

Manage the Cloud Security App for IBM QRadar

Contents

[Introduction](#)

[Overview](#)

[Accessing the Cisco Cloud Security App](#)

[Cisco Cloud Security App Components](#)

[Cloud Overview](#)

[Umbrella](#)

[Investigate](#)

[CloudLock](#)

[Enforcement Tab](#)

Introduction

This document describes how to manage the Cisco Cloud Security app for IBM QRadar.

Overview

QRadar from IBM is a popular SIEM for log analysis. It provides a powerful interface for analyzing large chunks of data, such as the logs provided by Cisco Umbrella for your organization's DNS traffic. Information displayed in the Cisco Cloud Security App for IBM QRadar comes through the API's of Cisco Umbrella, CloudLock, Investigate and Enforcement.

When you set up Cisco Cloud Security app for QRadar, it integrates all the data from Cisco Cloud Security platform and allows you to view the data in graphical form in the QRadar console. From the application, analysts can:

- Investigate domains, ip addresses, email addresses
- Block and Unblock domains (enforcement)
- View the information of all the incidents of the network.

This article walks you through how to navigate the Cisco Cloud Security App. Instructions on how to set-up the application can be found here: [Configuring the Cisco Cloud Security App for IBM QRadar](#)

Accessing the Cisco Cloud Security App

To navigate to the Cisco Cloud Security App in IBM QRadar, go to the homepage and click on the **Cisco Cloud Security** tab. The **Cloud Overview** tab and the Dashboard appears. You can then access the **Umbrella**, **Investigate**, **CloudLock** and **Enforcement** tabs to view your logs.

The Cloud Security App is set to show the data from the last 7 days by default. You can change the time frame by clicking on the date range on the top right:

ite

Cloudlock

Enforcement

2018-04-13 18:18 - 2018-04-19 18:18

2018-04-13 18:18

🕒

18

:

18

2018-04-19 18:18

🕒

18

:

18

Last 1 Day

Last 2 Days

Last 7 Days

Last 30 Days

This Month

Last Month

Custom Range

Apply

Cancel

<

Apr 2018

>

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

<

May 2018

>

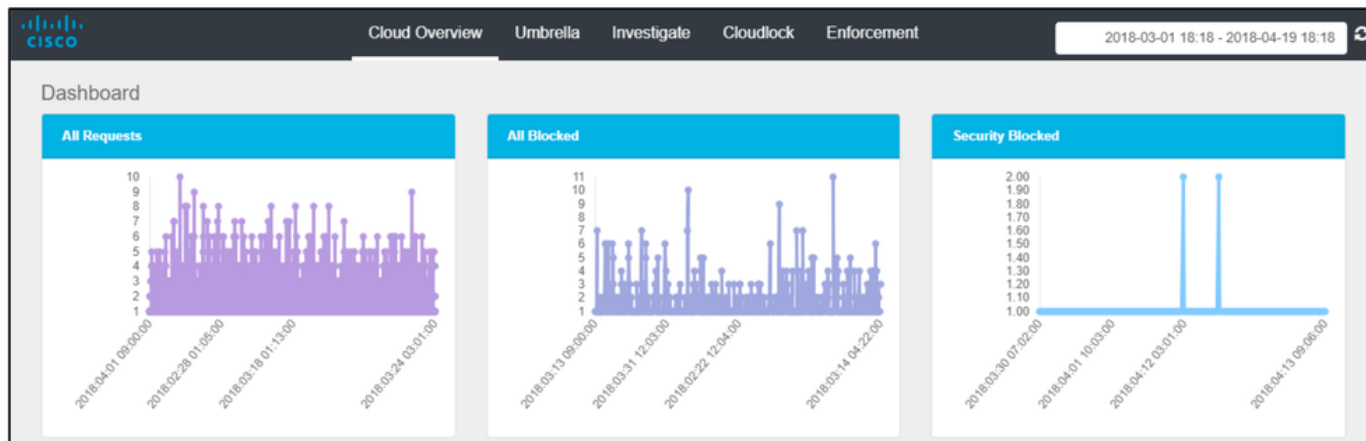
Su	Mo	Tu	We	Th	Fr	Sa
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

360072030052

Cisco Cloud Security App Components

Cloud Overview

The Cloud Overview Tab displays information such as All Requests, All Blocked, Security Blocked, Likely DGA's, Suspicious Secure Rank, Cloudlock Incidents, CloudLock Overall, Top Policies, and Top Offenders in a chart based visual representation.



