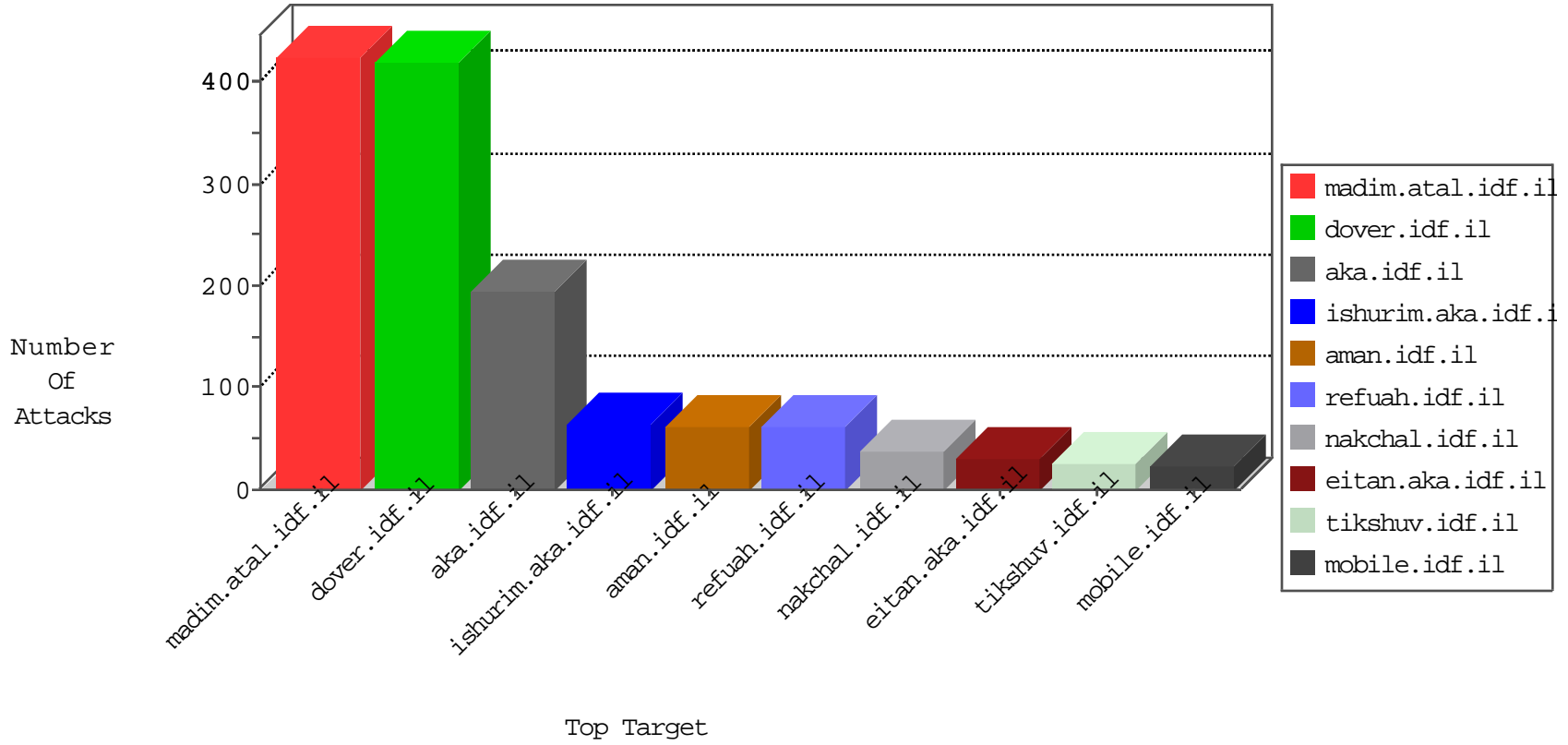


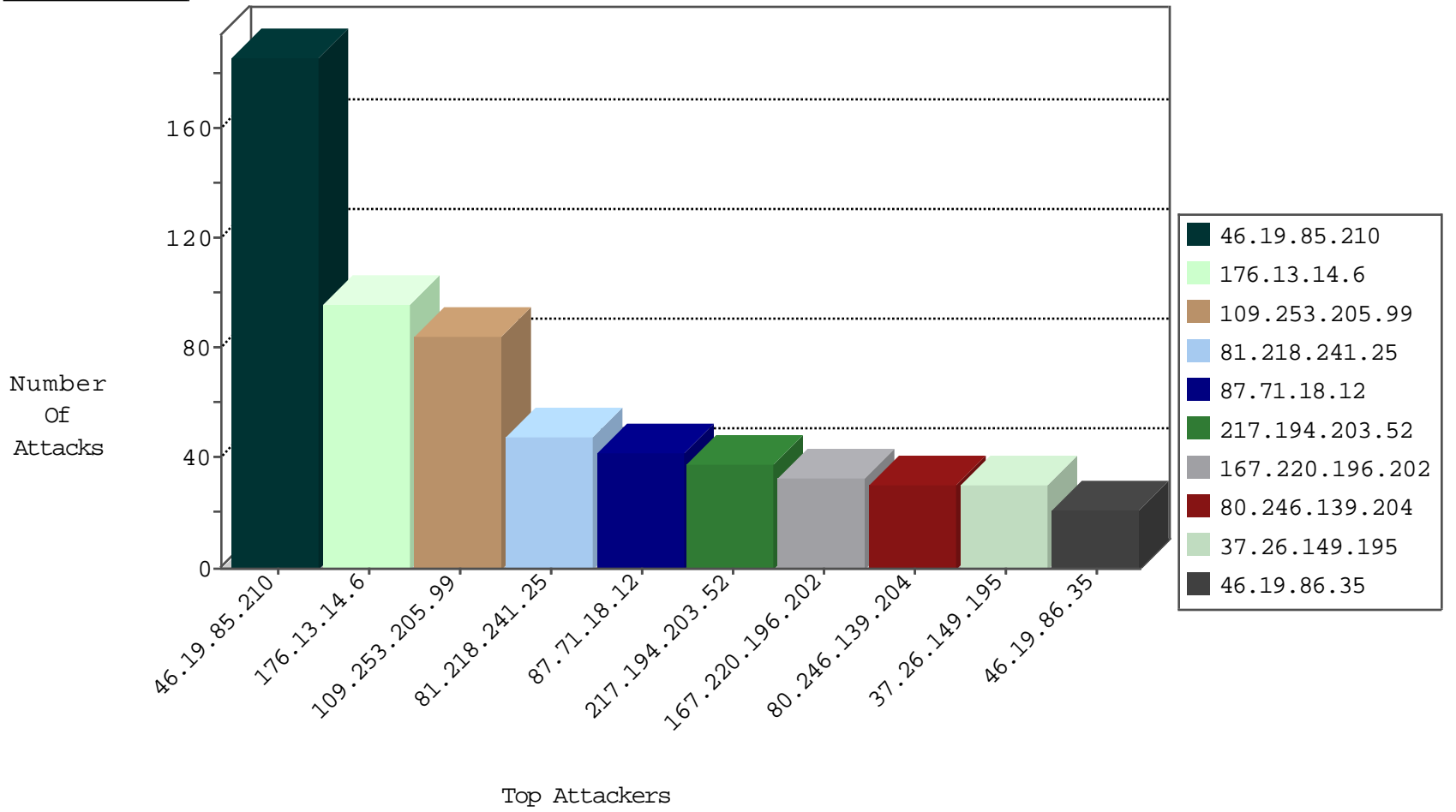
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
37.26.149.195	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
87.70.242.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
2.54.19.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
199.203.136.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.7.104	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.81.37.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
79.183.227.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
184.105.139.126	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
152.178.71.13	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.98	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
23.94.69.234	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
46.19.85.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.98	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
23.94.69.234	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.93	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.82	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
2.52.11.36	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.114	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.94	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.182.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.65.121.179	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.117.164.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
2.54.141.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
176.13.11.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.150.201.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.10	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
149.88.58.169	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.186.167.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -f -sS	1
84.109.208.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.87.243.150	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.69.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.171.176	147.237.77.216	Israel	dover.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
192.114.23.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.66.43.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.76.31	Canada	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.140.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.205.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.21	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
87.71.18.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
46.19.86.35	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	18
167.220.196.202	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
167.220.196.202	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
217.194.203.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
2.54.49.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
96.47.68.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.183.131.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.152.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.130.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.105	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
165.225.72.80	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.22.130.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.231	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.90.85.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.241.254	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
79.183.153.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.146.236	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.130.65	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
217.194.203.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.149.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.146.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.137.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.29.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.14	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.116.219.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.231	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.189	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.151.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.41.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.166.21.135	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
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
176.13.14.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.205.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
80.246.139.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
2.54.154.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
176.13.21.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
80.246.130.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.71.48.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.171.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.223	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.109.3.71	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
84.108.121.103	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.108.121.103	Block	2
2.52.138.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	2
91.199.69.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.143.90.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
84.109.3.71	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
5.29.74.167	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
2.54.17.237	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
147.236.32.17	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.74.116.135	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
212.235.68.118	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
109.64.33.196	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
62.178.4.65	Austria	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
203.133.168.75	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
85.64.181.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.251.250	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.74.167	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
173.24.218.51	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
109.253.223.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
104.33.210.207	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
212.199.244.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
181.169.127.10	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
84.109.3.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
5.29.74.167	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
149.78.241.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.42	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
212.235.68.118	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.177.201.62	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
207.241.229.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.130.211.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.74.167	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
173.24.218.51	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1