



GREAT
Global Research
& Analysis Team

THE ETHICS AND PERILS OF APT RESEARCH

An Unexpected Transition into Intelligence Brokerage

Juan Andres Guerrero-Saade
Senior Security Researcher, GREAT, Kaspersky Lab
[@juanandres_gs](#)



THE ETHICS AND PERILS OF APT RESEARCH

An Unexpected Transition into Intelligence Brokerage

Juan Andres Guerrero-Saade
Senior Security Researcher, GReAT, Kaspersky Lab
@juanandres_gs





A Little Meta-Discussion

FIRST THINGS FIRST...

- This is a complex topic
- I will refer you to the paper
- I may refer you to a second paper
- I am genuinely interested in further discussion

WHAT CAN WE COVER?

WHY COVER IT THIS WAY?

FIRST THINGS FIRST...

This is a complex topic

I will refer you to the paper

I may refer you to a second paper

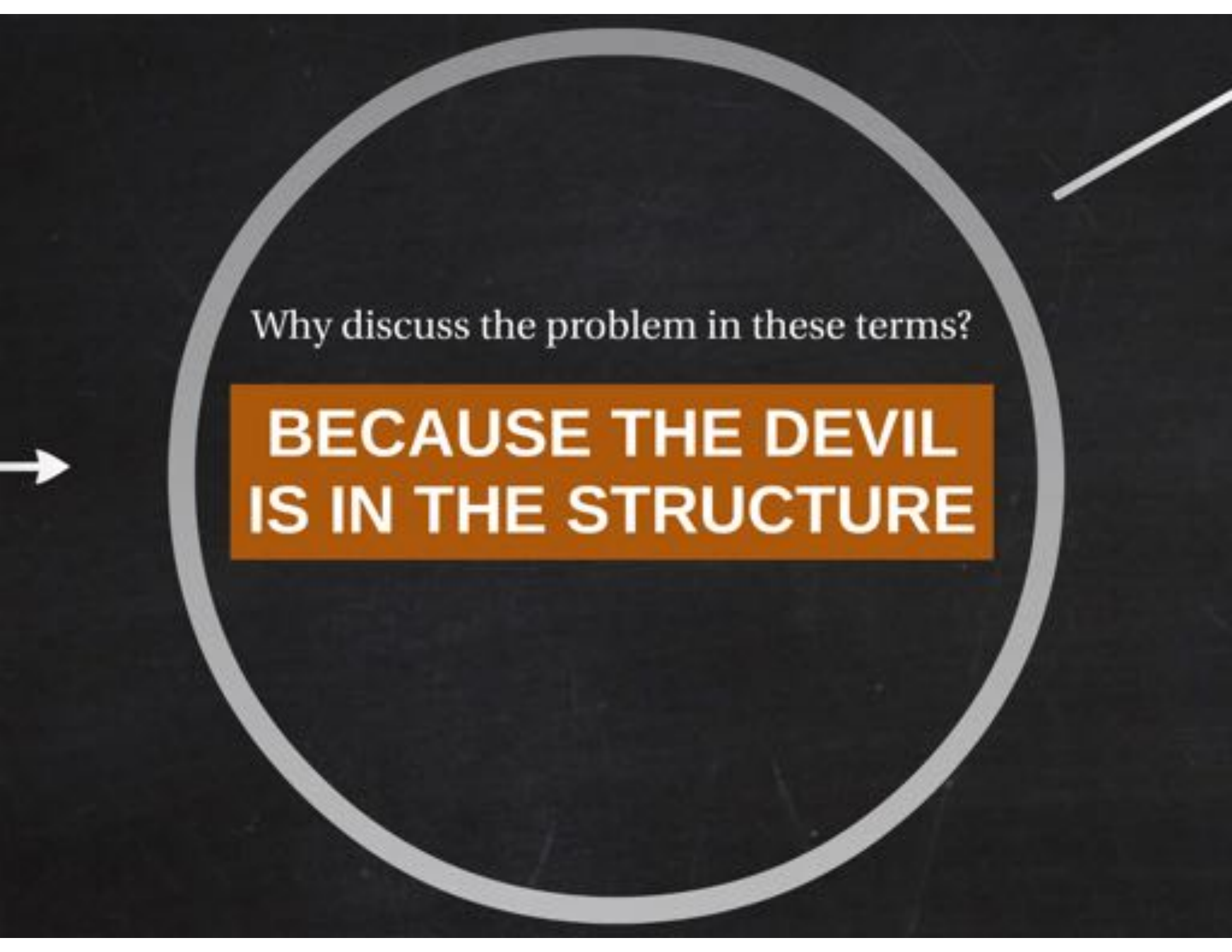
I am genuinely interested in further discussion



