RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: **HTA-R09**

Reverse Engineering Attribution: The Man Behind the Man Behind the Curtain

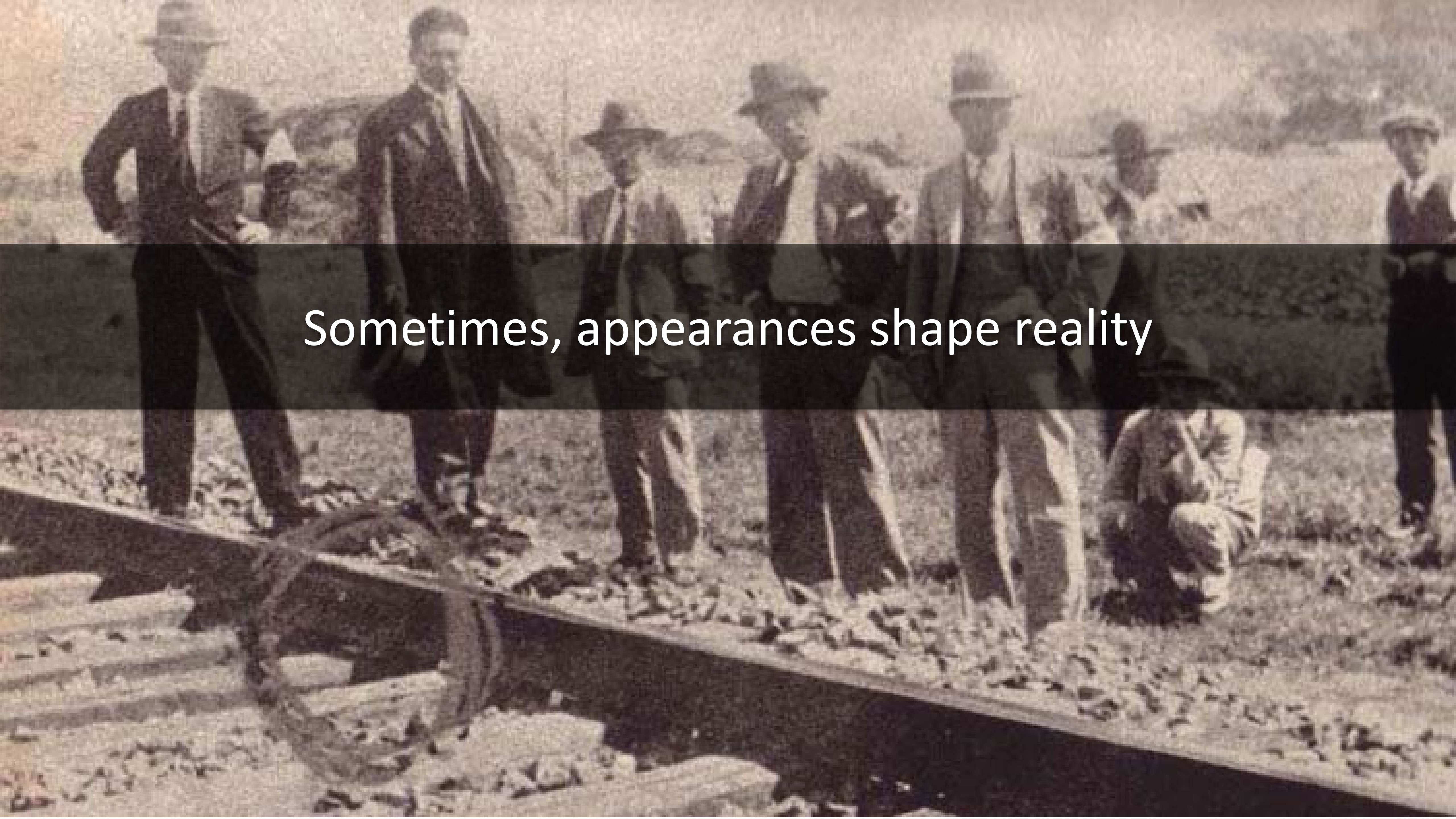
Jayce Nichols

Senior Director, Intelligence Research
FireEye

John Miller

Director, Intelligence Analysis
FireEye

#RSAC



Sometimes, appearances shape reality

What’s the “real story” on cyber false flags?

What should I do about it?

RSAConference2019

Attribution Analysis Today

What factors are considered in attribution analysis?

Group activity together

- Tools | *malware, certificates…*
- TTPs | *lures, exploits…*
- Identifiers | *passwords, registrants…*
- Infrastructure | *domains, netblocks…*
- Metadata | *PDB strings, doc authors…*

Identify the culprit

- Infrastructure | *IPs, domains.…*
- Online identity | *social media, email…*
- Targets | *dissidents, politicians…*
- Linguistics | *code comments, typos…*
- Pattern of life | *timezone, holidays…*

How Hard Is Misattribution, Really?

