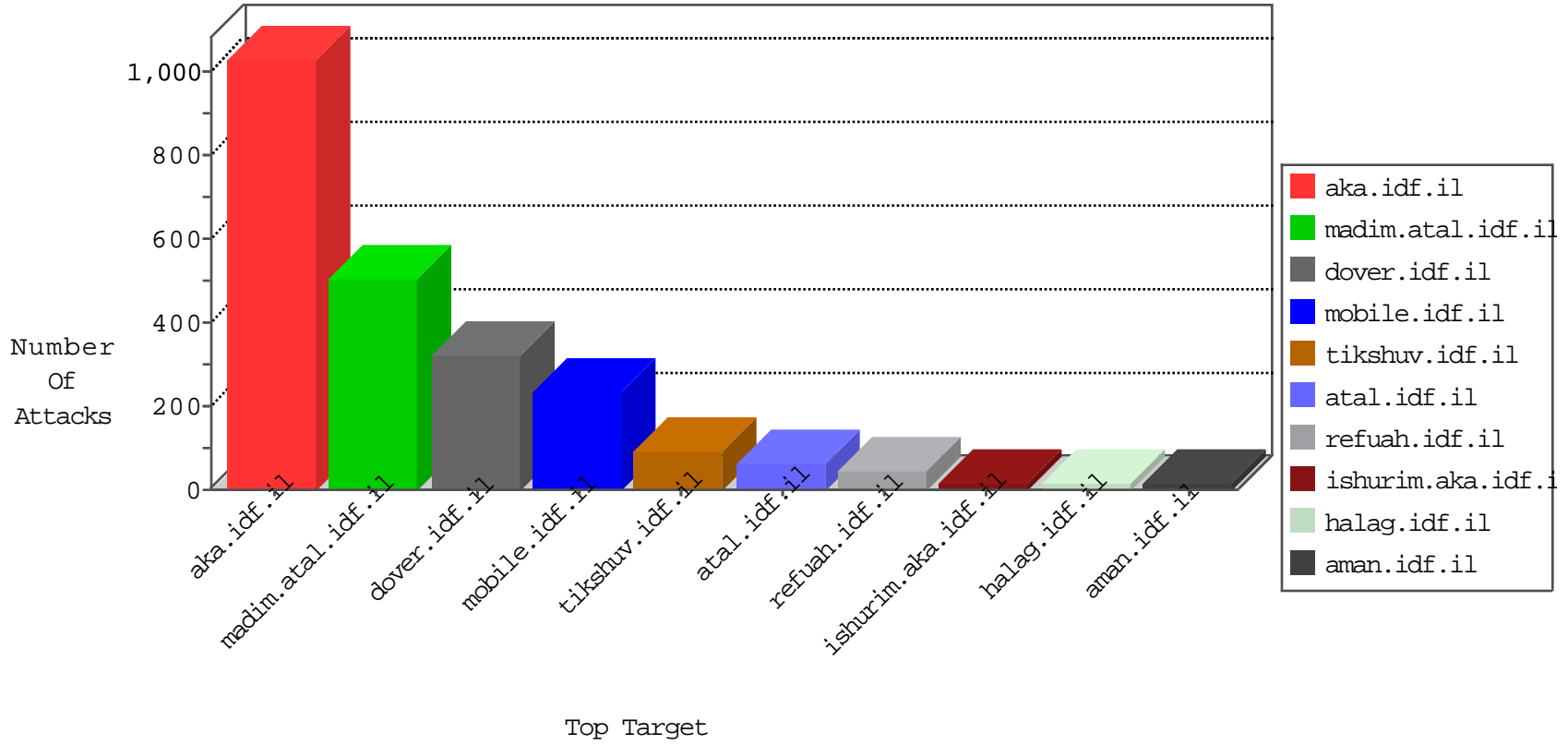


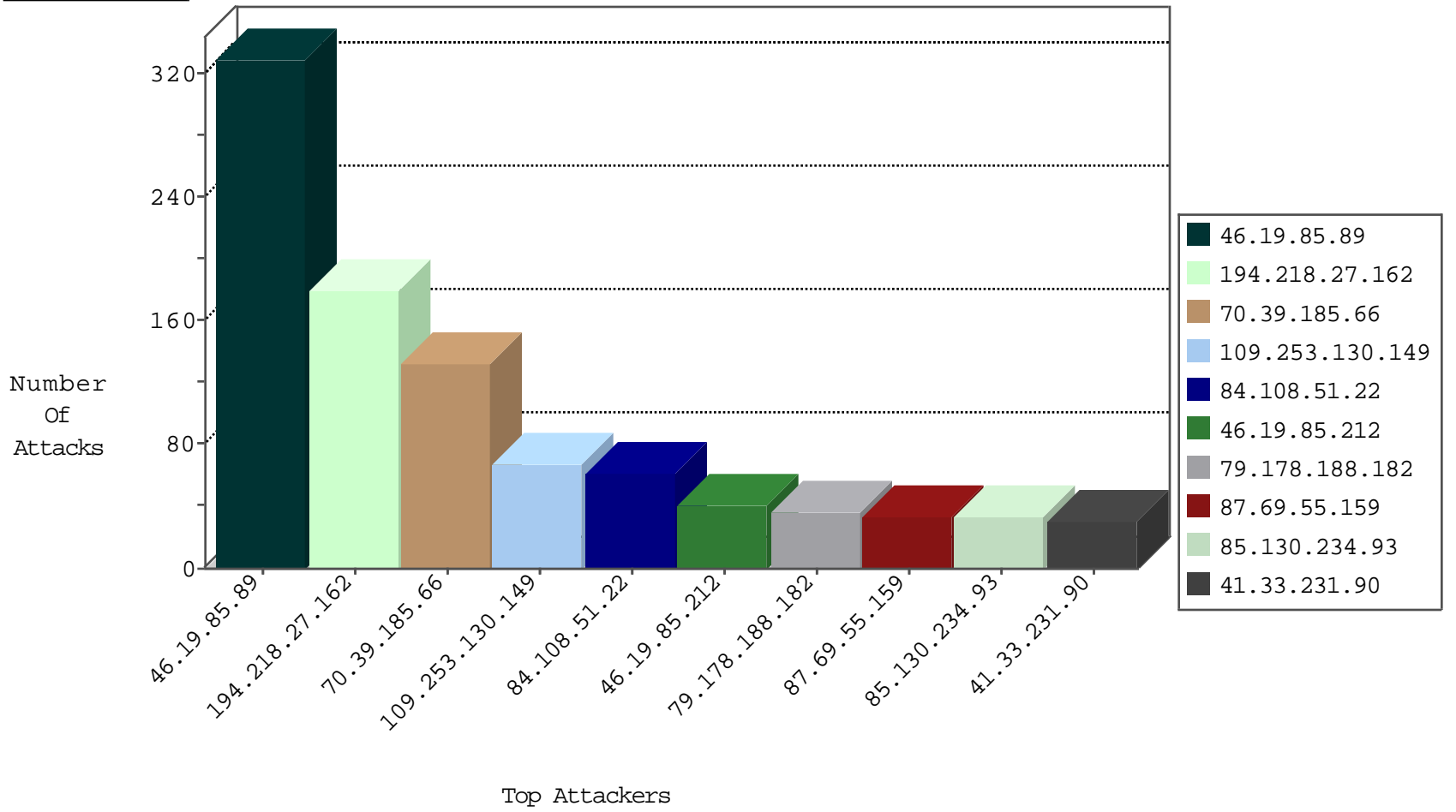
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.5.106	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.217.44	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	4
81.218.165.186	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP_Page_Flood_Attack	drop	2
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
23.239.64.15	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
79.183.135.7	Israel	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
61.93.214.238	Hong Kong	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
46.116.28.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
95.86.124.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
185.120.126.121		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.253.139.85	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.0.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.8.204.53	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.146.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.135.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
85.130.236.191	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.4	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	3
82.221.48.130	147.237.76.42	Iceland	refuah.idf.il	Tehila - Perl LWP with fake user agent	2
85.64.71.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.238.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
204.108.105.13	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.13.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.170.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
87.101.205.108	147.237.0.33	Saudi Arabia	idf.il	ET SCAN Potential SSH Scan	1
85.65.5.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.208.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.65.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.151.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.60.232.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.56.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.242.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.197.40.56	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
93.173.179.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.101.205.108	147.237.0.17	Saudi Arabia	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
79.178.188.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
70.39.185.66	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
46.19.85.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
87.69.55.159	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.16.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.212.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
94.159.167.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.228.176.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.54.4.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
194.90.222.225	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.201.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.16.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.234.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.234.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
99.225.142.37	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.234.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
93.173.90.84	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.228.133.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.6.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.195.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.129.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.61.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.137.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.119.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.59.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.83.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.38.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.127.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.5.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.83.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.37.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.158.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.114.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.55.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.146.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.136.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
85.130.234.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	330
109.253.130.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
84.108.51.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.19.86.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	8
46.19.85.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
89.138.68.53	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
176.13.2.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.66.200.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.182	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
109.253.205.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.212.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.178.102.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.16.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.129.34	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	4
109.253.156.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.201.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
85.65.151.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.133.110.35	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/rabanut/	Block	2
66.249.66.75	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	2
82.221.48.130	Iceland	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
62.128.48.50	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
149.78.7.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.221.48.130	Iceland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/index.php	Block	2
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.45.133	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.3.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
182.118.54.17	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.56.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
149.78.84.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
84.109.235.26	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
41.248.126.186	Morocco	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.142.176	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.125.76.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
185.3.144.80	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
5.29.71.130	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
95.153.129.178	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
85.130.207.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
82.81.240.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
149.50.104.19	United States	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 149.50.104.19 (Open Mode)	None	1
37.26.149.141	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
109.186.49.80	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.74.90	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1