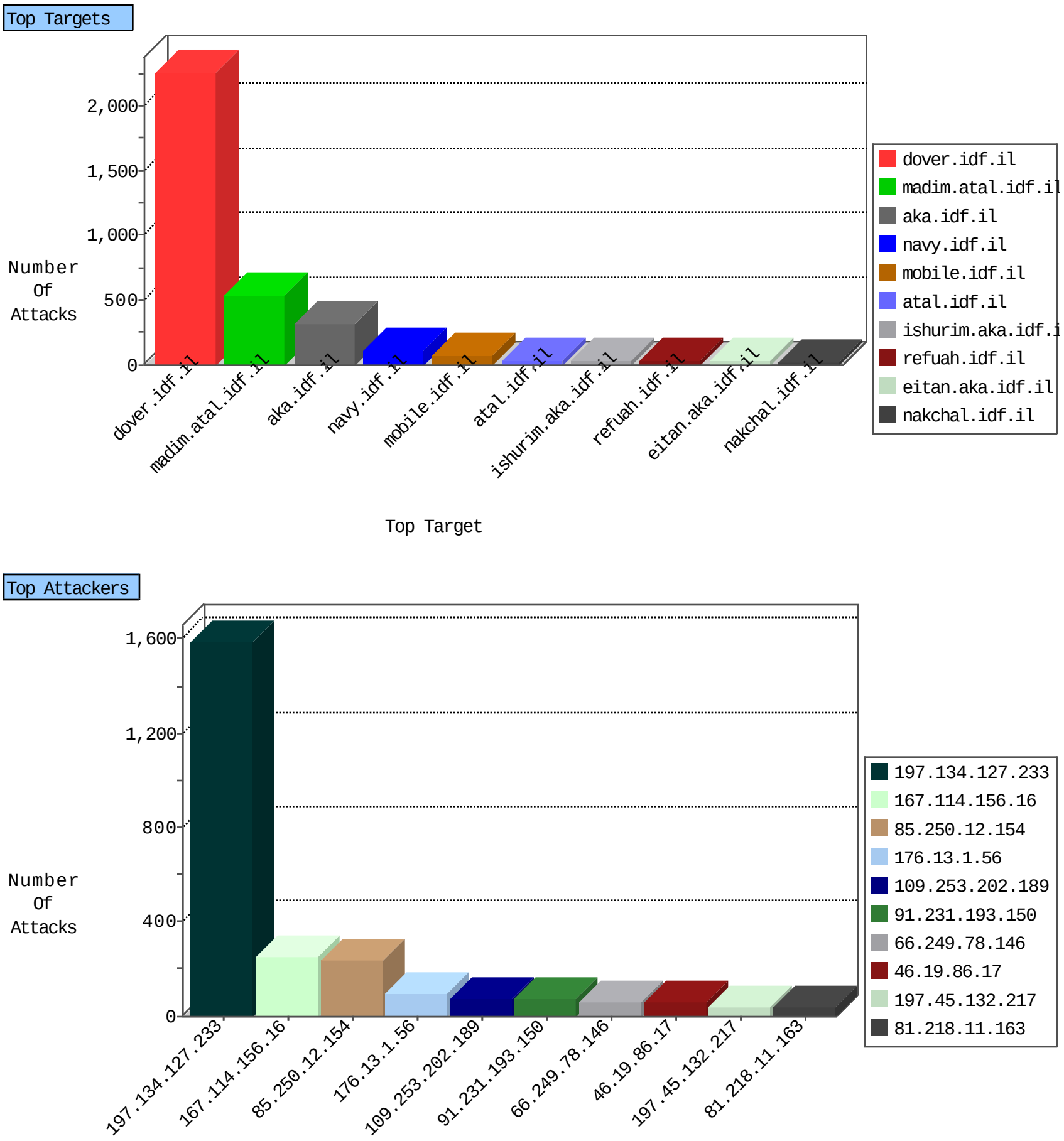
05-03-2016-09:04:04 to 05-03-2016-10:04:04

IDF Under Attack Daily Report



05-03-2016-09:04:04 to 05-03-2016-10:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	9938
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	754
109.253.202.189	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	356
91.231.193.150	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	41
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
197.134.127.233	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
180.97.106.161	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
39.116.82.215	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.52	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.216.48	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.216.49	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.52	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-09:04:04 to 05-03-2016-10:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-09:04:04 to 05-03-2016-10:04:04

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	3
46.19.85.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
109.65.97.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.36.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.84.62	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.32.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.43.69	147.237.76.31	Israel	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.74	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
194.56.215.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
128.127.0.45	147.237.0.17	Italy	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
109.64.33.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.4.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.21.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-09:04:04 to 05-03-2016-10:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.134.127.233	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1584
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
91.231.193.150	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	46
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
178.20.190.202	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
81.218.11.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.246.133.86	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
81.218.11.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
58.8.156.74	Thailand	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.179.132.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.81.223	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.202.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.165.251.68	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.26.146.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.166.240.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
91.231.193.150	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.166.240.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
167.220.196.107	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
182.184.79.28	Pakistan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.231.193.150	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.166.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.166.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.27.106.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.222	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
80.179.202.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.227.147	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.222	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.11.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.117.64.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.9.48.215	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

05-03-2016-09:04:04 to 05-03-2016-10:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.12.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	235
176.13.1.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
109.253.202.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
80.246.139.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
217.132.146.48	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	19
2.53.176.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	12
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	6
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	6
2.53.42.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	4
80.246.136.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.146.48	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	3
80.246.136.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.206.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.13.214	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
46.19.85.27	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
37.26.148.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
116.247.85.130	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
2.53.151.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/fə	Block	2
117.18.0.21	Hong Kong	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
95.86.79.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
2.55.173.35	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.172	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
51.255.65.94	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
37.26.149.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	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
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
123.125.71.79	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1613.jpg	Block	1
46.19.85.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
109.65.29.19	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
2.55.173.182	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.117.143.250	Block	1
171.96.172.159	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/patzar/home/default.asp	None	1
54.146.25.95	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
116.247.85.130	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
213.191.229.163	Ireland	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
194.90.99.193	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/images/shared/mailthisclose.png	Block	1
141.212.122.145	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
5.153.233.130	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
212.117.143.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
54.153.104.111	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/home.asp	Block	1
37.46.43.69	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
117.18.0.21	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 117.18.0.21	Block	1

05-03-2016-09:04:04 to 05-03-2016-10:04:04