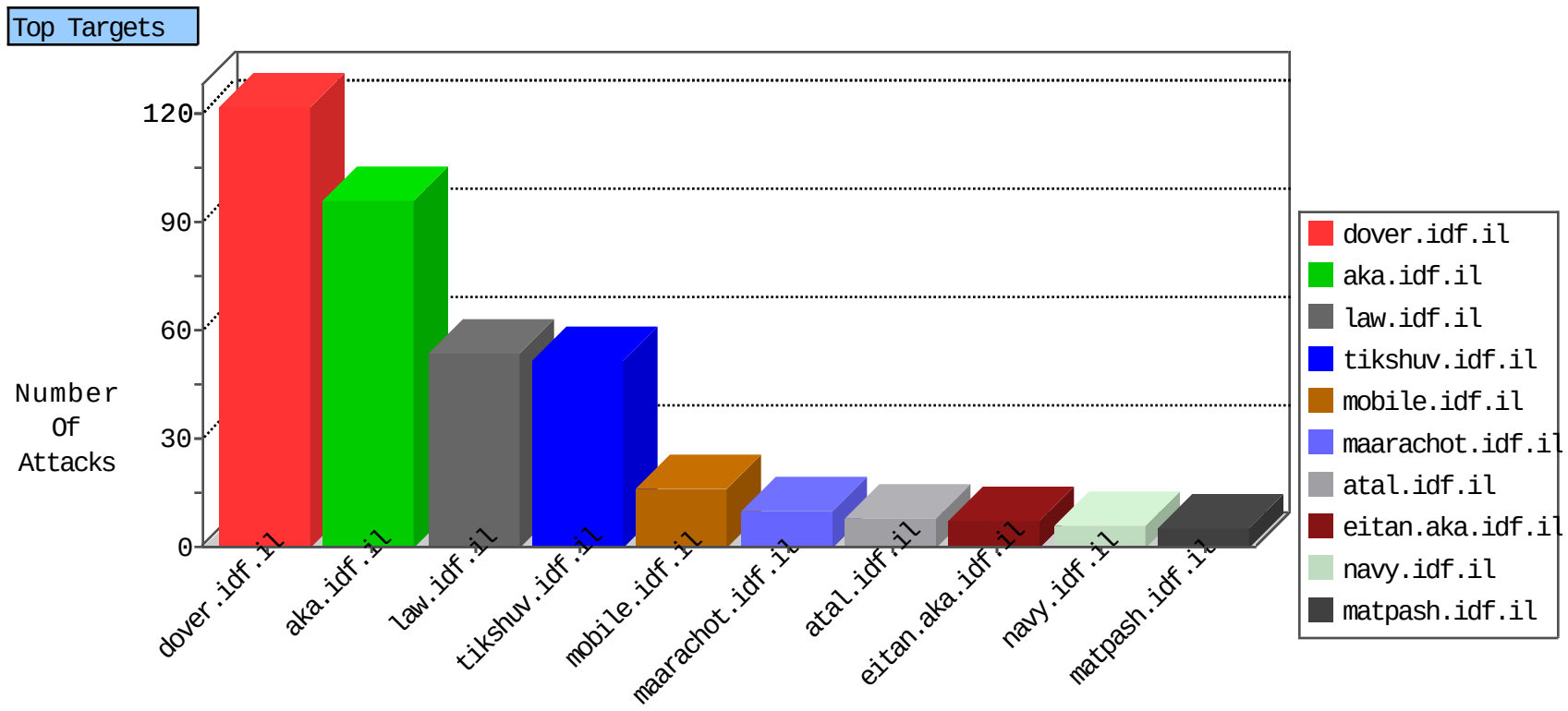
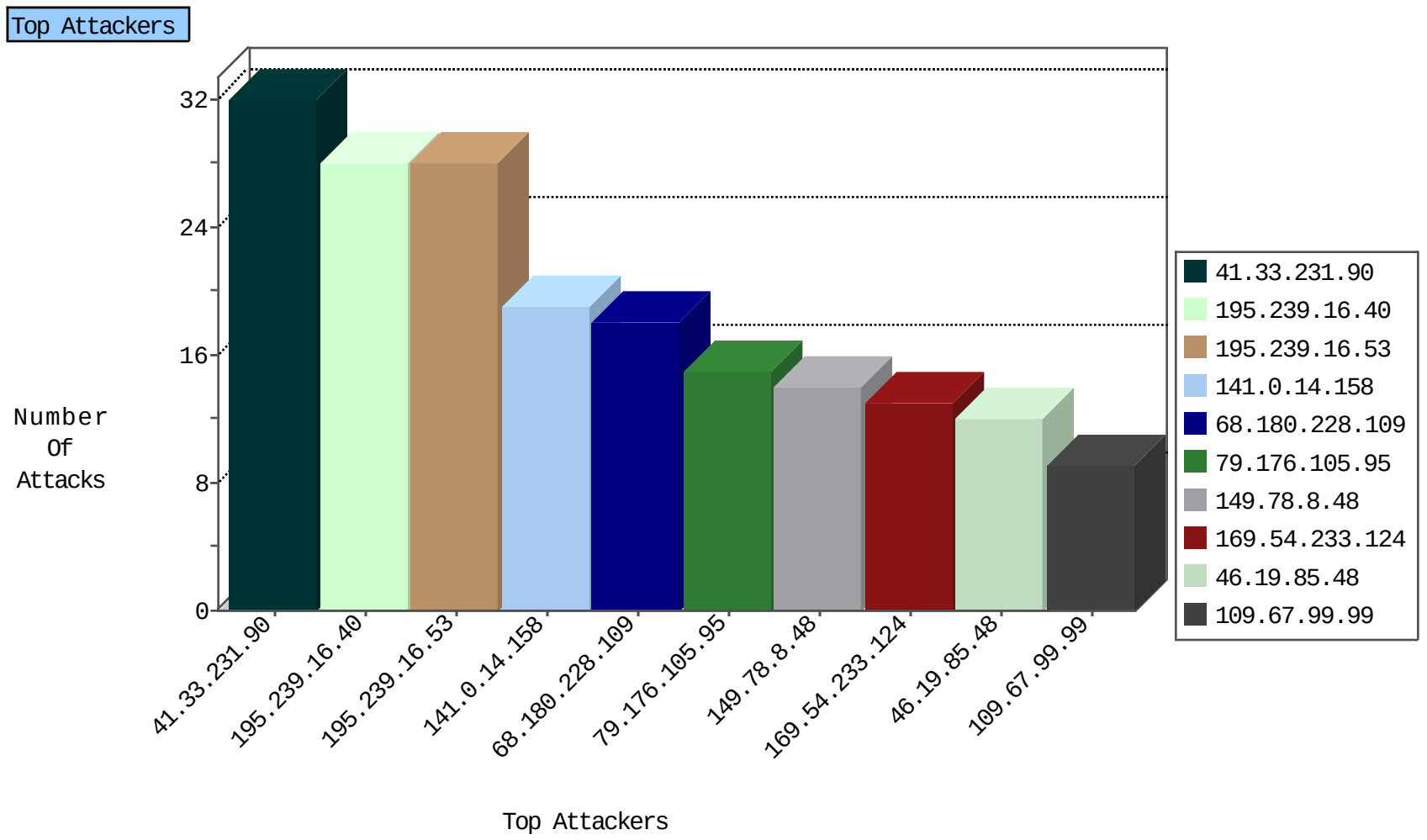
02-26-2016-23:04:04 to 02-27-2016-00:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-26-2016-23:04:04 to 02-27-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.228.101.206	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.219	Switzerland	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
109.236.93.206	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
109.236.93.206	Netherlands	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

