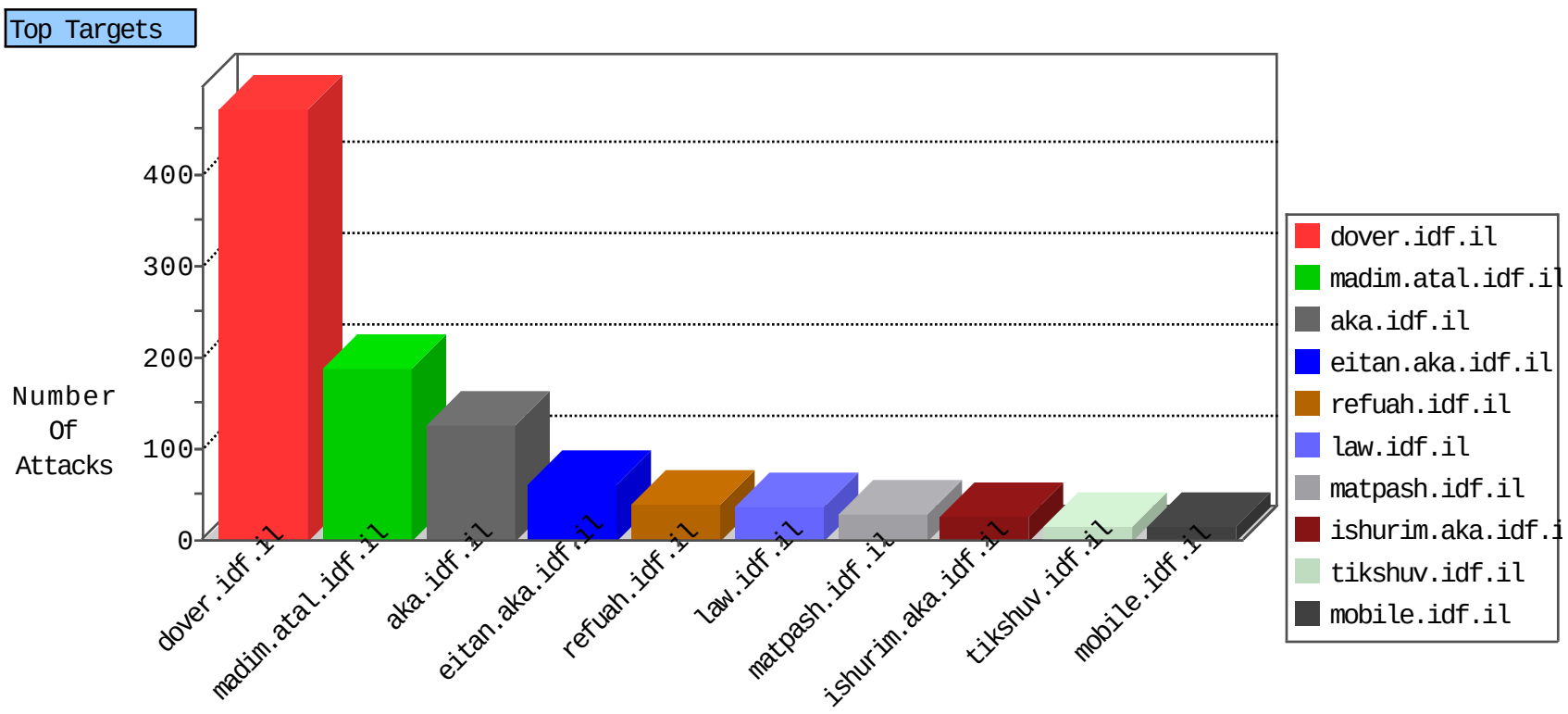
04-20-2016-20:04:03 to 04-20-2016-21:04:03

