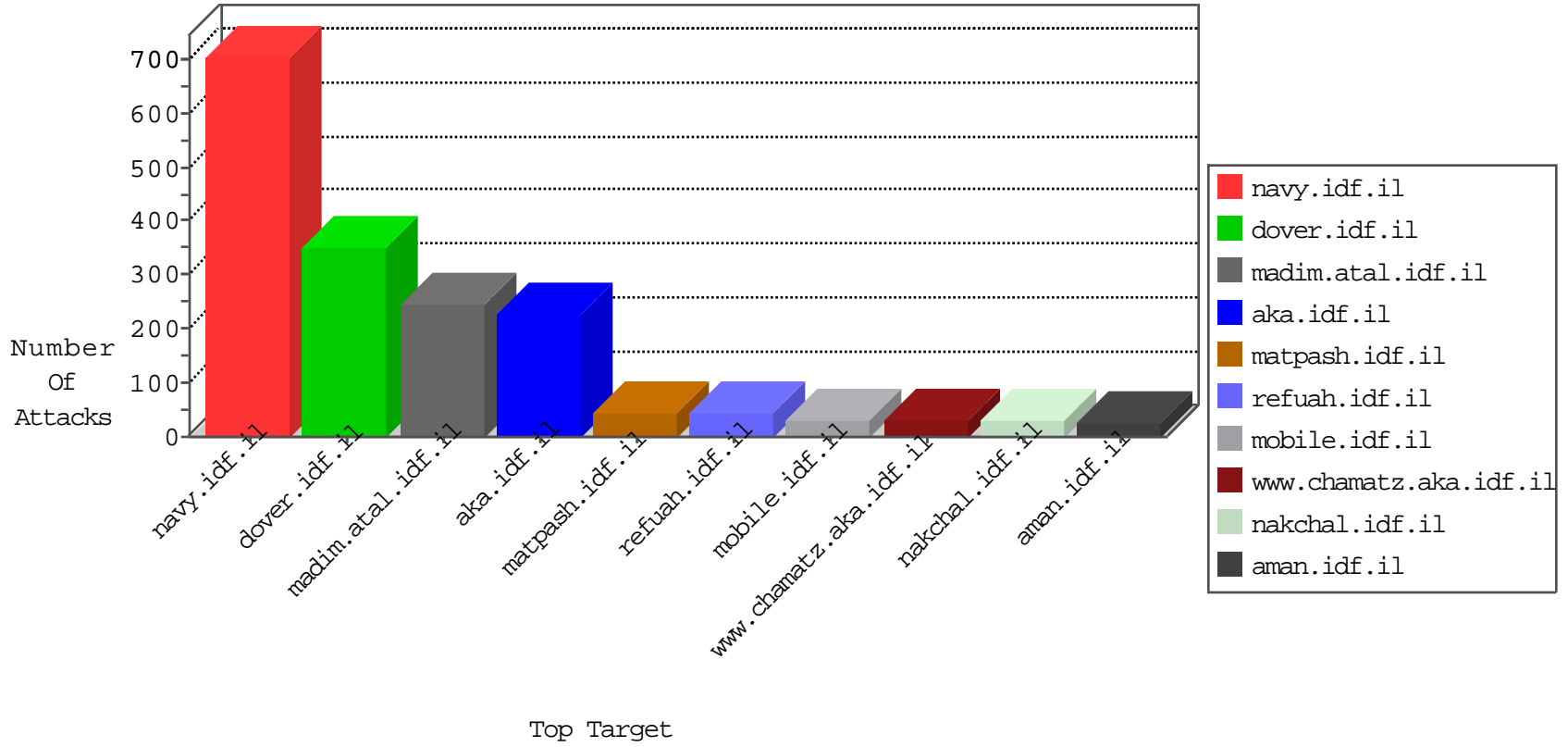


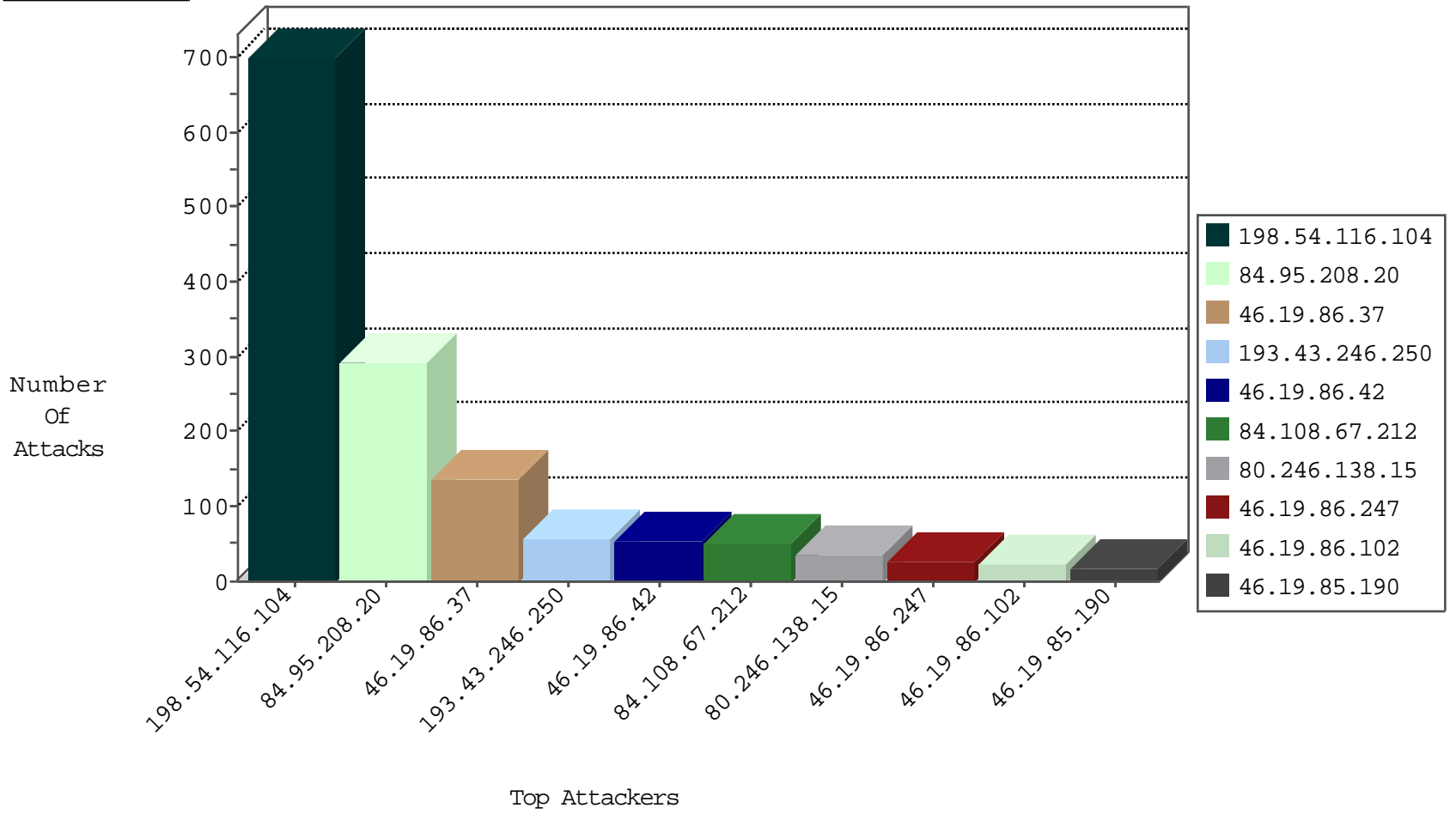
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
70.88.180.181	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
37.48.83.137	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
37.48.83.137	Netherlands	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
70.88.180.181	United States	147.237.76.42	refuah.idf.il	Black List	drop	1

09-06-2016-12:04:01 to 09-06-2016-13:04:01

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
85.65.20.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.7.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.101.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.242.157	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
185.40.4.92	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.72.63.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.247.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.38.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.196	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
88.208.26.13	147.237.72.166	Netherlands	aka.idf.il	Tehila - Perl LWP with fake user agent	1
84.108.67.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.208.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.47.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.143.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.170.178.155	147.237.77.179	Colombia	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
77.124.17.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.24.184.193	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
121.46.108.138	147.237.77.61	India	e.cogat.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
2.53.173.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.196	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.2.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
198.54.116.104	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	700
84.108.67.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
193.43.246.250	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.93.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.53.189.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.253.214.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.190	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
85.250.188.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.190	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.222.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.52	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
81.218.154.181	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.52.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.155.89.140	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.5.202	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
132.70.66.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.180.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.247	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
80.246.136.219	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.169.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.117.170.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.4.32	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.46.41.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.135.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.90	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.156.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
89.139.137.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.32.179.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.142.209	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.149.188	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	131
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	93
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
80.246.138.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	20
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	8
176.13.13.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
62.90.194.225	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
185.32.179.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.152.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
77.138.208.130	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
2.53.189.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
109.253.214.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.130.223.17	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
79.180.215.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/haredim/default.aspx	Block	2
91.143.234.207	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.75	Block	1
2.53.147.74	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.53.147.74 (Open Mode)	None	1
212.117.140.170	Israel	147.237.76.30	himush.idf.il	Unknown Parameter amp;t in www.tech.atal.idf.il/webresource.axd	None	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
154.66.161.61	Burkina Faso	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.69.18	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/881-he/patzar.aspx	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
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
95.35.135.175	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	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69851.pdf	Block	1
2.53.147.74	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.235.113.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
77.138.31.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.95.251.243	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.208	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/gyius/general.aspx	Block	1
185.32.179.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.76.111	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/cityofficers/	Block	1
109.66.146.226	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.153.73	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
77.138.31.109	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/main/main.asp	Block	1
84.229.26.199	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1