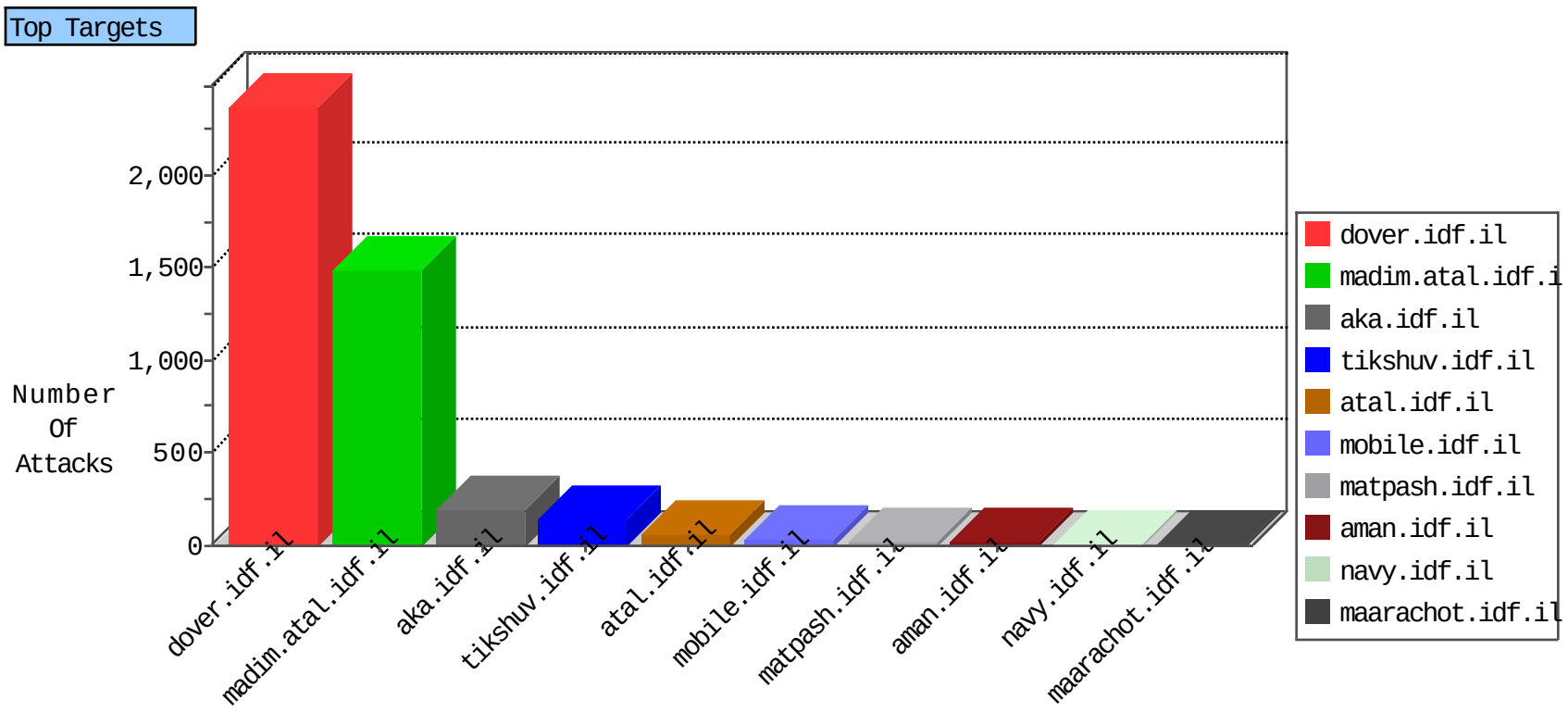
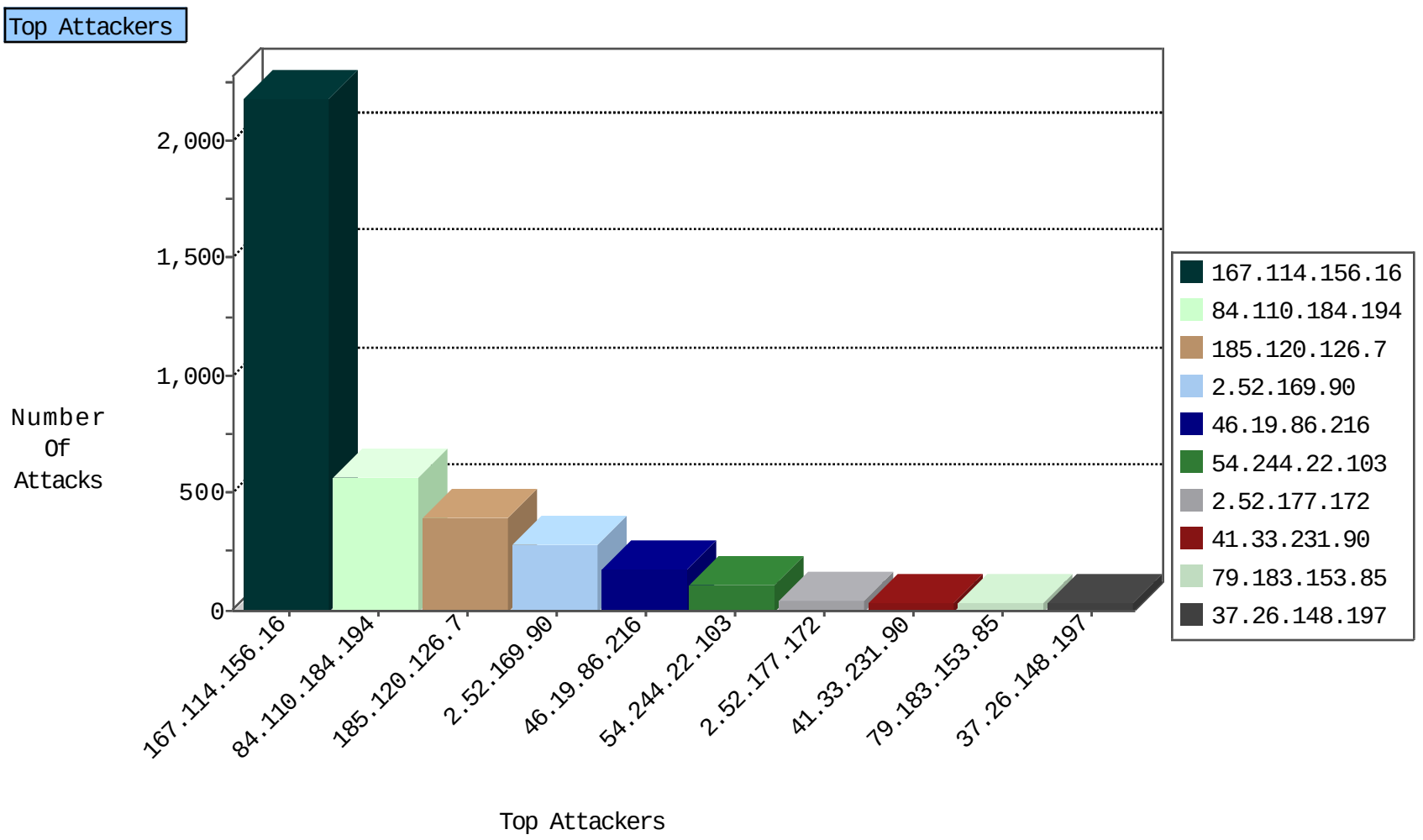
01-22-2016-16:04:03 to 01-22-2016-17:04:03

