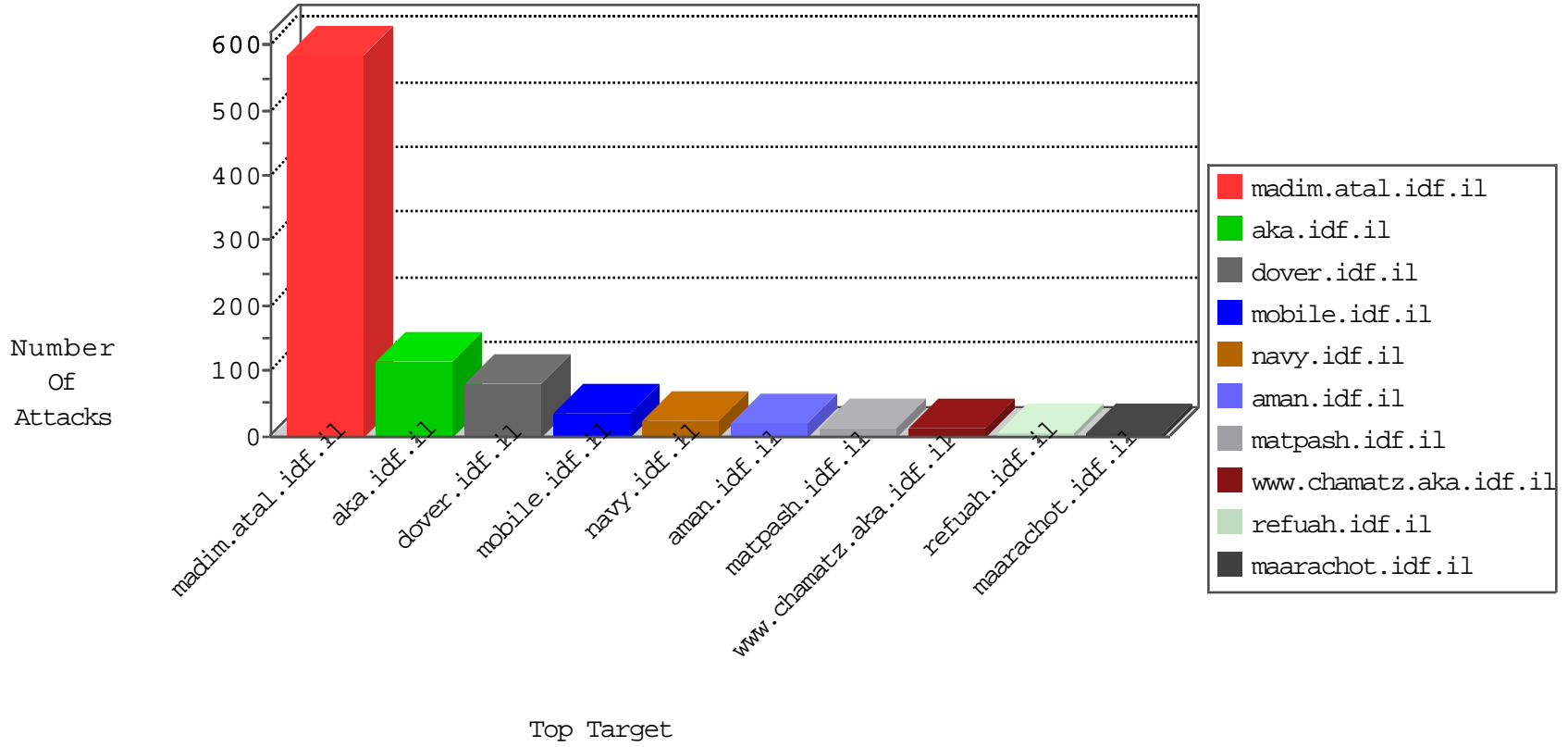


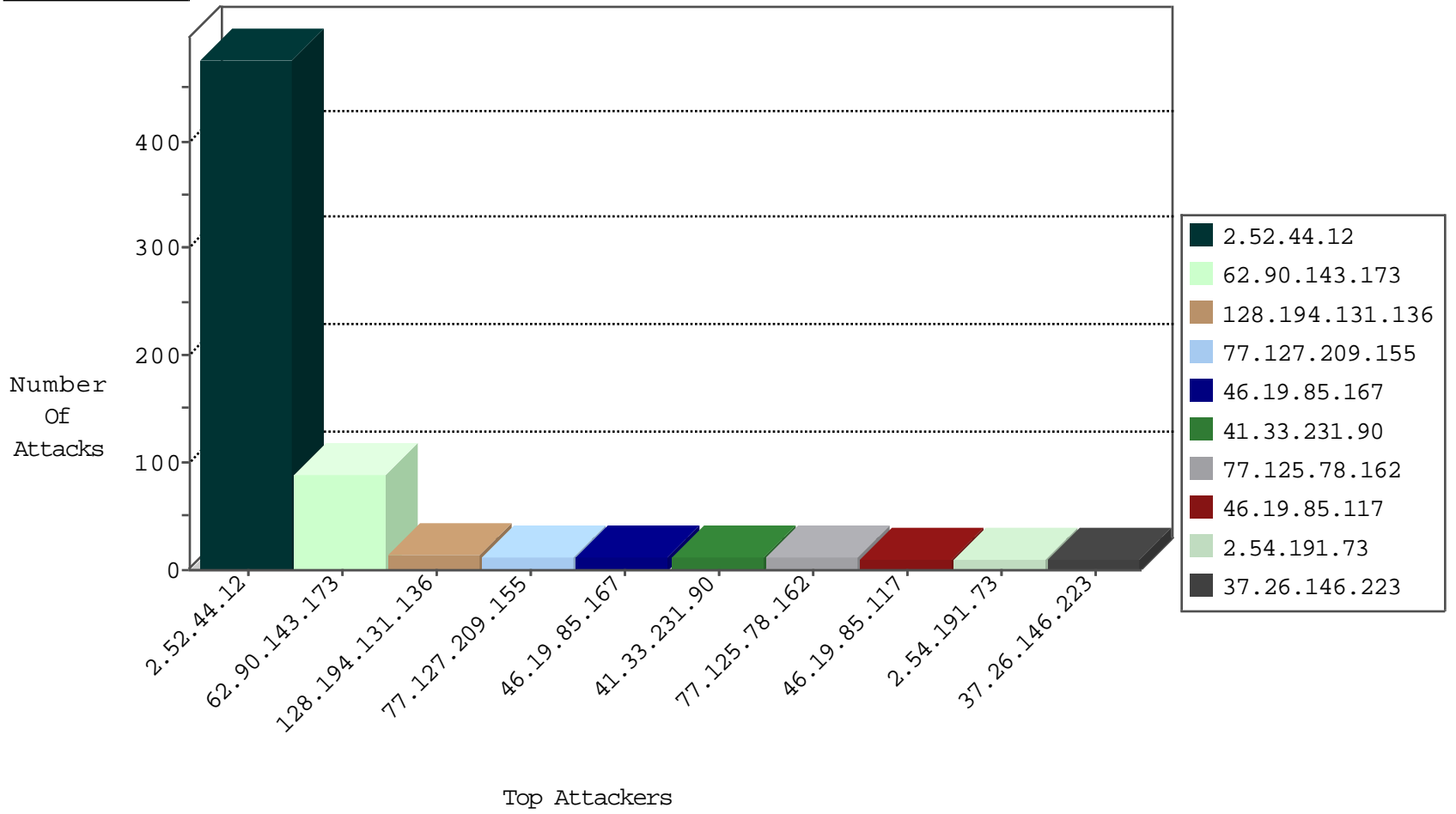
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
123.151.42.61	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Udp	drop	2
5.249.139.184	Italy	147.237.76.38	e.e.meitav.idf.il	Invalid L4 Header Length	drop	2
139.129.96.25	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	2
83.169.202.180	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Invalid TCP Flags	drop	1
123.151.42.61	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.90.118	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
77.125.78.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.117	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.146.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
128.194.131.136	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.183.233.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.169.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.54.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.222.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
128.194.131.136	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.179.159.253	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.178.48.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.64.106.2	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.36.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.137.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.12		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.167	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.215.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.254.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.124.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.174.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.167	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.68.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.151.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.177.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.148.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.120.26	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.66.18.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
5.22.131.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.178.48.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.54.191.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.169	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.28.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
2.54.191.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.44.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.44.12	Block	270
2.52.44.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
62.90.143.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
2.52.44.12	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.44.12	Block	63
