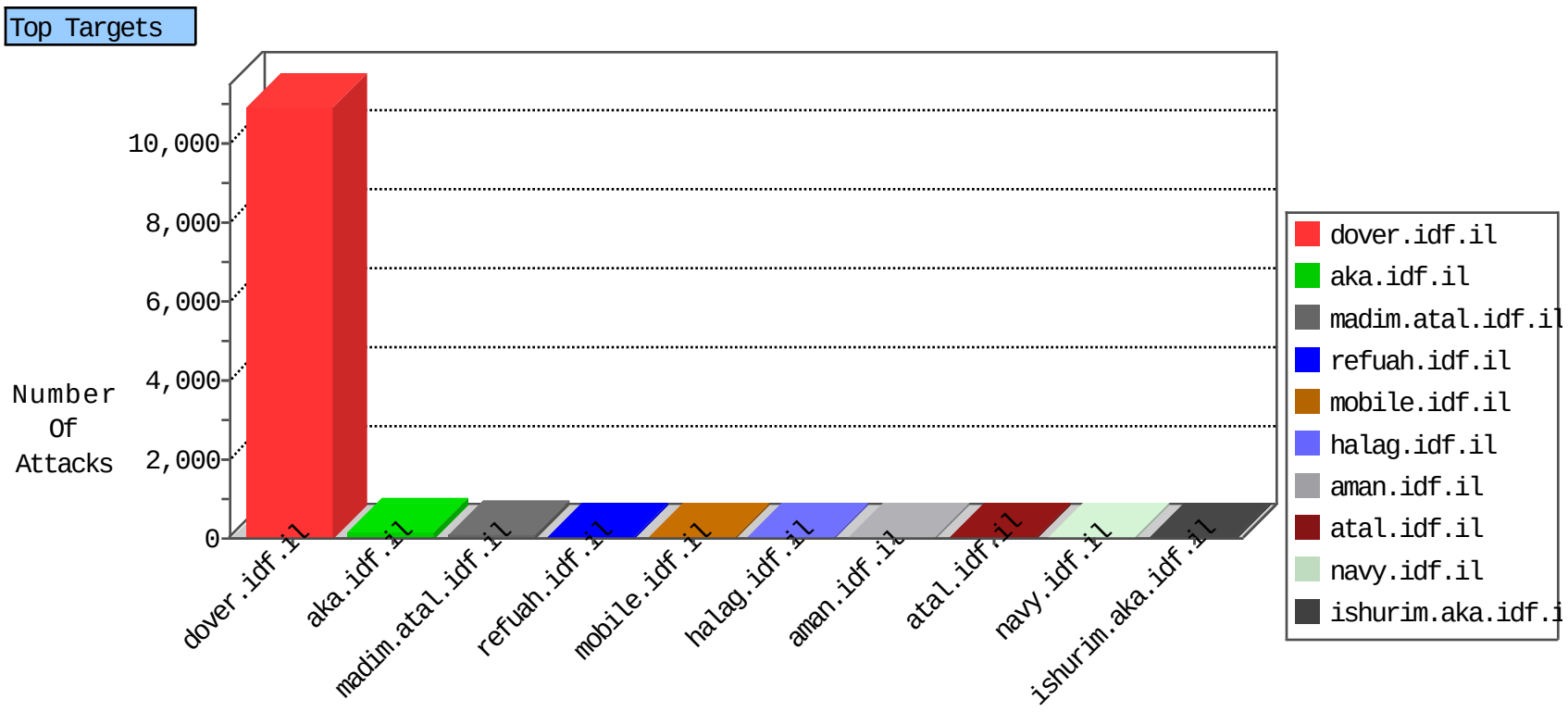
04-27-2016-17:04:05 to 04-27-2016-18:04:05

