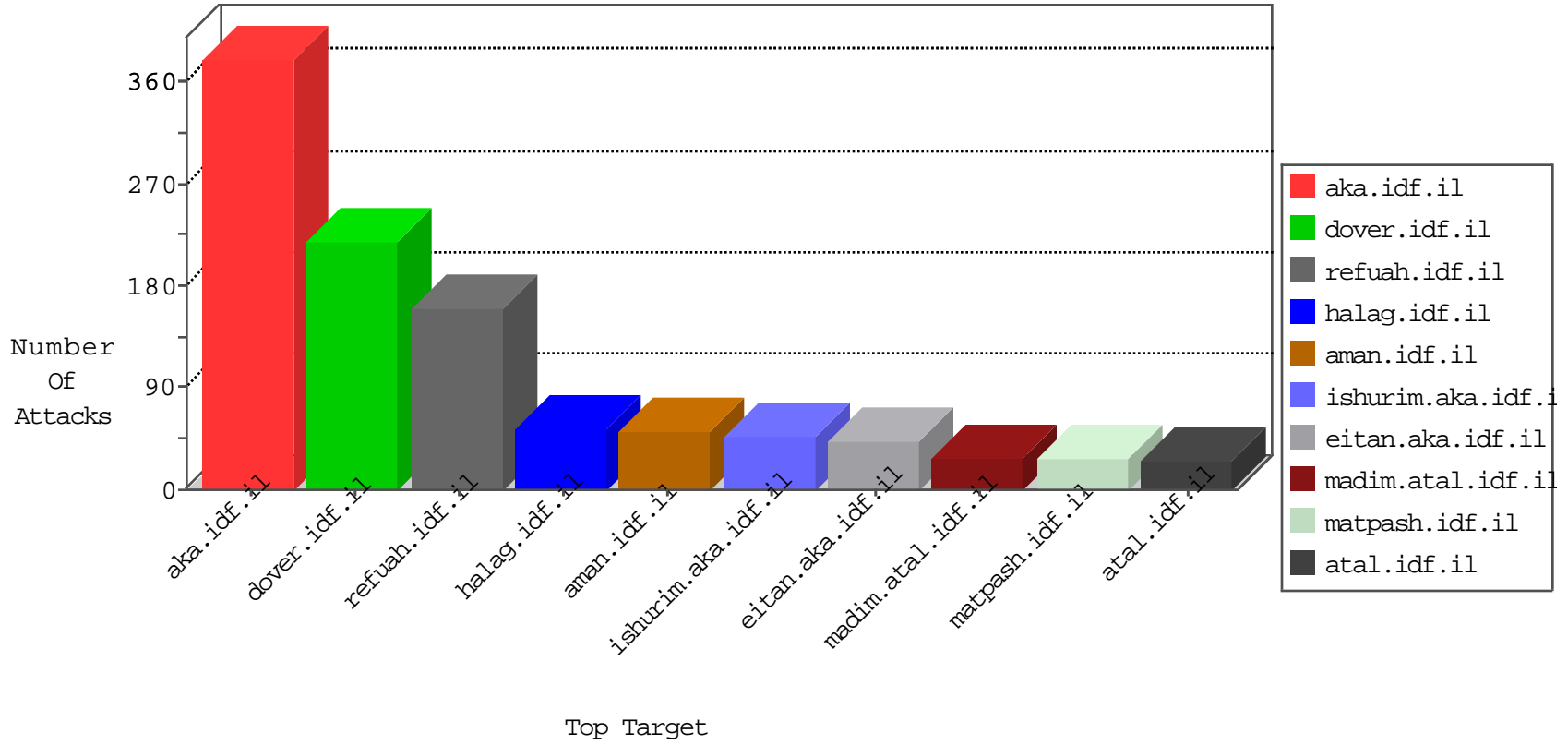


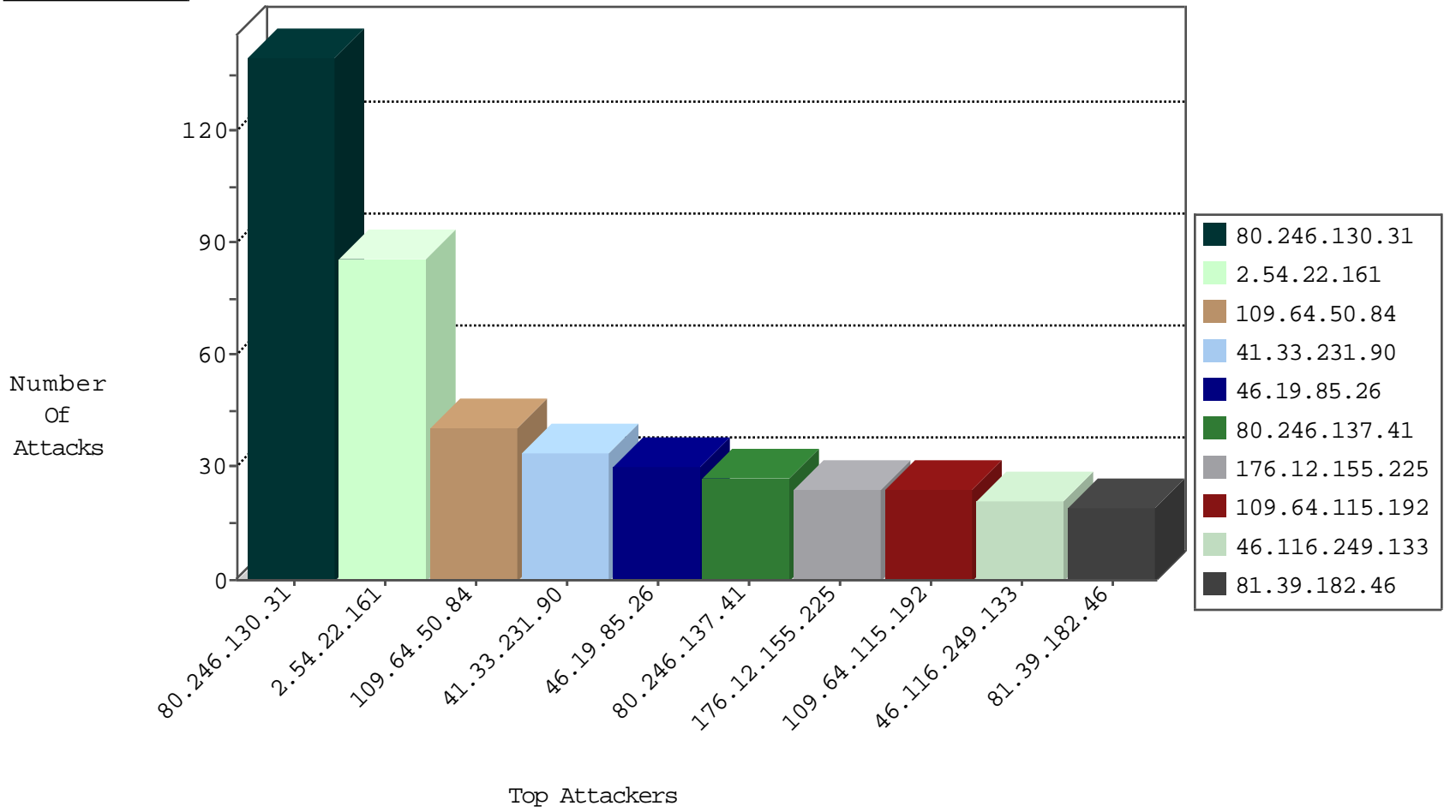
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.102.126	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.178.56.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
142.54.160.213	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1
85.25.43.146	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-10-2016-19:04:06 to 02-10-2016-20:04:06

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
88.249.106.23	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.72.217	United States	e.idf.il	ET DROP Dshield Block Listed Source	1
183.64.161.26	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.212.232.144	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
125.212.232.144	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
109.64.9.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.23.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.144	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.8.28	China	e.mobile-ks.idf.i	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	139
109.64.50.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
176.12.155.225	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.22.161	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
81.39.182.46	Spain	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	19
46.116.249.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
109.64.32.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.22.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
82.145.221.90	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.64.191.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.137.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
149.78.250.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
77.126.209.51	Israel	147.237.72.166	aka.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
46.19.86.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.254.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.115.192	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
188.120.148.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.115.192	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	7
2.54.22.161	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.22.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.161	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.131.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.108.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.149.132	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.22.161	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.22.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.78.250.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.22.161	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	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
2.54.22.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.195	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.22.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.179.195.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.115.192	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.133.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.115.192	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.129.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
157.55.39.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.207.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.213.108	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