IDF Under Attack Daily Report





01-22-2016-16:04:03 to 01-22-2016-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3159
79.176.164.22	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
142.54.169.162	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
36.38.35.85	Korea, Republic of	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
142.54.160.212	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
223.158.153.54	China	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	1

01-22-2016-16:04:03 to 01-22-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.70.232.65	Turkey	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
95.70.232.65	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
115.163.56.112	Japan	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-22-2016-16:04:03 to 01-22-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

01-22-2016-16:04:03 to 01-22-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	101
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.253.223.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.86.164	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
37.26.147.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
41.44.177.41	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.148.197	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.148.197	Israel	147.237.0.34	tikshuv.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.148.197	Israel	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	9
37.142.252.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.188.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.80.130.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.6.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.198.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.229.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.229.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.80.130.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.188.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.44.245.213	Egypt	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	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
5.28.150.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.253.198.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.38.214	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.44.245.213	Egypt	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.56.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.144.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.206.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.37.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.15.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.152.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.248.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.126.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.91.70.94	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.64.50.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	360
185.120.126.7		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	213
185.120.126.7		147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	183
2.52.169.90	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.169.90	Block	152
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.52.169.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	129
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	104
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
2.52.177.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
188.161.236.121	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	7
95.70.232.65	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.70.232.65	Block	6
84.94.23.154	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	5
95.70.232.65	Turkey	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 95.70.232.65	Block	4
95.70.232.65	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
95.70.232.65	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 95.70.232.65	Block	4
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	3
109.253.208.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.70.232.65	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
2.54.167.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.177.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	2
213.57.226.144	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.55.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.160.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.70.232.65	Turkey	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 95.70.232.65	Block	2
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Too Many 403: Response Code per Session	Block	1
173.252.114.116	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/miktzoa/default.asp	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.65.6.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.252.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
85.65.133.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
23.91.70.94	United States	147.237.72.156	aman.idf.il	Distributed MSSQL Data Retrieval with Implicit Conversion Errors(+)	None	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Unknown HTTP Request Method R8AlÂ-Ã‡Â¾Â“pÂ,Ã˜Â¤7DQdÂŽÂ°Ã’ÂšÂ„Ã˜Â¿Â£\Â¾Ã¢CÃºÃ»GN_Ã©<{Ã¥^FOg` in URL	Block	1
149.78.53.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
79.181.137.59	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/information.aspx	Block	1
176.13.10.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.46.38.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1