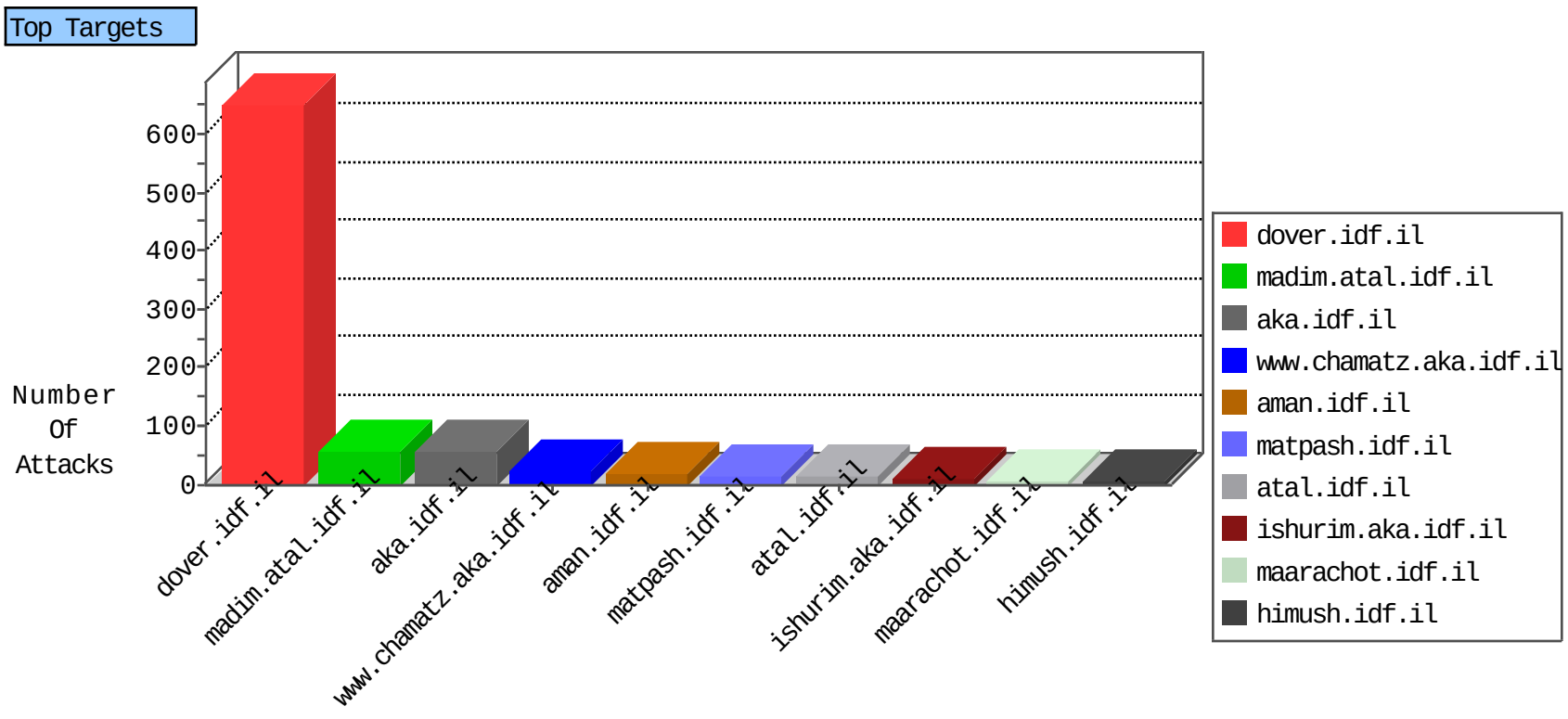
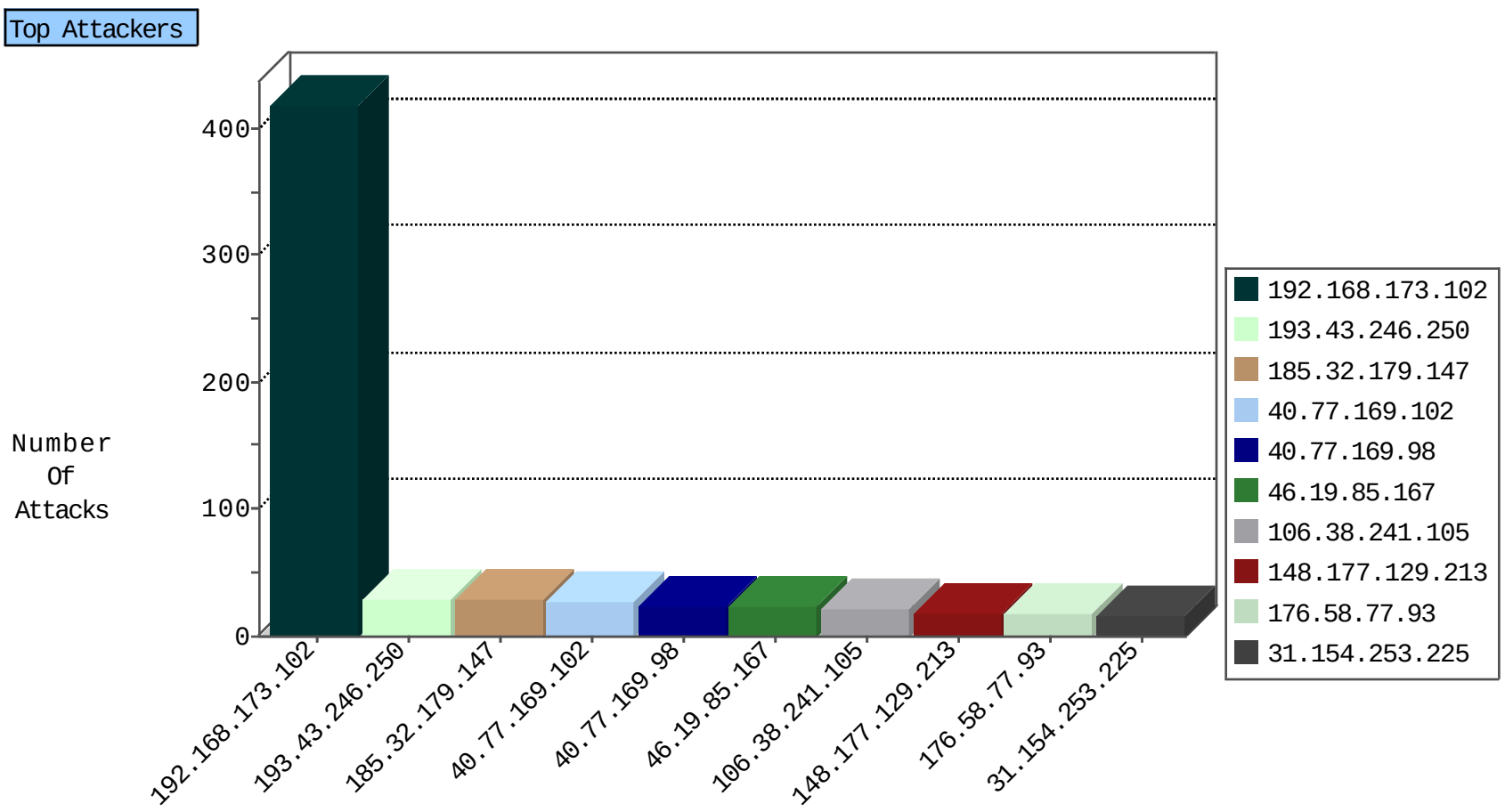
08-25-2016-12:04:07 to 08-25-2016-13:04:07

