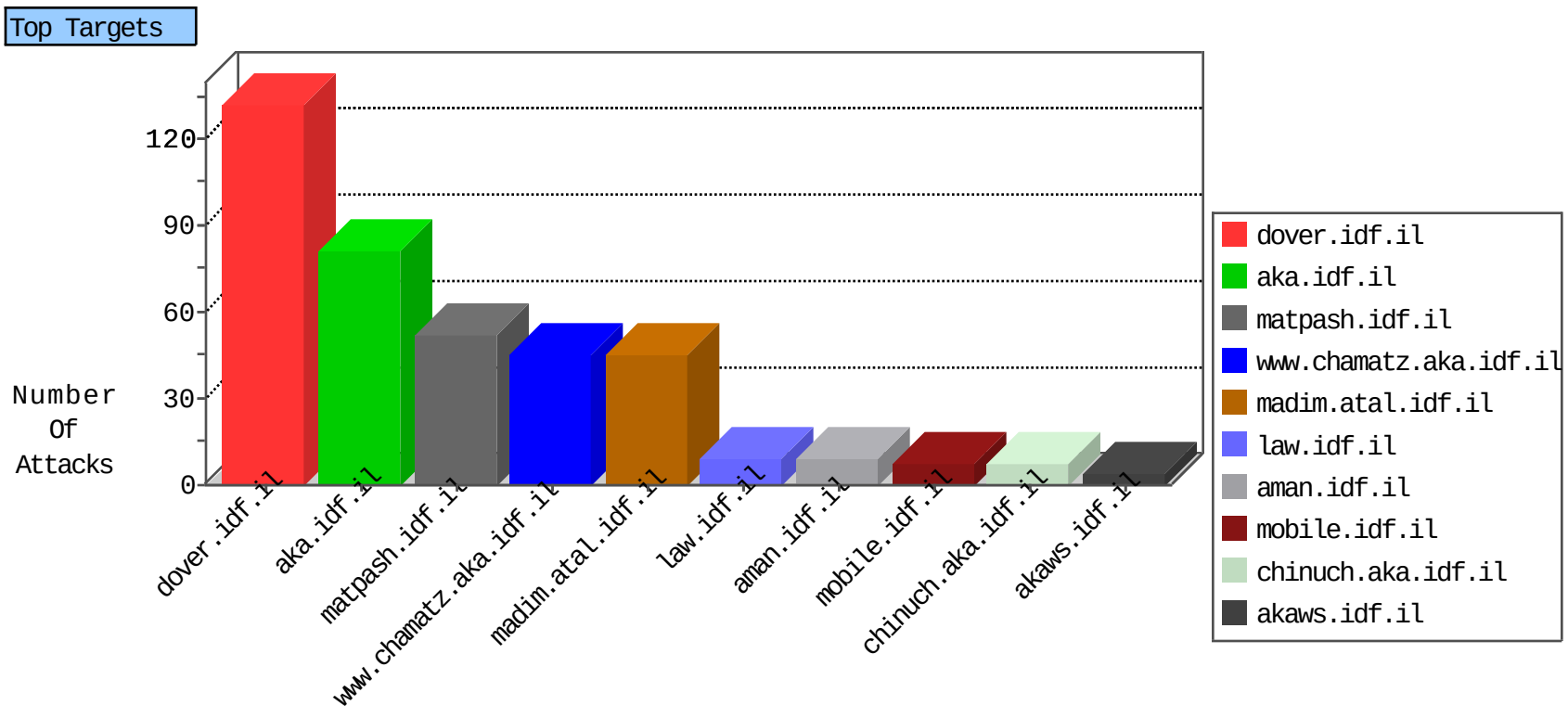
08-25-2016-15:04:00 to 08-25-2016-16:04:00

