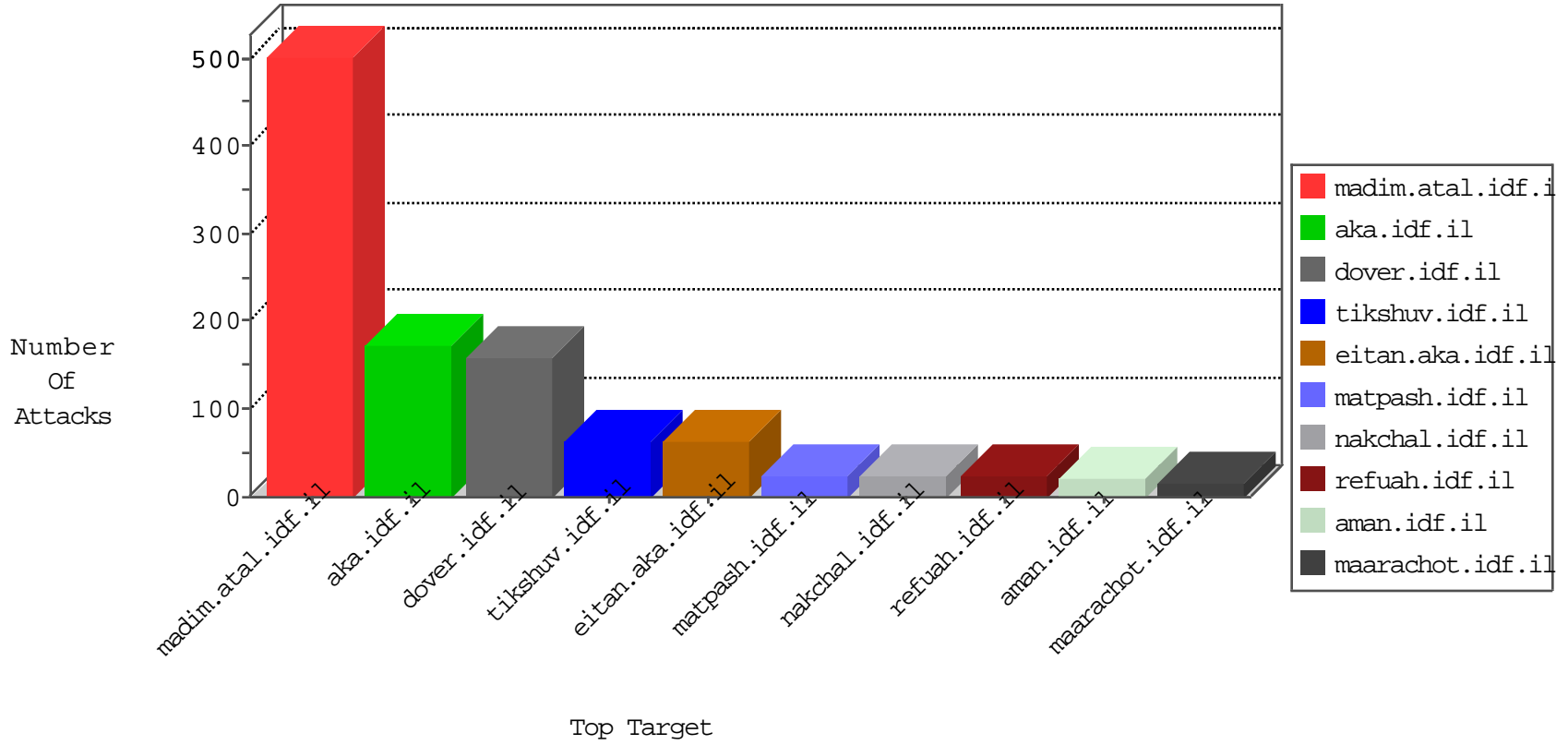


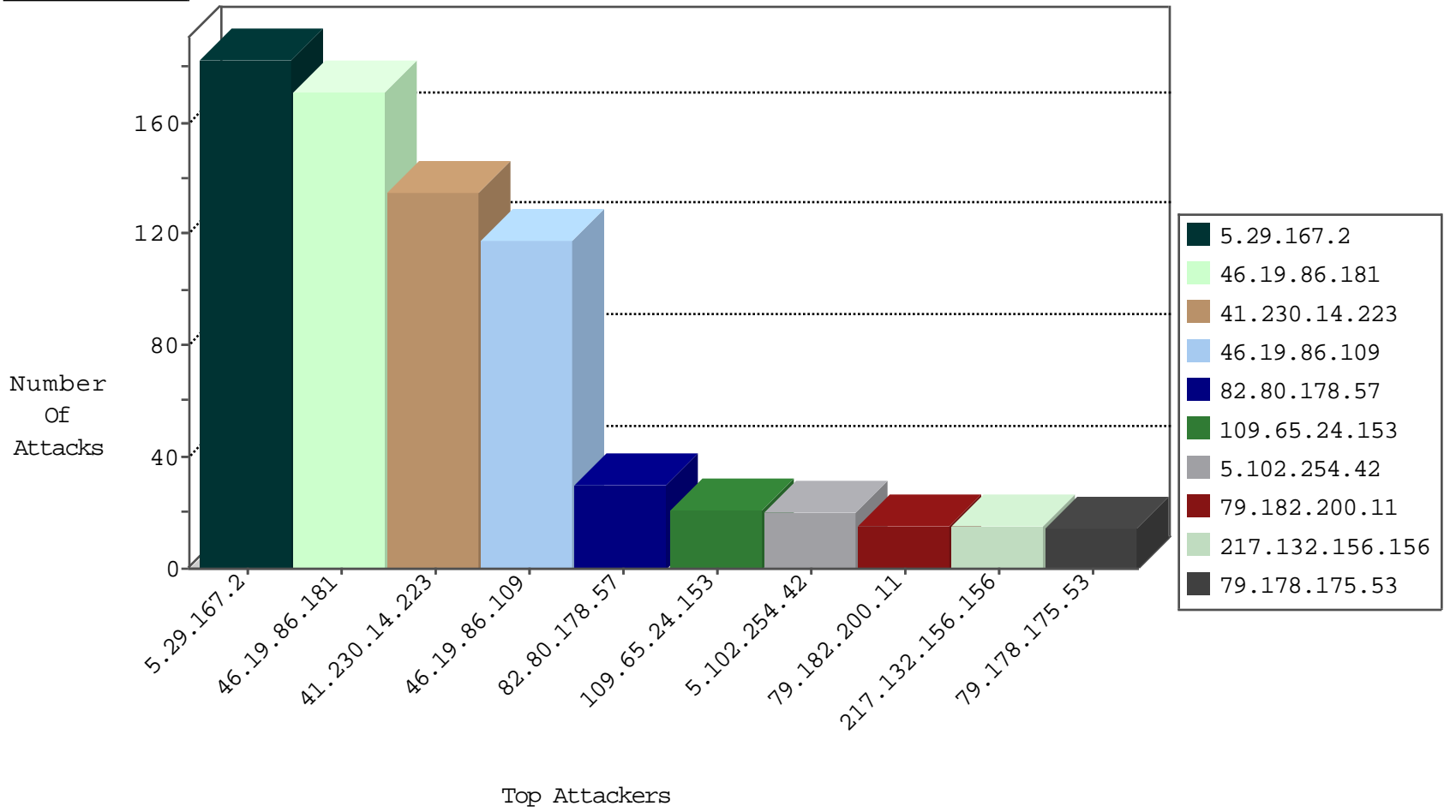
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.220.82	Europe	147.237.77.216	dover.idf.il	Block_Tp_Web_In	drop	10
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
220.144.250.83	Japan	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
212.71.235.23	United Kingdom	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.178.57	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
176.13.19.240	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
79.177.159.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.71.28.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## 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
107.150.36.36	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
107.150.36.36	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.71.133.133	147.237.76.147	Israel	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
47.88.10.97	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.244	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
162.243.227.19	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
107.150.36.36	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
107.150.36.36	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.87.205.254	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
109.65.24.153	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
82.80.178.57	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.182.200.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
5.102.254.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.177.143.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.220.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
24.113.64.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.254.42	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.170.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.107.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.217.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
106.38.241.151	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.214.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.129	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.242.189	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.25.159	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.63.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.61.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.184.132	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.19.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.237.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.180.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.112.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.214.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.37.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.102.195.108	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.130.170.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.18.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.102.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.6		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.31.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.216.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.20.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.207.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-05-2016-23:04:08 to 03-06-2016-00:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.22.129.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.167.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	183
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	171
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
217.132.156.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	12
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	12
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	12
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	9
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
41.230.14.223	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	9
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	4
109.253.138.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.175.53	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
80.84.1.10	Satellite Provider	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.76.112.169	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/113394.pdf&sa=u&ved=0ahukewiarp-sw6rlahvkkpokhts3daqgfggjmak&usg=afqjcnhjoxlzbtsylysyayrqhv7bxmema	Block	2
80.179.96.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.116.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
77.127.240.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.136.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.178.175.53	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
149.78.114.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
79.181.141.191	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
64.71.32.29	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
109.64.33.196	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
94.230.86.46	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
79.181.13.2	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.69.158.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
79.178.175.53	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
207.46.13.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
78.191.140.125	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
149.78.5.115	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
80.84.1.27	Satellite Provider	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.141.191	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.238.147.235		147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
79.180.184.115	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.57.149.169	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
93.172.168.193	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
84.108.102.179	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
79.178.175.53	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
197.35.225.175	Egypt	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
79.181.141.191	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.181.141.191	Block	1
109.64.33.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
94.230.86.46	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
79.181.141.191	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
79.178.175.53	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
207.241.229.198	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/eitan/pratim/pirteyerua	Block	1
5.29.203.171	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1