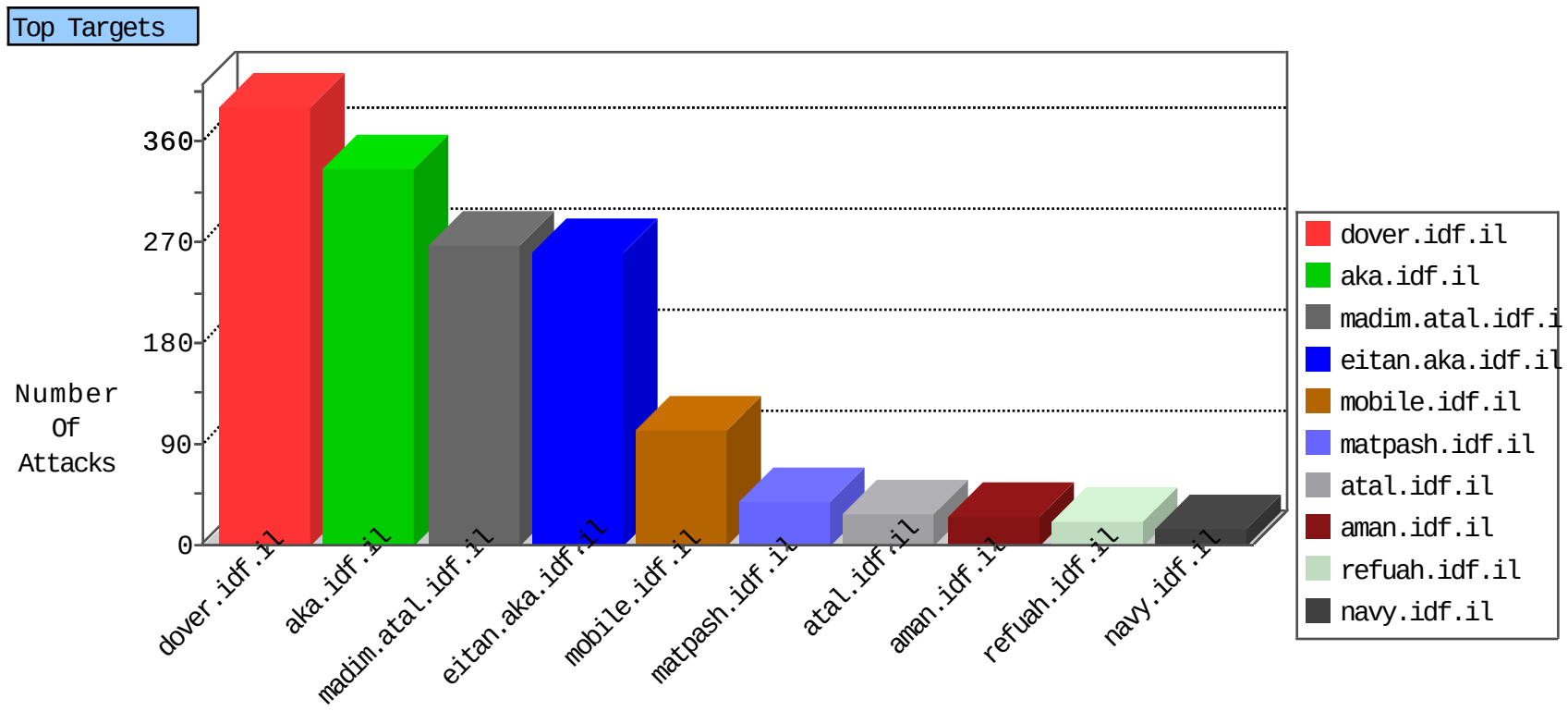
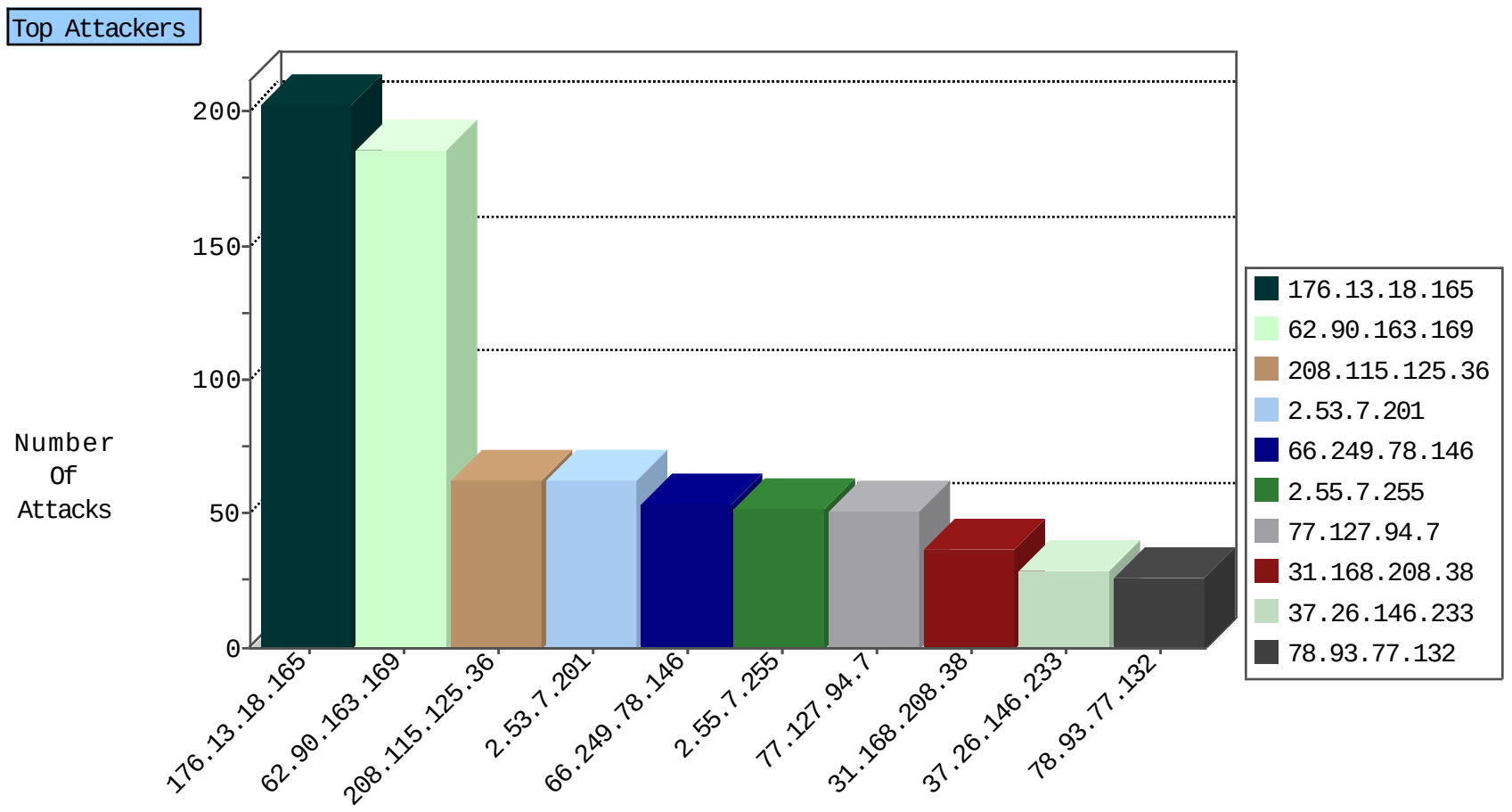
04-27-2016-12:04:07 to 04-27-2016-13:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-27-2016-12:04:07 to 04-27-2016-13:04:07

