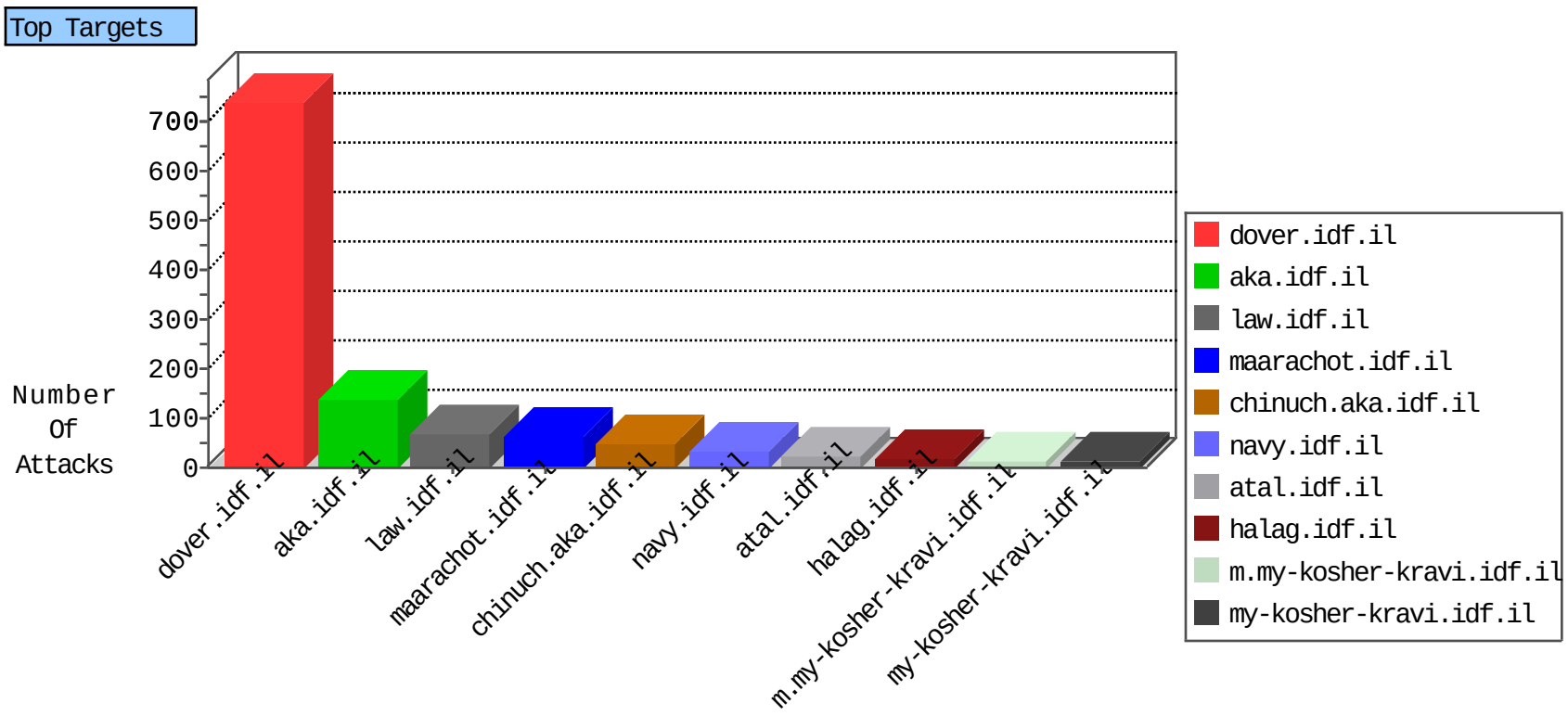
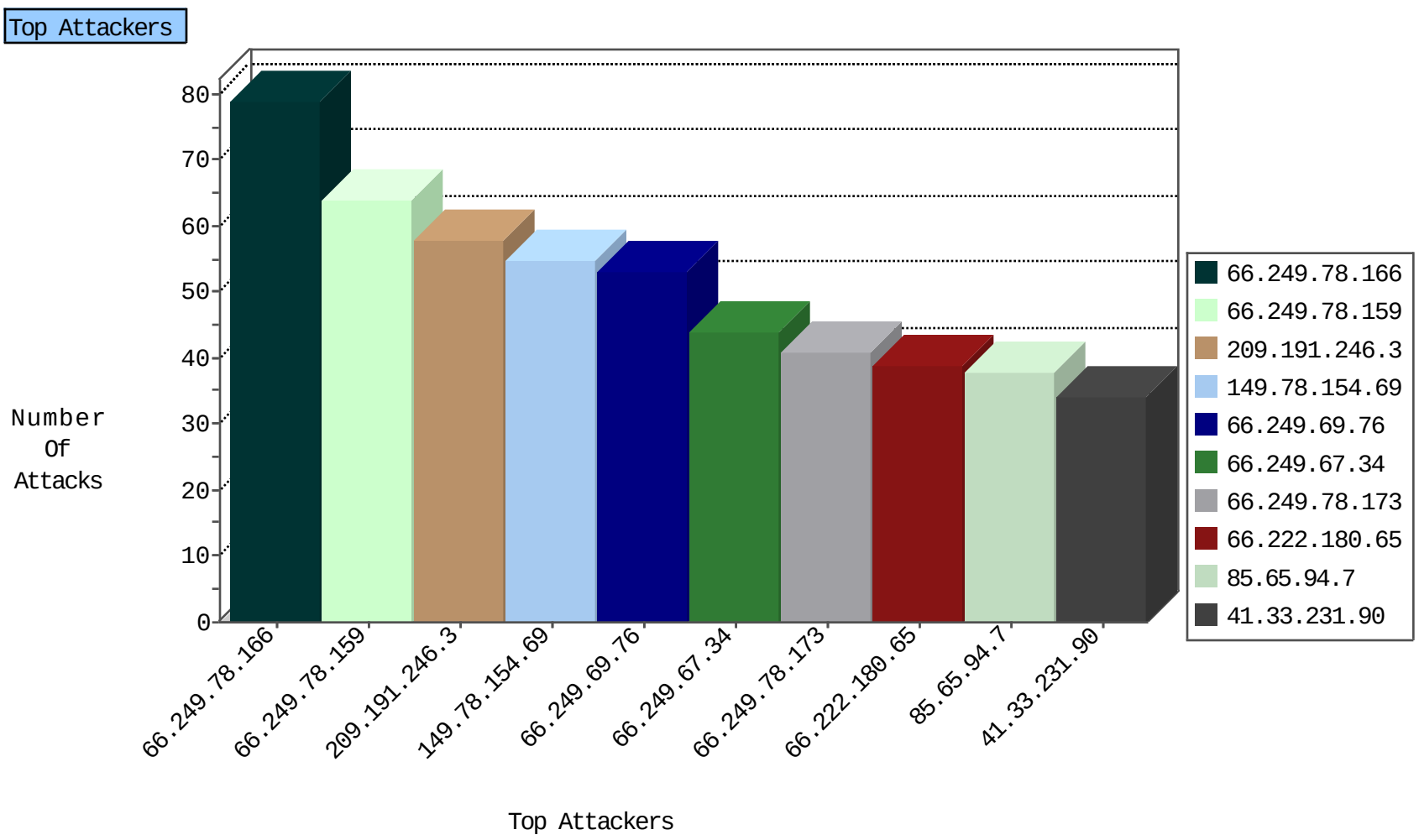
11-01-2015-04:04:03 to 11-01-2015-05:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-01-2015-04:04:03 to 11-01-2015-05:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7201
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2780
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2769
66.222.180.65	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1837
66.249.65.26	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1620
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1490
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	705
66.2.62.178	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	674
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	641
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	444
66.249.75.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	408
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	311
66.249.75.106	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	237
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	229
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	86
85.65.94.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
5.9.156.150	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
66.249.75.2	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.3.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

