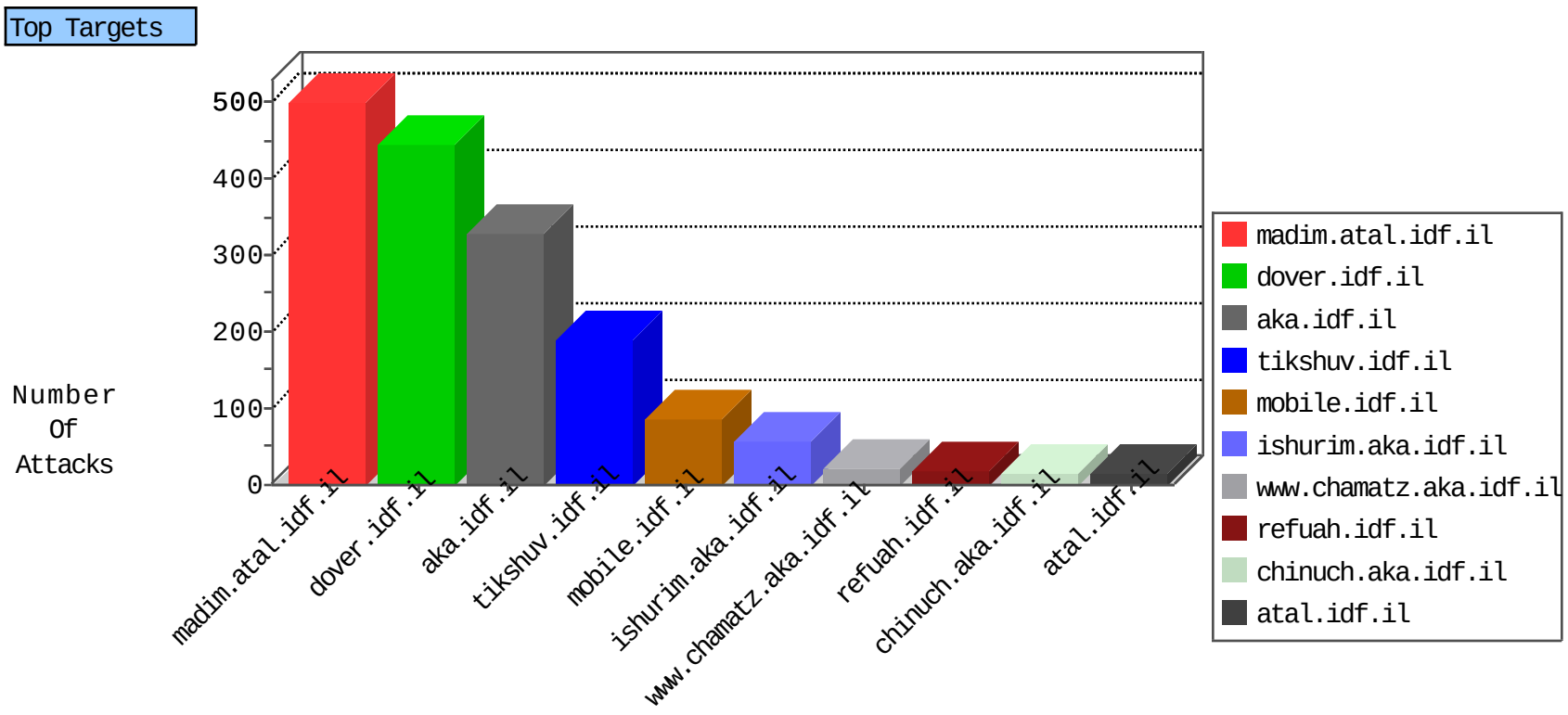
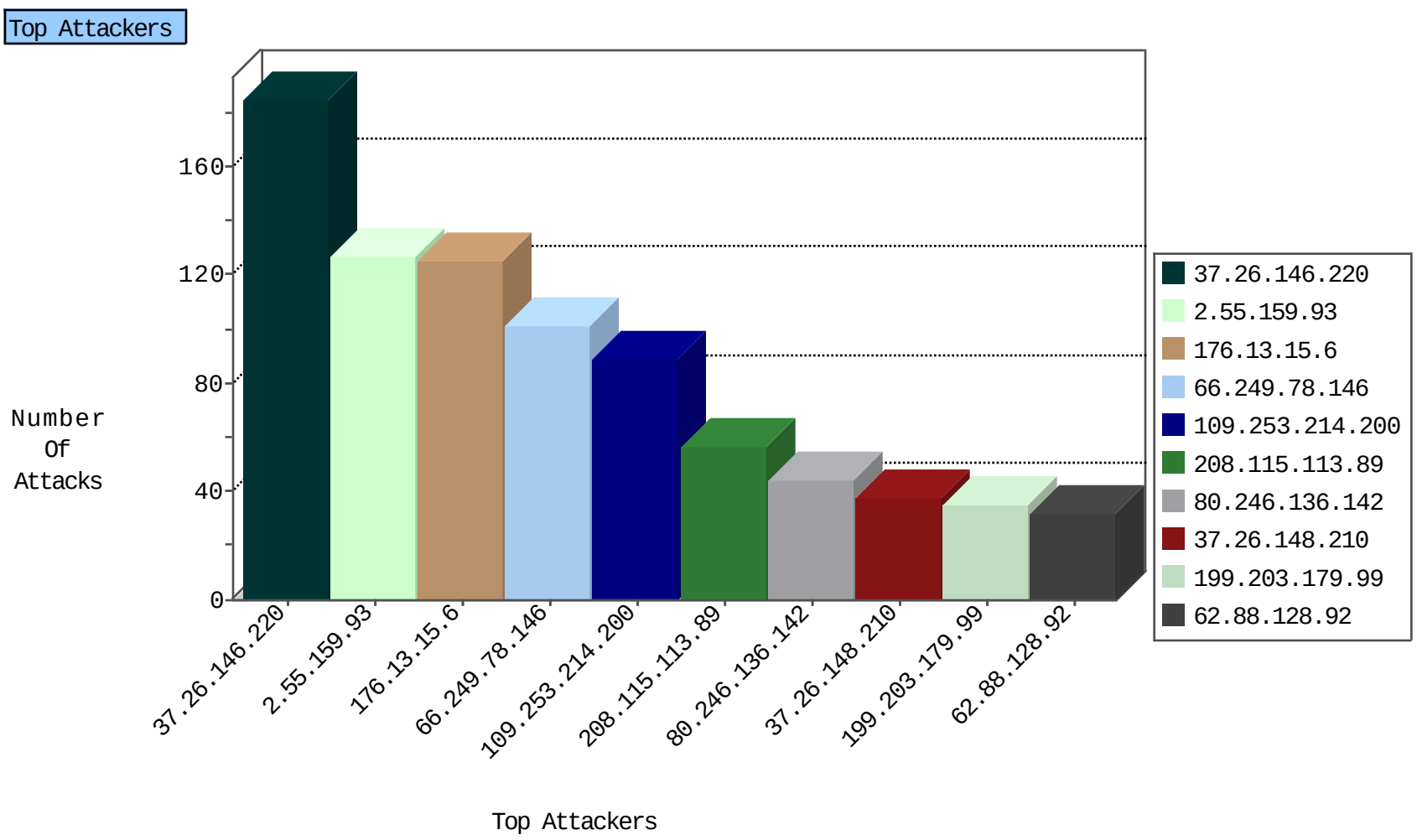
05-03-2016-13:04:06 to 05-03-2016-14:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