Likely DGA's		Suspicious Secure Rank ⓘ			
Destination	Last Queried	Destination	Securerank	Status Label	Last Queried
example.com	2018:06:05 01:11	example.com	5.64000	safe	2018:06:05 04:16
example.com	2018:06:02 09:01	example.com	-0.03000	malicious	2018:06:01 01:06
example.com	2018:06:05 01:15	example.com	-0.01000	malicious	2018:06:04 09:20
example.com	2018:06:02 11:04	example.com	-18.92000	malicious	2018:06:03 12:03
example.com	2018:06:08 11:05	example.com	-0.01000	malicious	2018:06:05 01:10
example.com	2018:06:02 01:09				
example.com	2018:06:06 03:20				
example.com	2018:06:04 01:07				
example.com	2018:06:08 12:05				

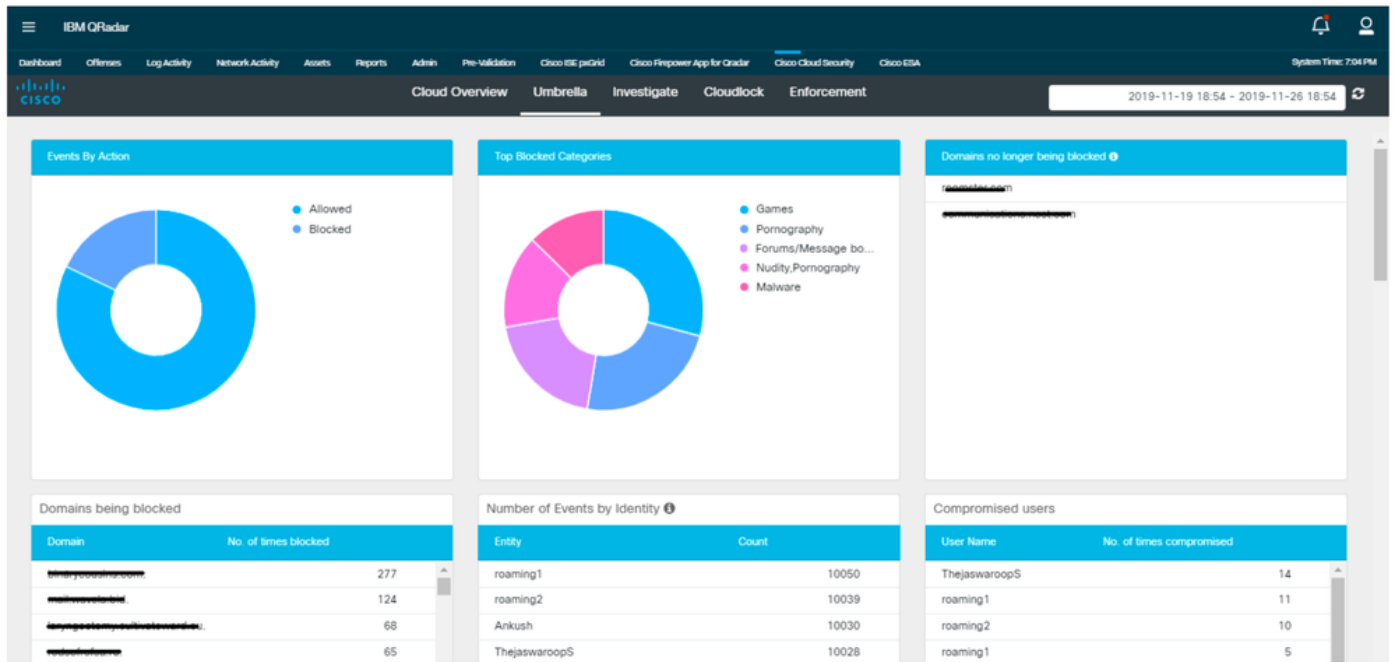
360072257631

Cloudlock Incidents		Cloudlock Top Policies		Cloudlock Top Offenders	
Status	Count	Policy	Count	User Name	Count
New	102548	Social Security Number	1	unknown user	3549
In Progress	12	New Unclassified App Installs	120	Sarat Kumar	3061
Dismissed	3	AppTest	102441	Anuraj C	2205
Resolved	2			Mohit Vaish	2002
				Kedar Bhat	1937
				Touseef Jagirdar	1893
				Rajeev Menon	1818
				Sameer Shelke	1814