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	HTTP-POST-Segmented-DoS	dest-reset	278
89.46.102.242	Romania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
89.46.102.242	Romania	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.46.102.242	Romania	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

04-27-2016-12:04:07 to 04-27-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-12:04:07 to 04-27-2016-13:04:07

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
66.249.93.219	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
163.172.140.23	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.183.183	147.237.0.33	Philippines	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.251.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
77.149.248.13	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 3072	1
220.231.195.122	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.86.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.174.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.102.240.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
185.120.126.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.77.19	Japan	law-forum.idf.il	ET SCAN Potential SSH Scan	1
84.108.27.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.46.39.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.61.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.195.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-27-2016-12:04:07 to 04-27-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.90.163.169	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
2.53.7.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
208.115.125.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
77.127.94.7	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
31.168.208.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
37.26.146.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.251.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.0.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.66	Israel	147.237.76.200	eitan.aka.idf.i	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
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.213.149.147	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
78.93.77.132	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.157.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
78.93.77.132	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
78.93.77.132	Saudi Arabia	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
86.104.164.120	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.160.206.146	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	6
109.253.196.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.130.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.16.54	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.24.207.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.166.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.16.54	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
97.74.24.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.3.211	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
130.192.232.23	Italy	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.159	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

04-27-2016-12:04:07 to 04-27-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	201
2.55.7.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
89.238.188.119	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.238.188.119	Block	5
31.210.179.160	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 31.210.179.160	Block	5
80.246.133.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.150.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.168	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 37.26.146.168	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
109.253.218.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.40.25	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request request version	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
2.53.23.19	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.94.235.0	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.120.233.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 169.229.3.91	Block	1
31.168.208.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
109.253.130.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
37.26.146.168	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method ~}[[#6]]•	Block	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.53.180.253	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
188.247.79.72	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.64.229	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/150302011yezu.aspx	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
109.253.196.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.169.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
40.77.167.8	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in URL [[ב#26[[,,˛]]#21]]4'ו€ש,•¬fkq'בdd·ˇŽšנ{› d!Œ¼@3וו-˜]]#26[[ת†üfs]]#12[[ת	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
208.115.125.36	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
31.210.179.160	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Malformed URL [[ב#26[[,,˛]]#21]]4'ו€ש,•¬fkq'בdd·[[ת›{ˇŽšנ#12]]üfs†ת d!Œ¼@3וו-˜]]#26[[	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
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
109.65.132.63	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	1
212.143.152.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2970.jpg	Block	1
37.26.146.144	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/contactus/mobile	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
130.185.155.10	Sweden	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
82.80.48.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method ~}[[#6]]• in URL [[ב#26[[,,˛]]#21]]4'ו€ש,• ¬fkq'בdd·[[ת›{ˇŽšנ#12]]üfs†[[ת#26וו-˜]]d!Œ¼@3	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1

04-27-2016-12:04:07 to 04-27-2016-13:04:07