Security Response in Today's Ecosystem

Phillip Misner,
Principal Security Group Manager
Microsoft Security Response Center

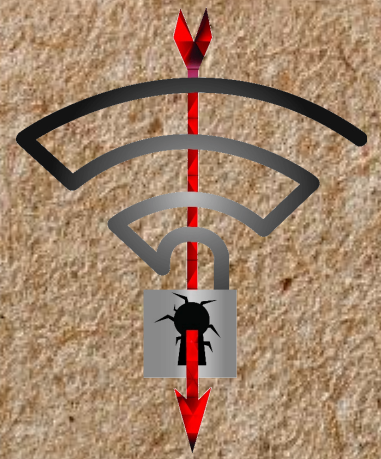
2017 In Review

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CU

BIZ & IT —

NSA-leaking Shadow Brokers just dumped its most damaging release yet

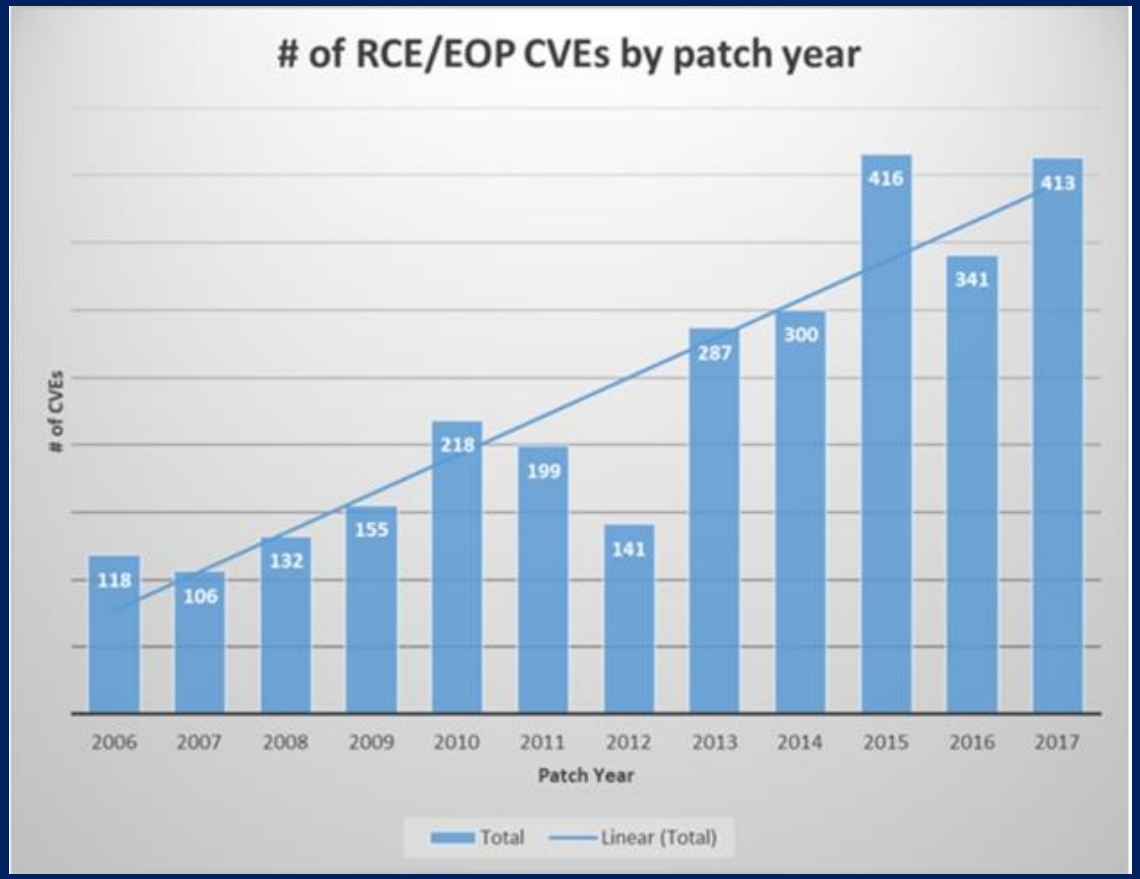
Windows zero-days, SWIFT bank hacks, slick exploit loader among the contents.



The WannaCry code demonstrates how petty criminals can adapt leaked intelligence tools to their uses.