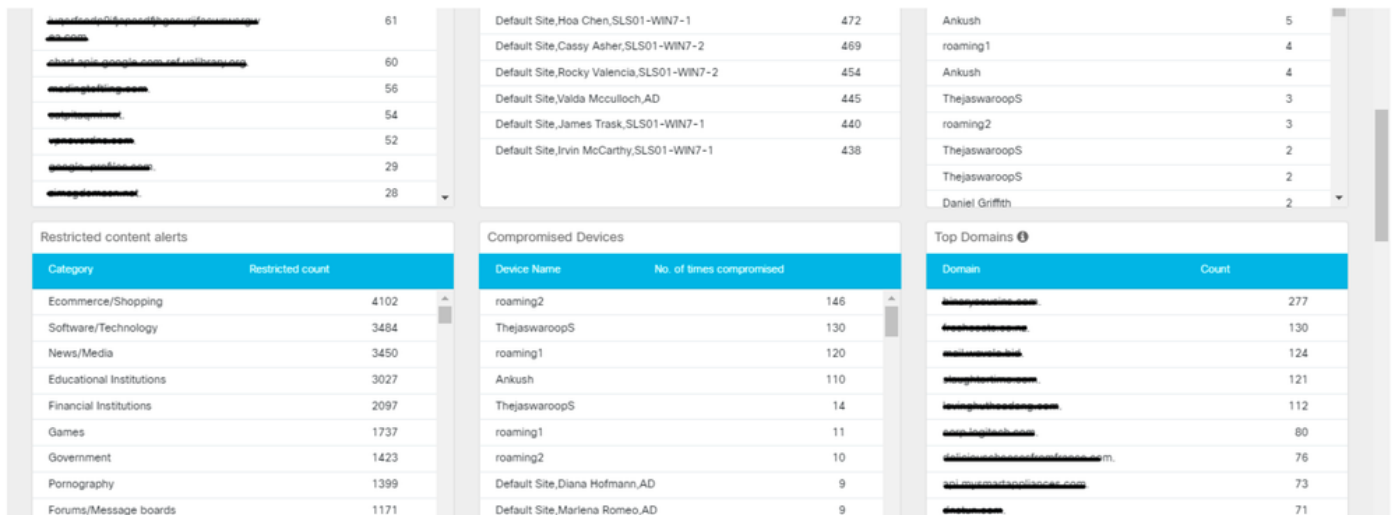
360072257611

Umbrella

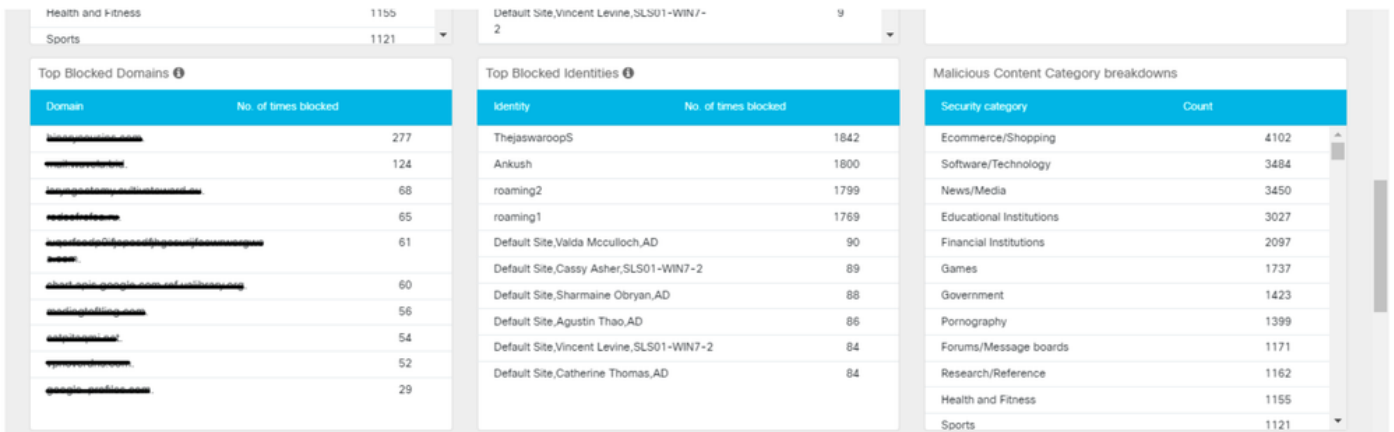
The Umbrella Tab displays information such as Events By Action, Top Blocked Categories, Number of Events by Identity, Domains Being Blocked, Domains No longer being blocked, Compromised Users, Restricted content alerts, Compromised Devices, Top Domains, Top Blocked Domains, Top Blocked Identities, Malicious Content Category breakdowns, Top Categories, Activity and User Access Trend in a chart based visual representation.



