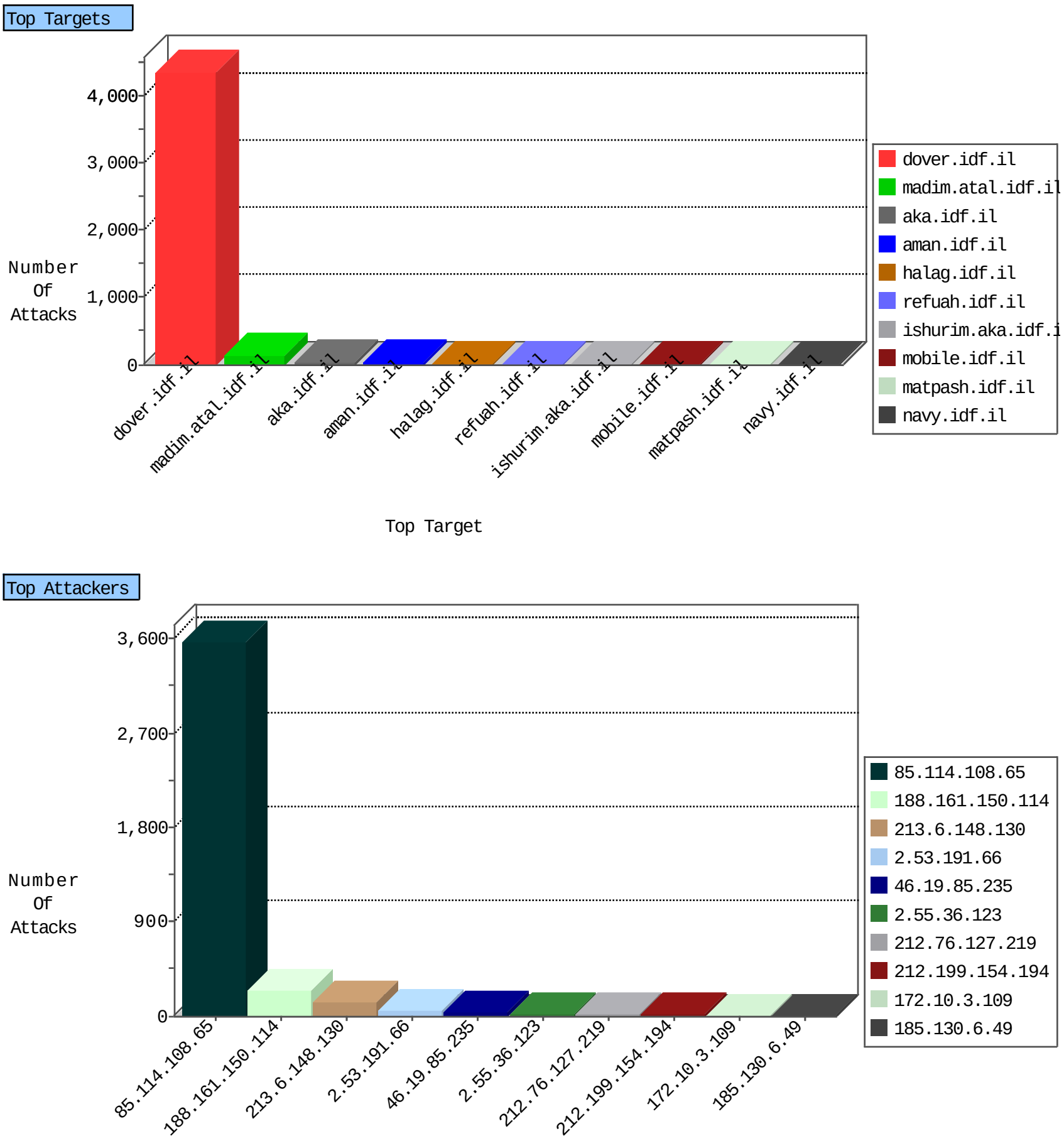
08-23-2016-09:04:05 to 08-23-2016-10:04:05

IDF Under Attack Daily Report



08-23-2016-09:04:05 to 08-23-2016-10:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	11596
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4517
212.199.154.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	247
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	151
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	91
212.76.127.219	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	25
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	22
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	16
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	13
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11
156.205.43.56	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	5
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
104.237.146.124	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	3
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	1
176.13.227.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
123.249.0.134	China	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.i	Black List	drop	1
148.251.136.8	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
86.59.4.133	Austria	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	1

08-23-2016-09:04:05 to 08-23-2016-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.132.212.167	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	2
144.76.12.75	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	2
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
164.132.161.91	Italy	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-23-2016-09:04:05 to 08-23-2016-10:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3
85.114.108.65	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	Tehila - Perl LWP with fake user agent	3
188.161.150.114	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
85.114.108.65	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
62.210.148.91	147.237.76.200	France	eitan.aka.idf.i	ET WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability	1
37.26.147.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.238.226.157	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.151.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.114.108.65	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
85.114.108.65	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	SERVER-IIS scripts-browse access	1
85.114.108.65	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	GPL EXPLOIT formmail access	1
79.181.113.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.124.11.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.24.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.53.196	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.5.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.196.110.125	147.237.72.166	Romania	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.103.48	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1

08-23-2016-09:04:05 to 08-23-2016-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	993
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
172.10.3.109	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.130.6.49	Lithuania	147.237.77.234	halag.idf.il	drop	SAM rule	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
100.92.122.16		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.166.40.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.134.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.49.68.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
100.92.119.109		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
109.253.241.157	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
80.178.210.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
64.47.85.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.44.132.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.210.242.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.249.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.138.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.4.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.1.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.43.120.15	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.2.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.210.188.85	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.208.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.137.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
80.178.138.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.156.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.129.190	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.202.74	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-09:04:05 to 08-23-2016-10:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.114.108.65	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.114.108.65	Block	932
188.161.150.114	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.150.114	Block	194
213.6.148.130	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.6.148.130	Block	106
2.53.191.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.55.36.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.149.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.230.137	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
80.246.138.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.244.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	3
2.53.182.57	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
79.177.54.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.228.248.251	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1571.jpg	Block	1
77.138.2.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
84.94.41.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.179.155.26	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.200.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
85.64.60.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
62.219.118.68	Israel	147.237.72.166	aka.idf.il	Unauthorized Request Content Type text/ping	Block	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
193.188.70.138	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
219.75.81.93	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.168.196.25	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
80.246.138.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.39	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
2.53.28.57	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
89.237.106.63	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.210.188.85	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.132.156.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.246.139.25	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.179.42.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

08-23-2016-09:04:05 to 08-23-2016-10:04:05