How Hard Is Misattribution, Really?

if you can….

Use malware tied to previous operations ✓

How Hard Is Misattribution, Really?

if you can….

Manipulate code metadata ✓

How Hard Is Misattribution, Really?

if you can….

Use documented TTPs ✓

How Hard Is Misattribution, Really?

if you can….

Create a confusing targeting picture ✓

How Hard Is Misattribution, Really?

if you can….

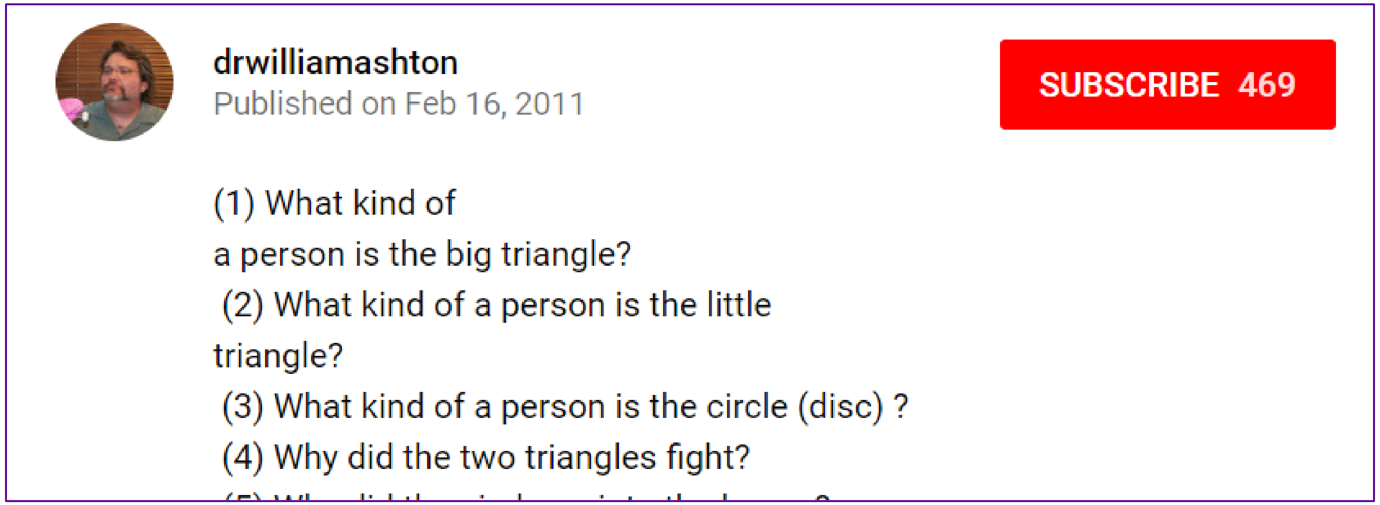
Avoid dumb mistakes ✓

RSA®Conference2019

Fundamental Challenges to Attribution Analysis

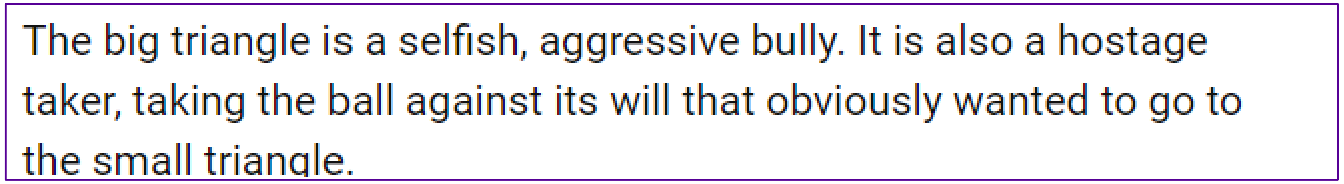
Cyber threat intelligence can be a bit like this

Cyber threat intelligence can be a bit like this

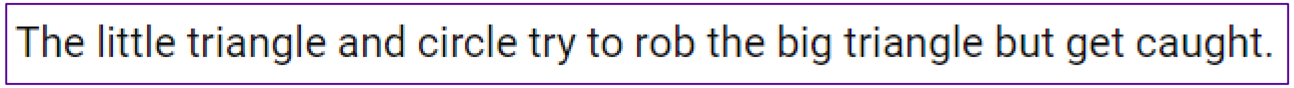


drwilliamashton
Published on Feb 16, 2011

(1) What kind of
a person is the big triangle?
(2) What kind of a person is the little
triangle?
(3) What kind of a person is the circle (disc) ?
(4) Why did the two triangles fight?

