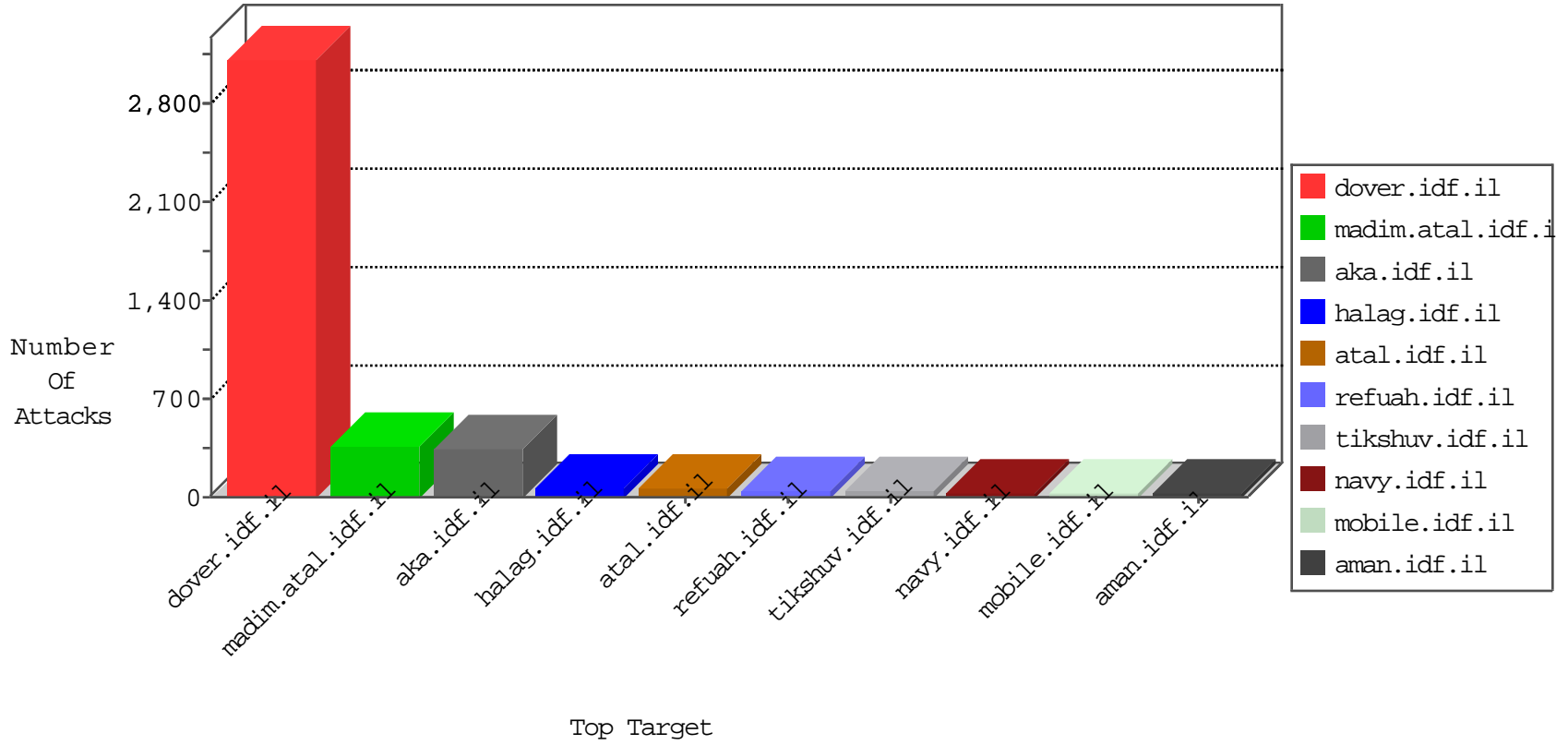


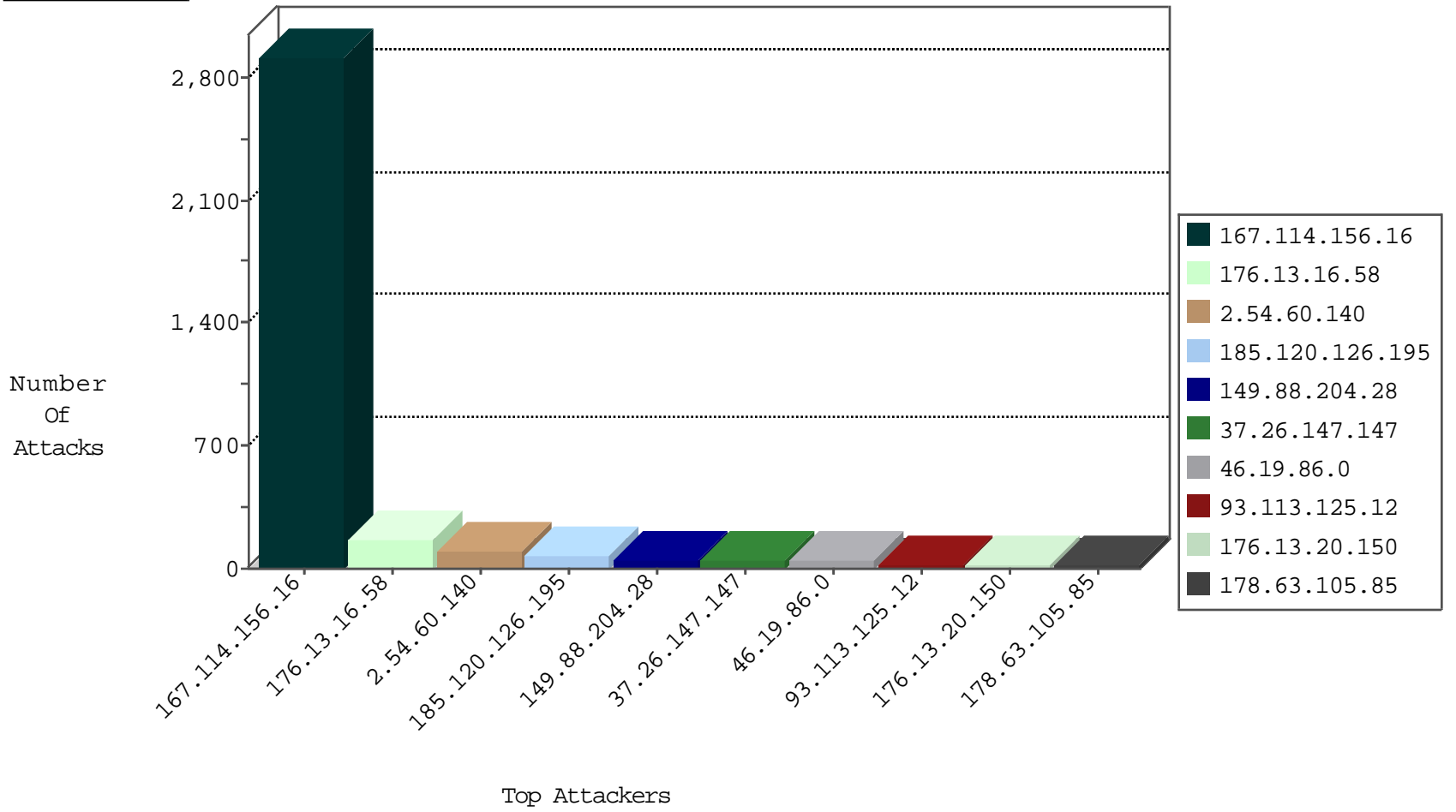
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3530
109.65.133.31	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.65.133.31	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
87.106.151.104	Germany	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
213.159.209.5	Russian Federation	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	1
37.26.148.138	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
120.26.121.229	China	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.70.1.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
80.246.133.70	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.200.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
109.67.184.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.213.31	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.13.19.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	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	4
198.20.69.74	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.64.153.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.12	147.237.77.235	Romania	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
87.70.95.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.149.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
176.13.14.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.0.19	Austria	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.199.69.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.194.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.192.6.154	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.56.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.217.47	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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	56
149.88.204.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
185.120.126.195		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
85.250.30.159	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
37.26.146.244	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.150	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.210.150.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.20.150	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.180.212.7	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.146.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.135.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
80.246.137.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.209.245	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.4.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.232.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.66.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.120.126.195		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
2.54.175.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.152.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	6
37.142.231.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.108.104.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.103.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
109.64.103.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.103.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.176.70	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.126.195		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.120.126.195		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
