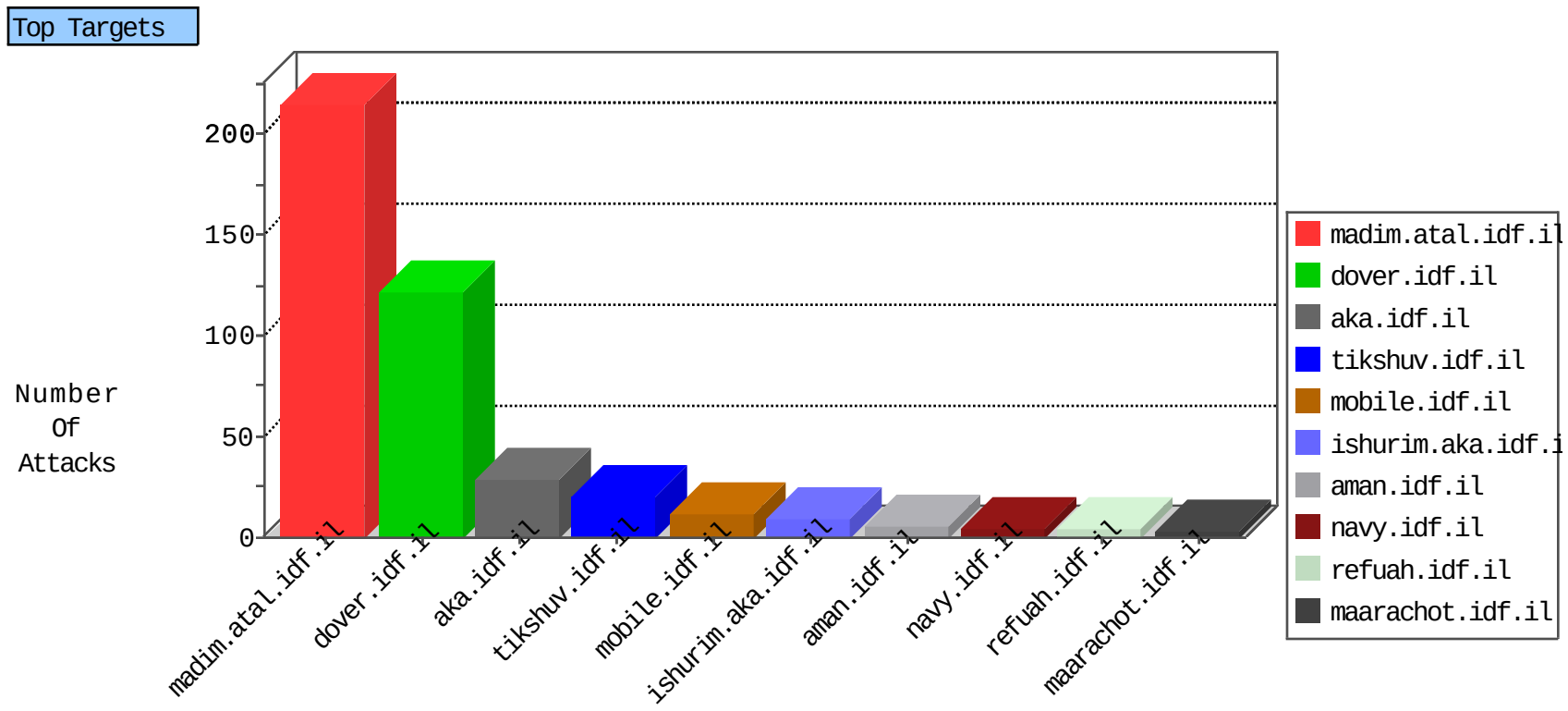
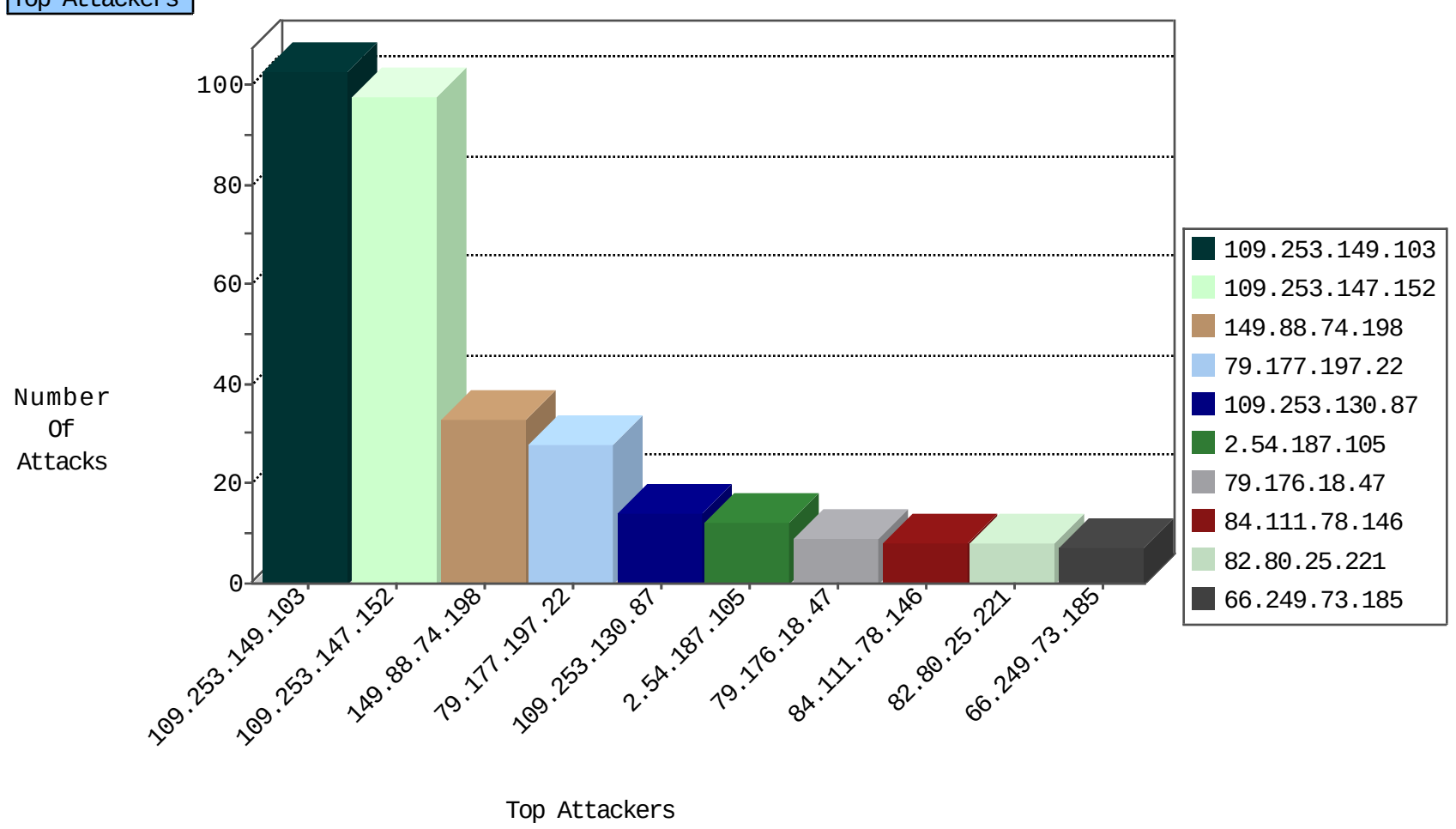
04-25-2015-14:03:02 to 04-25-2015-15:03:02

