

黑客视界

EPCYBER 

**Complete this
10 step CTF
and receive a
certification**



INTRODUCTION TO..

***CHINESE
OSINT***

Briefing

Greetings, Special Agent K.

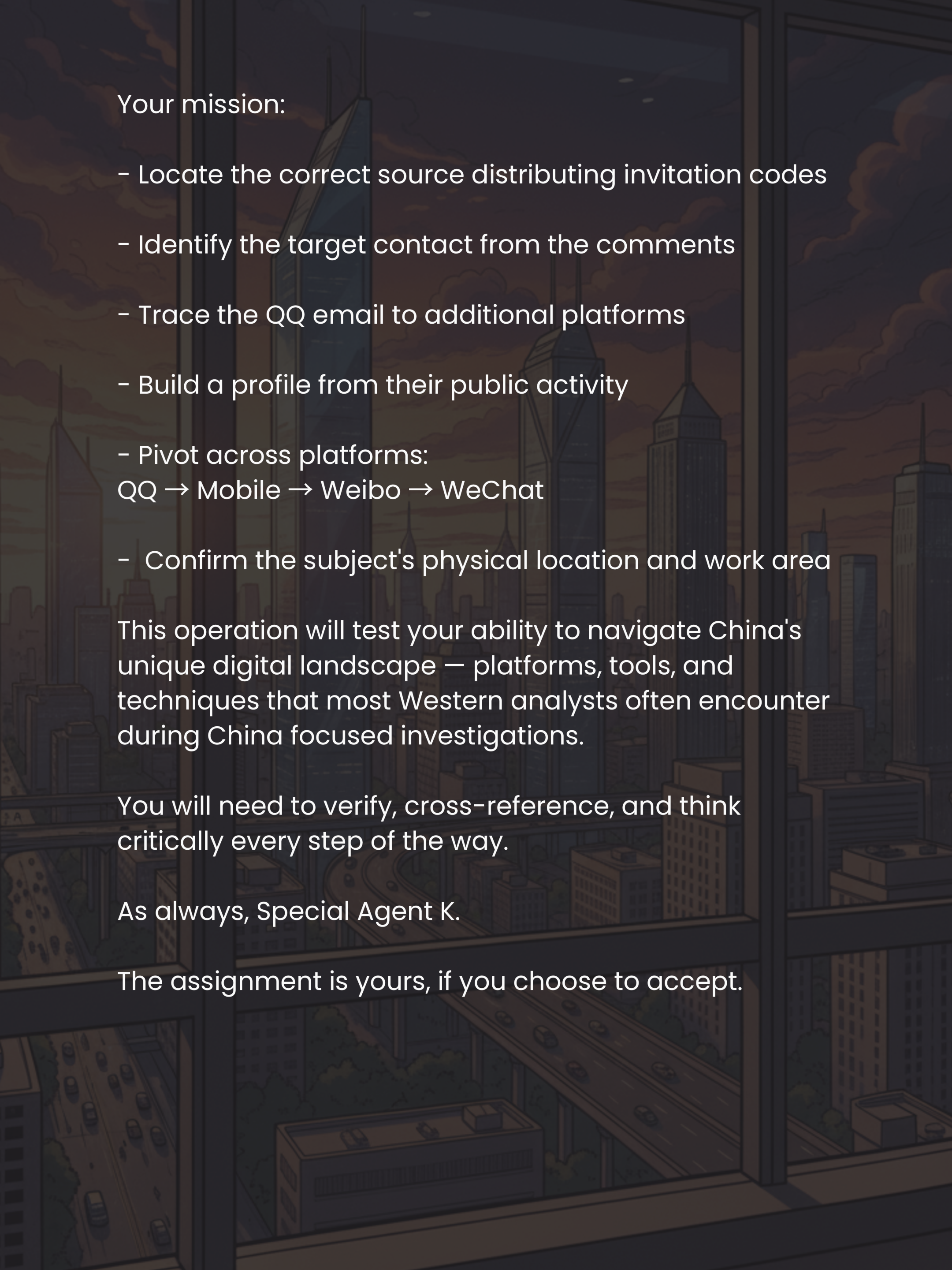
Our signals intelligence specialist, Oriana, intercepted unusual traffic patterns originating from Chinese digital sources. Multiple sites appear to be distributing invitation codes for t00ls — one of China's hacking forums. The codes themselves are not our concern.

What matters is the trail left behind by those publicly asking for access. In the comments sections, individuals have exposed their contact information, unaware they've created a chain of digital breadcrumbs spanning the entire Chinese internet ecosystem.

One such individual caught our attention. We believe they may be connected to a larger network, but we need you to confirm their real identity and location before we can proceed.

Complication: The target did not just leave an email address. They have an extensive digital footprint across Chinese platforms — answering questions, revealing their profession, their daily commute, their neighborhood.

Every answer they gave was another breadcrumb.



Your mission:

- Locate the correct source distributing invitation codes
- Identify the target contact from the comments
- Trace the QQ email to additional platforms
- Build a profile from their public activity
- Pivot across platforms:
QQ → Mobile → Weibo → WeChat
- Confirm the subject's physical location and work area

This operation will test your ability to navigate China's unique digital landscape — platforms, tools, and techniques that most Western analysts often encounter during China focused investigations.

You will need to verify, cross-reference, and think critically every step of the way.

As always, Special Agent K.

The assignment is yours, if you choose to accept.

Materials

Eleven objective files, start with the first.

Answer Instruction

Each ZIP archive is unlocked with the answer to the previous objective. When you unlock the last objective, you find a certificate PDF. The first file has no password.

This is a certification CTF, there are no hints. You will find pointers to the answer formats in the files.

Using the ZIP files

Be advised, the archives are encrypted ZIP. Make sure your OS supports the ZIP format. Ensure the passwords contain no hidden characters or formatting.

Support

If you get stuck, head over to our Discord and ask around in the #CTF-SUPPORT channel.

Acknowledgements

This CTF was made by Eva Prokofiev from EPCYBER.
Artwork and cert by Frank Diepmaat from HACKTORIA.
QA done by Joseph Leroux from HACKTORIA.

In collaboration with EPCYBER

Learn advanced threat detection skills on China, OSINT and the Dark web.

Equip professionals and those who want to become them with real industry-relevant skills. The main issue with existing training vendors in the industry, especially in areas of China OSINT, dark web, is you mostly get information instead of learning the actual skills you need to move up in your careers.

<https://epcyber.com>



Eva Prokofiev

Former Military Intelligence Officer from a Special Operations Division, I work at the intersection of OSINT, cyber threat intelligence, and intelligence collection across high-risk digital environments.

Over the past 15+ years, I've trained and supported European defense contractors, US and NATO-aligned agencies, and intelligence teams operating in complex and sensitive regions.

My core expertise centers on China OSINT, dark-web intelligence, and advanced threat detection.