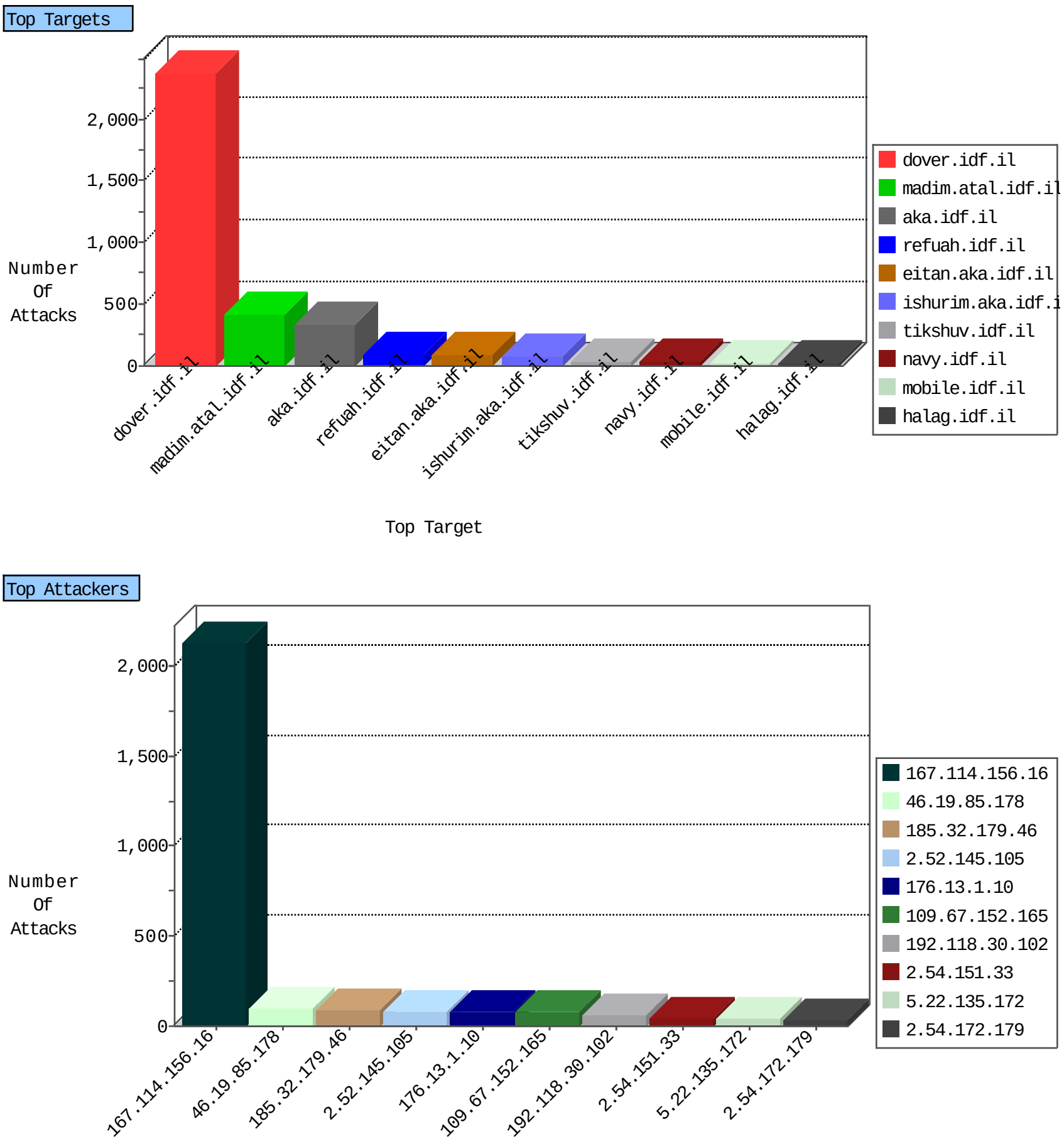
03-13-2016-10:04:06 to 03-13-2016-11:04:06

IDF Under Attack
Daily Report



03-13-2016-10:04:06 to 03-13-2016-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3780
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	508
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.145.222.170	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3

03-13-2016-10:04:06 to 03-13-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.66	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
136.243.5.87	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	5
136.243.5.87	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
89.203.221.120	Czech Republic	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	4
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
136.243.5.87	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	3
136.243.5.87	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
2.54.190.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.177.243.217	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
85.14.245.175	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
85.14.244.114	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	1

03-13-2016-10:04:06 to 03-13-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
40.74.124.12	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
2.52.145.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
94.230.93.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.76.202	Ukraine	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.69.34	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.169.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.226.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.121.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.56.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-13-2016-10:04:06 to 03-13-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	90
109.67.152.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	51
109.253.157.221	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.22.135.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
82.166.93.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
79.182.121.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.176.149.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
5.102.254.144	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
109.253.193.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
107.170.58.12	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.19.85.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.145.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.145.105	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
2.52.145.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.52.145.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.145.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.52.145.105	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.172.179	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.162.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.145.105	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.127.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.229	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.145.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.28.50.127	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.145.105	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
213.8.94.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.229	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
149.78.59.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.167.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.90.193.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
149.78.182.189	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.168.134	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.178.53.148	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
46.19.85.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	101
185.32.179.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
2.54.151.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
2.54.172.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
2.54.181.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
80.246.136.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
79.181.103.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.64.80.202	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
109.64.80.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	5
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	5
176.13.6.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.6.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
80.246.137.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.6.241	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.223.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.195	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
79.183.103.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
183.206.175.39	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/fckeditor/editor/	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.i	Distributed Unauthorized URL Access on 147.237.72.167/	Block	1
62.90.181.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
149.78.182.189	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
5.102.254.144	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.179.230.18	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspxaman	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter request in www.aka.idf.il/	None	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/services.asp	Block	1
87.71.15.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.15.13	Block	1
79.179.14.95	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.193.162	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
149.88.207.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.44.137.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
140.115.111.116	Taiwan	147.237.72.166	aka.idf.il	Unknown Parameter service in www.aka.idf.il/main/home/default.aspx	None	1
91.177.1.89	Belgium	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
187.188.111.60	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/index.php	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.135	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-ar/cogat.aspx	Block	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1
109.253.193.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
80.246.139.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1875	Block	1
141.212.122.64	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /x	Block	1
103.242.216.226	Bangladesh	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
192.117.190.138	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in aka.idf.il/kamlar/klali/	None	1
66.249.64.147	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.i	Abnormally Long Request method	Block	1