27 ‘Petya’ Ransomware Outbreak Goes Global

JUN 17



Coordinated Vulnerability Disclosure

Security on the Mind

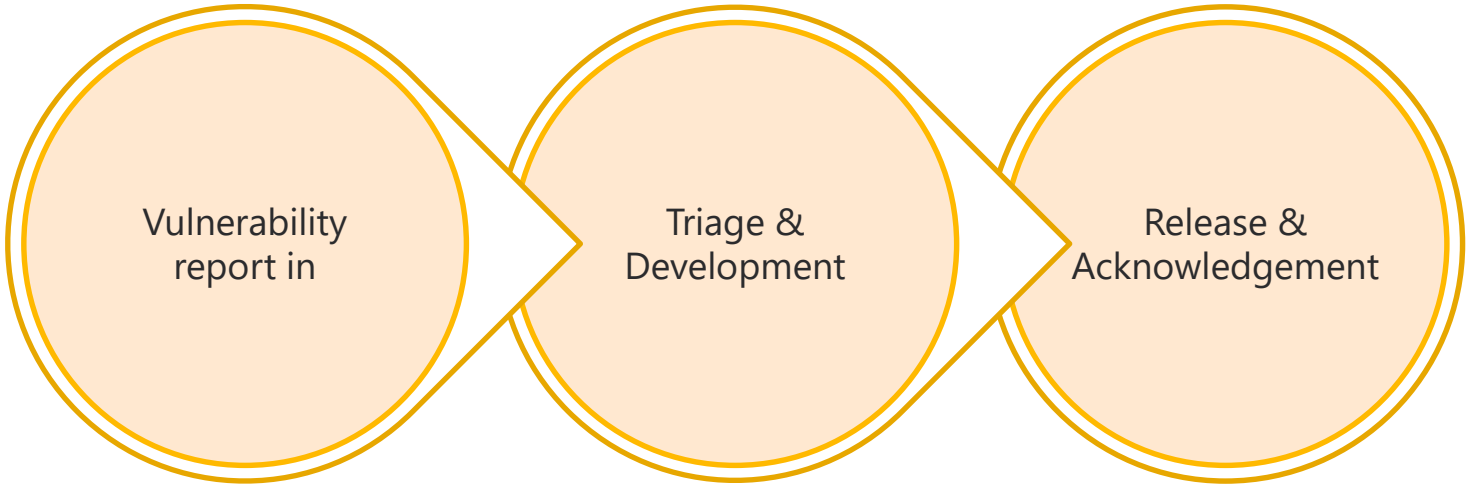
September 27, 2017

Equifax CEO departs, following CSO & CIO; breaches truly a board issue

Technology in Our Lives

Transactional Approach

- Vulnerabilities as rare occurrence
- One bug at a time
- Often quick band aids



2017 Anomaly?

The common threads:

- How interconnected the ecosystem is becoming
- The need to re-examine how best to do vulnerability disclosure

Challenges in Evolving Ecosystem

- Multiparty Vulnerability Disclosure
- Mixed environments
- Shared source or vulnerable foundational standards
- Long supply chains
- Government protectionism
- New players awoken to security who don't know where to start


WELCOME
TO THE
PARTY!
GO


2017 in Retrospective

Shadow Brokers & WikiLeaks

- Mass disclosures of cyberweapons
- +8700 documents & files
- They came with the manuals!

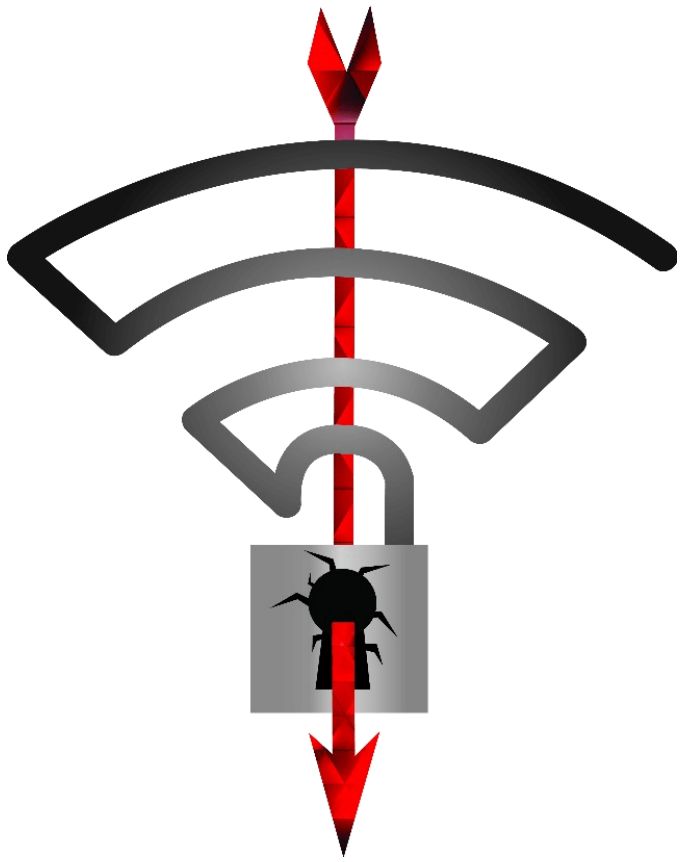
- Challenges posed:
  - assessment (from legal to sheer volume)
  - determining how to defend or patch against the cyberweapons
  - ultimately in asset management knowledge

