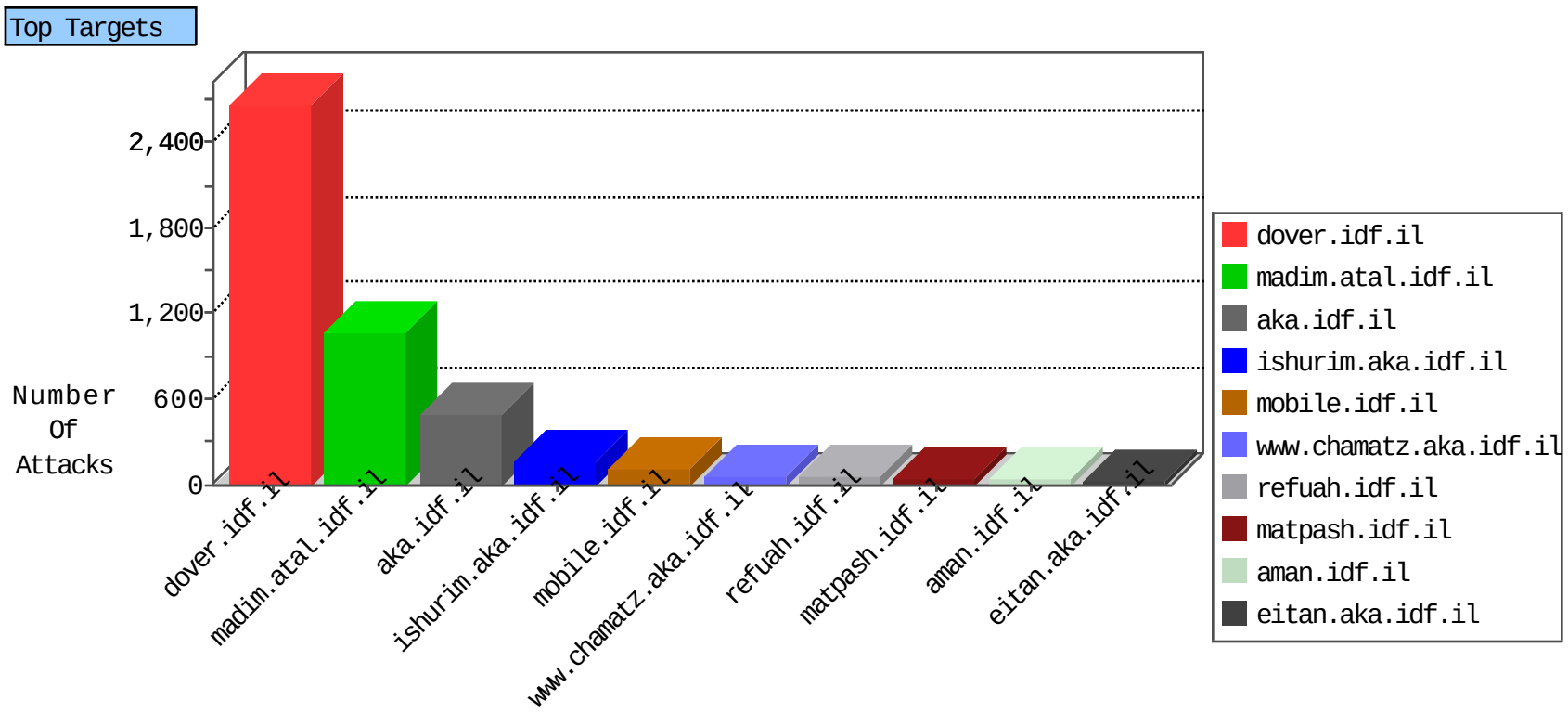
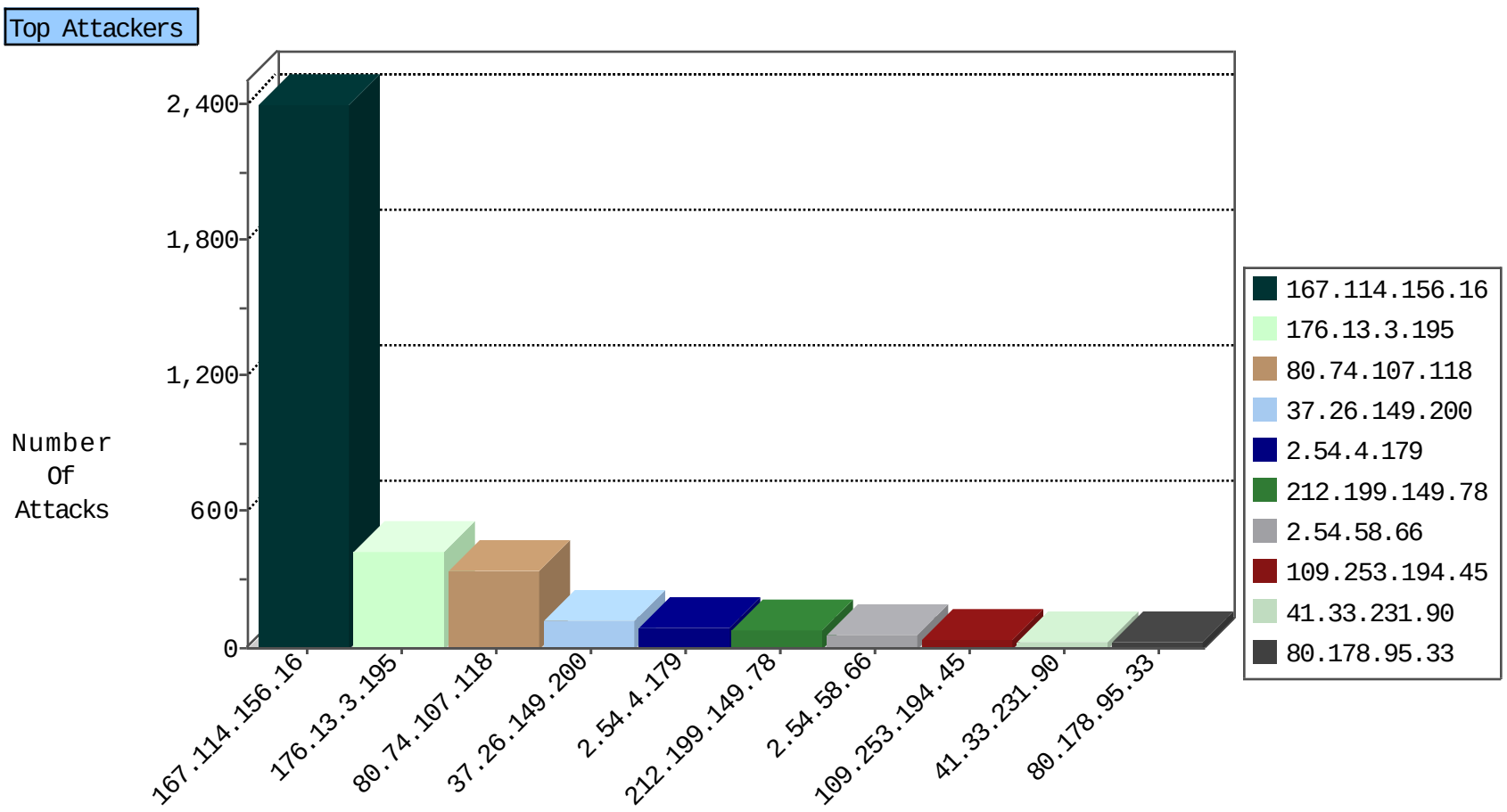
01-21-2016-14:04:04 to 01-21-2016-15:04:04

