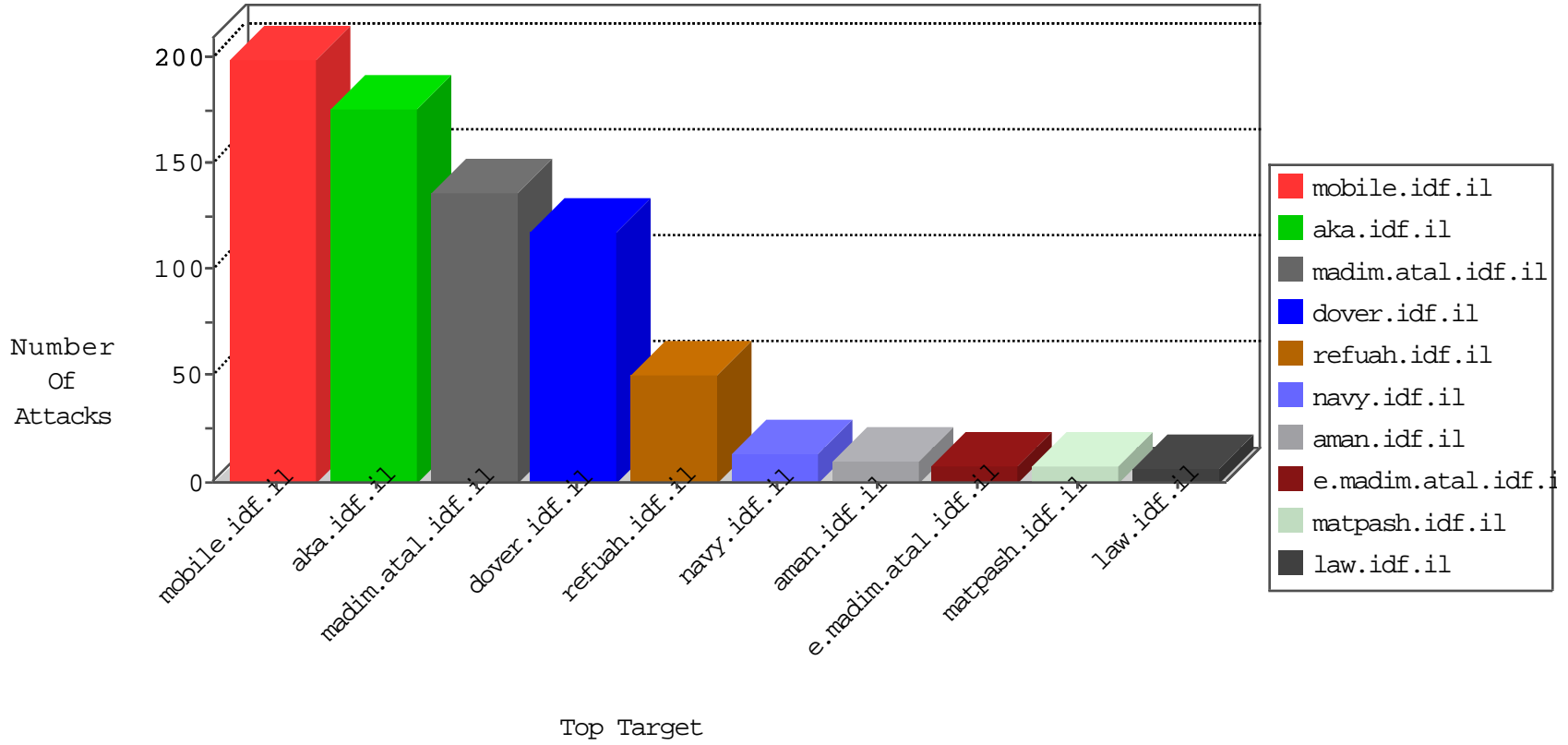


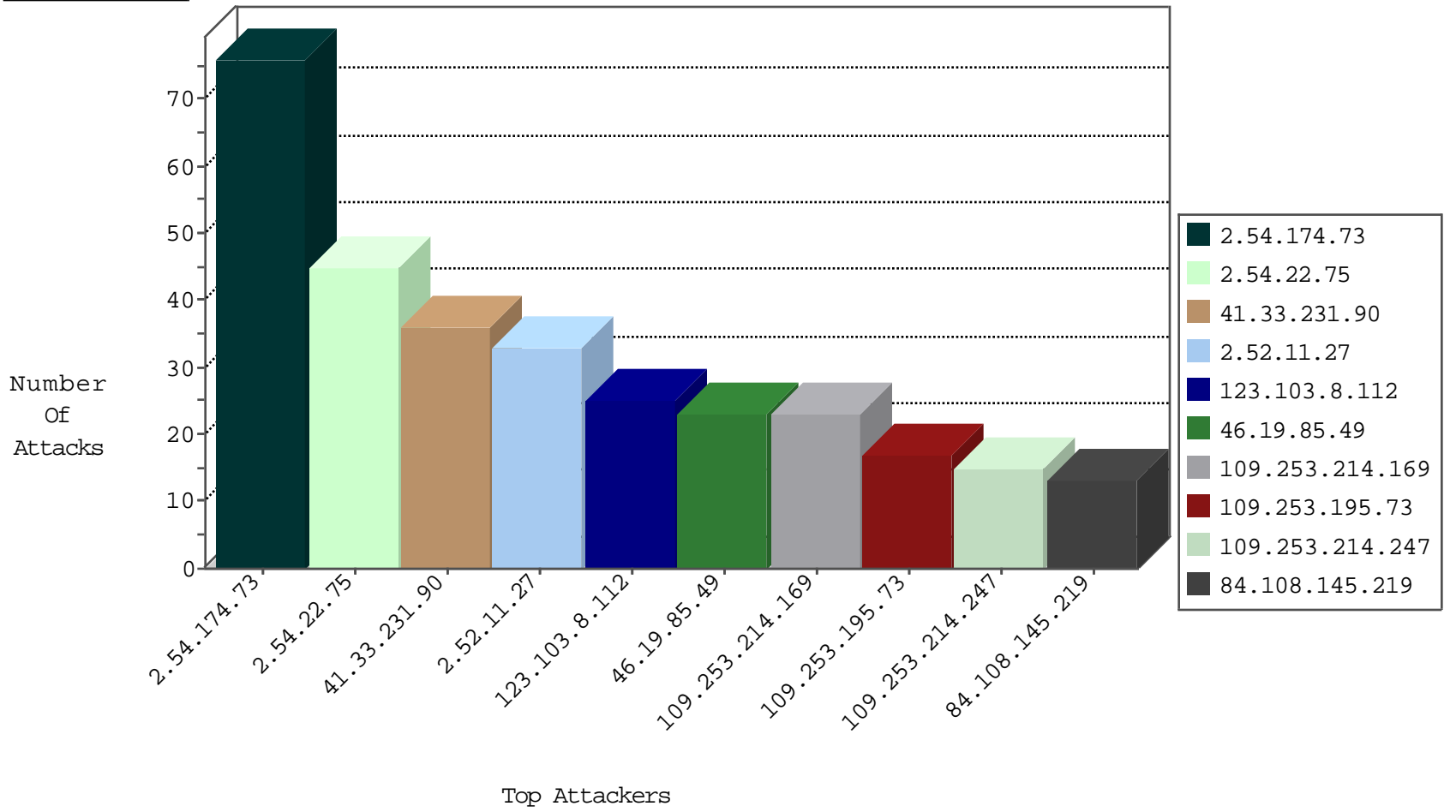
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.116	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.83	United States	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.112	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
198.167.129.9	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.18	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.48	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.51	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.85	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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
79.180.210.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
109.64.95.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.187.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.158.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.151.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.14.157.131	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
79.180.183.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.160.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.35.161.193	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.253.96.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.201.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20	147.237.76.176	United States	test.noore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.22.135.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.19	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.54.128.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.6.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.133.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.76.31	India	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
79.177.136.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.209.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.115.159	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	36
46.19.85.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
123.103.8.112	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.253.195.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
109.253.214.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.138.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.145.219	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.253.214.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
123.103.8.112	China	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
82.81.17.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.16.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.133.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.37.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.136.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.159.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.32.179.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
79.179.54.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.193.169	Israel	147.237.77.243	mobile.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
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
5.22.135.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.9.184	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.242.114	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.24.104	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.168.115.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.203.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.138.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.161.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.15.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.183.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.128.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.18.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.183.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.146.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.8.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.221.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.128.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.47.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.99.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.174.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
2.54.22.75	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	45
2.52.11.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
109.253.214.169	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	12
109.253.159.133	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	11
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.202.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	5
46.19.85.49	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
178.137.81.41	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
149.78.40.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.214.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.146.93	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
5.29.160.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.214.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.102	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
109.226.49.85	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	2
176.13.16.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.109.240.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.69.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/109714.pdf	Block	1
131.253.25.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.52.159.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
74.82.47.4	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
54.147.176.220	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
109.66.133.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.60.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
31.168.70.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
109.67.232.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.79.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
149.78.40.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.54.98.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.193.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.33	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/111075.pdf	Block	1
37.26.148.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
157.55.39.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
109.253.195.73	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.94.199.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
66.249.69.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
131.253.25.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.3	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.146.93	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.253.146.93	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
46.121.154.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __ in www.aka.idf.il/main/sachar/default.aspx	None	1
5.29.122.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1