- Subsequent Impact
  - WannaCry (+30 days)
  - Petya (+60 days)

Infineon TPM

- Multiparty Vulnerability Disclosure
  - Hub Model (Infineon engaged parties separately)
- Documentation at disclosure was vague and disparate
- End users had difficulty understanding what the risk was
- Many TPMs still vulnerable to this issue

KRAck Attack



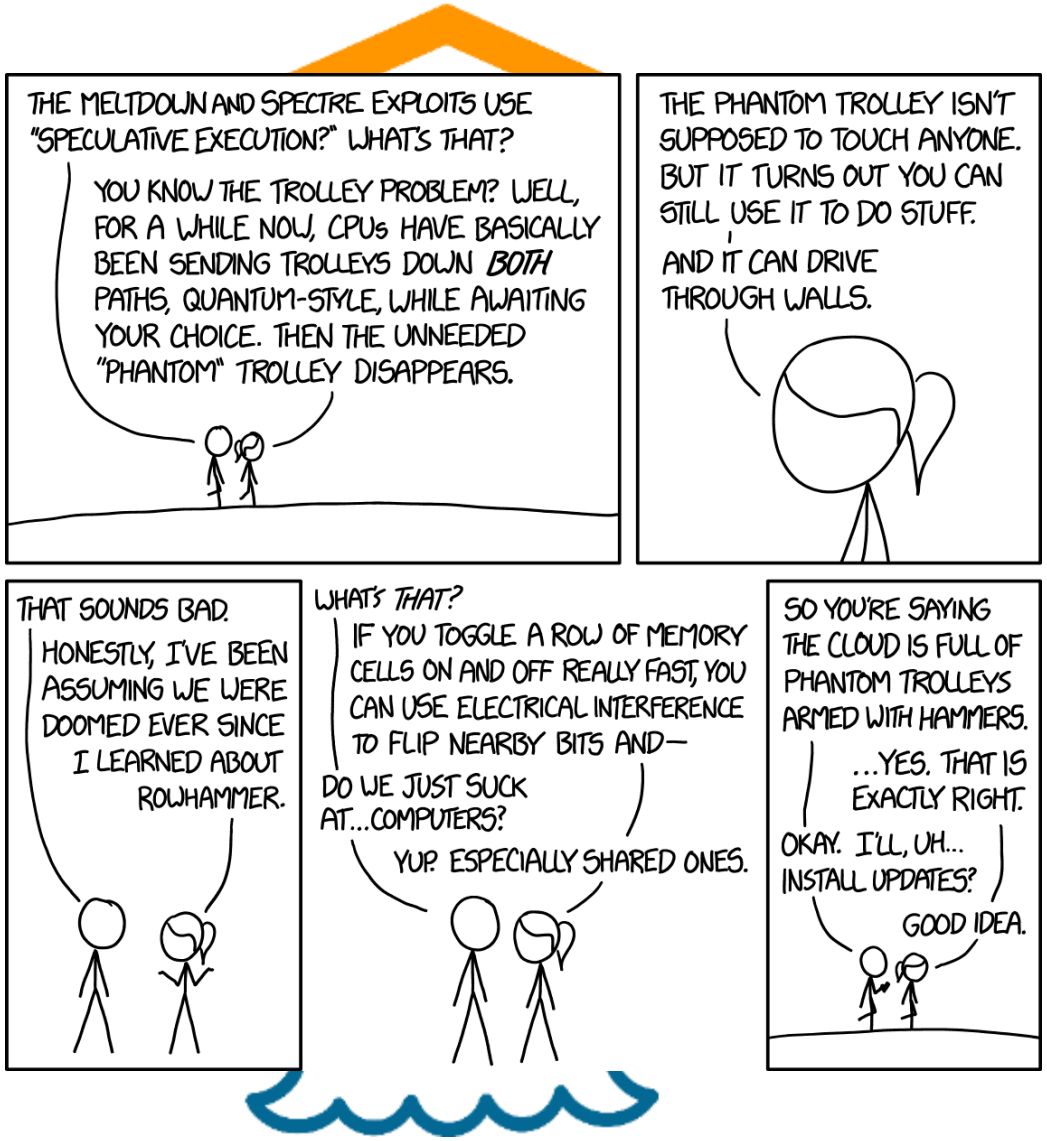
- Multiparty Vulnerability Coordination/collaboration
- Industry companies and partnering with organizations like CERT/CC, ICASI, and the WiFi Alliance
- Disclosure tent did not cover everyone
- Confidentiality within the tent was basically maintained
- Still struggle with understanding who all is impacted and how to get those outside the disclosure tent quickly up to speed.

