RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO3-W12

Unmasking Operation Shaheen

Kevin Livelli

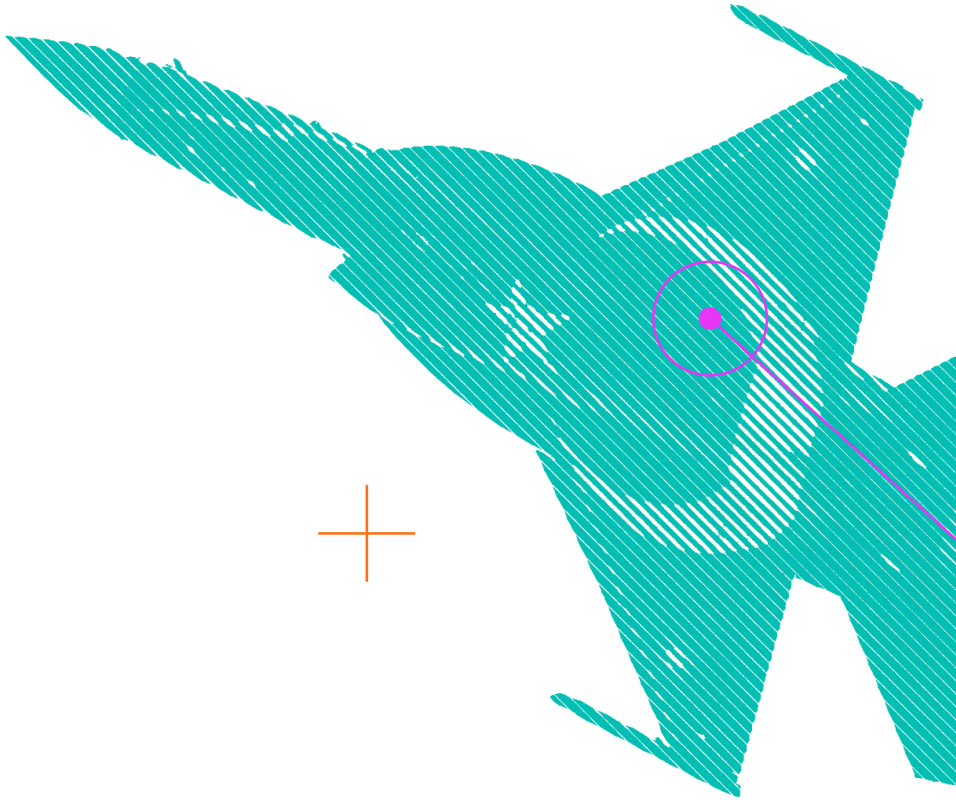
Director of Threat Intelligence,
Cylance®

Tom Pace

Senior Director, Worldwide Consulting,
Cylance

About Us

- Kevin Livelli
  - Currently: Director of Threat Intelligence, Principal Intel Analyst
  - Previously: 10 years, Emmy and Peabody Award-winning investigative journalist at 60 MINUTES
  - Four years, Supervising Investigator at nation's largest police oversight agency (NYPD)
- Tom Pace
  - Currently: Senior Director, Worldwide Consulting
  - Previously: 11 years of security experience (government, law enforcement, financial)
  - Four years Marine Corps (infantry, intelligence, Afghanistan, Iraq)
- Acknowledgements
  - Authors: Kevin Livelli, Ryan Smith, Jon Gross
  - Research Support: Cylance Applied Security Team