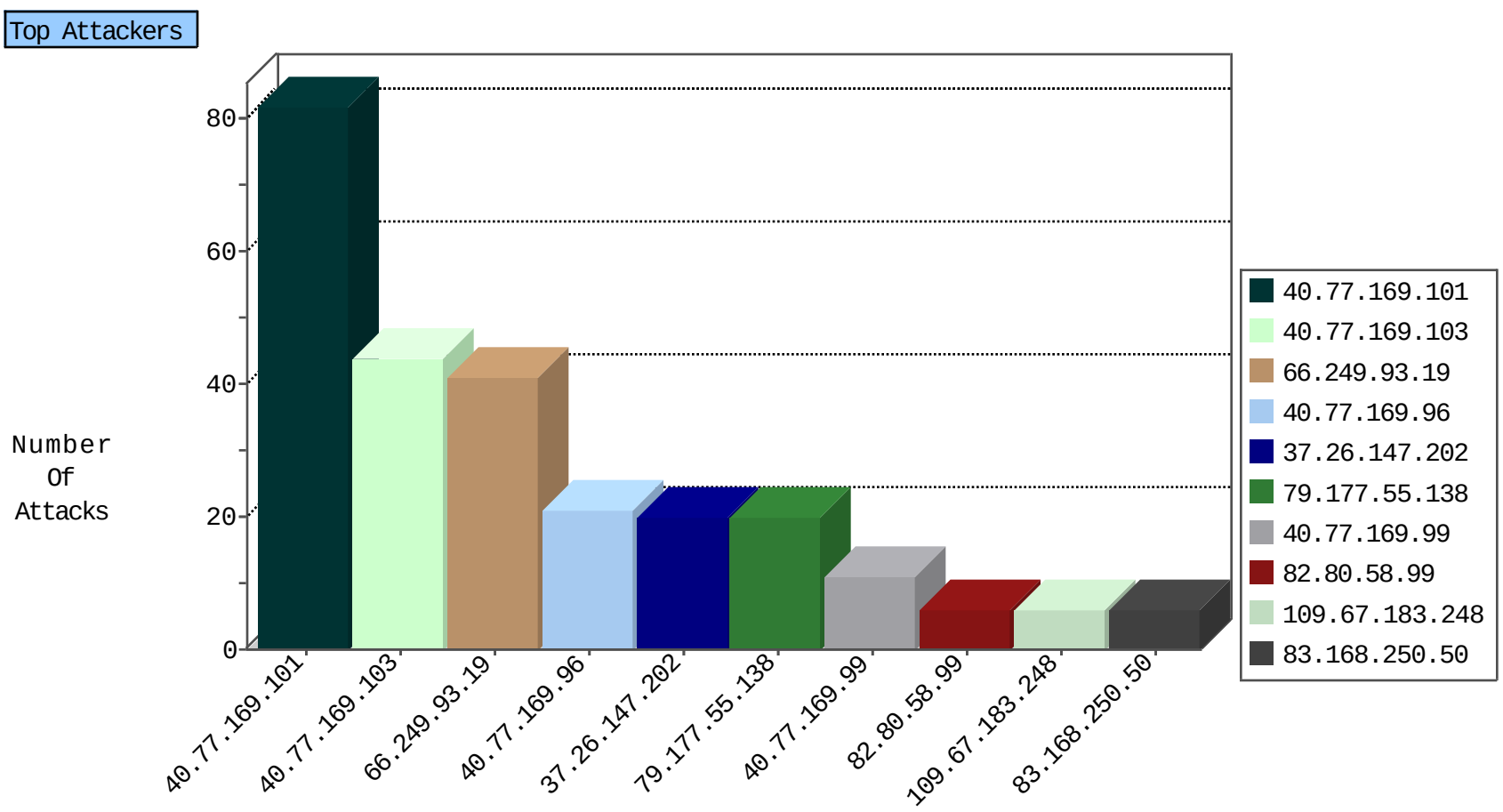
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-25-2016-15:04:00 to 08-25-2016-16:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.183.248	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	6
62.219.25.21	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
120.132.50.135	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
199.203.37.52	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1
93.174.95.106	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
176.13.244.204	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.136.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
192.81.135.222	United States	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
192.162.101.50	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-25-2016-15:04:00 to 08-25-2016-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

08-25-2016-15:04:00 to 08-25-2016-16:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.19	147.237.77.226	Europe	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	41
93.174.91.29	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.238	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.1.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.105.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.121.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.45.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.133.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
71.231.47.109	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
203.4.240.101	147.237.77.121	Australia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
189.106.200.15	147.237.77.216	Brazil	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
65.156.199.242	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
176.67.60.183	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
46.227.67.172	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
154.73.162.30	147.237.77.216	Chad	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.15.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.91.29	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.9.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.67.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
1.125.48.197	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.51.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.64.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
190.252.106.198	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.203.215.242	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
185.56.80.144	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.46.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.129.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.210.138.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-25-2016-15:04:00 to 08-25-2016-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	43
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	23
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
82.80.58.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.130.6.49	Lithuania	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	6
83.168.250.50	Sweden	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
185.120.125.16	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.207.60.229	Netherlands	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
192.10.10.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.64.121.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.37.222.199	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
176.77.24.122	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
91.227.165.5	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
212.150.82.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.5.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.67.59.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.82	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
46.19.86.138	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.11.181	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.253.133.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.200	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
87.70.48.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
62.0.213.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
195.154.14.134	France	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.164	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
91.227.164.5	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.67	United States	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
141.212.122.165	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
66.249.65.50	Israel	147.237.0.33	idf.il	drop		drop	1
184.105.139.71	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
192.10.10.182	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.2.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-15:04:00 to 08-25-2016-16:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
79.177.55.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.53.179.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
108.171.128.166	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 108.171.128.166	Block	4
77.139.197.79	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	3
79.180.235.127	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
77.239.224.35	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.13.13.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.78.123	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.125.13.23	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
46.19.86.138	Israel	147.237.72.167	ishurim.aka.idf.il	Double URL Encoding - parameter: rdfrom in www.ishurim.aka.idf.il/1050-he/pickcertificates.aspx	Block	1
109.186.93.41	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
2.53.190.118	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
79.180.235.127	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.180.235.127	Block	1
66.249.76.67	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
207.46.13.164	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/maslulim/leftarrowdisabled.gif	Block	1
108.171.128.166	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
46.19.86.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.74.169.115	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/113098.pdf	Block	1
2.55.46.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/home	Block	1
71.6.146.185	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/robots.txt	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.199.71.30	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
5.29.91.16	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.180.235.127	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/2/	Block	1
77.125.13.23	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.13.23	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
109.67.186.235	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113575.pdf	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
5.102.254.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
176.13.3.108	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.243.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdate Question in www.aka.idf.il/main/giyus/faq.aspx	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
109.186.93.41	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
79.177.171.193	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
37.26.146.144	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.210.170	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1

08-25-2016-15:04:00 to 08-25-2016-16:04:00