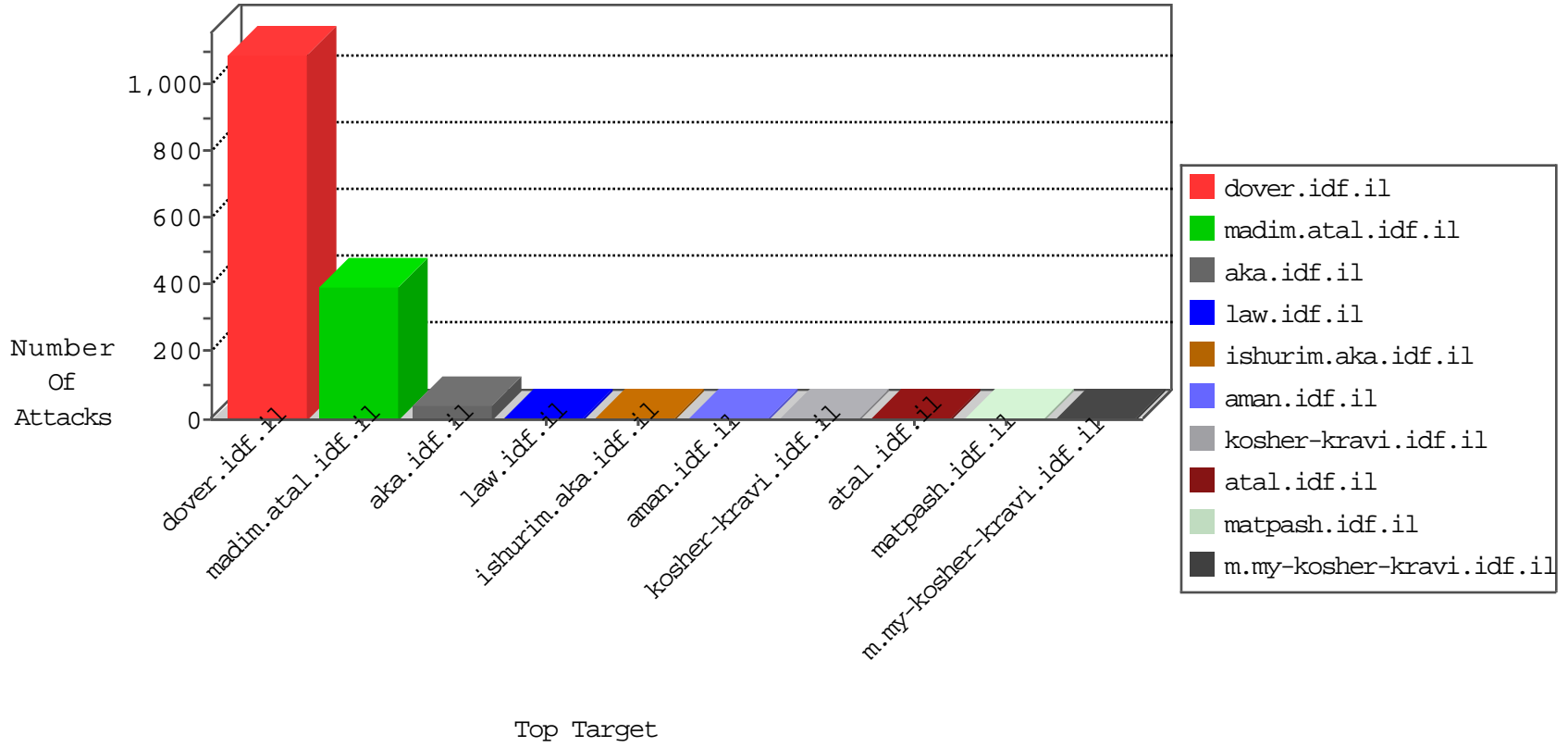


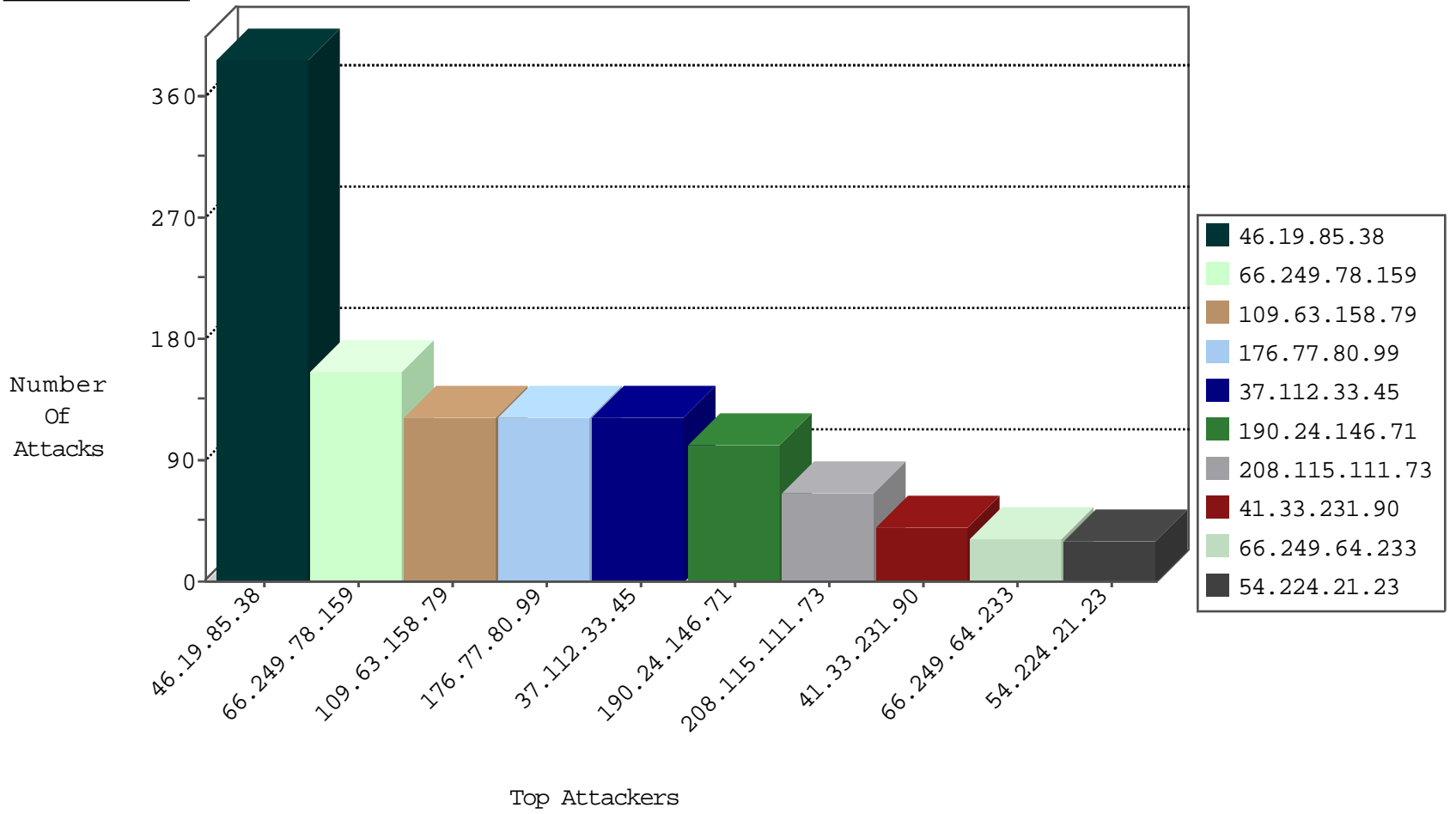
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.190	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	351
66.249.66.125	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	118
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
80.246.136.80	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
142.4.193.203	United States	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
104.192.0.226	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
42.159.26.35	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
42.159.26.35	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.127.194.190	147.237.8.24	Philippines	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.126.13	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
42.159.26.35	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
42.159.26.35	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
42.159.26.35	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
27.211.15.50	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.185.238.118	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
42.159.26.35	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	148
176.77.80.99	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
109.63.158.79	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
37.112.33.45	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
95.25.11.184	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.67.142.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
24.179.71.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
24.184.79.229	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
105.227.60.140	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.121.94.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.228.118.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.13.14.100	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.179.18.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.166.114.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.55.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
83.253.193.29	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
131.253.25.249	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
40.77.167.63	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.183.38.219	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.167.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
99.225.79.83	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.181.202.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.3.212.18	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.2.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
173.252.80.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.117.171.106	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	3
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.136	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.30.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.171.106	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.38	Block	239
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.38	Block	36
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
37.142.243.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.22.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.67.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
46.166.188.247	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/size220x0/17543.jpg	Block	1
88.75.61.15	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/government/pages/health.aspx	Block	1
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	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8935-he/refuah.aspx	Block	1
150.70.173.42	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation pageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
61.135.190.200	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/3/size220x0/17543.jpg	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
150.70.173.42	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.63	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.180.172.130	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9301-he/dover.aspx	Block	1
64.141.114.31	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/1/size220x0/17281.jpg	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1415-he/dover.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
188.106.104.39	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
82.166.114.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
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	1
46.19.85.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Double URL Encoding - parameter: in www.idf.il/hebrew/organization/patzar/atar1/mls1/pirsumim/journal/15%5caviram15.doc	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17281.jpg	Block	1
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
84.94.171.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1