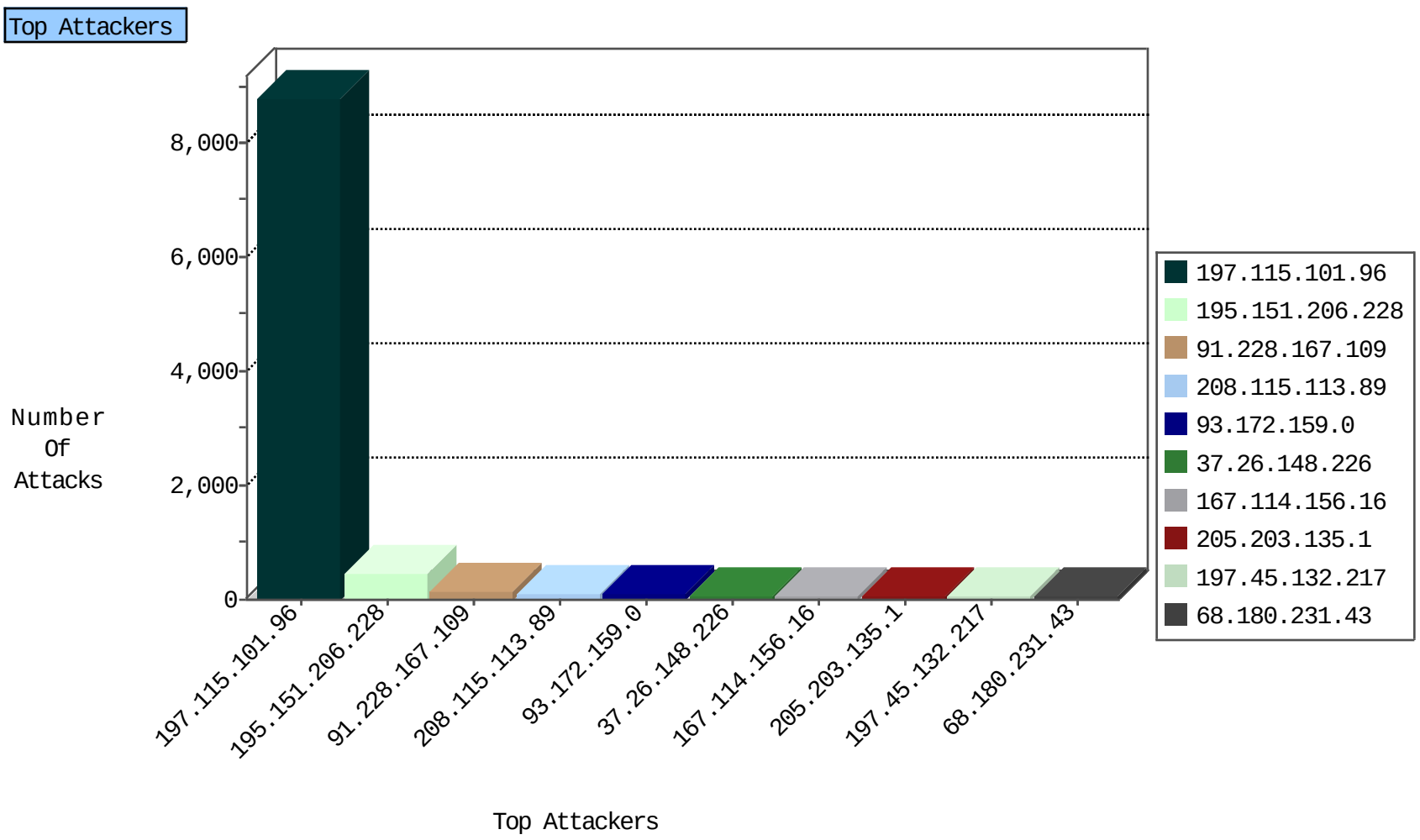
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-27-2016-17:04:05 to 04-27-2016-18:04:05

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	TCP handshake violation, first packet not syn	drop	3457
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2646
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1510
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	677
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	13
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
180.157.15.150	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
108.7.152.220	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2
123.171.174.64	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
117.57.60.139	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.49.116	Netherlands	147.237.76.39	mobile.meitav.idf.i	Block_Ntp_All_Net	drop	1
117.90.97.26	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
222.174.213.195	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
182.202.27.0	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
112.12.187.176	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
125.90.244.142	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
82.102.199.46	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-27-2016-17:04:05 to 04-27-2016-18:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.220.63.148	Korea, Republic of	147.237.77.233	atal.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-27-2016-17:04:05 to 04-27-2016-18:04:05

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
84.94.235.121	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.214.249.150	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
80.82.78.38	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
46.19.85.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.220.63.148	147.237.77.233	Korea, Republic of	atal.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
202.115.30.83	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
177.9.12.3	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.71.75.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
78.139.8.198	147.237.8.28	Hungary	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
213.151.45.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
202.115.30.83	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.100.128	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
195.216.176.244	147.237.8.50	Latvia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.132	147.237.77.176	Japan	matpash.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-27-2016-17:04:05 to 04-27-2016-18:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4929
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	drop		drop	2458
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	706
195.151.206.228	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	453
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
37.26.148.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.152.1.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
176.31.117.76	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
93.80.165.230	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
192.206.203.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
46.19.86.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
91.228.167.38	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
85.250.157.239	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
198.100.144.55	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
88.198.157.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
107.77.68.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.133.178.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
73.37.30.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.115	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	alert	12
69.137.40.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.115	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.116.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
204.237.2.151	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.238	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

04-27-2016-17:04:05 to 04-27-2016-18:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.159.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.228.244.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
149.78.84.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	2
2.53.42.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
71.6.146.185	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1316-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
157.55.39.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
87.69.89.8	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
77.75.76.165	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/29/	Block	1
46.117.24.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.64.26.109	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/extras	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/buttonback.png	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.120.154.10	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
87.70.103.156	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.75.79.11	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
65.55.210.12	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.29.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
195.151.206.228	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/russian/	Block	1
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1117-he/nakhal.aspx	Block	1
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.86.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.186.113.132	Japan	147.237.77.176	matpash.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
80.246.130.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3241.jpg	Block	1
149.88.189.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
85.250.157.239	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

04-27-2016-17:04:05 to 04-27-2016-18:04:05