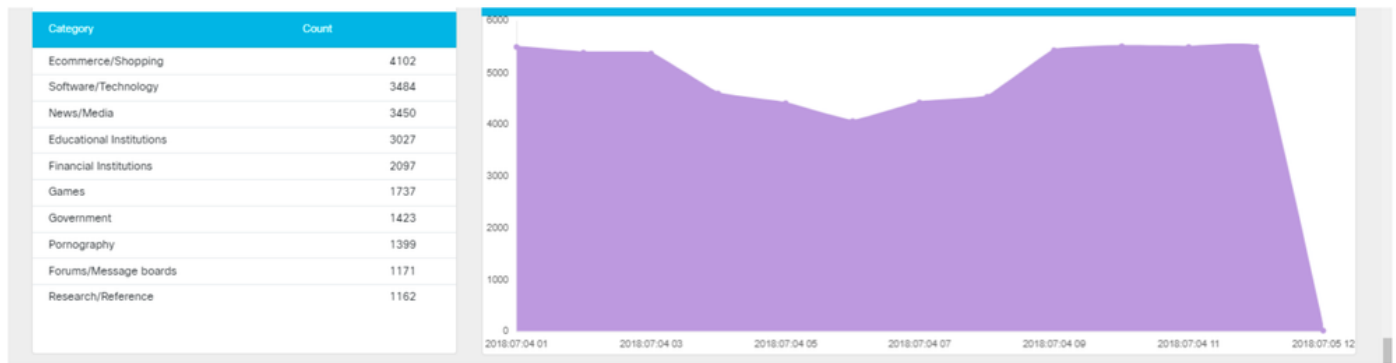
360072263411



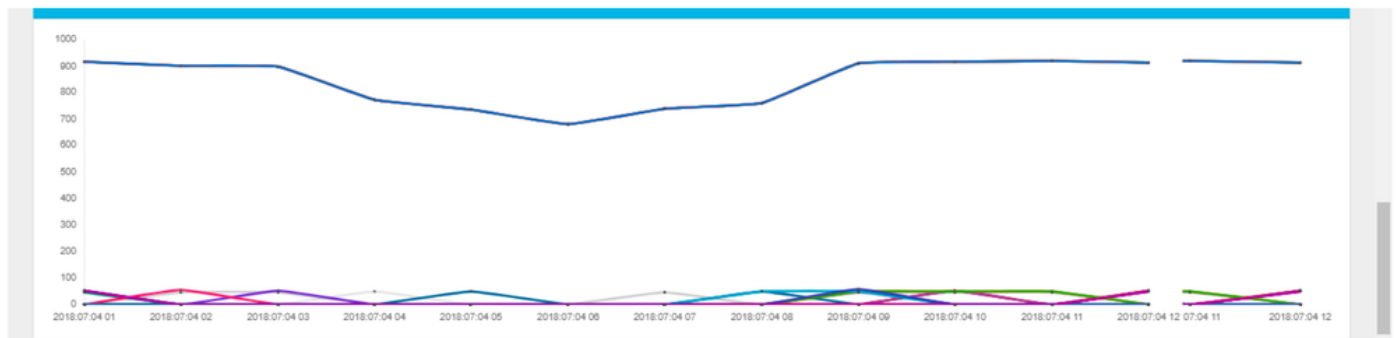
360072263391



360072037372



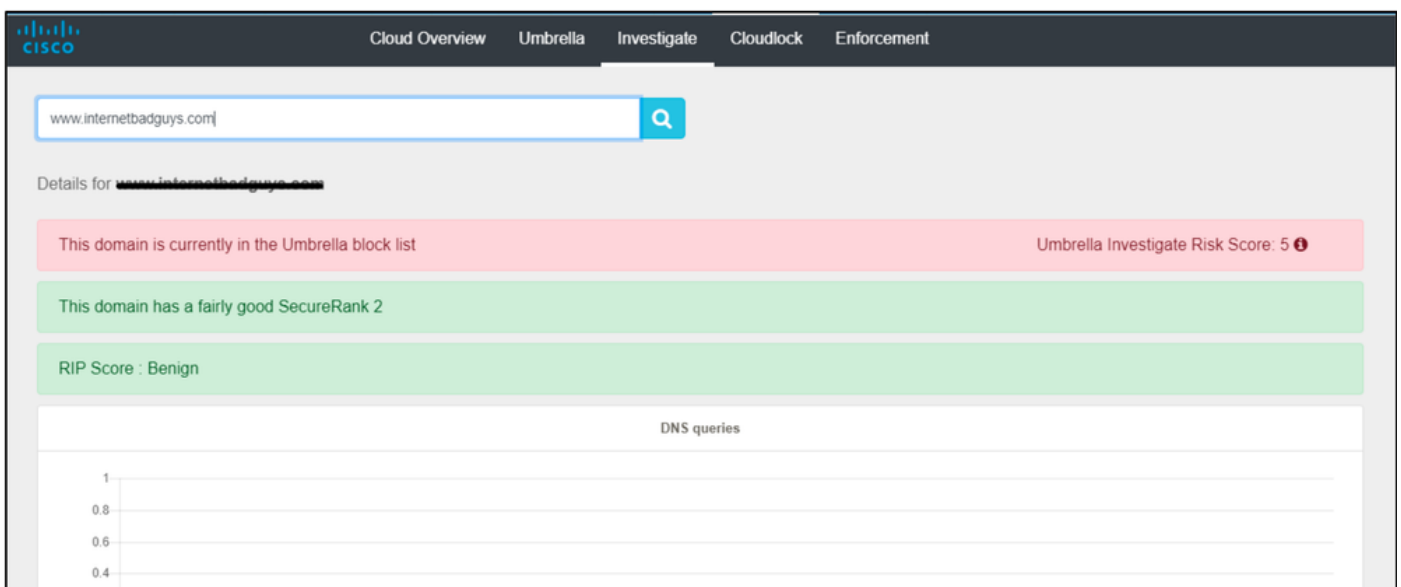
360072263331



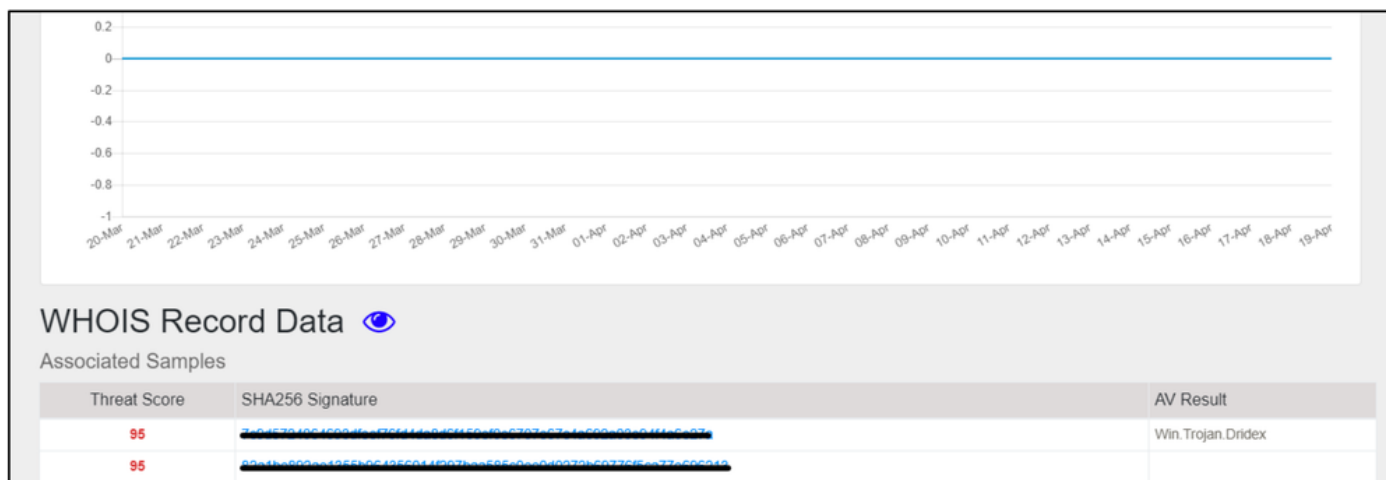
360072263351

Investigate

The Investigate Tab enables the user to search the information related to hostname, URL, ASN, IP, Hash or email address. It also has information such as WHOIS record, DGA information and so on.

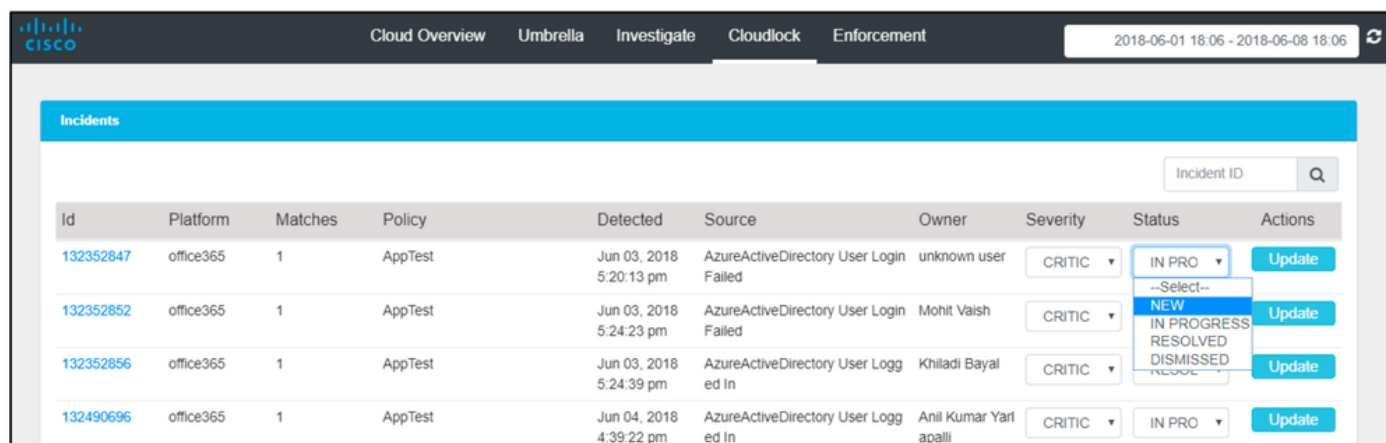


360072263511



Features	
TTLs min	1
TTLs max	1
TTLs mean	1
TTLs median	1
TTLs standard deviation	0
Country codes	US
Country count	1
ASNs	AS 36692
ASNs count	1
Prefixes	67 215.88.0
Prefixes count	1

CloudLock



Users can click on any of the events to view more details about the incident.

Incident Details

Objective Type

Name

Codesign Production

Platform

office365

Owner

██████████@aujas.com

Policy

New Unclassified App Installs

Time

IP Address

Status

NEW

Severity

ALERT

Detected

Match Type

Match

New Unclassified App Install
s

360072042332

Enforcement Tab

The Enforcement tab displays information about which domains are blocked. Users can also select blocked domains and unblock them from this interface.

cloud

cisco

Cloud Overview

Umbrella

Investigate

Cloudlock

Enforcement

2018-04-13 18:18 - 2018-04-19 18:18

Blocked Domains

☐

Domain

Last Seen

☐

aujasdigital.com

Mar 16, 2018 9:46 AM

☐

havanacubanrealestate.co

Mar 28, 2018 11:47 AM

1 - 2 < >

Unblock

360072038472