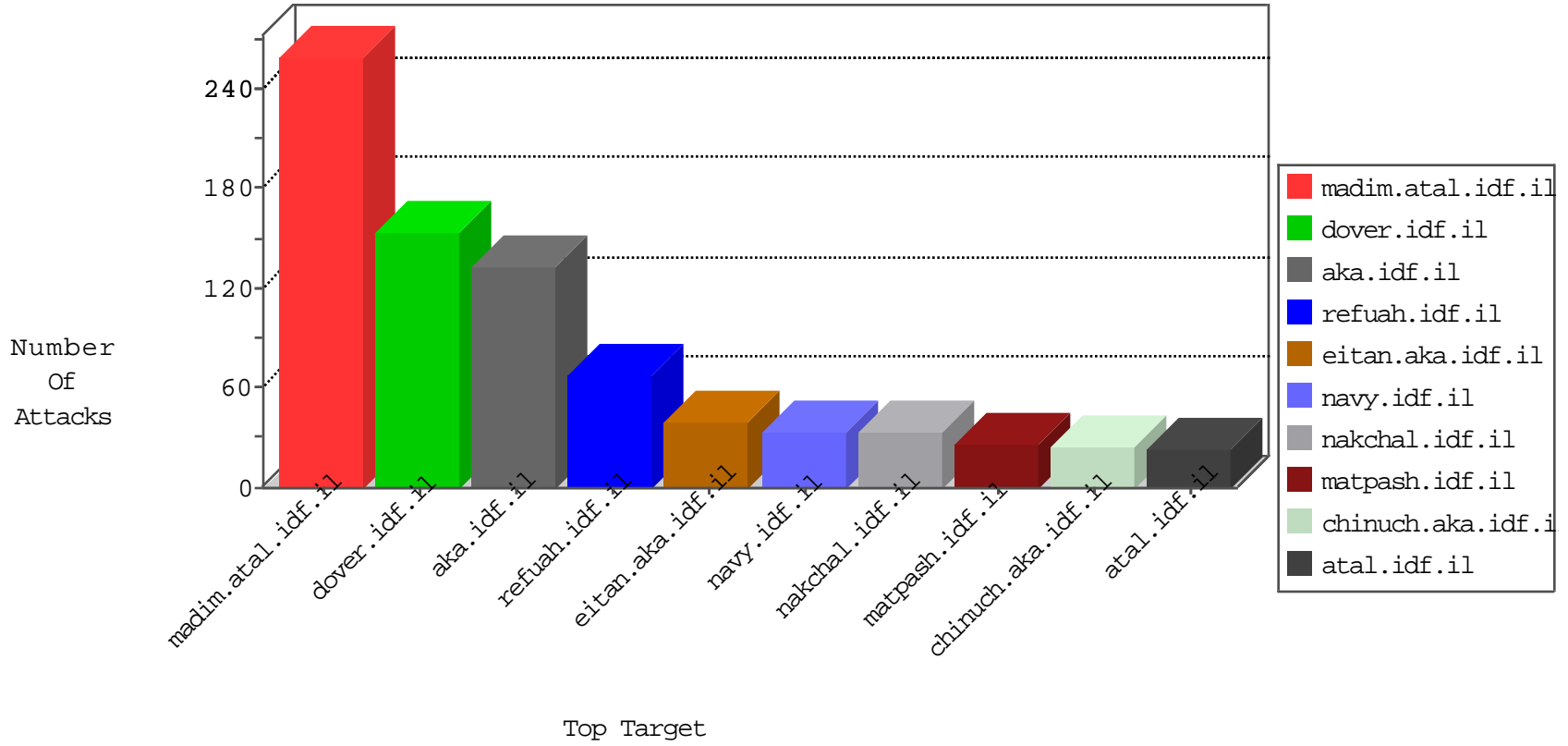


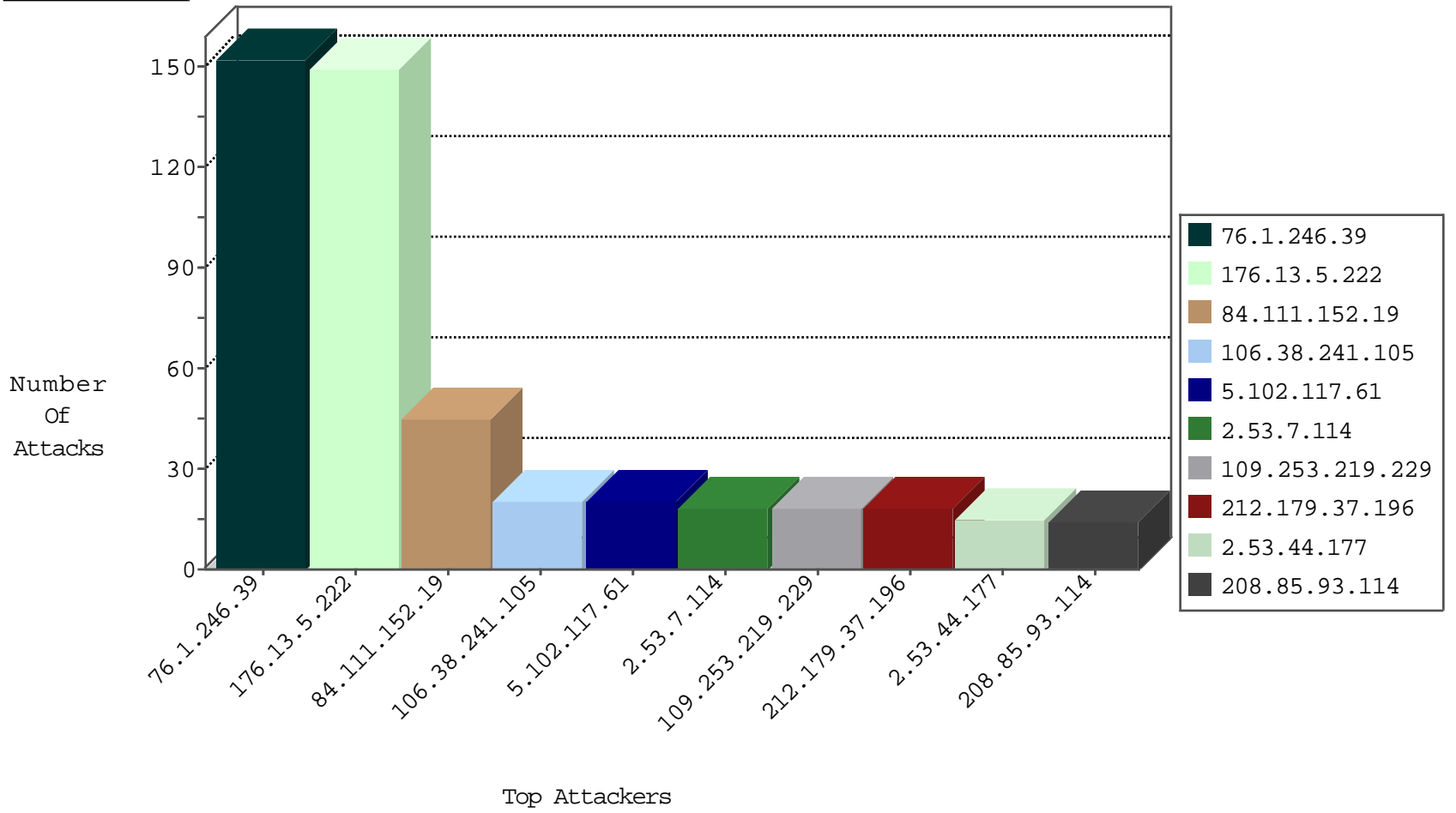
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.59.238	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	15
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
115.159.97.197	China	147.237.77.176	matpash.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
80.78.250.21	Russian Federation	147.237.77.176	matpash.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
82.221.105.7	Iceland	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.44.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.123.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.102.9.157	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
185.110.132.201	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
2.53.146.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.246.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.145.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.66.105.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.178.85.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.54.79	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
5.102.195.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
213.57.220.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.16.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
150.242.238.99	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
212.76.97.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.132.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.80.57.79	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
207.232.5.85	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
76.1.246.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
5.102.117.61	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
76.1.246.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
76.1.246.39	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
2.53.7.114	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.179.37.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
76.1.246.39	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
76.1.246.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.86.92	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
85.65.23.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
80.178.212.239	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
109.253.219.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.53.45.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
62.219.134.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
176.13.15.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.46.74	Palestinian Territory Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
62.0.225.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.95.251.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.247.36.75	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.154.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.249.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
84.95.251.245	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.177.53.122	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.140.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.95.251.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.93.15	Europe	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
62.90.99.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
176.13.11.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.15	Israel	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
176.13.238.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.227	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.244.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.211.108	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.136	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.5.222	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
2.53.44.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
81.218.241.25	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
89.139.222.0	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.222.0	Block	6
79.179.103.11	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
109.253.196.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.211.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.247.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
14.0.155.56	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	3
81.218.241.25	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
109.253.241.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.201	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	2
80.246.136.181	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
80.246.139.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.22	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00\$ContentPlaceHolder1\$txtLastName	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
37.26.147.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.114.5.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.30.141	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.30.141	Block	1
115.159.97.197	China	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/1043-en/cogat.aspx parameter PageNum	Block	1
86.40.80.207	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/templatecontrols/news/www.google.com	Block	1
2.53.9.29	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
176.13.15.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
37.204.209.87	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
192.116.127.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/	Block	1
132.68.26.96	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
77.138.30.141	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
87.69.36.210	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.147	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
84.111.70.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
147.236.238.85	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.54.79	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1