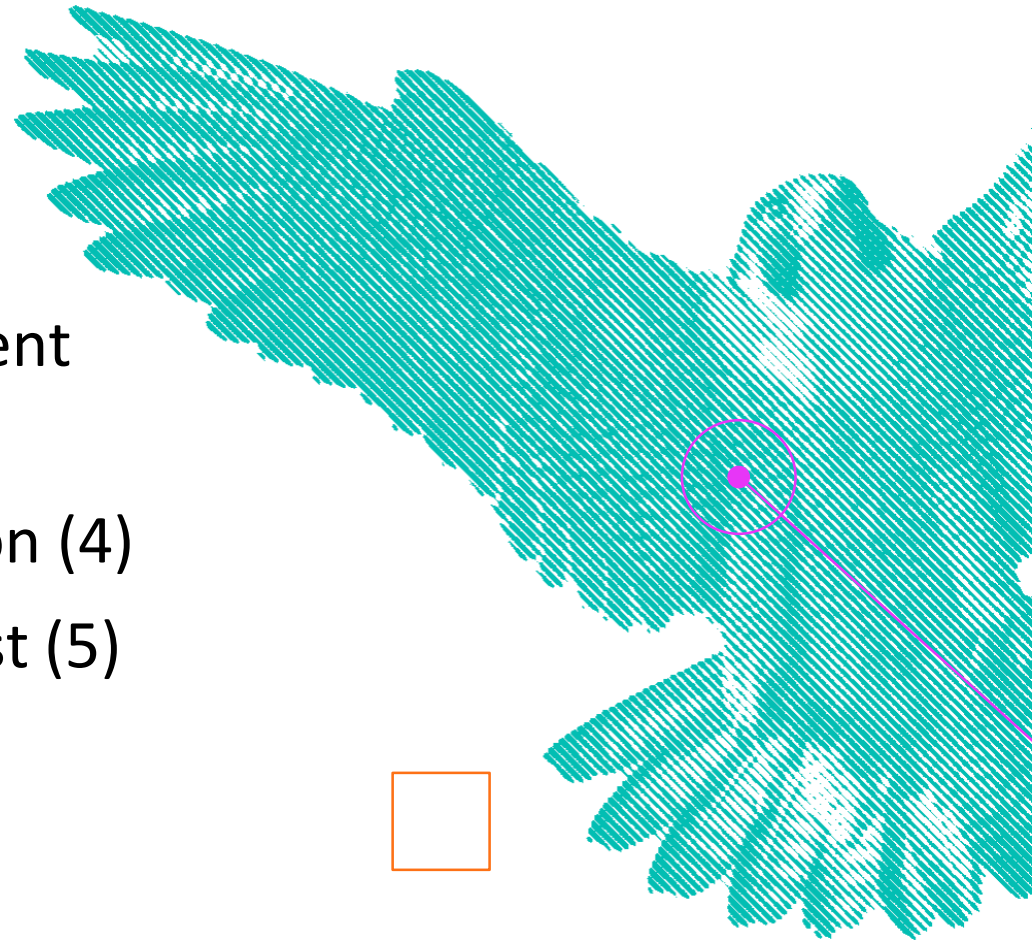
Summary

- A New Campaign – Operation Shaheen
  - Target: The nuclear-armed, Pakistani military and government
  - Length: More than a year, in multiple phases
  - Reason: Espionage
- A new threat actor – The White Company
  - Likely state-sponsored and Middle Eastern
  - Access to zero-day developers
  - Highly complex, automated exploit build set
  - Capacity for advanced reconnaissance
  - Concurrent management of multiple targets
- New reasons to care
  - Pakistan as “pivot of the world”
  - A powerful new threat actor with an unknown target list
  - Tools that allow the time-triggered evasion of eight antivirus products
  - Tools that deliberately surrender to the target
  - Explicit use of contradictory indicators to delay/degrade incident response
  - Exploitation of vulnerabilities, not just in software, but in thinking and methodology

