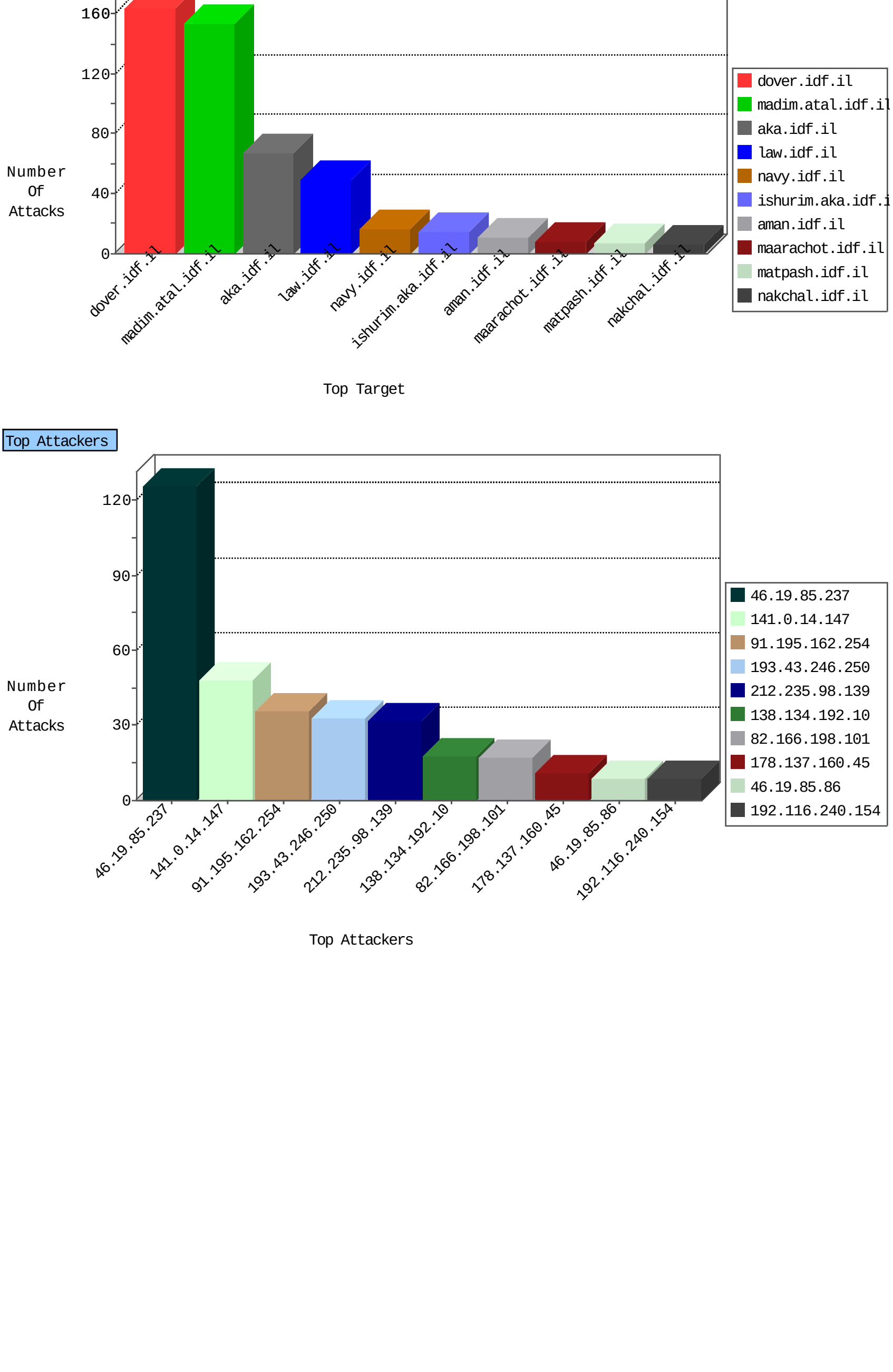
08-21-2016-14:04:04 to 08-21-2016-15:04:04

IDF Under Attack Daily Report



08-21-2016-14:04:04 to 08-21-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.198.101	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
107.150.53.170	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
121.52.223.228	China	147.237.77.179	e.mazi.idf.il	JLM_Purple_Con_Limit_Http	drop	1
62.90.16.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
172.98.67.35	Canada	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

08-21-2016-14:04:04 to 08-21-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.137.160.45	Ukraine	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Permit	7
178.137.160.45	Ukraine	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Permit	4
5.9.87.111	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.19	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
213.57.80.226	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.107	France	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-14:04:04 to 08-21-2016-15:04:04

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	2
91.125.184.101	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
82.81.73.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.54.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
213.6.3.25	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.0.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.65.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.82.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.76.176	United States	test.ncore.idf.il	ET DROP Dshield Block Listed Source	1
80.246.133.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.94	147.237.72.166	Europe	aka.idf.il	portscan: TCP Distributed Portscan	1
122.72.53.188	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.66.52.121	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.215.60.214	147.237.0.17	Spain	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.55.153.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.37.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.30.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.121.220.181	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
212.25.102.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.121.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.150.38.110	147.237.77.243	Mexico	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
192.117.174.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.124.27.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.20.106.62	147.237.72.166	Iran, Islamic Republic of	aka.idf.il	portscan: TCP Distributed Portscan	1
61.163.35.221	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
109.67.124.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.227.17.3	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
46.19.85.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-21-2016-14:04:04 to 08-21-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.14.147	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	48
91.195.162.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
138.134.192.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
82.166.198.101	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.86	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
95.35.146.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.116.240.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.16.67.249	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.136.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.150.232	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.164.116	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.64.165.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.130.249.166	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.237.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.192.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
109.253.205.251	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.166.198.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
134.191.232.68	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.1.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.50	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-21-2016-14:04:04 to 08-21-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
46.19.85.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
37.26.149.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
217.132.61.200	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7
80.246.136.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.199.224.24	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	5
62.90.100.121	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	4
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
72.9.148.10	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
212.150.83.94	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.83.94	Block	2
89.139.102.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.11.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.86.87.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.226.15.48	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
62.90.100.121	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.90.100.121	Block	1
212.179.21.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
5.28.171.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.116.240.154	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20477-he/dover.aspx	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/	Block	1
157.55.39.145	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
62.90.100.121	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/atuda/atuda.aspx	Block	1
212.179.226.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
8.37.225.174	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/	None	1
82.166.84.16	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: catId%5Cu003d58624 in www.aka.idf.il/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.138.173.202	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.102.9.19	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	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
52.16.137.212	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
212.150.83.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
2.53.34.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.139.203.85	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/links.asp	Block	1
213.8.53.102	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
37.46.41.196	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
212.150.167.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyushttps:/main/home/default.aspx	Block	1
2.53.191.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.116.96.192	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.239.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

08-21-2016-14:04:04 to 08-21-2016-15:04:04