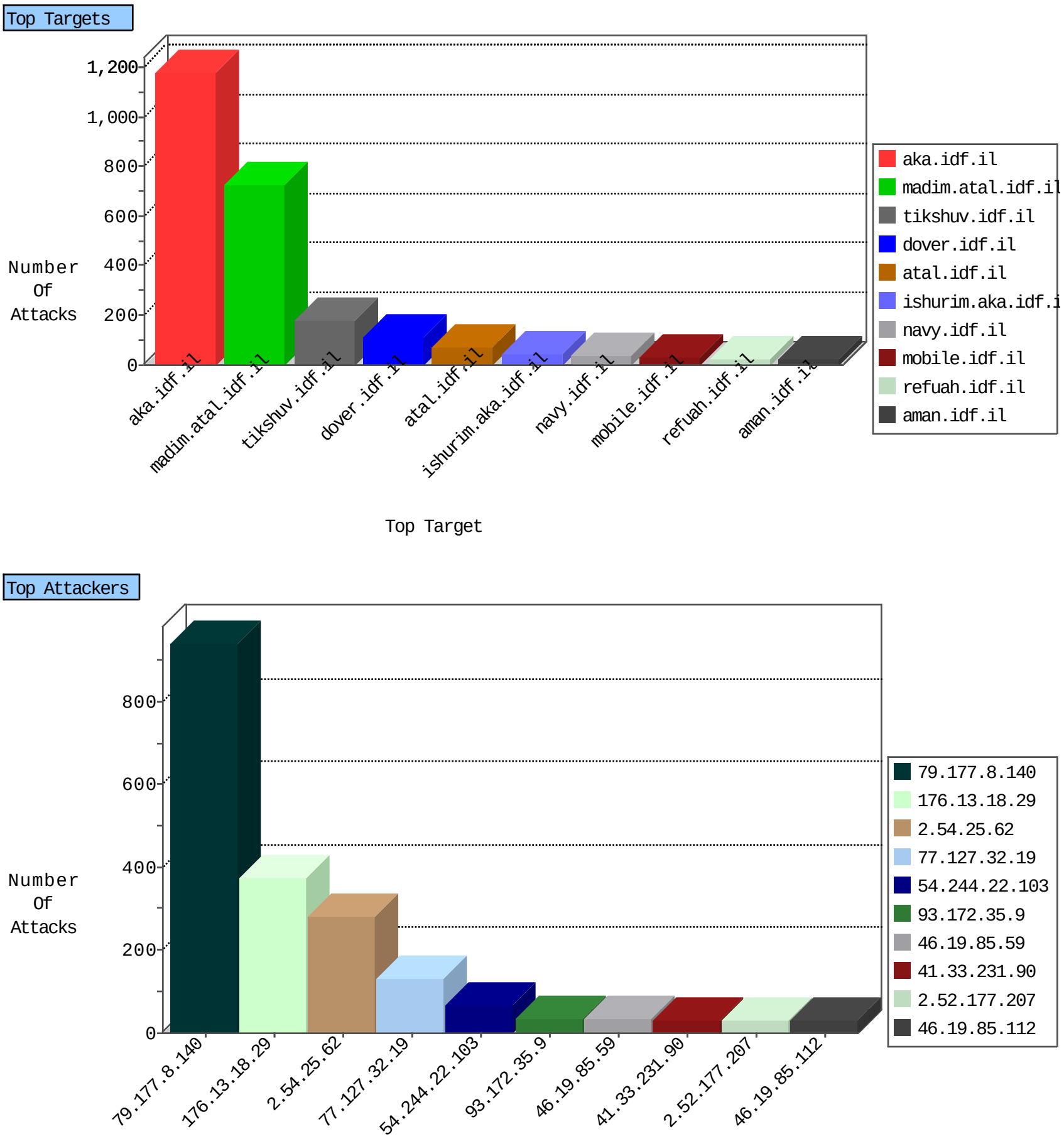
02-05-2016-12:04:04 to 02-05-2016-13:04:04

IDF Under Attack Daily Report



02-05-2016-12:04:04 to 02-05-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.188.23.221	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
46.188.23.221	Russian Federation	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
141.212.122.86	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.87	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
177.183.193.99	Brazil	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
177.183.193.99	Brazil	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

02-05-2016-12:04:04 to 02-05-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.219.122.4	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

02-05-2016-12:04:04 to 02-05-2016-13:04:04

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	4
91.219.122.4	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	3
188.152.234.175	147.237.77.216	Italy	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
46.148.22.26	147.237.76.200	Lithuania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.72.167	Lithuania	ishurim.aka.idf.i	ET SCAN Potential SSH Scan	1
1.2.235.8	147.237.76.31	Thailand	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
52.33.66.29	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.148.22.26	147.237.76.38	Lithuania	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.8.46	Lithuania	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.42	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1

02-05-2016-12:04:04 to 02-05-2016-13:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	34
46.19.85.59	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	34
93.172.35.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
207.241.231.229	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	24
46.19.85.112	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
2.54.0.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.182.141.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.27.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.25.62	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.46.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.217.200	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.81.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.10.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.230.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.172	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
197.200.9.225	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.81.81.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.188.23.221	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.130.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.38.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.236.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.190.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.154.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.175.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.200.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.248	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
212.235.79.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.170.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.217	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

02-05-2016-12:04:04 to 02-05-2016-13:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
87.68.65.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
143.127.2.4	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.27.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.158.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-05-2016-12:04:04 to 02-05-2016-13:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	738
176.13.18.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	281
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.8.140	Block	203
2.54.25.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
77.127.32.19	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
2.54.25.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
176.13.18.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
2.52.177.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
37.142.168.151	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
5.29.54.186	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	9
109.186.173.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.173.101	Block	7
37.142.207.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
176.13.9.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.128.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.184.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.214.253	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
79.180.33.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.170	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	2
5.29.172.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$20 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
79.177.8.140	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
109.253.202.19	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
85.65.49.191	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
178.35.45.197	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
79.182.144.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.102.196.189	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
72.191.176.27	United States	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™Ã?`Â¿Âª Â?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,ÃƒÃ‚Ã–ÃµSSÂ‚6Ã€[[#30]]Â©Â'[[#25]]Âª Â±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã'Œ Âƒ:[[#1]]Ã„%Â?[[#12]]Ã§[[#28]]Ã?qÃ«Ã°Â?[[#29]]Â“Â?ÃŠÃ½Ã°[[#2]]Œ[[#25]]	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1891	Block	1
107.182.20.202	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/templates/shared/usercontrols/headerupper/	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
2.54.158.88	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
72.191.176.27	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
85.250.247.180	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.247.180	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$81 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.147.205	Block	1
79.182.187.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
37.142.64.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$36 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.127.6.93	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/links/links.aspx	Block	1

02-05-2016-12:04:04 to 02-05-2016-13:04:04