11-01-2015-04:04:03 to 11-01-2015-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-01-2015-04:04:03 to 11-01-2015-05:04:03

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	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.65.37	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
5.160.187.97	147.237.77.212	Iran, Islamic Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
185.33.8.129	147.237.8.45	Austria	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
180.174.214.26	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.243.34.204	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.52.8	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.76.44	Morocco	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
185.33.8.129	147.237.8.45	Austria	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
169.57.5.20	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.76.44	Morocco	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
41.140.253.9	147.237.76.44	Morocco	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

11-01-2015-04:04:03 to 11-01-2015-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
209.191.246.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.222.180.65	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
50.43.50.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.182.219.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
76.78.229.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
162.236.89.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.94.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
24.214.201.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.2.35.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.35.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
101.226.33.205	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.9.156.150	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
156.184.80.31		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
108.228.145.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.67.6	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.234	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.60	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
197.39.183.77	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
88.198.25.217	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.71.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.3.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.2.62.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-01-2015-04:04:03 to 11-01-2015-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	30
40.143.1.4	United States	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	16
40.77.167.104	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
149.78.197.160	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	15
24.214.201.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	15
207.46.13.177	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	15
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	15
149.78.197.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	15
74.82.47.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	15
49.148.164.106	Philippines	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	15
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/kkkkkkk=748f35d0kkkkkkk_748f35d0	Block	15
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	15
40.77.167.74	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
85.64.154.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	15
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17329.jpg	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	15
40.77.167.80	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
85.65.94.7	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 85.65.94.7	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/inner.asp	Block	15
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/14570.jpg	Block	15

11-01-2015-04:04:03 to 11-01-2015-05:04:03