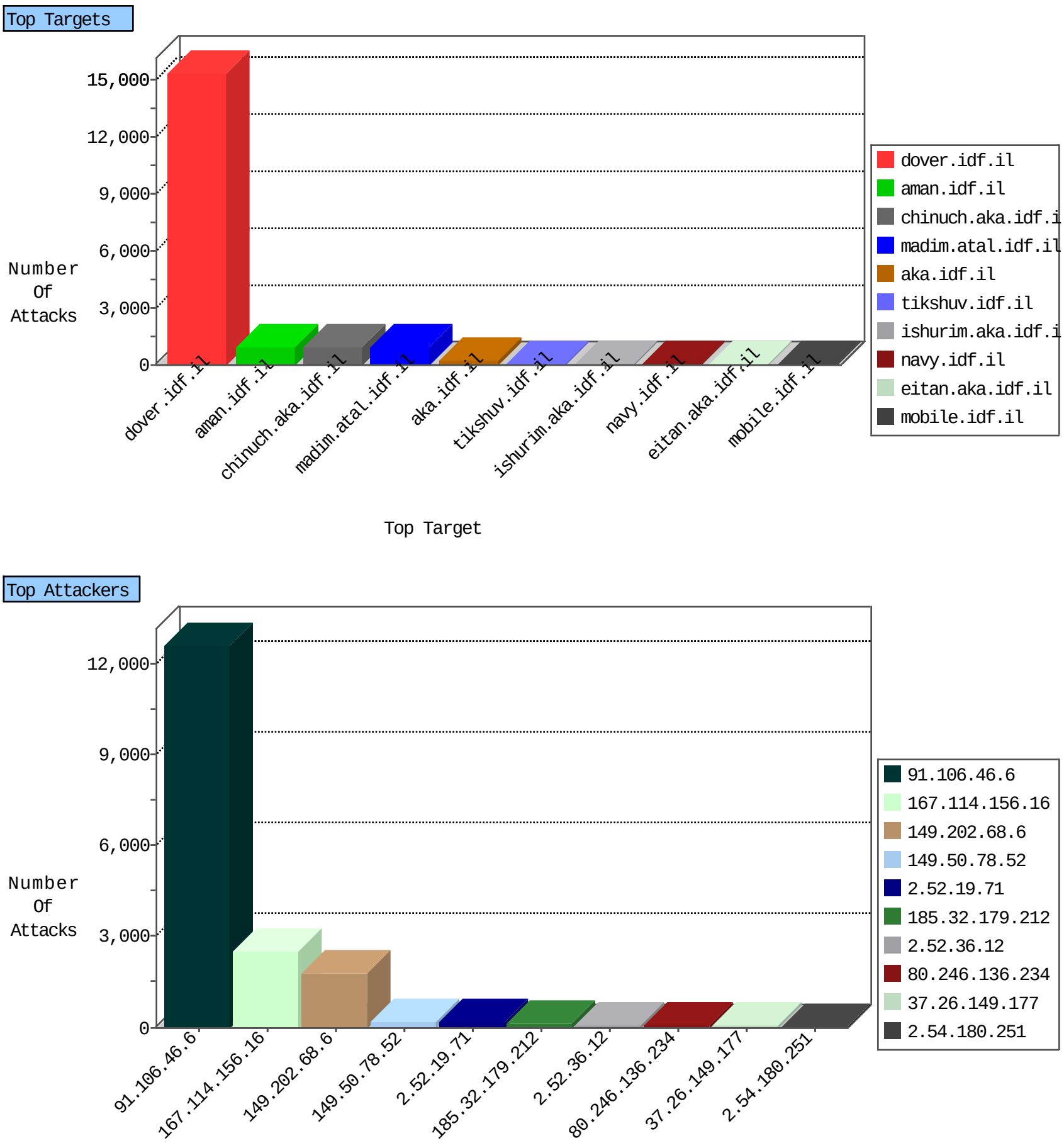
03-16-2016-14:04:05 to 03-16-2016-15:04:05

IDF Under Attack Daily Report



03-16-2016-14:04:05 to 03-16-2016-15:04:05

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	3706
91.106.63.46	Iraq	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
159.104.163.20	United Kingdom	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
159.104.163.17	United Kingdom	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
159.104.163.18	United Kingdom	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
159.104.163.19	United Kingdom	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

03-16-2016-14:04:05 to 03-16-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.18.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
81.218.245.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.25.127	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.131.243	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.16	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-16-2016-14:04:05 to 03-16-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.88.114.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.77.104.17	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.6.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
40.121.136.51	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -f -sS	1
218.57.11.7	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
209.162.248.93	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.160.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.220.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.121.136.51	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.31.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-16-2016-14:04:05 to 03-16-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11496
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	621
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack		reject	477
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	drop		drop	408
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	392
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	204
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	156
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	156
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	146
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	91
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	89
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
91.106.46.6	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	71
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
149.202.68.6	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	59
149.202.68.6	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
176.13.20.81	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
107.167.108.157	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
176.13.11.41	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
94.230.86.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.21.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.2.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.31.168	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	5
2.54.193.124	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.8.18.35	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
2.54.6.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.58.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
84.94.203.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.83	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.55.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.111.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.20.81	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.229	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
193.43.246.250	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
2.54.156.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.236.1	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	3

03-16-2016-14:04:05 to 03-16-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.50.78.52	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	190
2.52.19.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	189
185.32.179.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
2.52.36.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
80.246.136.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
37.26.149.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.180.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.149.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
212.235.103.203	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
212.235.103.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
212.235.124.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
212.235.103.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.131.167	Block	4
82.166.53.161	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.9.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.180.136.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.106.63.46	Iraq	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.199.66.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.104.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.22	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	2
66.249.74.75	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.156.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.83.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.29.211.150	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/205-he/patzar.aspx	Block	2
85.250.31.129	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	2
79.182.245.191	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
192.186.102.34	Canada	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
183.206.172.12	China	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 183.206.172.12	Block	1
66.249.66.65	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
207.46.13.21	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.83.84	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.186.102.34	Canada	147.237.76.86	navy.idf.il	Distributed Illegal HTTP Version	Block	1
46.121.104.199	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
183.206.164.12	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/fckeditor/editor/	Block	1
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.179.19.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainqsachar	Block	1
192.186.102.34	Canada	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
185.3.144.67	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.66.105	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.66.105	None	1
46.19.85.56	Israel	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	1
109.65.132.25	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
37.26.146.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
75.132.103.226	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.186.102.34	Canada	147.237.76.86	navy.idf.il	Distributed Malformed URL	Block	1

03-16-2016-14:04:05 to 03-16-2016-15:04:05