CROWDSTRIKE

# LANGUAGE AND CULTURE IN THREAT INTELLIGENCE

MITCHELL EDWARDS

CROWDSTRIKE VIRTUAL OPERATIONS SPECIALIST, DEV OPS

OG FUZZYSNUGGLYDUCK

CROWDSTRIKE

# ABOUT ME

(关于我）

BA Computer Science, BA Mandarin Chinese (University of Mississippi)

CROWDSTRIKE

# ABOUT ME

(关于我）

BA Computer Science, BA Mandarin Chinese (University of Mississippi)

3 months intensive study in Shanghai Pudong University (上海浦东大学）

CROWDSTRIKE

# ABOUT ME
(关于我）

BA Computer Science, BA Mandarin Chinese (University of Mississippi)

3 months intensive study in Shanghai Pudong University (上海浦东大学）

Chinese social media and hacktivism research

CROWDSTRIKE

# ABOUT ME
(关于我）

BA Computer Science, BA Mandarin Chinese (University of Mississippi)

3 months intensive study in Shanghai Pudong University (上海浦东大学）

Chinese social media and hacktivism research

Hacking the Great Firewall

CROWDSTRIKE

# ABOUT ME

(关于我）

Crowdstrike Virtual Operations Specialist, Dev Ops

CROWDSTRIKE

# ABOUT ME

(关于我）

Crowdstrike Virtual Operations Specialist, Dev Ops

Chinese-language targeting, collections and collections automation

CROWDSTRIKE

# ABOUT ME

(关于我）

Crowdstrike Virtual Operations Specialist, Dev Ops

Chinese-language targeting, collections and collections automation

Trigger words:

“Dark/Deep Web”

“Blockchain”

CROWDSTRIKE

# CHINESE COLLECTIONS

(中国情报研究）

CROWDSTRIKE

# LANGUAGE AND CULTURE

(语言和文化)

Culture : the customary beliefs, social forms, and material traits of a racial, religious, or social group also : the characteristic features of everyday existence (such as diversions or a way of life) shared by people in a place or time. (Webster's)

CROWDSTRIKE

# LANGUAGE AND CULTURE

(语言和文化)

Culture : the customary beliefs, social forms, and material traits of a racial, religious, or social group also : the characteristic features of everyday existence (such as diversions or a way of life) shared by people in a place or time. (Webster's)

Culture affects how we interact with those within our own culture and those outside of it.

CROWDSTRIKE

# LANGUAGE AND CULTURE

(语言和文化)

Language : a series of grunts we use to trade memes. (Me)

CROWDSTRIKE

# LANGUAGE AND CULTURE

(语言和文化)

Language : a series of grunts we use to trade memes. (Me)

While culture is the set of rules and customs we use to interact with others, language is the medium by which we take part in those interactions

CROWDSTRIKE

# INTELLIGENCE AND LANGUAGE

(情报和语言）

Intelligence is shaped by data and information collection, which takes different forms depending on the target region’s language.

CROWDSTRIKE

# INTELLIGENCE AND LANGUAGE

(情报和语言）

Intelligence is shaped by data and information collection, which takes different forms depending on the target region’s language.

Cultural, ethnic and regional nuances shape each character’s meaning, with connotation potentially changing the entire meaning of a word.

CROWDSTRIKE

# INTELLIGENCE AND LANGUAGE

(情报和语言)

Intelligence is shaped by data and information collection, which takes different forms depending on the target region's language.

Cultural, ethnic and regional nuances shape each character's meaning, with connotation potentially changing the entire meaning of a word.

Edgar Snow's interview with Mao Zedong (毛泽东) is a great example.

CROWDSTRIKE

# INTELLIGENCE AND CULTURE

(情报和文化)

Interacting with sources relies on deep cultural and lingual knowledge.

CROWDSTRIKE

# INTELLIGENCE AND CULTURE

(情报和文化)

Interacting with sources relies on deep cultural and lingual knowledge.

Knowing how to create a cover, interact with sources and gather intelligence relies on using regional, ethnic and political cultural knowledge.

CROWDSTRIKE

# INTELLIGENCE AND CULTURE

(情报和文化)

Interacting with sources relies on deep cultural and lingual knowledge.

Knowing how to create a cover, interact with sources and gather intelligence relies on using regional, ethnic and political cultural knowledge.

Creating a persona that is supposedly based in Shanghai while using Beijing's harsh accent in writing or speech is a sure-fire easy way to be uncovered.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

China used to run wide open.

