HACKING EXPOSED

PHOENIX ISSA 2017-01-10

ADVERSARIAL TECHNIQUES OBSERVED IN THE WILD

WES BATEMAN

CROWDSTRIKE

CROWDSTRIKE

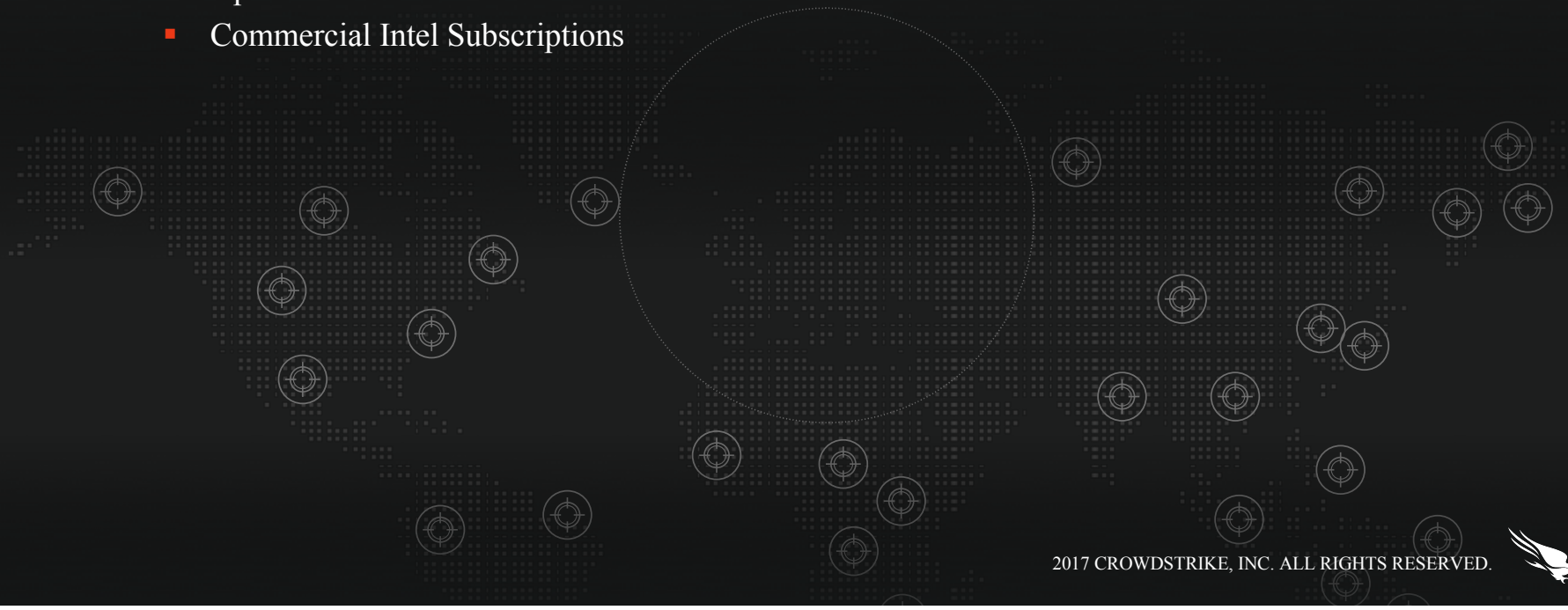
Adversarial Emulation

- Emulating actual adversary behavior seen in the wild
  - Red Team
    - Targeted and Relevant Pen Testing
  - Blue Team
    - Testing Defenses Against Threat Actors Who Actually Target Your Type of Organization
    - Testing Defenses Against Techniques, Not Just Tools/Malware

CROWDSTRIKE

Threat Intelligence

- What TTPs Are Currently Being Used in the Wild
  - Open Source Intel
  - Commercial Intel Subscriptions



CROWDSTRIKE

Two Hacking Exposed Scenarios

- Phishing attack
  - Establish remote access
  - Initial reconnaissance
  - Exfiltrate data (may happen quickly but often continues over time)
  - Credential theft for lateral movement
  - Establish persistence
- Public-facing server attack
  - Exploit a vulnerability found in the web application
  - Establish remote access
  - Reconnaissance
  - Attack other internal infrastructure for later lateral movement, persistence, and data exfiltration

CROWDSTRIKE

References / Links

- Meet the Adversaries
  - https://www.crowdstrike.com/blog/meet-the-adversaries/
- Cozy Bear and Fancy Bear
  - Bears in the Midst: Intrusion into the Democratic National Committee
    - https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/
  - Bear Hunting: Tracking Down COZY BEAR Backdoors
    - https://www.crowdstrike.com/blog/bear-hunting-tracking-cozybear-backdoors/
- Silent Chollima
  - Unprecedented Announcement by FBI Implicates North Korea in Destructive Attacks
    - https://www.crowdstrike.com/blog/unprecedented-announcement-fbi-implicates-north-korea-destructive-attacks/
    - https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/
    - http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf
    - https://www.us-cert.gov/ncas/alerts/TA14-353A


CROWDSTRIKE