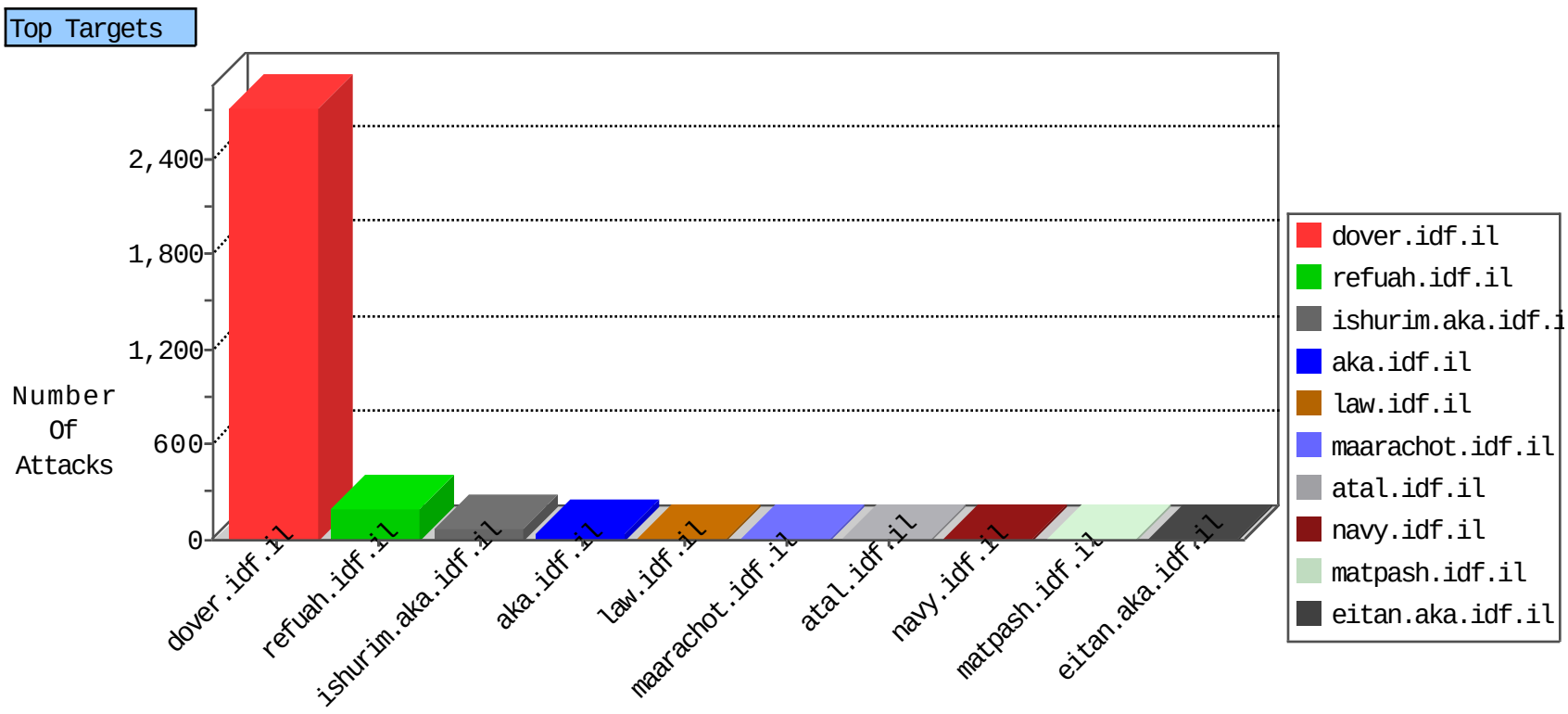
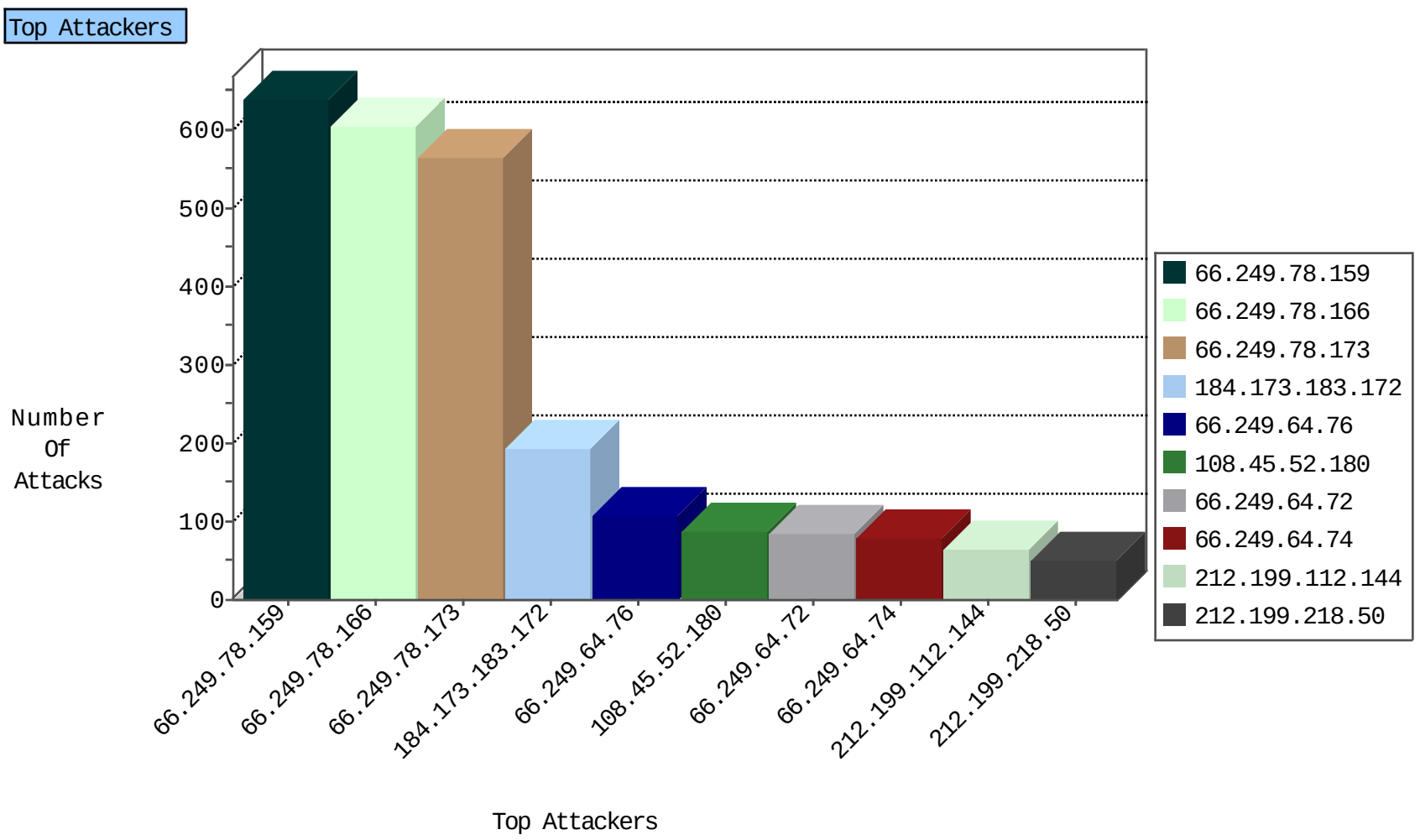
05-02-2015-07:03:02 to 05-02-2015-08:03:02