05-03-2016-13:04:06 to 05-03-2016-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	455
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
109.65.30.6	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	5
87.118.124.186	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
71.6.216.48	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
82.221.105.6	Iceland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
176.31.60.249	France	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
125.202.88.129	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
45.32.79.225	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

05-03-2016-13:04:06 to 05-03-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-03-2016-13:04:06 to 05-03-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.219.116.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.195.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.29.17	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.219.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.236	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
62.219.13.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.44.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
85.64.3.102	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.38.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-03-2016-13:04:06 to 05-03-2016-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	164
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	99
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
37.26.148.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
62.88.128.92	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
199.203.179.99	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	27
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.144.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.60.84	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.90.8.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.27.80.144	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.27.69.217	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.158.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.50.242.19	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.150.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
198.50.242.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.130.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
69.31.50.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.186.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
149.78.45.179	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.50.242.18	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
194.177.16.3	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.109.46.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
198.50.242.17	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.167	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
73.75.48.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.88.141.89	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

05-03-2016-13:04:06 to 05-03-2016-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.159.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
109.253.214.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
176.13.15.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
80.246.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.226.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
80.246.136.79	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.136.79	Block	22
185.32.179.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
37.26.147.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
109.253.226.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.139.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.178.157.101	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
149.88.141.89	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	5
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.7.104	Israel	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 176.13.7.104	Block	4
199.203.151.13	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
109.253.210.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.240.182	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 79.177.240.182	Block	3
2.53.186.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.203.151.13	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/	Block	3
46.19.86.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.144.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.203.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.226.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.176.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
109.253.139.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
69.89.31.228	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	2
109.253.198.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.37.129	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.143.162	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 79.177.143.162	Block	2
198.50.242.19	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
62.90.165.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
95.86.104.79	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method [[#20]][[#27]]¤ùdÕÍ„R%o»ëä[[[#6]]²	Block	1
80.246.137.61	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
130.185.155.82	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
199.203.151.13	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 199.203.151.13	Block	1
85.117.123.57	Kazakstan	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/unit.aspx	Block	1
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
149.88.101.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
176.13.7.104	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/m	Block	1
103.231.241.37	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

05-03-2016-13:04:06 to 05-03-2016-14:04:06