The Campaign

Targeting – Pakistan's Air Force in the Crosshairs

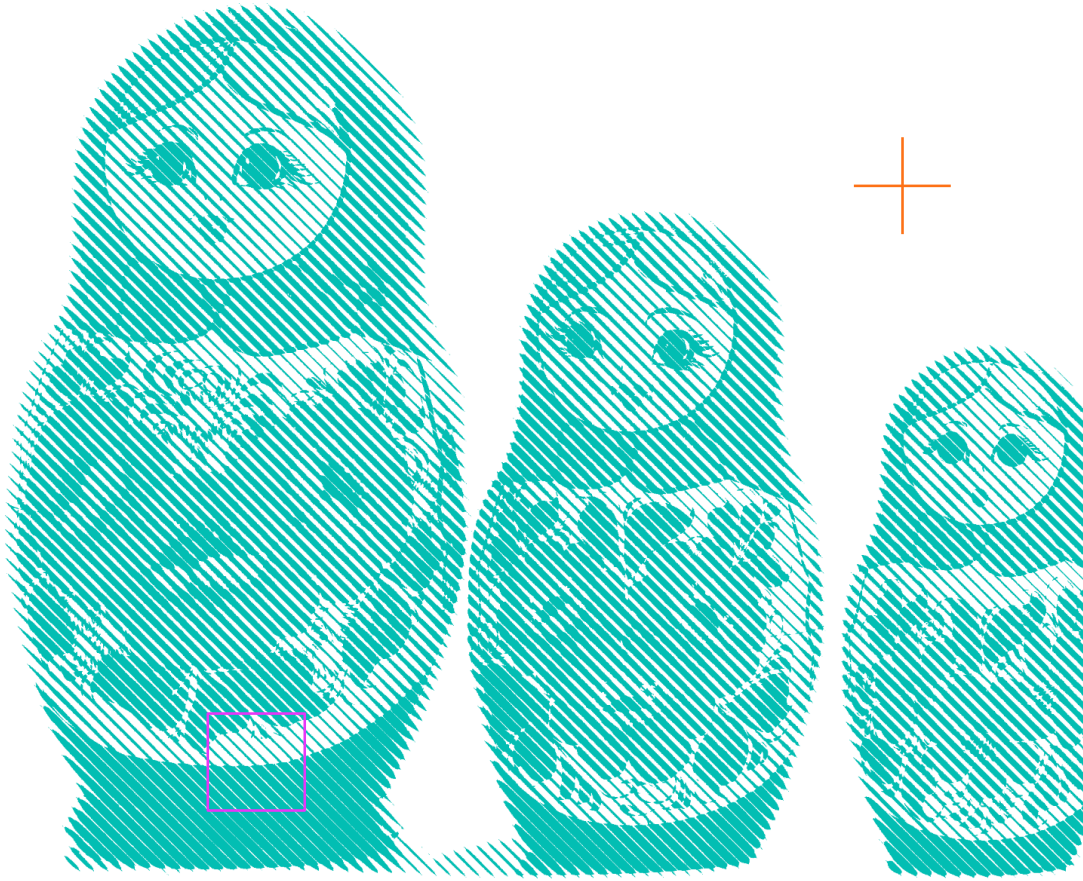
- Lures:
  - The Pakistani Air Force or military (10)
  - The Pakistani government or other government agencies (11)
  - Chinese military or foreign affairs in the region (4)
  - Subjects of topical or general regional interest (5)



