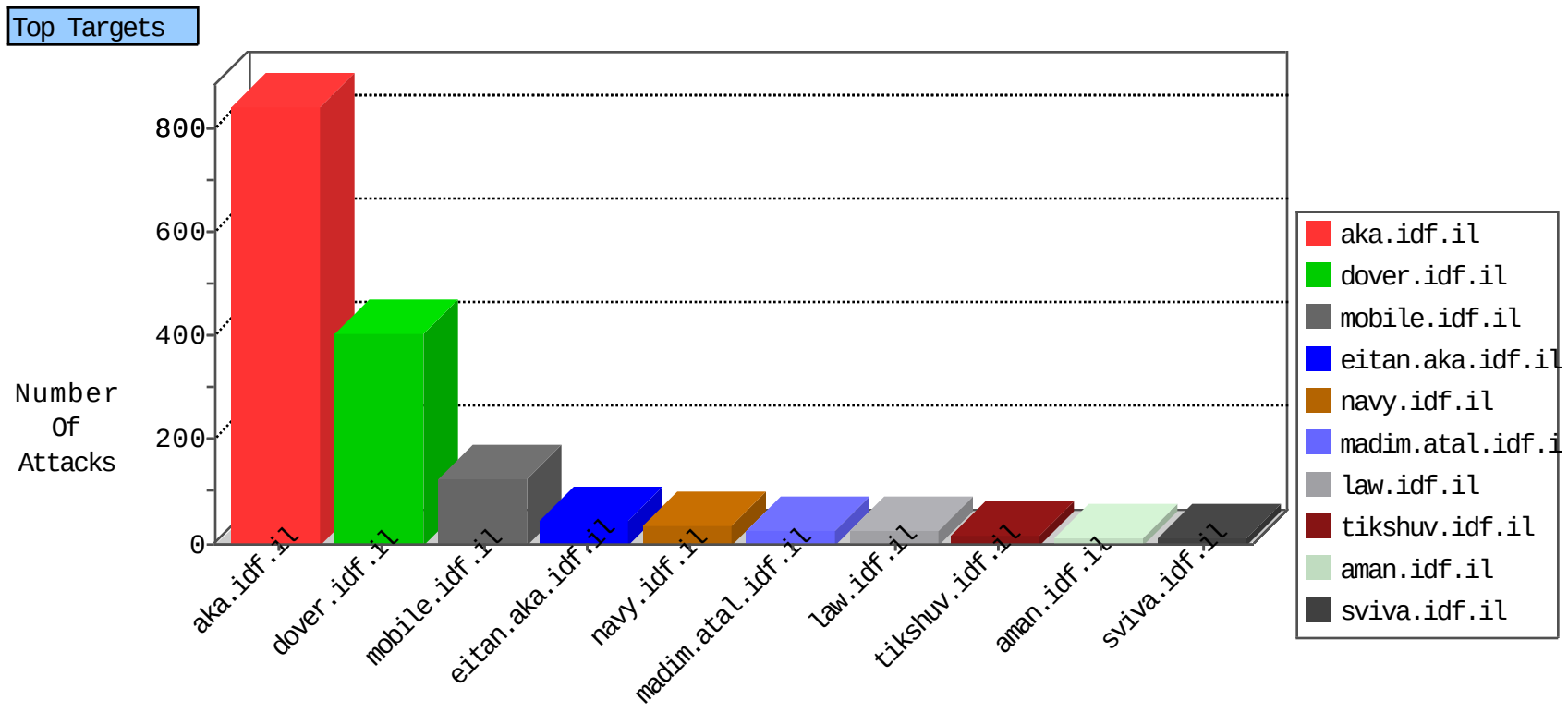
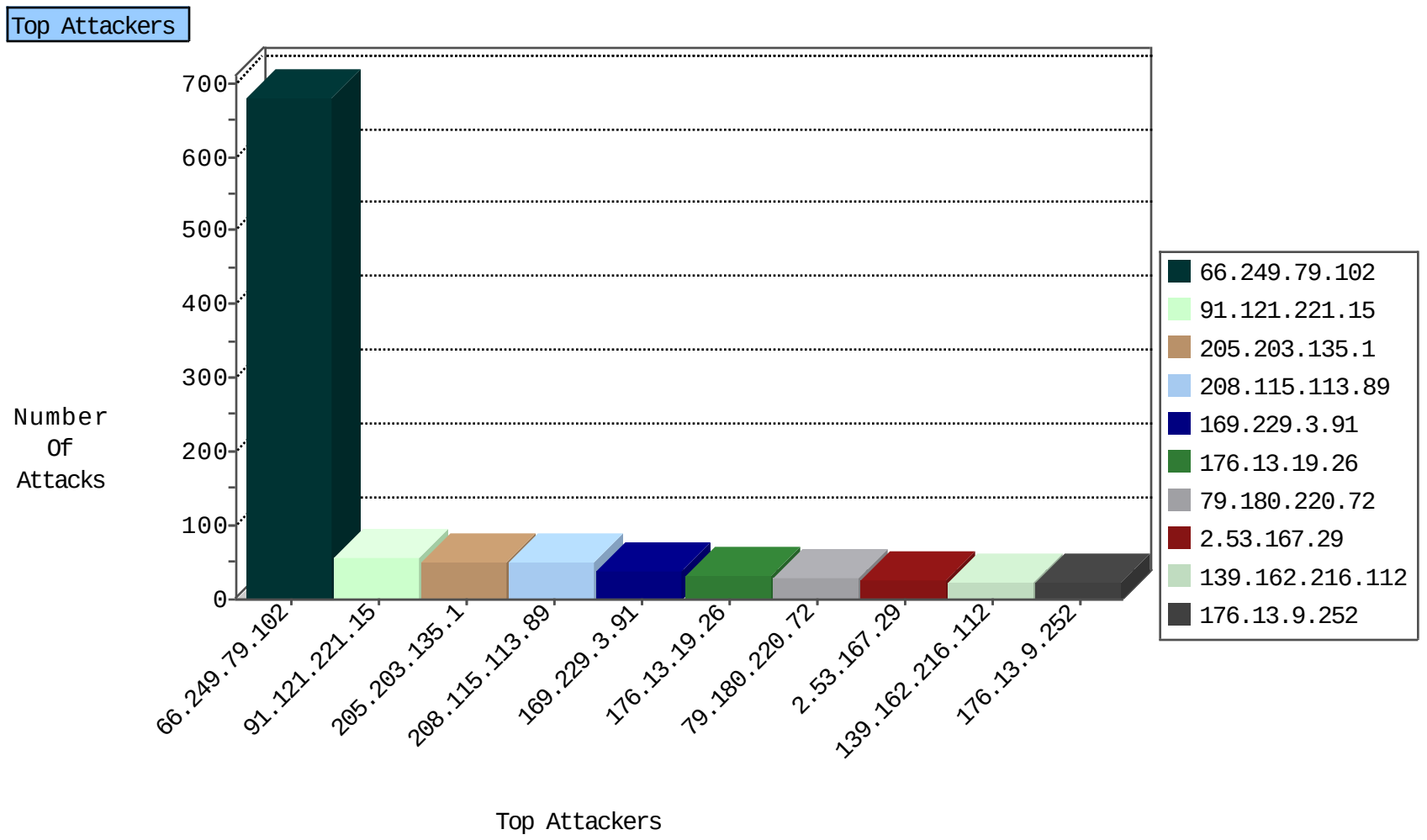
04-30-2016-13:04:09 to 04-30-2016-14:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-30-2016-13:04:09 to 04-30-2016-14:04:09