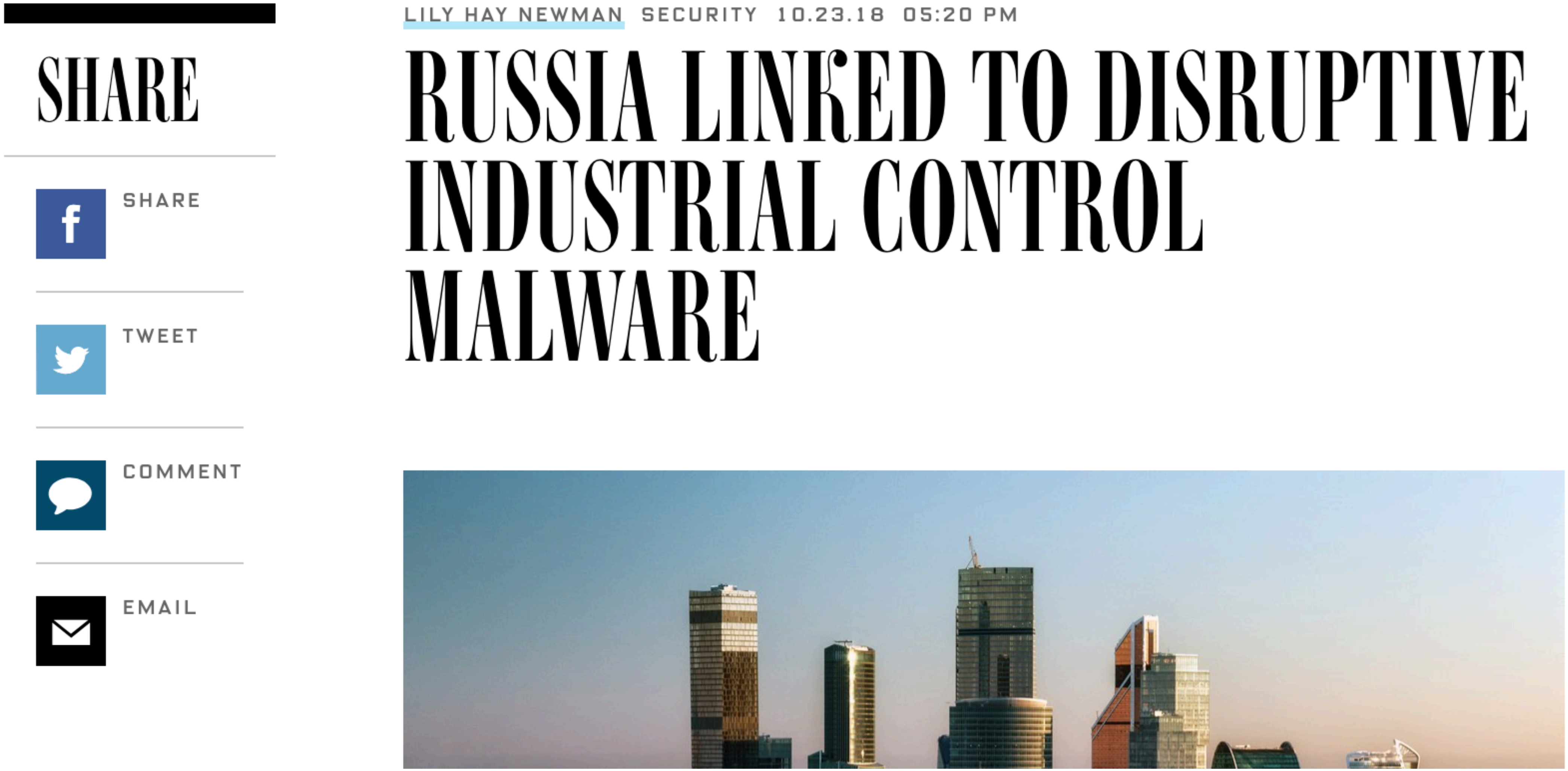


The big triangle is a selfish, aggressive bully. It is also a hostage taker, taking the ball against its will that obviously wanted to go to the small triangle.



The little triangle and circle try to rob the big triangle but get caught.