IDF Under Attack
04-25-2015-14:03:02

Top Targets



Top Attackers



04-25-2015-14:03:02 to 04-25-2015-15:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.4	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	4318
79.176.18.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
89.139.43.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.29.155.177	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
46.29.155.177	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

04-25-2015-14:03:02 to 04-25-2015-15:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-14:03:02 to 04-25-2015-15:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
79.177.197.22	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	17
2.54.187.105	Israel	147.237.77.243	mobile.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
79.177.197.22	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
2.54.58.90	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
139.194.160.216	Indonesia	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.219.187.9	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
217.91.181.112	Germany	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.130	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
207.59.239.34	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
61.160.224.130	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
139.194.160.216	Indonesia	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 2048	1
139.194.160.216	Indonesia	147.237.72.156	aman.idf.il	ET SCAN NMAP -f -sS	1
89.248.171.167	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.219.187.9	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
217.91.181.112	Germany	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
207.59.239.34	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.130	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
207.59.239.34	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
61.160.224.130	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
188.95.158.103	Ukraine	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2015-14:03:02 to 04-25-2015-15:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.88.74.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
84.111.78.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.177.197.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.66	Israel	147.237.0.34	tikshuv.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
67.82.197.219	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
81.218.192.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
87.174.254.75	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.149.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.121.253.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.64.154.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.65.181.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.65.17.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.144.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.104.120.34	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
125.202.25.184	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
94.230.86.179	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-25-2015-14:03:02 to 04-25-2015-15:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.149.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	103
109.253.147.152	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.147.152	Block	97
109.253.130.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	7
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	6
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	6
37.142.126.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
84.228.126.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
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
46.19.85.251	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
46.117.112.247	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templatecontrols/tags/tags.aspx	Block	1
66.249.75.80	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.95	Block	1
109.253.147.152	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
79.181.182.196	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.188	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/registrationwizard/register.aspx	Block	1
85.64.155.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-en	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2004/january/22.stm	Block	1
80.178.28.138	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
87.69.55.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
216.127.180.38	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
80.246.130.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.68	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/..aspx	Block	1
91.200.12.22	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
69.199.171.13	United States	147.237.77.74	law.idf.il	Distributed eMail Hoarding	Block	1
217.132.208.25	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
144.76.93.118	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
46.119.113.155	Ukraine	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
84.228.102.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.72	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
66.249.69.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935	Block	1
194.90.129.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-25-2015-14:03:02 to 04-25-2015-15:03:02