02-26-2016-23:04:04 to 02-27-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.105.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	15
149.88.201.246	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
85.65.167.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
87.71.75.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.5	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.39	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.42	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.62	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-26-2016-23:04:04 to 02-27-2016-00:04:04

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	4
66.249.81.152	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
82.205.35.253	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
211.154.163.110	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	2
176.53.115.114	147.237.76.147	Turkey	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
88.200.214.8	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
66.192.6.154	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
50.60.153.98	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.124	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
146.185.250.2	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.52	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
88.200.214.8	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.124	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.182.170.38	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.124	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
45.43.226.154	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.124	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
169.54.233.124	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.201.227.52	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
107.6.130.113	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1

02-26-2016-23:04:04 to 02-27-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
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
141.0.14.158	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	18
109.67.99.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
182.50.130.134	Singapore	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.2.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.135.205	Israel	147.237.77.170	maarachot.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
2.52.60.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.138.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.102.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.135.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.59.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.192.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
77.125.138.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.120.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
40.77.167.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
211.154.163.110	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.84.70.91		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
31.210.187.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.25	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.82.200.91		147.237.77.19	law-forum.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
84.132.58.161	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.249.109.116	Jordan	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
213.57.37.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
88.200.214.8	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.228.75.121	Hungary	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.177.153.77	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.48.64.20	Netherlands	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
88.200.214.8	Russian Federation	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.229.53.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.82.200.91		147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
213.57.37.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-26-2016-23:04:04 to 02-27-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
105.107.55.237	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding	Block	1
108.61.166.66	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
186.156.100.202	Chile	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.33	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109346.pdf	Block	1
5.153.182.204	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
217.78.57.111	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.82.200.91		147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
108.61.166.66	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/popups/popup.aspx	Block	1
195.9.77.44	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Ò•¯Â	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Ò•¯Â	Block	1
185.82.200.91		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
47.18.173.185	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
198.58.103.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.69.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/112435.pdf	Block	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.232 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL	Block	1
79.182.2.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
186.13.2.161	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
63.231.69.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.78.8.48 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
211.154.163.110	China	147.237.72.166	aka.idf.il	Illegal Host Name	Block	1
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.249	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
186.91.99.182	Venezuela	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at êËŽS<•[[#2]]â¹§Øb~'sB[[#7]]M©Ù¤zSÆ g[[#18]][[#14]]6auúÊ.®[[#19]][[#25]][[#23]]švŸLàÃ[[#6]]8E[[#28]]'•¨ÃÂ©;À/0ž[[#29]]I]-OK¢Ä%°•[[#18]]üô[[#0]]°rÆZ•™•{	Block	1
5.153.182.204	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
149.78.8.48	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name Óß)Öp'¹F,)â}•Ì^x#011i‰]S"[[#1]]…C®o7wqI=½" B°R;-_„×Ú¯Ô	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
211.154.163.110	China	147.237.72.166	aka.idf.il	Multiple Illegal Host Name from 211.154.163.110	Block	1
180.76.15.150	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

02-26-2016-23:04:04 to 02-27-2016-00:04:04