Attribution publication cuts both ways



SHARE

SHARE

TWEET

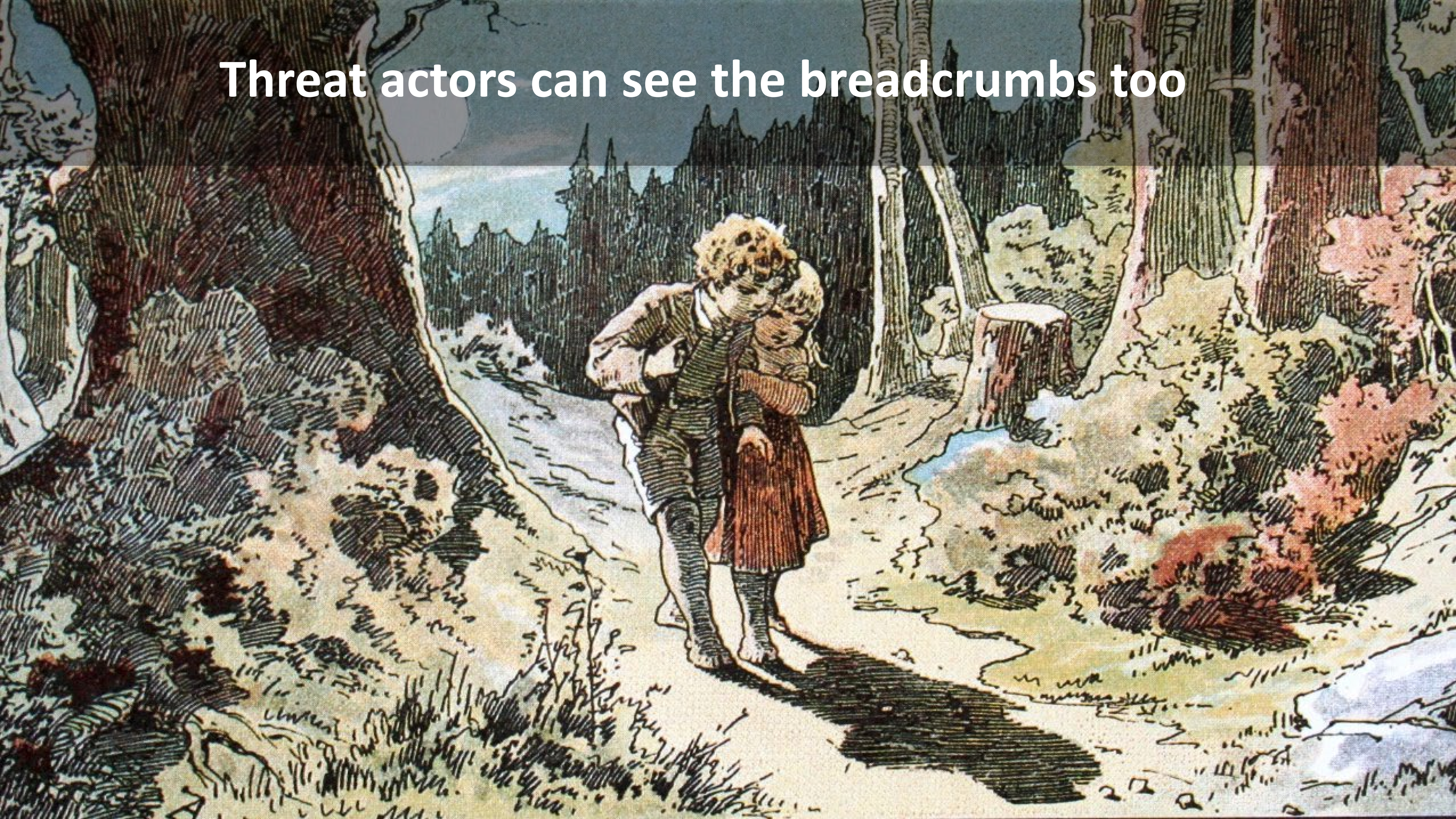
COMMENT

EMAIL

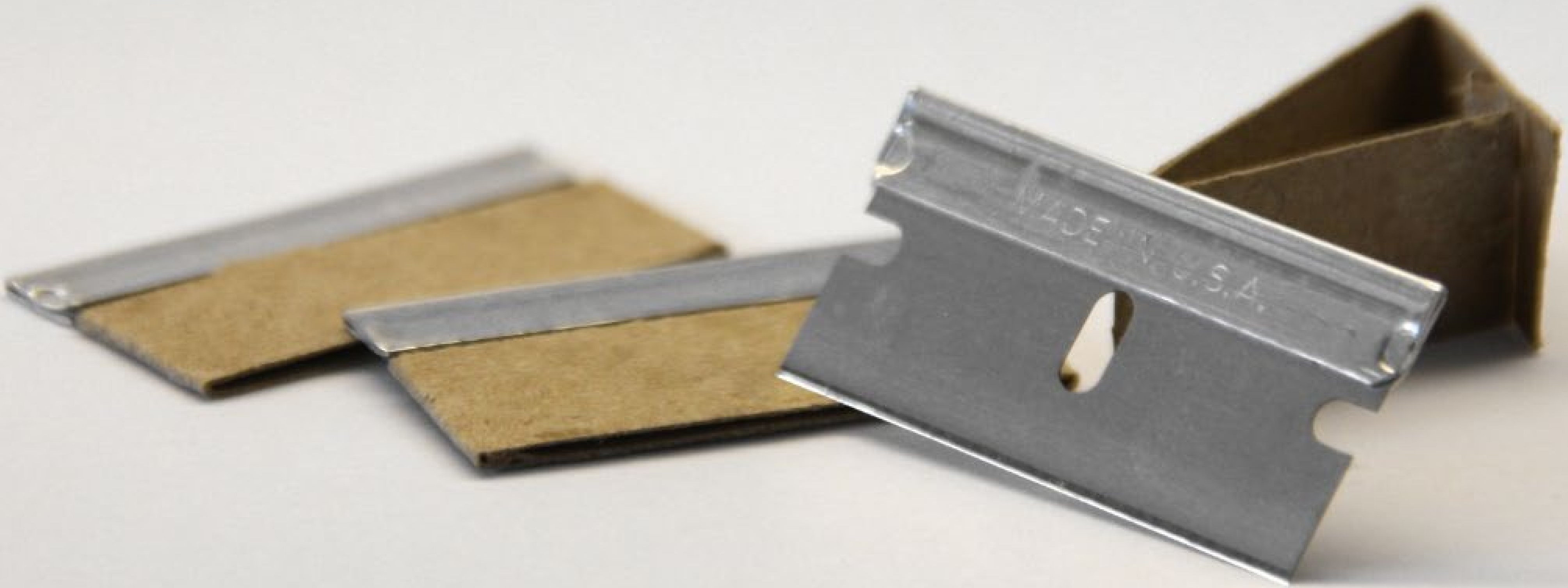
LILY HAY NEWMAN SECURITY 10.23.18 05:20 PM

RUSSIA LINKED TO DISRUPTIVE INDUSTRIAL CONTROL MALWARE

Threat actors can see the breadcrumbs too



When is the simplest explanation wrong?



Attribution makes headlines

RSAConference2019

Why Misdirect Attribution Analysis?

Why misdirect attribution analysis?