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	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
163.172.153.224	United Kingdom	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-30-2016-13:04:09 to 04-30-2016-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.192.77	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

04-30-2016-13:04:09 to 04-30-2016-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.102	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	592
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.81.233	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
195.16.127.148	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
195.16.127.148	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.200.15.174	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
195.16.127.148	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.16.127.148	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.72.14	Italy	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
113.240.250.154	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.211	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

04-30-2016-13:04:09 to 04-30-2016-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	89
91.121.221.15	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
79.180.220.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
176.13.19.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.9.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.124	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
199.30.120.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.177.174.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.152.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.120.126.91	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.185.141.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
125.126.151.192	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.55.119	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
162.194.160.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.178.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.129.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.178.187.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.12.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.103.11.66	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.49.153.32	Portugal	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.141.19	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.144.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.121.13.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.127.233	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.169.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.110.210.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.182.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.177.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.195.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-30-2016-13:04:09 to 04-30-2016-14:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.28.167.93	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
2.53.167.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.27.106.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	5
176.13.9.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.19.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	4
213.8.204.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.55.152.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.8.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
195.154.59.69	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
85.250.127.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.116.238.196	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	2
90.229.230.192	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	2
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in URL z„¥ךֻצru„€§v=r[[#25]]ט%ֻ>פß"×	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9740-he/refuah.aspx	Block	1
46.118.116.239	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method 5Ãº¹Ê<EF†uskÏ}ò°	Block	1
84.110.34.246	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.110.34.246	Block	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
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
51.255.65.95	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0113-3.stm`	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/apple-app-site-association	Block	1
109.65.242.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal HTTP Version	Block	1
46.120.169.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Malformed URL	Block	1
2.53.134.181	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.110.34.246	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	NULL Character in Method	Block	1
37.145.130.154	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt'a=0	Block	1
125.126.151.192	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
68.180.230.187	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal URL Path Encoding z„¥ךֻצru„€§v=r[[#25]]ט%ֻ>פß"×	Block	1
46.121.13.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Unknown HTTP Request Method 5Ãº¹Ê<EF†uskÏ}ò°	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.64.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1130-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Abnormally Long Request method	Block	1
79.180.149.208	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding ctl00_ctl00_ScriptManager1_HiddenField in www.aka.idf.il/main/sachar/	None	1