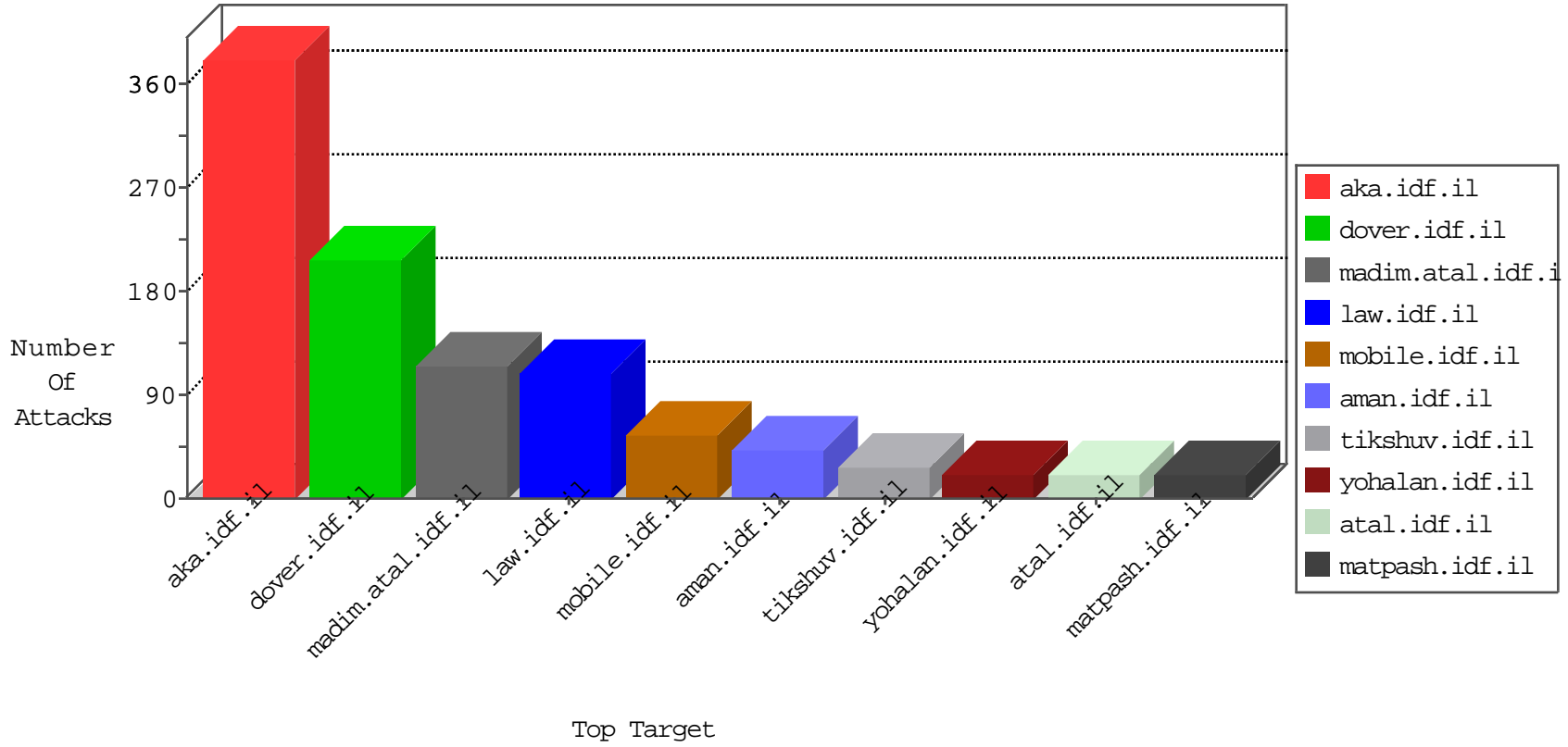


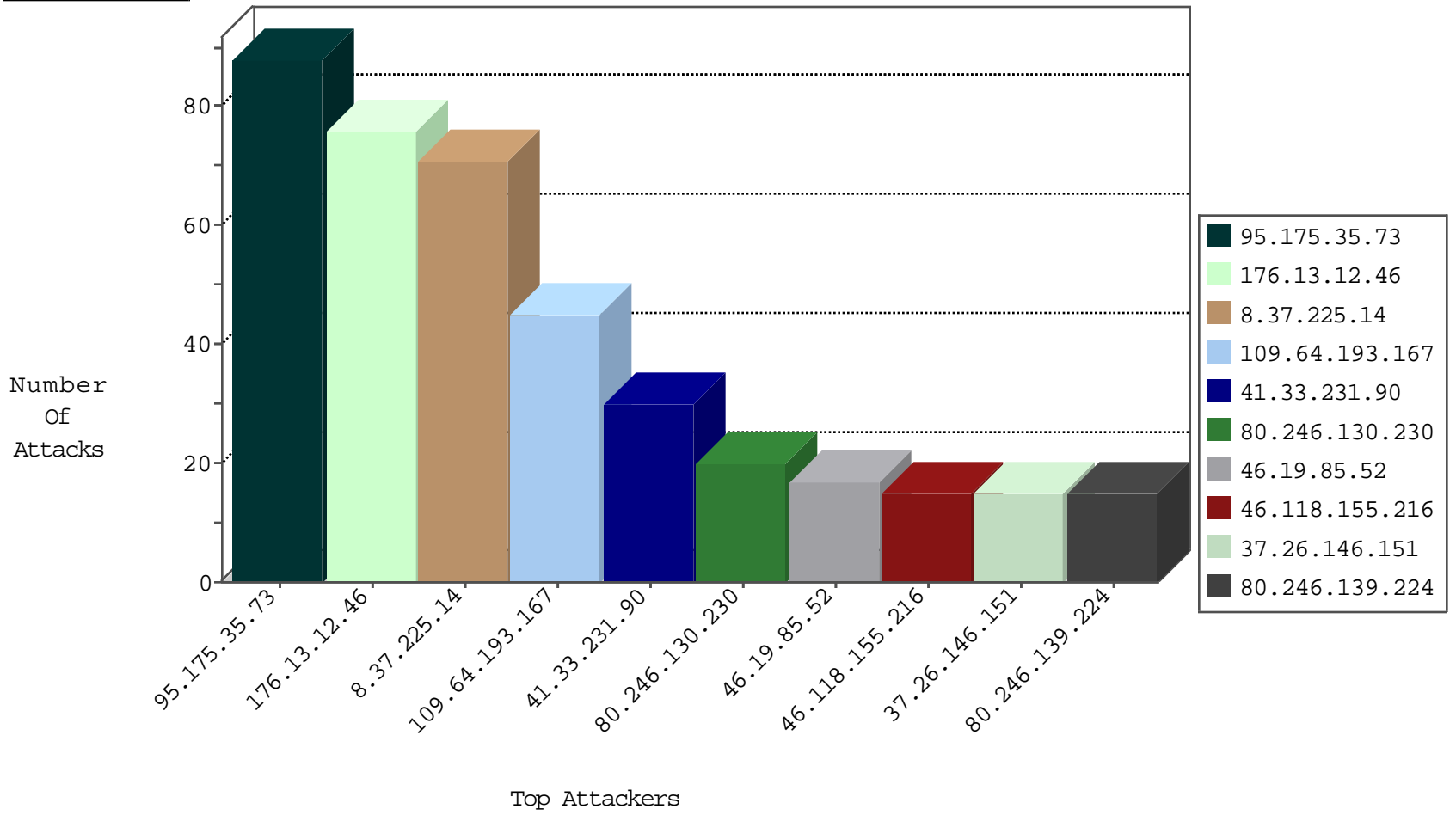
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
78.193.2.8	147.237.0.35	France	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.7.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.86.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.34	United States	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.145.0.51	147.237.77.121	China	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.90.26.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.186.147.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.183.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.6.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.1.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.154.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.193.2.8	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.45.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.190.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.233.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.130.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.139.186.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.101.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.154.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.14	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
109.64.193.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
80.246.130.230	Israel	147.237.76.34	yohalan.idf.il	drop		drop	20
37.26.146.151	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
37.26.148.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.66.6.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
217.194.202.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.102	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.24.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.167.109	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.139.224	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
188.140.171.178	Oman	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.98.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.10	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.224	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
199.203.196.237	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.146.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.200.12.136	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
82.102.170.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.129.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
94.230.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.52.149.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.168.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.21.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.76.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.65.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.139.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
92.61.233.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.10.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.216.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.143.201	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
95.175.35.73	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 95.175.35.73	Block	86
176.13.12.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
2.54.167.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.167.50	Block	9
176.13.14.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.54.18.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	4
108.61.128.54	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
2.54.29.169	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	4
176.13.21.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.198.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.1.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
2.52.148.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.1.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.40.15	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
2.54.57.196	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.212.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.197.252	Israel	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in URL from 85.250.197.252	Block	2
27.159.208.122	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
95.86.115.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
176.13.17.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
85.65.177.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.245	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/x"x?x*x"	Block	1
2.54.167.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m	Block	1
141.212.122.177	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
95.175.35.73	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
85.65.177.246	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 85.65.177.246	Block	1
46.19.86.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
27.159.208.122	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
79.177.61.49	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
85.250.197.252	Israel	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /602-2265-he/patzar.aspx	Block	1
84.109.196.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct102\$ct103\$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	1
68.180.230.57	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
5.39.222.159	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/rom-0	Block	1
165.91.49.198	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
85.65.177.246	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.86.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$LoginControl\$captcha\$captchaText in aka.idf.il/main/giyus/default.aspx	None	1
37.26.147.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ge...04	Block	1