Decrease target’s prioritization of incident

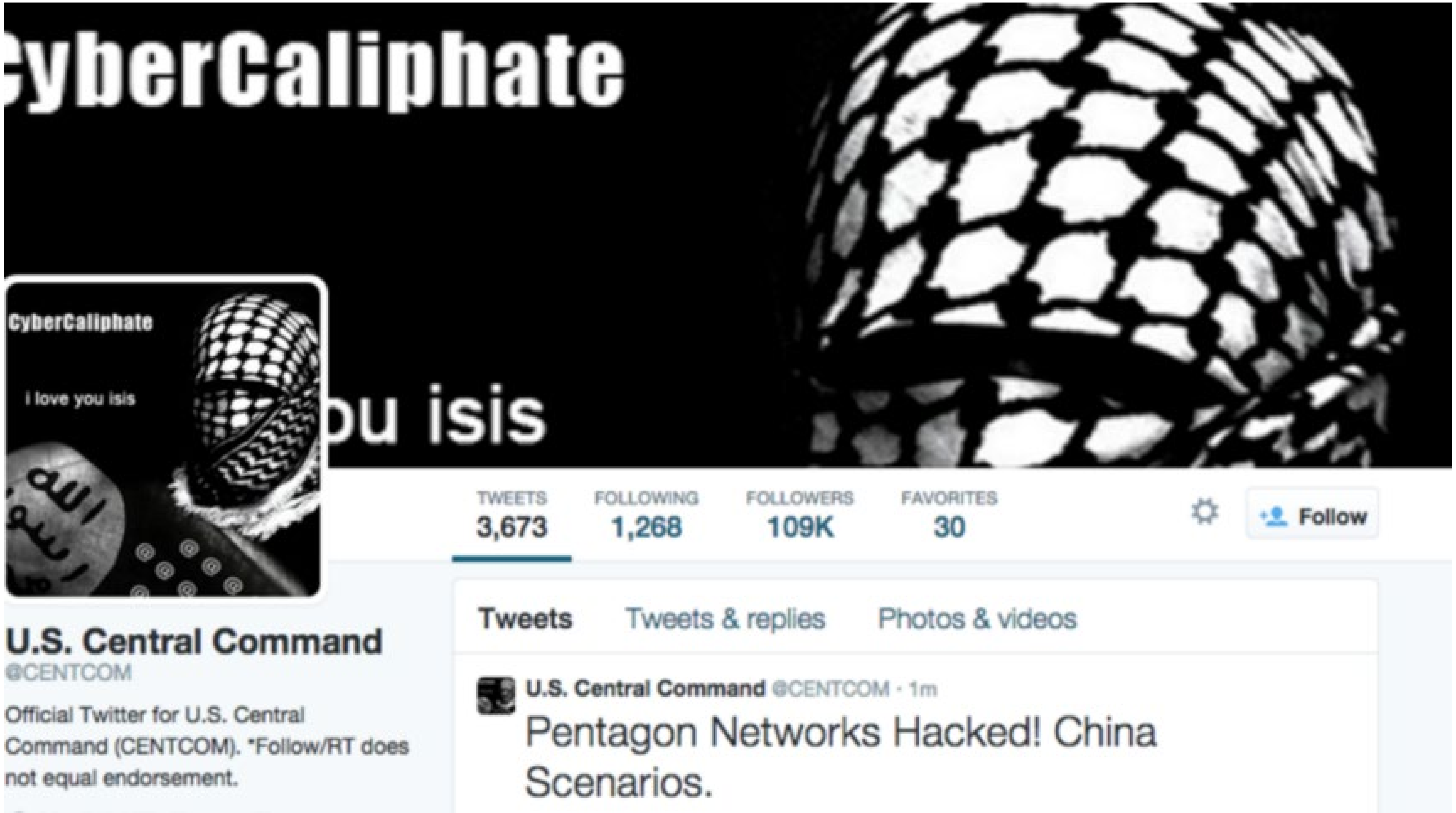
Reduce risk for sensitive operations

Create pretext for desired action

RSAConference2019

Attribution Deception Happens

Attribution deception happens!