188.120.154.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.189.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.71	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.55.210.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.210.197.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.126.195		147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.108.104.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.155.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.211.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.151.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.60.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
176.13.16.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
37.26.147.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.133.19	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
79.180.147.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
95.86.100.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim//sip_storage/files/6/66856.jpg 	Block	5
2.52.52.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
87.71.80.169	Israel	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	4
87.71.80.169	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	4
80.246.130.226	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.54.58.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.116.225.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
109.160.148.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.168.235	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
41.237.110.49	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
79.176.54.83	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.54.83	Block	2
46.116.113.204	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
212.76.112.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
41.237.110.49	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
79.176.54.83	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
37.26.148.237	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.29.236.93	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	2
66.249.93.182	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.8.17.222	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en/	Block	2
140.115.111.116	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
70.82.204.193	Canada	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.19.134	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
89.138.228.189	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
85.144.220.120	Netherlands	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.126	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
79.176.210.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
5.22.135.185	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/payslips.aspx	Block	1
149.78.35.121	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
93.113.125.12	Romania	147.237.77.235	sviva.idf.il	Abnormally Long Request URL	Block	1
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.64.27	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyius	Block	1
89.138.69.162	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
5.102.254.242	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.25.151.159	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
71.105.41.221	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.135.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.116.113.204	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.116.113.204	Block	1
91.196.50.33	Poland	147.237.76.30	himush.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
85.250.30.159	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.148.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.115.113.82	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
149.88.204.28	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1