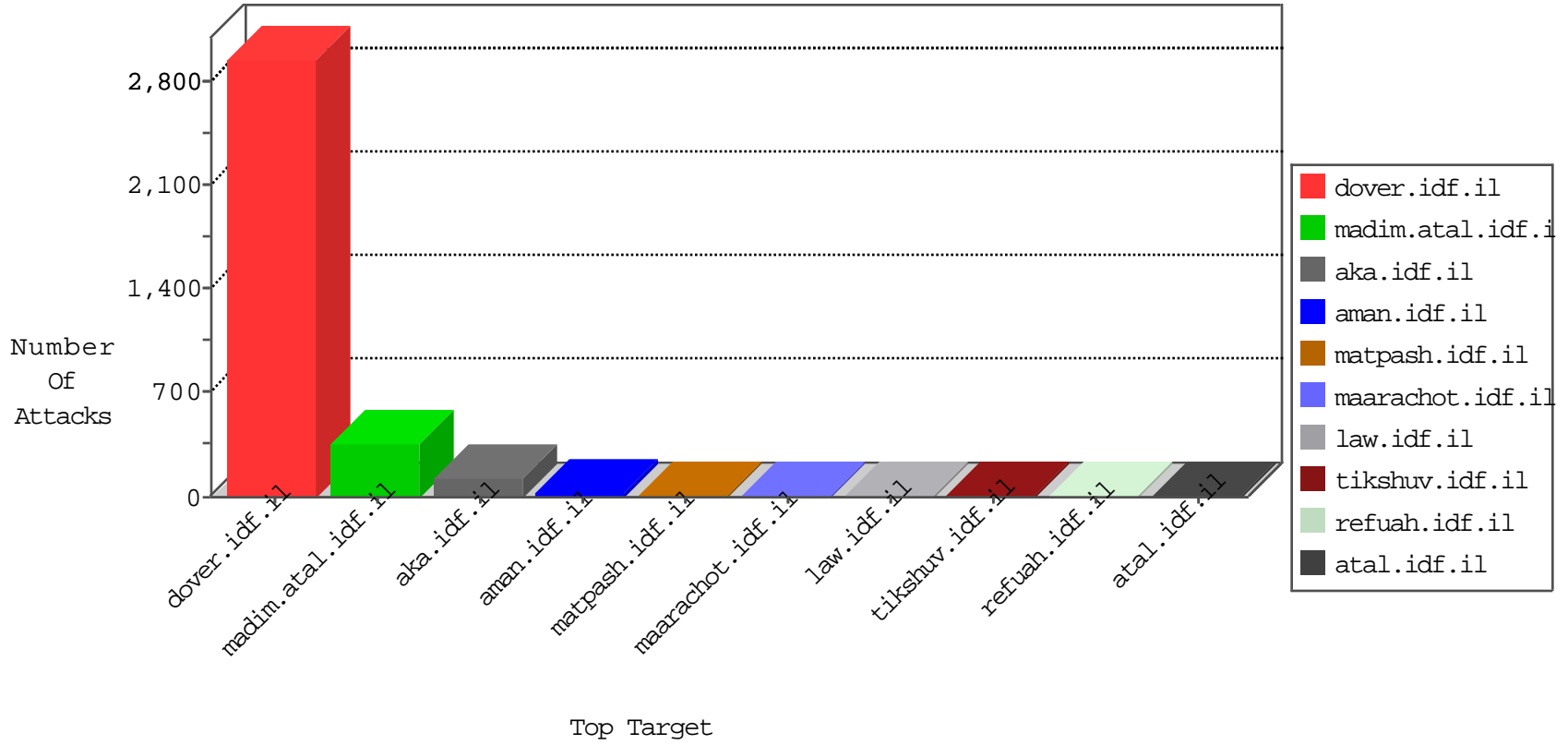


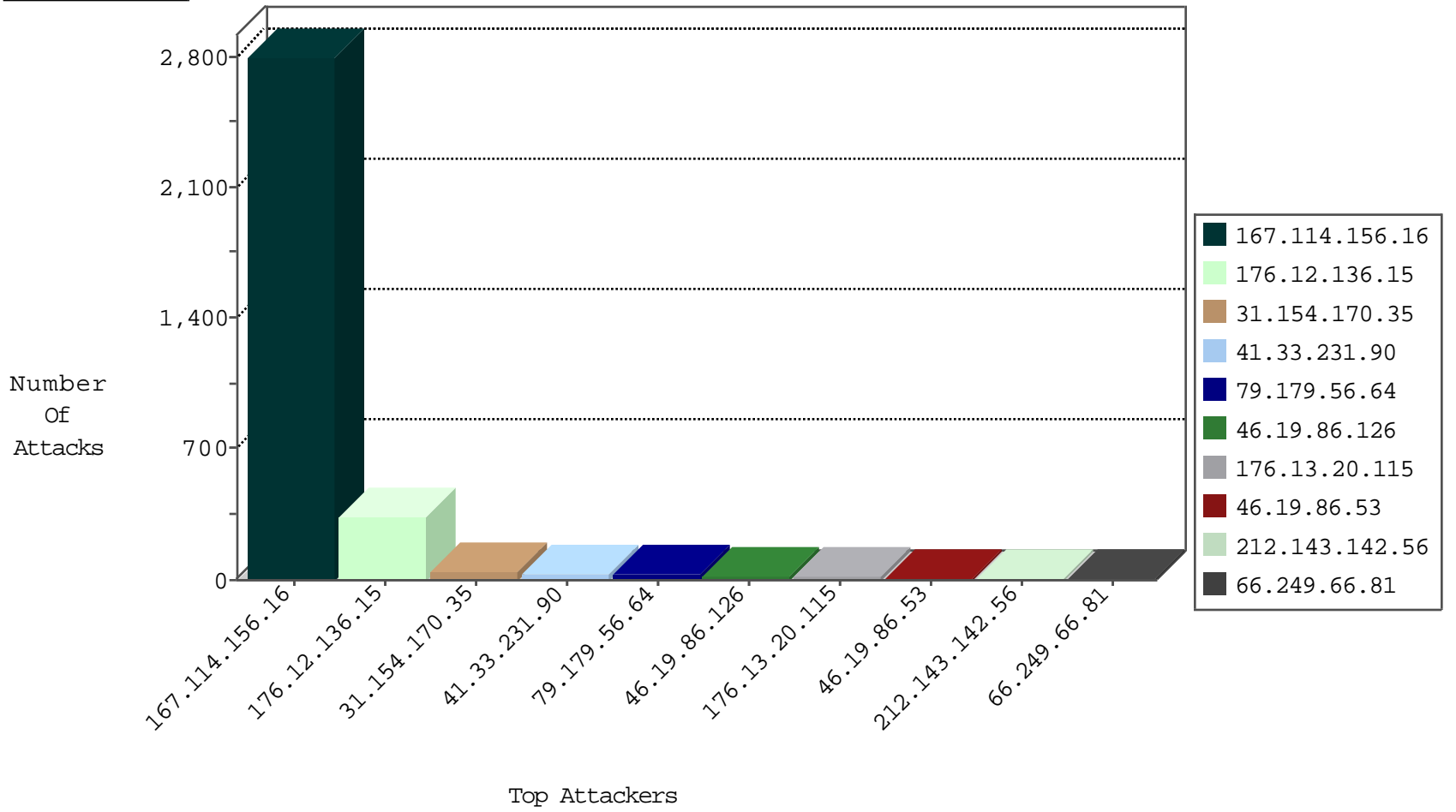
IDF Under Attack Daily Report



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	3583
66.249.66.81	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	688
31.154.170.35	Israel	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	324
66.249.66.107	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	47
202.112.51.96	China	147.237.77.170	maarachot.idf.il	block-sp-trafl	drop	1
96.40.134.2	United States	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1
202.112.51.96	China	147.237.76.86	navy.idf.il	block-sp-trafl	drop	1
94.102.56.238	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

12-04-2015-23:04:04 to 12-05-2015-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.160.147.108	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	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
66.249.66.81	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.186	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
193.105.134.220	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
121.7.149.109	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.51.217.201	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.67	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
125.65.165.215	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
114.43.3.4	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.67.240	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.240.144.65	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.179.56.64	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.86.53	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
188.120.148.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.123.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
38.98.194.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.133.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.12.136.15	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.144.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.148.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.173.22	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
41.131.100.197	Egypt	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
207.232.55.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.117.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.157.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.173.22	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.11.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.41.66	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
84.229.248.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.66.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.172.207.143	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.218.27.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.210.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.172.207.143	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.166.204.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.75	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.243	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.203.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.64.64.142	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.174.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.243.31.2	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.95.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.120.148.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.76	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.150.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.136.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.136.15	Block	172
176.12.136.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
176.13.20.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
176.12.136.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.12.136.15	Block	8
176.13.18.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
86.121.13.253	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
87.69.109.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.175.193.164	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.12.141.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.4.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
109.64.133.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.175.13.138	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/general/default.a	Block	1
158.69.192.220	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
188.143.232.11	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
38.98.194.2	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
128.70.100.153	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
183.82.141.82	India	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.82.141.82	Block	1
84.111.155.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/106151.pdf	Block	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
192.185.6.25	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1
178.152.84.185	Qatar	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
141.212.122.64	United States	147.237.72.156	aman.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
183.82.141.82	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
84.228.115.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.69	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/tutum04012011.aspx	Block	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	1
31.154.170.35	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
195.154.73.222	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
178.152.84.185	Qatar	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8974-he/refuah.aspx	Block	1
176.12.136.15	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/61341.jpg	Block	1
157.55.39.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal/izkor/view_text.asp	Block	1
85.181.139.194	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
185.25.151.159	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.67.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ftb.imagegallery.aspx	Block	1
31.154.170.35	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
183.82.141.82	India	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1