U.S. Central Command
@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

U.S. Central Command @CENTCOM · 1m
Pentagon Networks Hacked! China Scenarios.

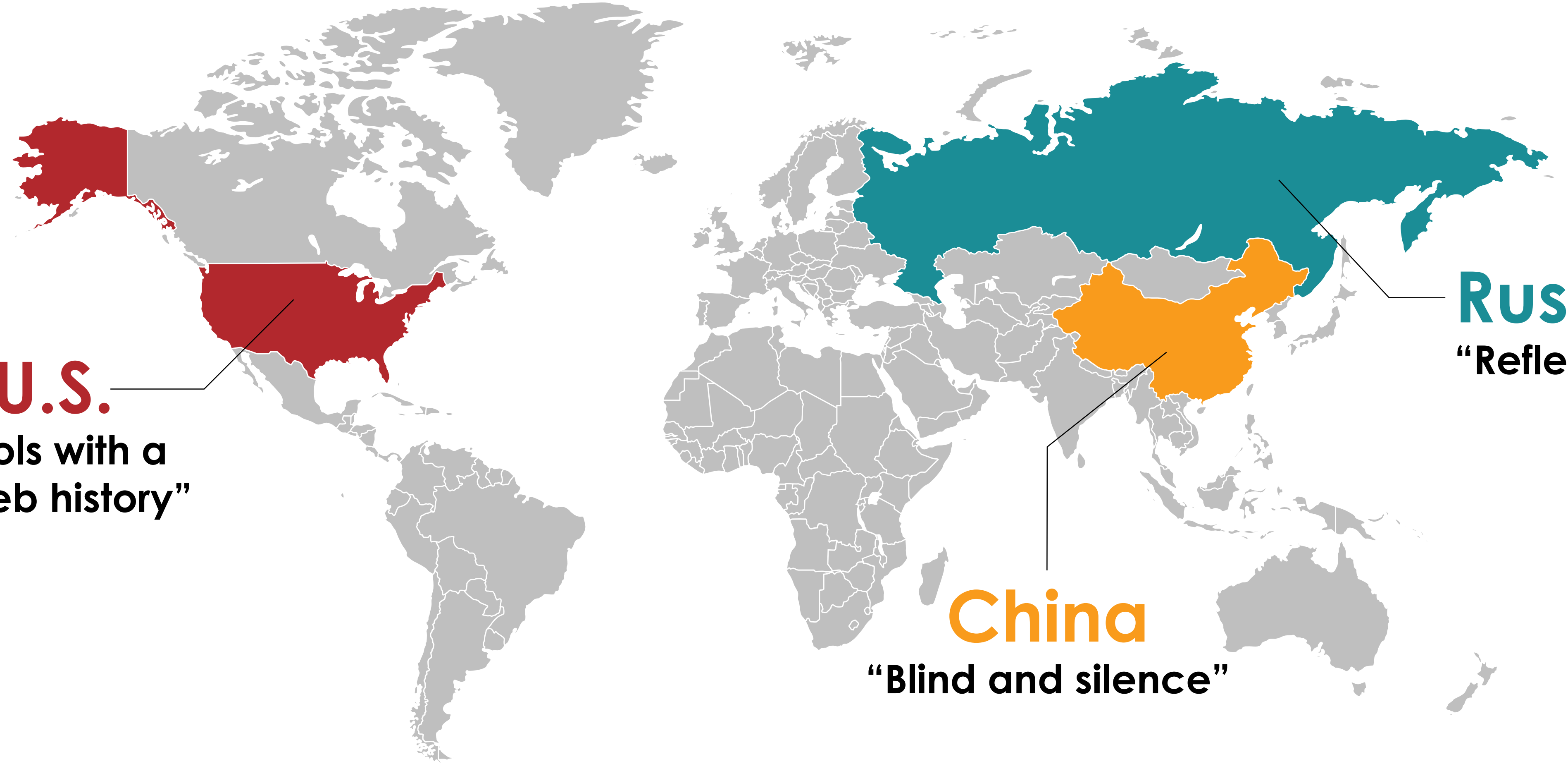
Attribution deception happens!

