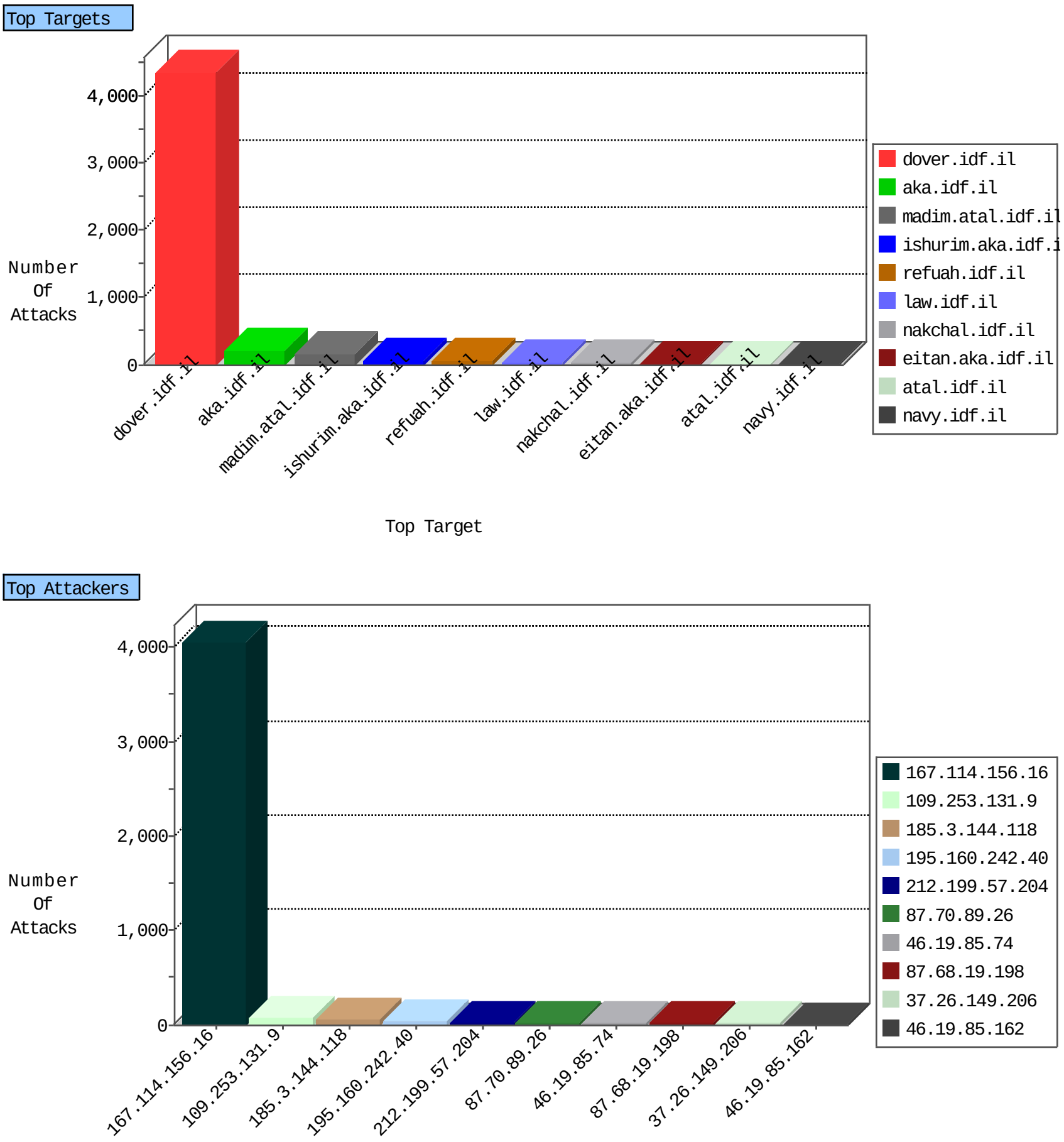
04-19-2016-14:04:06 to 04-19-2016-15:04:06

IDF Under Attack
Daily Report



04-19-2016-14:04:06 to 04-19-2016-15:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.5.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9183
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4037
120.132.50.135	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	4
46.19.85.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
82.145.218.105	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
93.174.93.50	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.21	United States	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.49	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

04-19-2016-14:04:06 to 04-19-2016-15:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-19-2016-14:04:06 to 04-19-2016-15:04:06

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	3
113.240.250.154	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.142.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.1.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.117.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.180.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
210.117.121.60	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN NMAP -f -sS	1
183.61.109.189	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.22.183	147.237.72.156	Israel	aman.idf.il	GPL SCAN myscan	1
91.218.246.103	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.188.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.169.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.15.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.128.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.117.121.60	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.22.183	147.237.72.156	Israel	aman.idf.il	INDICATOR-SCAN myscan	1

04-19-2016-14:04:06 to 04-19-2016-15:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.144.118	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
212.199.57.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
87.70.89.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
46.19.85.162	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
147.236.34.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.20.12	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.227.199	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
73.1.9.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
100.100.49.23		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.178.123.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.122.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.34.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.110.192.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.20.17	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.79.53	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
37.26.149.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
149.50.5.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.74	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
100.100.49.23		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
79.176.95.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
86.177.185.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.222.117	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.26.149.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
79.179.54.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.74	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.3.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.168.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.11.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.178.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.69.16	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.127.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.218.162.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.111.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.215.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-14:04:06 to 04-19-2016-15:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.131.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
176.13.2.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
37.26.149.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
192.116.232.69	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	10
109.253.218.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.55.43.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.53.38.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.171.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
64.79.85.205	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	4
91.227.165.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.129.208	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/mobile	Block	3
109.253.131.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.10.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.219.235	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.14.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.147.185	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	2
66.249.93.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
80.246.139.100	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.224.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.67.9.30	United Kingdom	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[0]]	Block	1
151.237.189.178	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.68.19.198	Block	1
79.179.54.84	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
87.71.79.53	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.180	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
212.199.51.250	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.mag.idf.il/421-he/patzar.aspx	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 87.68.19.198	Block	1
62.67.9.30	United Kingdom	147.237.77.74	law.idf.il	Malformed URL ¸[[#20]]¸	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed NULL Character in Header Name	Block	1
109.253.224.201	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
105.111.119.6	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17982-he/dover.aspx	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Too Many Headers per Request - 69 Headers	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 87.68.19.198	Block	1
62.67.9.30	United Kingdom	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]˜a»IÖÉ¹X˜^Ö±Êrñ#012M[[#30]]xw[[#22]]ª³•B[[#7]]P,»(Iœ[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Abnormally Long Request	Block	1
80.168.113.35	United Kingdom	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
91.199.69.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/popup.css	Block	1
216.218.206.68	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 87.68.19.198	Block	1
62.67.9.30	United Kingdom	147.237.77.74	law.idf.il	NULL Character in Header Name at [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
117.78.13.17	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/894-he	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL ¾epm[[ת×#26¬]]¥4q-˙pr“´¥`’·ה‹jŽœ'ın[[#0]]r˙.a[[#5]]`<œw€[[þ#31¸b]]ıЊüבת’([[51#]]±′פ„!‡_mŽx”»[[0#]].ע®–¦Þ	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

04-19-2016-14:04:06 to 04-19-2016-15:04:06