84.229.38.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.8.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.22.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.211.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.184.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.73.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
82.205.26.188	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
213.8.204.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.179.58.147	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
212.179.3.44	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
5.22.135.153	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
93.173.23.6	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.96.139.9	Poland	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
207.46.13.41	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
128.232.110.28	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
84.108.50.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl13\$ct101\$ct103\$cblQuestion\$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.77.51.35	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	1
109.65.73.234	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
79.183.179.89	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
212.179.3.44	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
79.176.96.94	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
212.25.119.136	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
89.138.252.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/webhp	Block	1
62.84.69.166	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
176.194.128.11	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
84.109.165.23	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
81.207.74.195	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.85.81	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
79.179.58.147	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
212.179.3.44	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.22.135.153	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
94.230.86.2	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
85.250.244.244	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
79.96.139.9	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-login.php	Block	1
207.46.13.152	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_text.asp	Block	1
46.120.70.149	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
157.55.39.35	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.142.197.45	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
79.183.179.89	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
212.179.3.44	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
79.176.96.94	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.76.97.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ctl155 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
89.139.244.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ctl138\$ct101\$ct103\$cblQuestion\$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.66.182	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/general.asp...669&docid=72592	Block	1
185.27.105.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
84.109.165.23	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.109.165.23	Block	1