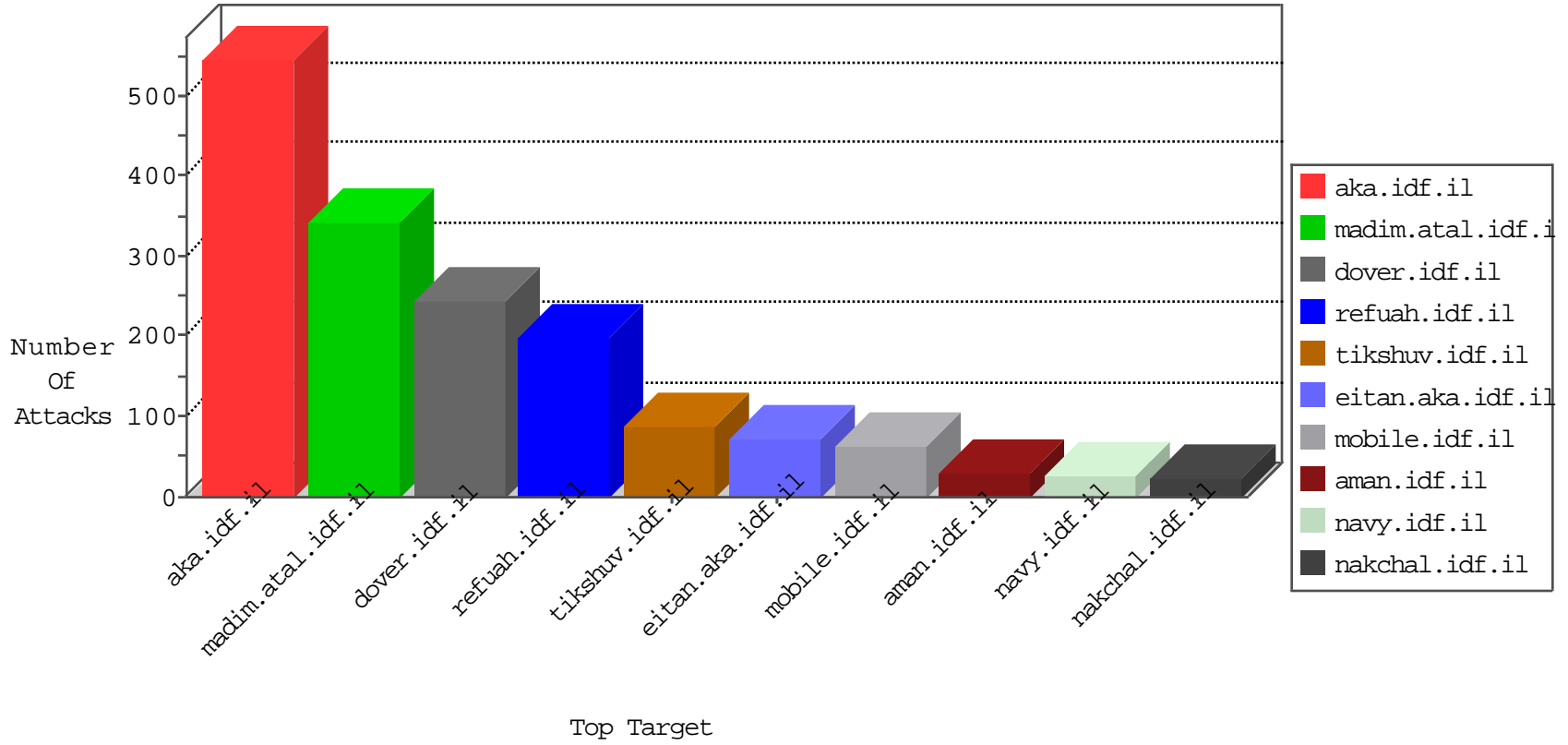


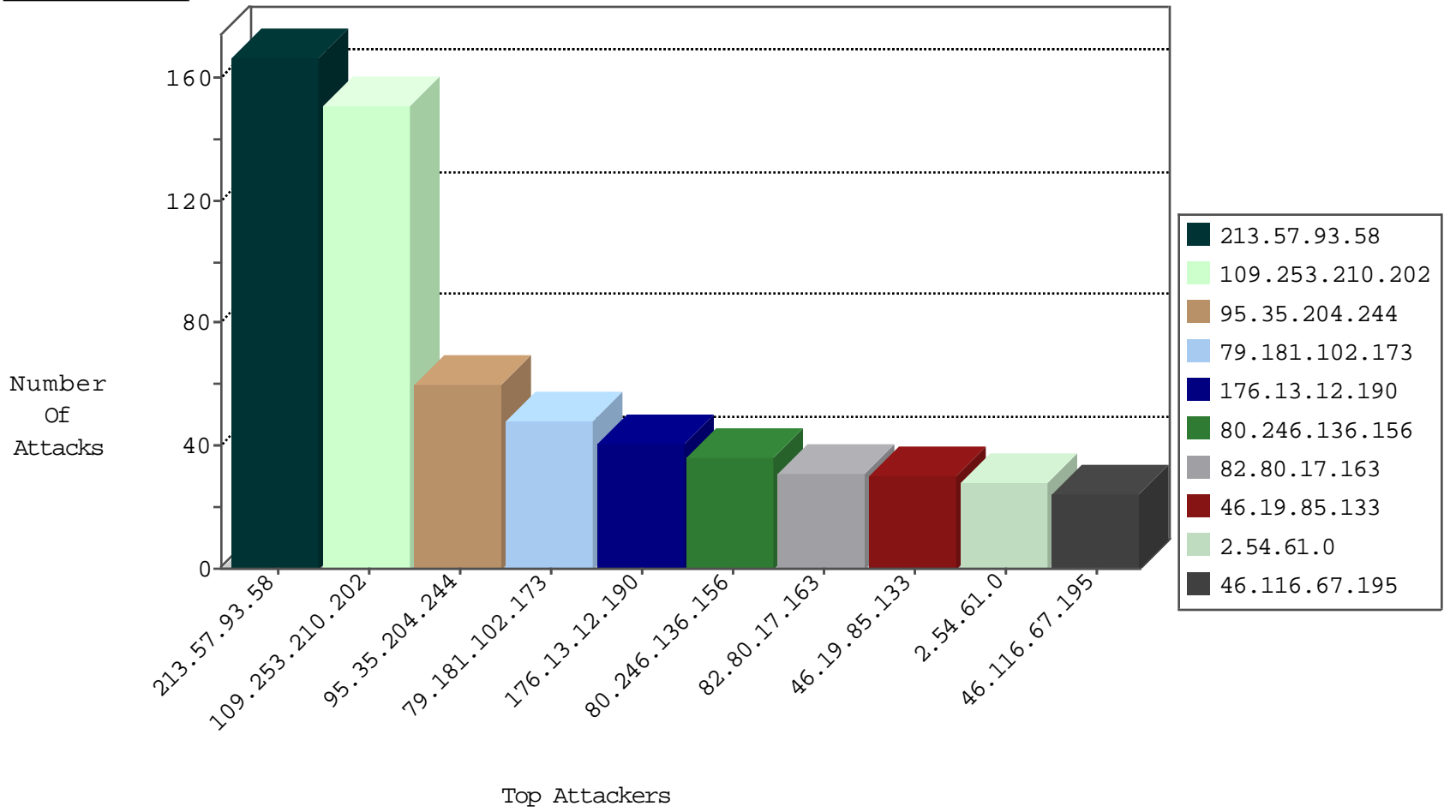
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.109.97.62	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32881
37.26.148.129	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	26051
37.26.148.178	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	22826
79.176.52.14	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
192.118.64.213	Israel	147.237.72.167	ishurim.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
176.13.11.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
212.179.61.82	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
149.88.175.22	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.94.41.65	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
95.86.92.46	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

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
176.13.13.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.64.197.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.6.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.204.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
212.199.244.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.26.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.183.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.7.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.174.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.211.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.37.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.93.211	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
213.57.93.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	164
95.35.204.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
176.13.19.110	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.108.193.162	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	14
2.52.160.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.102.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
79.181.102.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
79.181.102.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.146.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
84.108.193.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.132.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.154.154.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.128.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.17.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
165.72.200.11	Europe	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.253.198.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.80.17.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.91	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.114.23.208	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.29.90.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.93.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.208.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.187.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.10.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
52.71.155.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.120	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.96.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.138.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.228.172	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.116.43.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.78.189.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.135.102.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.181.102.173	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.210.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
176.13.12.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.136.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.61.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.116.67.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.13.17.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.52.155.114	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	12
5.29.90.179	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	6
213.8.204.53	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	6
85.64.174.180	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	3
79.182.184.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.11.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
132.71.100.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
37.26.149.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.183	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
46.117.16.92	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894- he/matpash.aspx	Block	2
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.119.193	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
81.218.241.26	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.128.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	2
46.19.85.199	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
192.114.105.254	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
82.80.156.169	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
37.26.146.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.53.105	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.253.156.192	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/	Block	1
212.97.132.130	Denmark	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
182.50.132.48	Singapore	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategori/oprolescategori.aspx	Block	1
66.249.93.239	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
2.54.184.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
94.159.159.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
81.218.11.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.152.17	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
37.26.146.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.209.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
212.143.133.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
37.26.148.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1