IDF Under Attack Daily Report





01-21-2016-14:04:04 to 01-21-2016-15:04:04

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	3086
212.199.149.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
185.7.227.195	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.7.227.196	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.7.227.205	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.26.161.65	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-21-2016-14:04:04 to 01-21-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-21-2016-14:04:04 to 01-21-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.58.66	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
223.252.32.73	147.237.76.196	Australia	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
146.200.221.93	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.162.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.122.130.215	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
223.252.32.73	147.237.76.31	Australia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.0.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.68.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.122.130.215	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.142.68.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-21-2016-14:04:04 to 01-21-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.149.78	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.34.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.43.70.222	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.235.98.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
2.52.37.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.178.95.33	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.58.66	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	14
185.89.217.230		147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.25	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
119.94.252.71	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
81.218.197.49	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.192.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.148.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.139.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.145	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.60.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.4.179	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.178.95.33	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.58.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.110.53.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.48.37	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
80.178.184.243	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.48.37	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.182.17.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
110.168.240.105	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.3.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.61.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.64.70	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
87.69.118.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.58.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.43.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.130.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
144.160.98.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.69.239.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
212.25.102.57	Israel	147.237.77.61	e.cogat.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.131.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.54.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.144.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.197.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.131.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.54.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-21-2016-14:04:04 to 01-21-2016-15:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.30		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6

01-21-2016-14:04:04 to 01-21-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	231
80.74.107.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	171
80.74.107.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	169
37.26.149.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
176.13.3.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.3.195	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.3.195	Block	96
2.54.4.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
109.253.194.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.86.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.15.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
37.26.149.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.54.186.79	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.186.79	Block	6
80.246.136.66	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	6
2.54.186.79	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	6
176.13.16.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.52.167.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.208.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.163.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.141.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.37.192	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	2
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.64.235.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
176.13.9.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.108.105.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.205	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
37.26.147.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	NULL Character in Method Â„sMÂ”•Ã?Â‡[[#0]]Ã¨Â…n>{ÂŒÂ²kÃ—Â?/Â•Â«Ã•ÂœT[[#21]]Ã?VÃµÂ·[[#15]]{Ã?Ã§Âš(	Block	1
80.69.206.55	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en/	Block	1
213.8.174.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.48.36.67	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
2.54.154.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
92.81.69.187	Romania	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
80.246.136.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.34.22.195	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in URL	Block	1
79.179.24.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
2.54.186.79	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
109.65.13.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
87.68.21.165	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1

01-21-2016-14:04:04 to 01-21-2016-15:04:04