Forums and group memberships were open, attacks easy to attribute and tools usually copies or rip-offs from the West.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

## (中国情报研究特色的问题)

Now, China is a hardened target.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Now, China is a hardened target.

High-value sites and group chats are often hard to come by, censorship is a constant issue and the GFW gives constant headaches.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Now, China is a hardened target.

High-value sites and group chats are often hard to come by, censorship is a constant issue and the GFW gives constant headaches.

Decentralization makes collections incredibly difficult.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

## (中国情报研究特色的问题)

Increasingly strict domestic hacking laws have made potential sources much quieter.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Increasingly strict domestic hacking laws have made potential sources much quieter.

Self-censorship creates better operational security.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Increasingly strict domestic hacking laws have made potential sources much quieter.

Self-censorship creates better operational security.

Isolationist policies, such as the Pwn2Own incident, has shown China is becoming increasingly adverse to international sharing efforts.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

## (中国情报研究特色的问题)

The Great Firewall is a problem for Chinese researchers, both foreign and domestic.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

The Great Firewall is a problem for Chinese researchers, both foreign and domestic.

You thought finding a good VPN for traveling inside of China was hard?

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Chinese hacker groups have a unique cultural hierarchy, and they are often close-knit groups.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Chinese hacker groups have a unique cultural hierarchy, and they are often close-knit groups.

Groups often congregate in invite-only forums or WeChat groups, a much more hardened target than wide-open eCrime forums seen in Eastern European and Western circles.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

(中国情报研究特色的问题)

Central hacking tools are often traded and sold in kits, with forums and WeChat/QQ groups used to propagate new versions and discuss use cases.

CROWDSTRIKE

# UNIQUE DIFFICULTIES IN CHINESE COLLECTIONS

## (中国情报研究特色的问题)

Central hacking tools are often traded and sold in kits, with forums and WeChat/QQ groups used to propagate new versions and discuss use cases.

This means there can be multiple versions of a single tool, spread among many different actors with different motivations and use cases.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

Technical, tactical intelligence is awesome, but we as intelligence professionals want to be proactive.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

Technical, tactical intelligence is awesome, but we as intelligence professionals want to be proactive.

Interacting with sources, those with access to tools, tactics, techniques and procedures before they’re ever used on a target network, is one of the best ways to be proactive.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看 )

There are plenty of certifications to prove or imply technical capability.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看 )

There are plenty of certifications to prove or imply technical capability.

Aside from college degrees and federal tests, we don’t have certifications or standards to judge an analyst’s lingual capability.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

There are plenty of certifications to prove or imply technical capability.

Aside from college degrees and federal tests, we don’t have certifications or standards to judge an analyst’s lingual capability.

Until such standards have been applied, we need to promote the hiring of interdisciplinary analysts from all walks of life, especially those involving lingual capabilities.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

As vendors, we need to hire and equip lingual and cultural experts with the tools, training and access they need to collect, process and disseminate foreign language intelligence.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

As vendors, we need to hire and equip lingual and cultural experts with the tools, training and access they need to collect, process and disseminate foreign language intelligence.

As intelligence consumers, we need to know what questions to ask, and we need to know what analysts or vendors to ask.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

Questions to ask vendors and analysts:

Do you foresee business ties with Taiwan or Hong Kong as being a future flashpoint for reactionary political attacks?

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

Questions to ask vendors and analysts:

Do you foresee business ties with Taiwan or Hong Kong as being a future flashpoint for reactionary political attacks?

Are there any opportunities for lingual/cultural trainings for in-house analysts, sales or management?
Does my vendor have lingual/cultural expertise in their wheelhouse?

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

Questions to ask vendors and analysts:

Do you foresee business ties with Taiwan or Hong Kong as being a future flashpoint for reactionary political attacks?

Are there any opportunities for lingual/cultural trainings for in-house analysts, sales or management? Does my vendor have lingual/cultural expertise in their wheelhouse?

What is happening in China that could effect operations or intellectual property? Follow the culture to the politics, follow the strategic to the tactical.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

We need basic lingual and cultural training for vendor and in-house analysts and collectors, and we need to get better at explaining these lingual and cultural nuances to consumers.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看）

We need basic lingual and cultural training for vendor and in-house analysts and collectors, and we need to get better at explaining these lingual and cultural nuances to consumers.

We need a strategic focus on threat intelligence that goes beyond YARA rules and binary reports.

CROWDSTRIKE

# LOOKING FORWARD

(给今后看 )

Proactive threat intelligence isn’t easy.

CROWDSTRIKE

# THANK YOU!

(谢谢你!)