WHAT CAN WE COVER?



WHY COVER IT THIS WAY?



Why discuss the problem in these terms?

**BECAUSE THE DEVIL
IS IN THE STRUCTURE**

WHY ARE WE IN THIS POSITION?

We have failed to understand
**CYBERESPIONAGE AS A
PART OF ESPIONAGE
PROPER**

We have failed to accept our role as
INTELLIGENCE BROKERS

We have failed to understand

**CYBERESPIONAGE AS A
PART OF ESPIONAGE
PROPER**

We have failed to accept our role as

INTELLIGENCE BROKERS

PERILS & ETHICAL COMPLICATIONS

Individual Perils

- Public Perilous
- Perilous Collisions
- Bribery
- Compromise and Bias
- Legal Rights Issues
- Threat to Confidentiality
- Threat to Safety

Continued...

Company Perils

- Public, financial, and regulatory exposures
- Disruption of government contracts and partnerships
- Reputational, financial, and legal damage

Continued...

Ethical Problems

- Lack of Whistleblower Identification
- Inability to Enforce Internal Control Systems

Continued...

Individual Perils

- Subtle Pressure
- Patriotic Enlistment
- Bribery
- Compromise and Blackmail
- Legal Repercussions
- Threat to Livelihood
- Threat to Viability of Life
- Threat of Force
- **Elimination...**

Company Perils

- Political, financial, and regulatory repercussions
- Termination of government contracts and partnerships
- Rumors, insinuation, and smear campaigns

**REDUCING THE FINANCIAL VIABILITY OF A
FOR-PROFIT ORGANIZATION IS TANTAMOUNT
TO ELIMINATION**

Ethical Problems

- Lack of Malware Diversification
- Inability to Discern Intention Behind Tasking

**INTELLIGENCE AGENCIES ARE A
SOCIETAL RESPONSE TO DUPLICITY**

OPERATIONAL METHODOLOGY

Threat Intelligence has appropriated a **patchwork intelligence production methodology** responsible for its woes

INTELLIGENCE AGENCIES

- Request
- Gather
- Analyse
- Strategize
- Deliver

Result: Actionable Intelligence



THREAT INTEL TEAMS

- No delimiting **REQUEST** necessary
- **Gathering** samples, indicators, C2 infra
- Myopic **analyses** based on oversimplification
- **Strategy** deferred to PR or Sales departments
- Non-actionable **delivery** or wide-distribution release

Result: PR, Marketing, Incident Response

INTELLIGENCE AGENCIES

- Request
- Gather
- Analyse
- Strategize
- Deliver

Result: Actionable Intelligence





THREAT INTEL TEAMS

- No delimiting **REQUEST** necessary
- **Gathering** samples, indicators, C2 infra
- Myopic **analyses** based on oversimplification
- **Strategy** deferred to PR or Sales departments
- Non-actionable **delivery** or wide-distribution release

**Result: PR, Marketing,
Incident Response**

AN UNACCEPTABLE GLIMMER...

Forcing the CameraShy into the Limelight



A STRATEGIC CALCULUS

WHAT IS ACTIONABLE?



AGENTIAL REGENCY





WHAT IS ACTIONABLE?



AGENTIAL REGENCY



**WHO WILL VALIDATE
THREAT INTELLIGENCE?**





THE ETHICS AND PERILS OF APT RESEARCH

An Unexpected Transition into Intelligence Brokerage

Juan Andres Guerrero-Saade
Senior Security Researcher, GReAT, Kaspersky Lab
@juanandres_gs