IDF Under Attack
Daily Report



Top Target



Top Attackers

08-25-2016-12:04:07 to 08-25-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.58.77.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13
176.13.226.216	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
77.126.4.151	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
95.6.43.153	Turkey	147.237.72.217	e.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
104.148.55.162	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
212.150.189.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
157.56.2.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.95.106	Netherlands	147.237.76.200	eitan.aka.idf.i	Black List	drop	1

08-25-2016-12:04:07 to 08-25-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.i	C1000071: HTTP: User Agent Sogou+web+spider	Permit	18
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
5.9.63.149	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	1
85.110.245.47	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
85.110.245.47	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

08-25-2016-12:04:07 to 08-25-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.68.31.27	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
66.203.215.242	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -f -sS	1
87.71.41.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
8.26.94.207	147.237.72.167	Canada	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.121.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.16.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.60.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.11.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.7.217.212	147.237.76.196	Brazil	e.sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.181.99.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.0.190.173	147.237.72.166	Colombia	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.137.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.23.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.26.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
89.138.154.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.203.215.242	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.62.0	147.237.77.176	Israel	matpash.idf.il	ET SCAN NMAP -sA (2)	1
46.172.71.251	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.184.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.67.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.15.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.77.178	Chile	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.201.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.224.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.239.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
161.18.114.136	147.237.76.42	Colombia	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.178.107.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.208.21.66	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.84.3	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
94.70.251.123	147.237.0.17	Greece	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.203.215.242	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 2048	1
89.138.125.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-12:04:07 to 08-25-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	418
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
148.177.129.213	Europe	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	18
31.154.253.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.58.77.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
91.197.103.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.102	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
84.94.67.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.120.135.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
62.0.238.55	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
176.13.0.153	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
84.94.67.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.53	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	3
195.212.29.184	Europe	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.209.18	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
105.105.79.48	Algeria	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
2.54.105.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.222.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
89.139.101.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.178.237.141	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.76	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
109.253.220.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.233.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.157.252	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
109.253.194.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
109.253.223.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.86.111	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
185.143.40.68		147.237.77.121	e.navy.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-12:04:07 to 08-25-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.86.24	Block	8
2.53.27.79	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
80.246.133.188	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	5
37.59.62.43	France	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	5
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
72.203.203.50	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.232.54.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.156.114	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.216.145	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
46.19.86.111	Israel	147.237.77.233	atal.idf.il	Distributed Malformed URL	Block	2
212.179.215.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
176.13.10.250	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
108.165.2.29	United States	147.237.76.86	navy.idf.il	Multiple Malformed URL from 108.165.2.29	Block	1
46.19.86.60	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.139.12	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslul.aspx?catid=60353&docid=72291	Block	1
199.203.84.84	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
46.19.86.111	Israel	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 46.19.86.111	Block	1
157.55.39.173	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
108.165.2.29	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Malformed URL from 108.165.2.29	Block	1
77.125.81.135	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.120.65.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
108.165.2.29	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
80.178.102.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
204.79.180.229	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
66.249.69.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1882	Block	1
46.19.86.111	Israel	147.237.77.233	atal.idf.il	Multiple Illegal HTTP Version from 46.19.86.111	Block	1
108.165.2.29	United States	147.237.0.19	madim.atal.idf.il	Distributed Malformed URL	Block	1
77.139.74.137	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
192.116.165.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
62.219.99.130	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/108971.pdf	Block	1
109.253.144.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.19.86.111	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
2.55.43.76	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
207.46.13.111	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/article4.aspx	Block	1
66.249.69.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
46.19.86.111	Israel	147.237.77.233	atal.idf.il	Multiple Unknown HTTP Request Method from 46.19.86.111	Block	1
157.55.39.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
108.165.2.29	United States	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.102.9.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim/	Block	1
147.236.238.22	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
84.94.26.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.99	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/4/394.pdftextgreater	Block	1

08-25-2016-12:04:07 to 08-25-2016-13:04:07