The Campaign

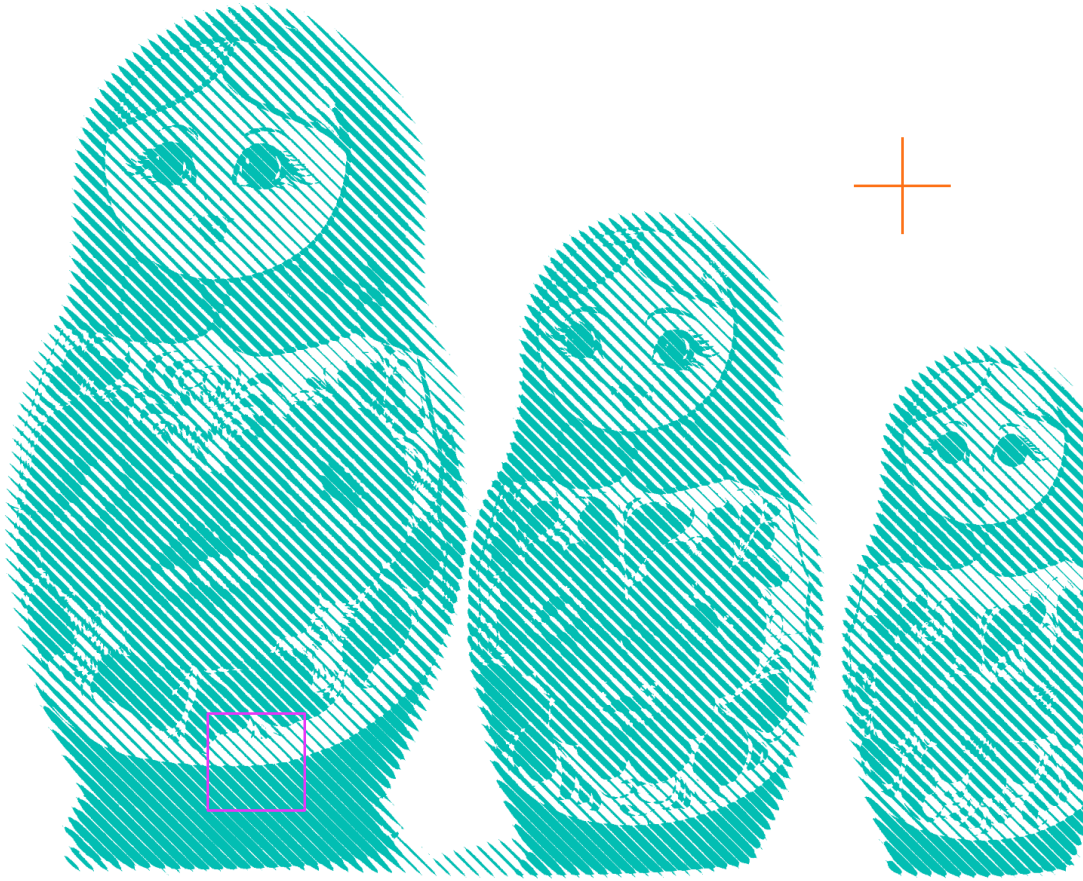
Evolves Over Multiple Phases

- Phase 1
  - Picking the locksmith
  - Pakistan's critical infrastructure as infrastructure for the attack
  - Open-source exploit of older vulnerability
  - Download and run delivery of malware
  - Russian doll RATs



The Campaign

- Phase 2 – Custom Job
  - Highly complex and customized exploit and newer vulnerability
  - Self-extracting of malware from exploit
  - Deliberate evasion of eight antivirus products:
    1. Sophos
    2. ESET
    3. Kasperksy
    4. BitDefender
    5. Avira
    6. Avast!
    7. AVG
    8. Quick Heal
  - Time-triggered surrender to those products



The Campaign
Disappearing Tricks

Within the exploit:

- Four different ways to check whether the malware was on an analyst's or investigator's system
- The capacity to clean up Word and launch a decoy document to reduce suspicion
- The ability to delete itself entirely from the target system

Within the malware:

- Five different obfuscation (packing) techniques that placed the ultimate payload within a series of nesting-doll layers
- Additional ways to check whether the malware was on an analyst's or investigator's system
- Anonymous, open-source payloads and obfuscation techniques
- Use of compromised or otherwise un-attributable network infrastructure for command and control

The Threat Actor

The White Company – Whitewashing as a Calling Card

- Attributes:
  - Access to zero-day exploit developers and, potentially, zero-day exploits
  - Complex, automated exploit build system
  - Ability to modify, refine, and evolve exploits to meet mission-specific needs
  - Capacity for advanced reconnaissance of targets
  - Concurrent management of multiple targets
  - Resources, know-how, and personnel for all of the above