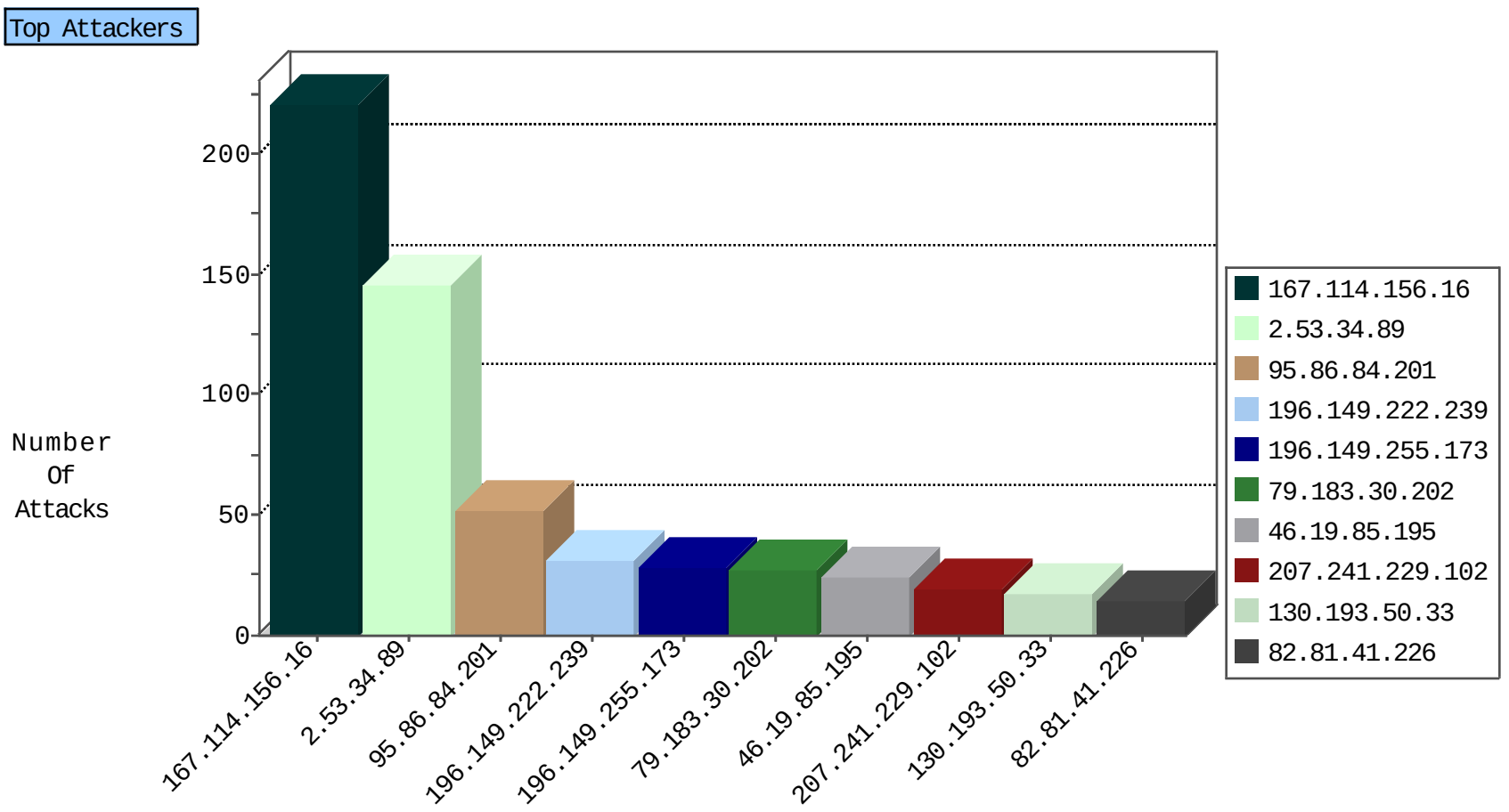
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-20-2016-20:04:03 to 04-20-2016-21:04:03

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	10973
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	6443
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	86
120.132.50.135	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
69.30.198.146	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
74.91.18.46	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
107.150.46.35	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
69.30.226.100	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
179.43.141.214	Switzerland	147.237.76.30	himush.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
74.91.20.194	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
107.150.46.34	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
74.91.17.180	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1

04-20-2016-20:04:03 to 04-20-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-20:04:03 to 04-20-2016-21:04:03

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
109.57.96.106	147.237.77.216	Denmark	dover.idf.il	Xenu Link Sleuth User Agent	2
198.54.90.200	147.237.76.31	United States	nakchal.idf.il	Tehila - Perl LWP with fake user agent	2
93.174.95.124	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.45.137.76	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
219.159.82.24	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
13.82.25.17	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
219.159.82.24	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.214	147.237.0.19	Switzerland	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.252.74.110	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
66.223.201.10	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
219.159.82.24	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
40.69.45.42	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
219.159.82.24	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.22.135.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
189.57.81.51	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.13.22.218	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
118.200.72.142	147.237.0.35	Singapore	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-20-2016-20:04:03 to 04-20-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.86.84.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
196.149.222.239	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
196.149.255.173	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
79.183.30.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	19
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.152.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.177.152.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
207.46.13.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
81.218.184.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.55.38.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.115.220	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.208	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.223.195.2	Botswana	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.176.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.176.101.57	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.143	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
176.13.22.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.106	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
85.65.81.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
176.13.22.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.8.102.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
158.140.1.28	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.129.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.33.122.163	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.88.78	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.214.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.184.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.83.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.106.75.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-20-2016-20:04:03 to 04-20-2016-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.34.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
80.246.136.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
82.81.41.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
80.246.136.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
64.233.173.41	Asia/Pacific Region	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.44.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.97.140	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
188.161.12.150	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	2
69.30.198.146	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
46.19.86.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/mobile	Block	1
149.50.12.164	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
31.44.133.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.183.30.202	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.106	Israel	147.237.77.176	matpash.idf.il	Abnormally Long Request request version	Block	1
207.46.13.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.111.94.77	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
71.199.122.157	United States	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/14-en/patzar.aspx	Block	1
157.55.39.120	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
64.233.173.46	Asia/Pacific Region	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.106	Israel	147.237.77.176	matpash.idf.il	Illegal HTTP Version _pk_id.21.b50e=4696f97ea27872db.1461171974.1.1461171974.1461171974.; _pk_ses.21.b50e=*	Block	1
213.8.204.13	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
93.172.247.43	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
71.199.122.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
46.120.20.176	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.120.20.176	Block	1
159.220.233.7	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
40.77.167.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/forgotpassword.aspx	Block	1
64.233.173.51	Asia/Pacific Region	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.106	Israel	147.237.77.176	matpash.idf.il	Malformed URL __atuvs=5717b70455cb096a000;	Block	1
213.57.183.64	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
95.86.120.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.120.227	Block	1
2.53.157.172	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
74.91.18.46	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.ps780.com/	Block	1
46.120.20.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
40.77.167.94	United States	147.237.72.166	aka.idf.il	Unknown Parameter 9ff3fe30 in www.aka.idf.il/main/home/default.aspx	None	1
176.13.22.218	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
2.53.18.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4546.pdf	Block	1
46.19.85.106	Israel	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method tuvc=1%7C16; in URL __atuvs=5717b70455cb096a000	Block	1
213.57.246.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
95.86.120.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/drushim/	Block	1
74.91.20.194	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.ps780.com/	Block	1
46.121.209.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
40.77.167.94	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
2.53.19.218	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

04-20-2016-20:04:03 to 04-20-2016-21:04:03