"[A US bank] is believed to have become the latest victim of a cyber-attack launched by a group pledging retaliation for the controversial Innocence of Muslims video that has triggered anger and violence across the Muslim world. A group calling itself Izz ad-Din al-Qassam Cyber Fighters has claimed responsibility…"

WHERE DID THIS NEWS STORY COME FROM?

ANSWER: ATTACKER PROPAGANDA

Attribution deception happens!



U.S.

“Tools with a Web history”

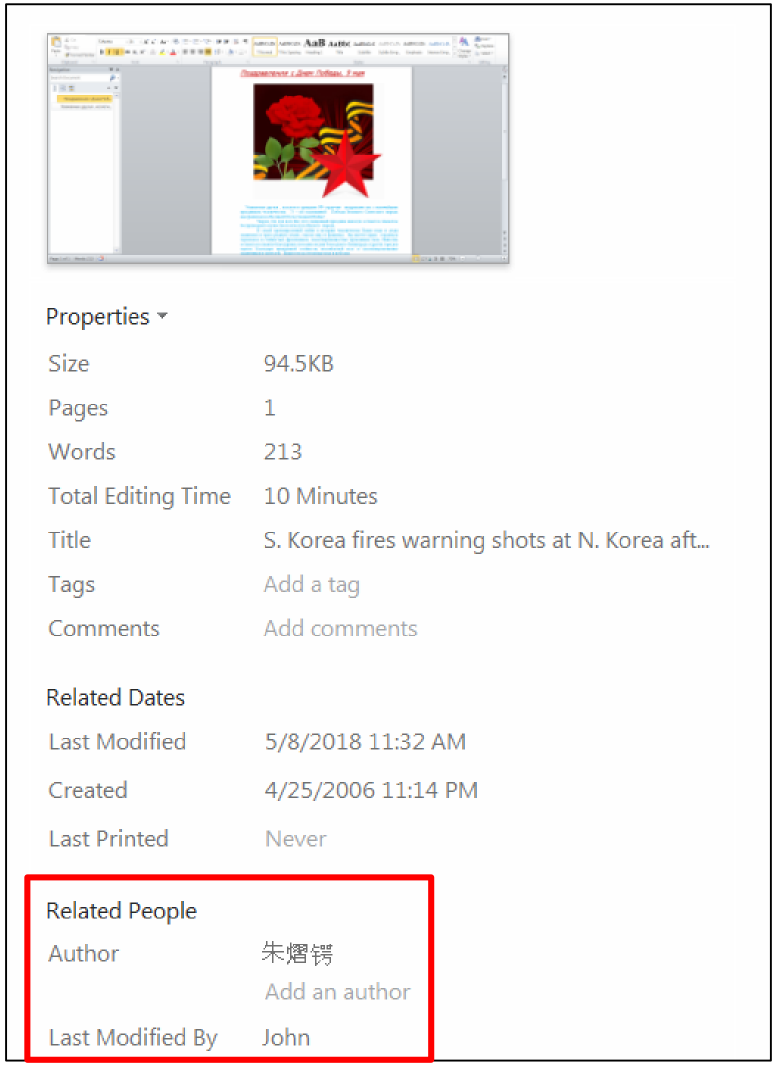
Russia

“Reflexive control”

China

“Blind and silence”

Attribution deception happens!



Properties

Size	94.5KB
Pages	1
Words	213
Total Editing Time	10 Minutes
Title	S. Korea fires warning shots at N. Korea aft...
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	5/8/2018 11:32 AM
Created	4/25/2006 11:14 PM
Last Printed	Never

Related People

Author	朱熠锷 Add an author
Last Modified By	John

Attribution deception happens!