Uber Breach

Uber paid hackers $100,000 to hide year-old breach of 57 million users

Elizabeth Weise, USATODAY Published 5:25 p.m. ET Nov. 21, 2017 | **Updated 12:09 p.m. ET Nov. 22, 2017**

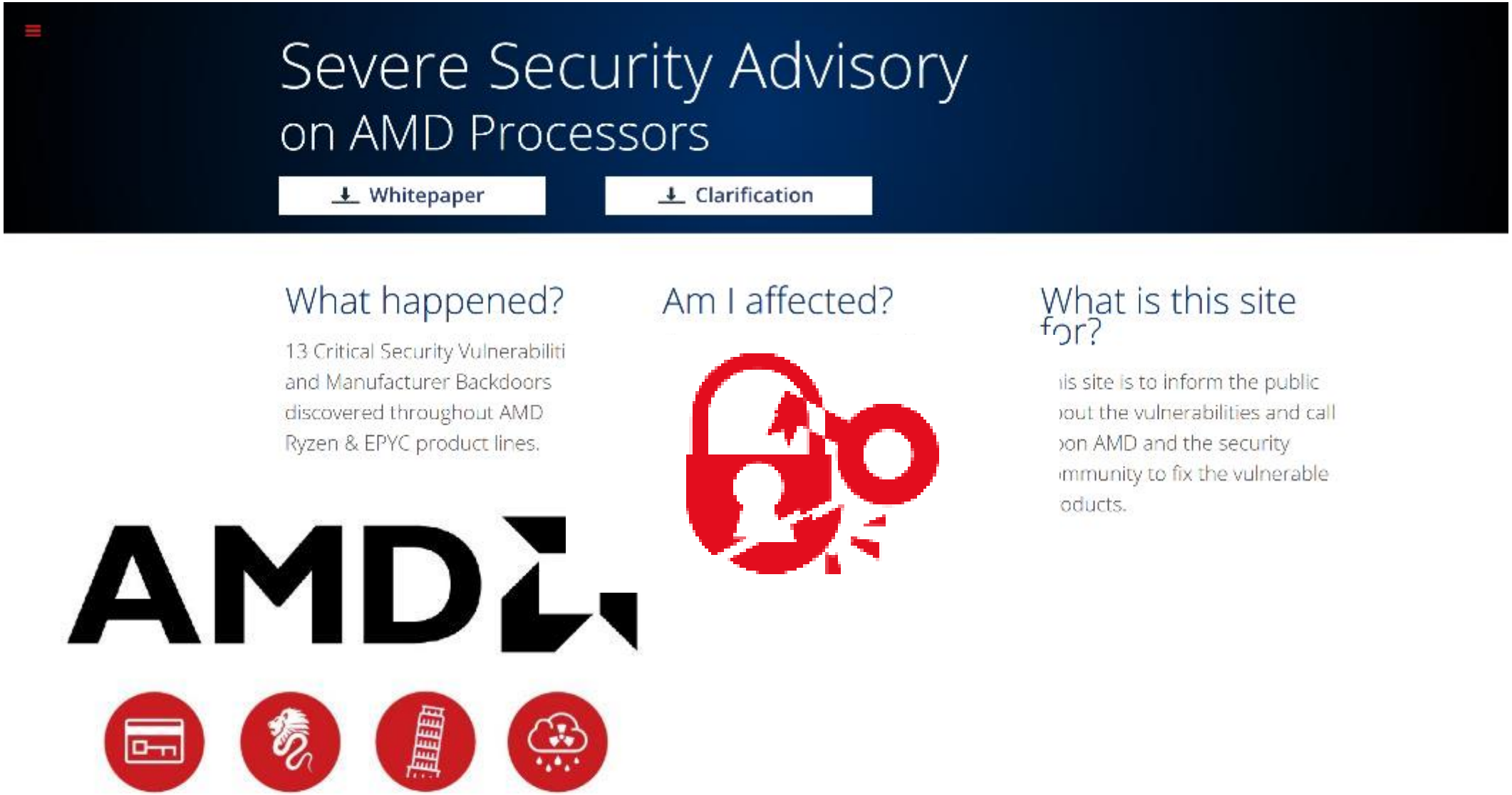
Meltdown / Spectre



- Multi-vendor vulnerability disclosure
  - 4 teams of researchers
  - Chip makers, software providers, cloud providers
- Confidentiality tent failed as tent enlarged
- Major media pickup
- No panacea for customers to take
- Initial disclosure was only part of known problem
- Quality issues with initial updates

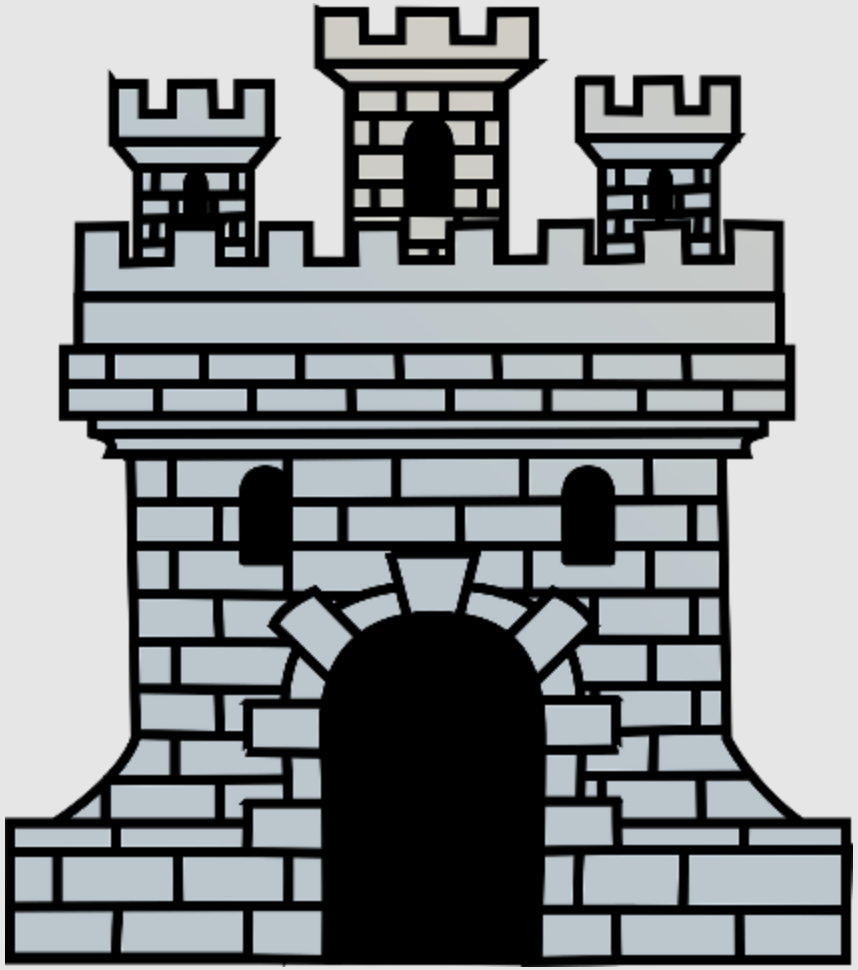
- Researchers and industry came together
- Industry Summit to pool brain power
- Continued efforts to engage on future research

Amdflaws.com




Loading
2018

Security from a View



Ecosystem Engagement

- Make it easy for security researchers to engage with Microsoft
- Be predictable in our actions
- Coordinated Vulnerability Disclosure
- Go where the researcher are!
  - Sponsoring/Talking/Engaging Conferences
  - Join and contribute to the social media conversation
- Bug Bounty Program
- Contribute back to ISO/ International Standards
- Participate in FIRST, APCERT, ICASI
- BlueHat Security Conference
  - Bring the community and engineering teams together to talk security