218.65.149.155	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 218.65.149.155	Block	6
87.69.196.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.38.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.54.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.88.101.173	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.36.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.143.36.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	2
2.52.151.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.182.97.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
210.172.183.48	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/112925.pdf	Block	1
149.78.169.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
91.196.50.33	Poland	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
218.65.149.155	China	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 218.65.149.155	Block	1
79.178.48.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1
177.185.192.77	Brazil	147.237.72.166	aka.idf.il	Multiple signatures from 177.185.192.77	Block	1
109.253.209.165	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/cportal/wifi_conf	Block	1
212.143.36.81	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.36.81	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
93.123.0.72	Bulgaria	147.237.77.216	doover.idf.il	Distributed PHP Attempt	Block	1
79.180.28.201	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
218.65.149.155	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/u	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3416.jpg	Block	1
185.25.151.159	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
128.194.131.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
14.139.227.147	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
87.69.241.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Question\$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
175.139.50.9	Malaysia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
93.123.0.72	Bulgaria	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/109703.pdf	Block	1
185.49.14.190	Poland	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
139.193.88.15	Indonesia	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
14.139.227.147	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
91.196.50.33	Poland	147.237.76.30	himush.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
213.8.204.18	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.64.53	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/110634.pdf	Block	1
175.139.50.9	Malaysia	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
2.54.22.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.106.171	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/7/2497	Block	1
84.94.20.189	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1