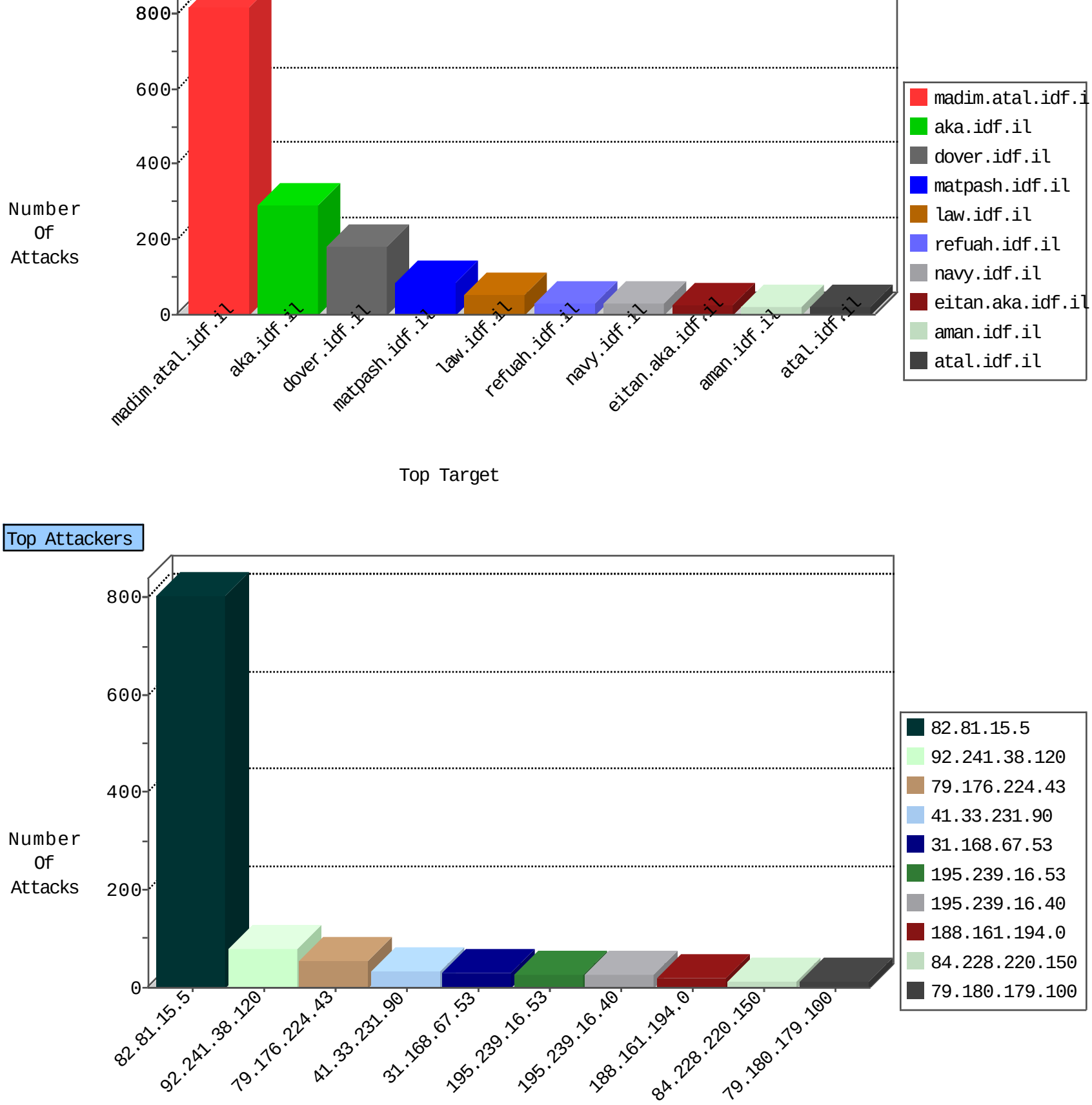
02-09-2016-23:04:02 to 02-10-2016-00:04:02

IDF Under Attack Daily Report



02-09-2016-23:04:02 to 02-10-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.215	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	2
142.54.160.210	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

02-09-2016-23:04:02 to 02-10-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
70.89.127.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
70.89.127.77	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
70.89.127.78	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
74.84.136.105	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

02-09-2016-23:04:02 to 02-10-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
70.89.127.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
70.89.127.78	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
74.84.136.105	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	3
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
77.126.190.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.108.164.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.132.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-09-2016-23:04:02 to 02-10-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.241.38.120	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	81
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
84.228.220.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.13.14.226	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
70.199.67.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.220.215	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.117.138.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
85.250.122.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.67.59.215	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
188.161.194.0	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.195.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.61.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.20.130	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.226	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
84.109.148.111	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.179.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.29.59.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.64.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
49.189.174.27	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.217.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.178.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.161.194.0	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.178.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.55.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.172.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.147.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.61.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.36.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.194.131.235	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	3
5.22.130.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.223.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.179.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3

02-09-2016-23:04:02 to 02-10-2016-00:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.22.135.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.145.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-09-2016-23:04:02 to 02-10-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	444
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 82.81.15.5	Block	199
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	160
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 31.168.67.53	Block	3
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 31.168.67.53	Block	3
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.20.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 31.168.67.53	Block	3
5.28.168.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	2
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 31.168.67.53	Block	2
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	2
5.102.254.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 31.168.67.53	Block	2
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	2
50.243.254.210	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-en/dover.aspx	Block	2
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 31.168.67.53	Block	2
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 31.168.67.53	Block	2
50.243.254.210	United States	147.237.77.216	dover.idf.il	Parameter Type Violation tab in www.idf.il/1065-en/dover.aspx	Block	2
66.249.78.233	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.233	Block	1
212.179.216.8	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.73.180.207	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
176.13.14.226	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
45.55.196.106		147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 45.55.196.106	Block	1
128.70.71.15	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Parameter Name from 31.168.67.53	Block	1
66.249.78.233	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/opevent/opevent.in.aspx	Block	1
213.184.119.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m	Block	1
157.55.39.239	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/page.asp	Block	1
46.73.180.207	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
95.86.118.90	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/1117-7835-he/nakhal.aspx&sa=u&ved=0ahukewinzbhizovkahvgprqkhsdtbacqfggmmae&usg=afqjcne85fgej8hlza-cyzhiprluyddmhg	Block	1
79.104.194.126	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
207.46.13.190	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-9665-he/cogat.aspx	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.64.229	Block	1
147.4.36.65	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.228.35.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$3 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Query String from 31.168.67.53	Block	1
165.91.48.186	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.65.186.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$12 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 31.168.67.53 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.183.53.230	Israel	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
212.76.116.123	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.116.123	Block	1
157.55.39.28	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
84.228.220.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
31.168.67.53	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 31.168.67.53	Block	1

02-09-2016-23:04:02 to 02-10-2016-00:04:02