IDF Under Attack
05-02-2015-07:03:02

Top Targets



Top Attackers



05-02-2015-07:03:02 to 05-02-2015-08:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	597
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
195.37.190.86	Germany	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

05-02-2015-07:03:02 to 05-02-2015-08:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
144.76.62.165	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-07:03:02 to 05-02-2015-08:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
119.92.202.251	Philippines	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
119.92.202.251	Philippines	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
218.241.153.80	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
178.32.251.100	France	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
119.92.202.251	Philippines	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.60.140	Netherlands	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.241.153.80	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.32.251.100	France	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1

05-02-2015-07:03:02 to 05-02-2015-08:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
108.45.52.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
212.199.218.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
36.252.154.104	Nepal	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
213.57.57.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
70.194.28.216	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
79.178.116.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	13
79.177.3.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
108.16.25.104	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.140.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.26.147.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
136.243.36.97	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
85.64.118.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.64.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
58.6.47.4	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.166	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
107.170.181.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.119.124.41	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

05-02-2015-07:03:02 to 05-02-2015-08:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	429
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	261
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	260
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	202
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	191
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	48
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	41
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	32
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	28
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	23
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	22
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
94.153.66.163	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
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
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
188.40.94.149	Germany	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 188.40.94.149	Block	1
157.55.39.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.47	Block	1
192.187.110.98	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
188.40.94.149	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-admin/	Block	1
194.90.167.179	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
46.229.164.102	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/gallery	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.195	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	1
79.183.137.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
46.229.164.111	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/17.stm	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
213.57.99.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20424-he/kkkkkkk=0c5ac057kkkkkkk_0c5ac057	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
46.229.164.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	1
188.165.15.236	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1

05-02-2015-07:03:02 to 05-02-2015-08:03:02