- (Likely) targeting Japan: C:\xingxing\snowball\Intl_Cmm_Inteface_Buld_vesion2.6\IMGJPS.pdb
- C:\share\moscow\work\upgraded\zark20rk-add support for httpdownloader\server\bin\zark20rk.pdb
- Targeting South Korea: “Пользователь Windows” and RU-EN PE resources

Application and Takeaways

Application: SOC Analyst or Lead

What should I do differently as someone who is on the front lines of defense for my organization?

- Evaluate current alert triage process against deception scenarios
  - Be careful about blindly ignoring alerts below a certain threshold
  - Think critically about your alert process; if you were an attacker, how could you exploit it?
- Don't just ignore "commodity" by default
  - Treat links to targeted threats as high priority, but remember that opportunistic compromises can still be damaging
  - Are your defenses set up to detect post-compromise activity or lateral movement?

Application: Incident Responder

What should I do differently as I investigate intrusions?

- Beware the smoking gun!
  - If your findings hinge on one key piece of evidence, reexamine your assumptions
- Rule out alternative explanations before moving on
  - Consider the possibility that a different adversary is reusing TTPs
  - Threat actors evolve; make sure your mental model is open to new information
  - Before wrapping up, consider: would you be done if you suddenly found out that a different threat actor was responsible?

Application: Intelligence / Threat Analyst

What should I do differently as someone who analyzes the threat landscape for my organization?

- Clearly identify, and attempt to disprove, your own hypotheses
  - Analyze means, motive, and opportunity
  - Identify lynchpin assumptions and data
  - Know common pitfalls in reasoning – cognitive biases – and when specialized analytical techniques can help avoid them
- Be impossible to misunderstand
  - It should not be reasonably possible for a reader or listener to misunderstand your conclusions, or your level of confidence in your conclusions
  - A consumer (with time to actually consume) should never have to come back to you for explanation of your reasoning

Application: Business Leader

What should I do differently as someone who makes strategic business decisions?

- Know the lines where attribution accuracy matters
  - What actions would significantly cost the business if the threat was misunderstood?
  - What bad outcomes for me could be highly desirable to a specific adversary? Which might be taboo for that actor?
- Have your teams prepare & practice for what they would do
  - Ensure your teams are taking the steps appropriate to their roles
  - In the heat of the moment, your team may not recognize cases where attribution matters unless they've worked through those in advance

RSAConference2019

Thank you

Jayce Nichols

Jayce.Nichols@FireEye.com

John Miller

John.Miller@FireEye.com

RSA®Conference2019

Appendix

Attribution: How It’s Done

Case sampling

	IP/Domain Registration	Online Identity	Targeting	Compile Times	Pattern of Life	Code Overlap	TTP Overlap	C2 Infra	Geopolitics	Financial Records	Linguistics	Who Benefits?	EXE Metadata
WannaCry, report 1						✓					✓		
WannaCry, report 2						✓	✓	✓					
Bangladesh SWIFT hack										✓	✓		
Taiwan SWIFT hack						✓	✓			✓			
APT39	✓		✓		✓	✓	✓		✓		✓	✓	
ME targeted attacks			✓		✓		✓					✓	
Crypto exchange targeting			✓			✓	✓					✓	
Ukraine / NotPetya			✓			✓	✓	✓					
LuckyMouse			✓			✓	✓	✓	✓				
VPNFilter						✓							
Iran disinformation	✓		✓						✓			✓	
DNC hack						✓							
Putter Panda	✓	✓					✓	✓					
Domestic Kitten			✓					✓					
APT37		✓	✓	✓									
APT38	✓	✓	✓					✓	✓				
Triton	✓	✓		✓				✓			✓		
APT32			✓									✓	

Suspected Deception: How It’s Done

Case sampling

	Linguistic Engineering	Artifact Metadata	Malware Reuse	Code Overlap	Targeting	C&C Infrastructure	TTP Overlap	False Front	Impersonation
Cloud Atlas	✓	✓	✓			✓			
Wild Neutron	✓				✓				✓
DPRK / Lazarus	✓					✓		✓	
CyberCaliphate	✓							✓	
CyberBerkut								✓	
Yemen Cyber Army								✓	
Duqu 2.0		✓							✓
TigerMilk							✓		
Turla			✓						
Iranian activity	✓							✓	
TRITON	✓								
"Crouching Yeti"						✓			
"Dancing Salome"			✓						
APT29							✓		
USG Zeus			✓			✓	✓		
Olympic Destroyer				✓					