The Threat Actor

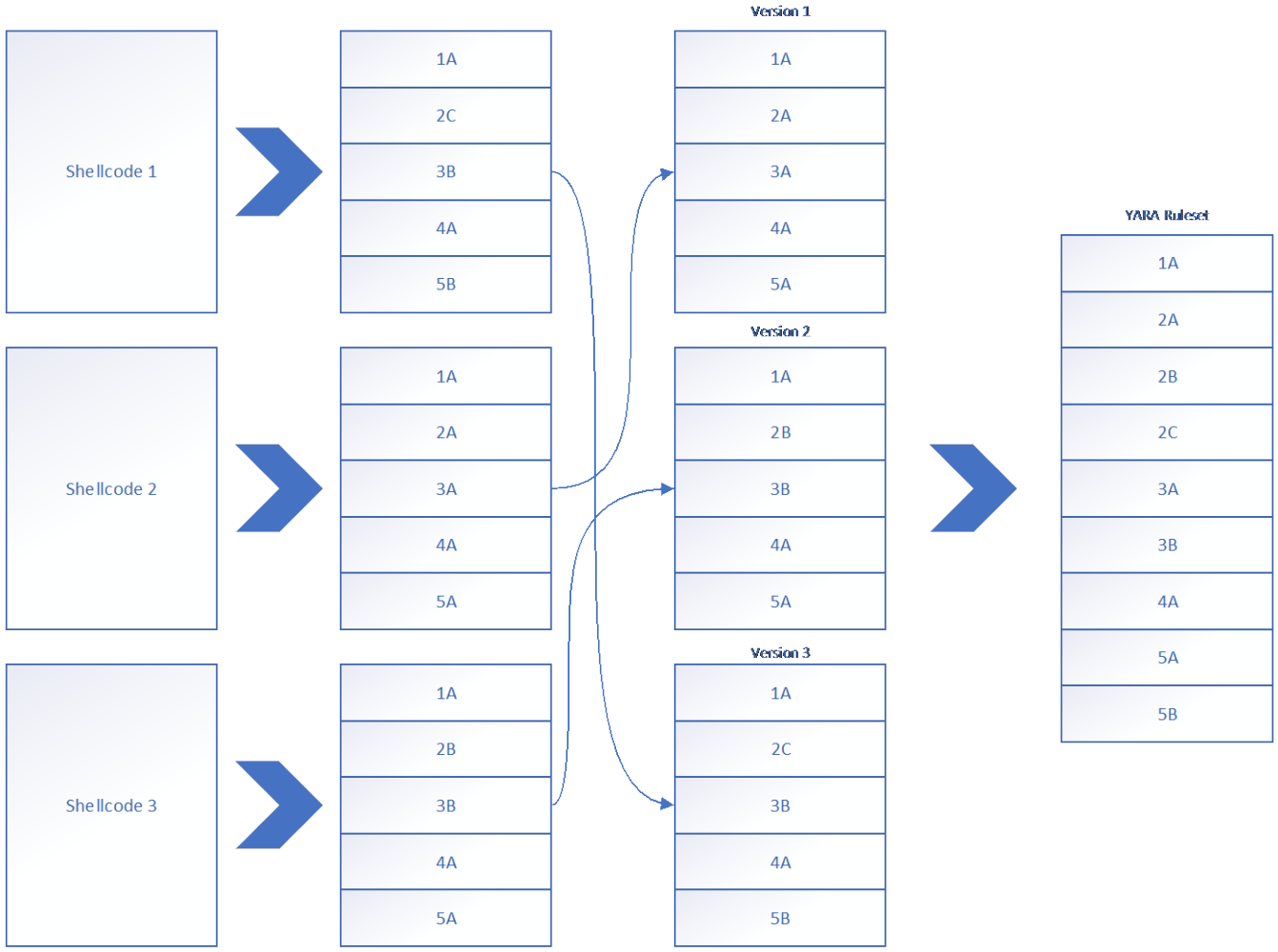
The White Company – Whitewashing as a Calling Card

- Comparison to Other APTs
  - Profile does not resemble public descriptions of the known Russian, Chinese, North Korean, Iranian, Israeli, Indian, or Five Eyes groups
  - Style evoking contradictions sets them apart
    - Some deliberate: stealth vs. surrender
    - Some not: exploits reflect both craftsmanship and sloppiness
  - Possibility of alignment with one of the states above, but in a way that has not yet been seen and written about publicly

The White Company

- A Different Approach To Attribution
  - The White Company's awareness of traditional methods
  - The futility of tracking malware and infrastructure
- Genetic Tagging and Tracking of Exploit Shellcode
  - 42 unique functions
  - Multiple variants of each function
  - Result = Establish chronology / version development
  - Result = YARA Ruleset on unique combination of function and variant nets larger sample set

