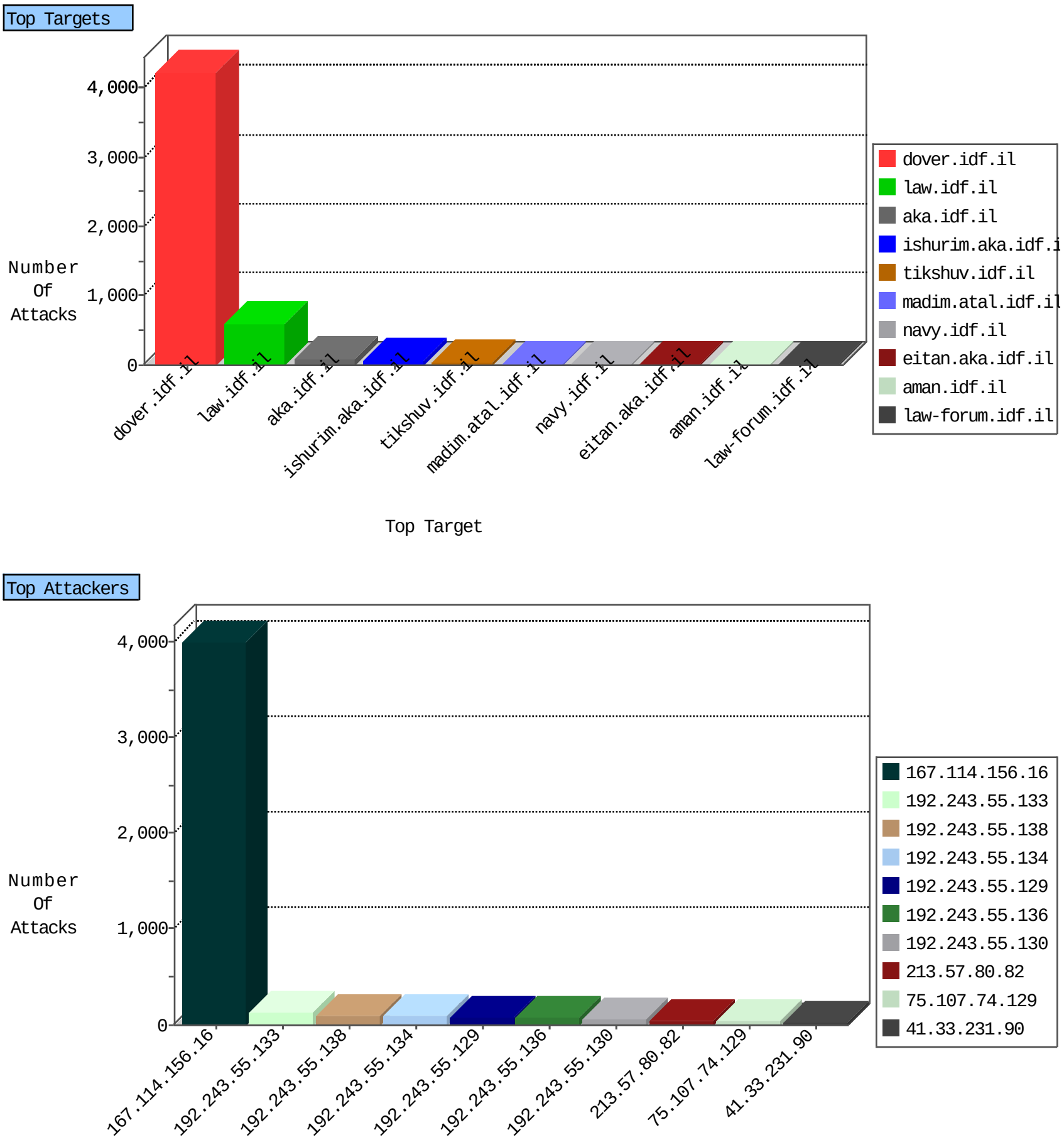
04-13-2016-00:04:05 to 04-13-2016-01:04:05

IDF Under Attack Daily Report



04-13-2016-00:04:05 to 04-13-2016-01:04:05

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	Block_Ip_Web_In	drop	4012
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	76
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
69.30.226.219	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
74.91.18.44	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
69.30.226.220	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
74.91.18.45	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.30.226.221	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
74.91.20.197	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
66.85.80.26	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
74.91.18.42	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
84.108.111.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
158.130.6.191	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
158.130.6.191	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1

04-13-2016-00:04:05 to 04-13-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.247.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.38.241.150	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
61.135.189.98	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
80.91.162.99	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.121.188	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.121.188	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-00:04:05 to 04-13-2016-01:04:05

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
163.172.140.23	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
114.35.125.220	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.161.10	147.237.72.14	China	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.24.40.78	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.153.46.212	147.237.72.156	Qatar	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
124.105.19.42	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.184.2.29	147.237.76.196	Japan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

04-13-2016-00:04:05 to 04-13-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.80.82	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	48
75.107.74.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	30
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	26
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	14
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
37.46.39.93	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
162.243.25.240	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.67.18.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
46.19.85.97	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.140	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
197.27.91.134	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
197.27.91.134	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.33.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.53.19.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.60.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
42.96.140.102	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 42.96.140.102	Block	1
109.64.4.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
69.30.226.220	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
66.249.66.167	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/print.css	Block	1
192.243.55.134	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem	Block	1
79.177.231.228	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/71706.pdf	Block	1
42.96.140.102	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.253.199.232	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
69.30.226.221	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
66.249.66.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/style/shared/960.css	Block	1
198.58.103.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
83.130.101.105	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
124.73.11.78	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-he/idfg.aspx/trackback/	Block	1
74.91.18.42	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
83.130.101.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
62.16.68.192	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
74.91.18.45	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
89.138.163.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1409-he/atal.aspx	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
66.249.65.20	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.91.20.197	United States	147.237.72.167	ishurim.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1