Shellcode Process



Impact

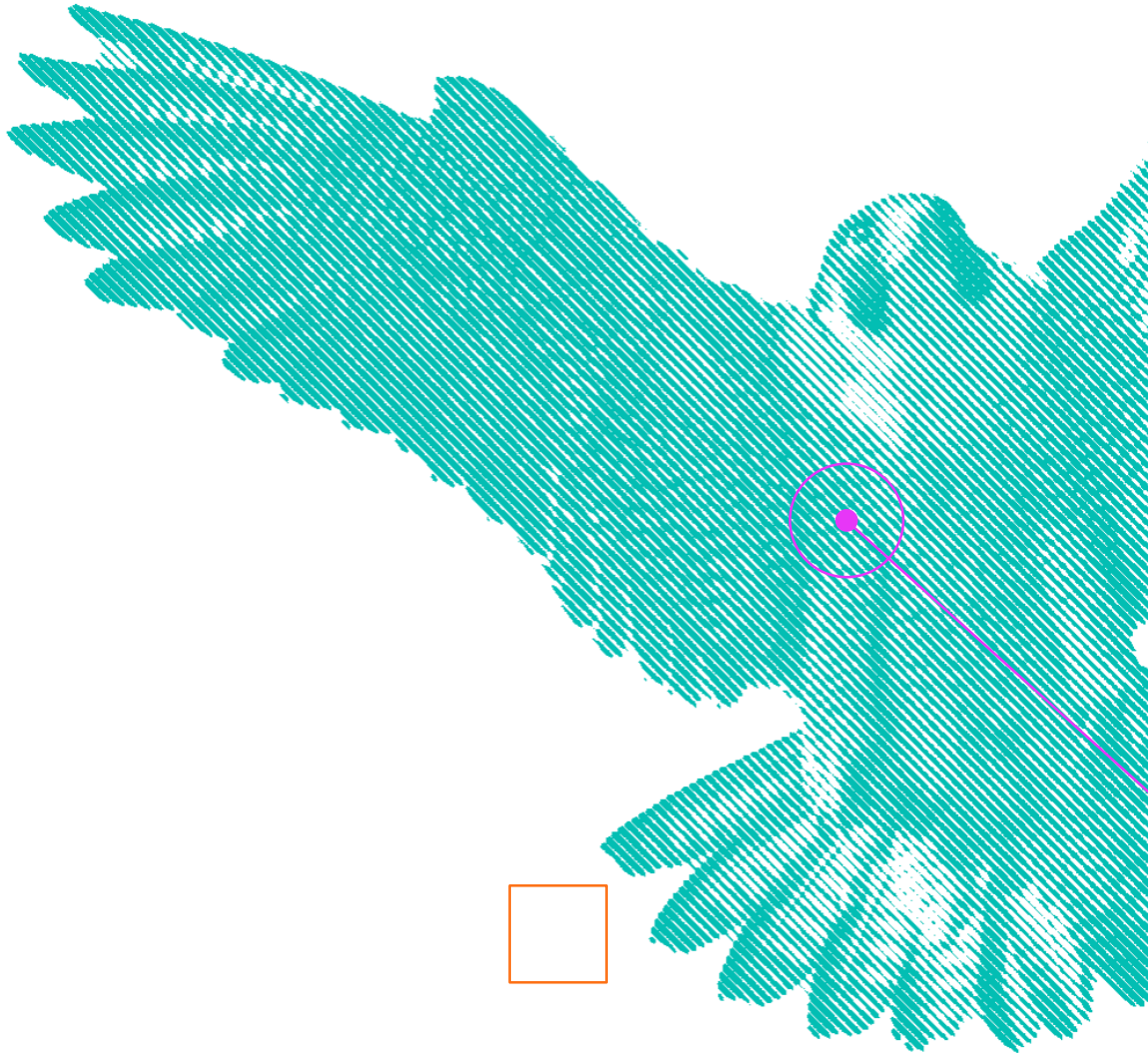
- Lessons for Enterprise
  - Hacking the methodology / common approach
    - A series of contradictions:
      - Evasion vs. surrender
      - Public tools vs. custom tools
      - Complex exploit vs. simple payload
      - Craftsmanship vs. sloppiness
  - Reliance on antivirus products to alert
  - Reliance on traditional EDR approaches to incident response

Impact

- Geopolitical Implications
  - “Pakistan is the pivot of the world”
  - Influence of the Pakistani military on domestic and foreign affairs
  - Nuclear weapons and terrorists: a volatile mix
  - Strategic rivals
  - The war in Afghanistan
  - China’s One Belt, One Road Initiative
  - The Port of Gwadar
  - Ties to the Gulf – religious and financial
  - Self-Defense: the new National Centre for Cyber Security

Takeaways

- Pakistan's ability to defend itself and its nuclear arsenal is challenged
- The White Company's unknown identity, interests, and target list changes the risk calculus for both public and private sector leaders
  - Who's next?
  - What are they after?
- A newly recognized, likely state-sponsored threat actor's appearance challenges policy makers and the strategic decision making of governments
- Reliance upon security solutions to identify, stop, track and properly alert to threats from the White Company is significantly undermined



RSAConference2019

Questions and Answers

Thank You