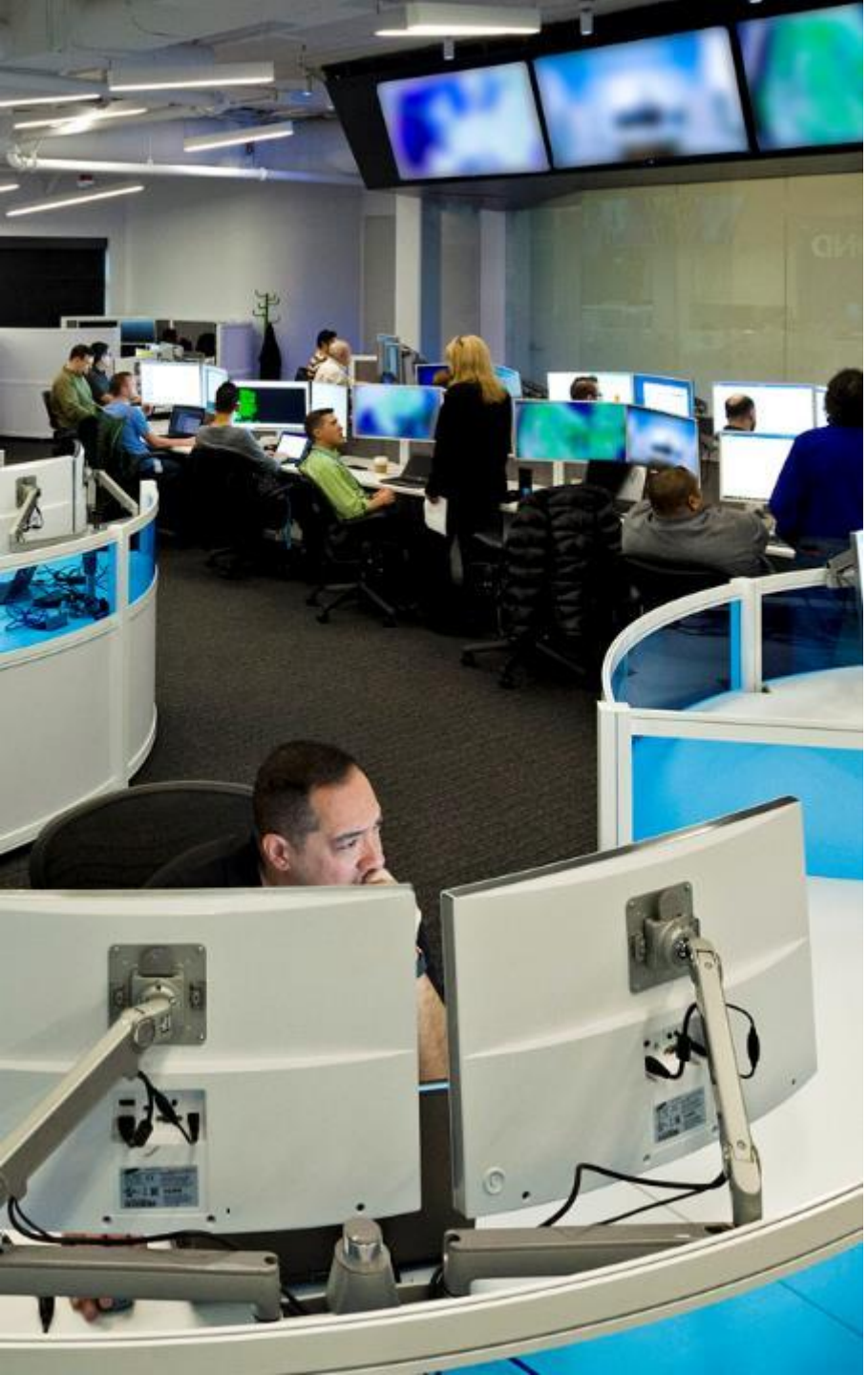
Becoming more accessible

- Continual promotion of where to submit vulnerabilities
- Working with FIRST on standard contact cards
- Translating disclosure and bounty webpages into seven major languages to match our documentation
- Simplifying terms of bounty program to make legal language easier to understand
- Talking more and starting to document what to expect when coordinating multiparty disclosure

Speculative Execution Side Channel Attack Bounty

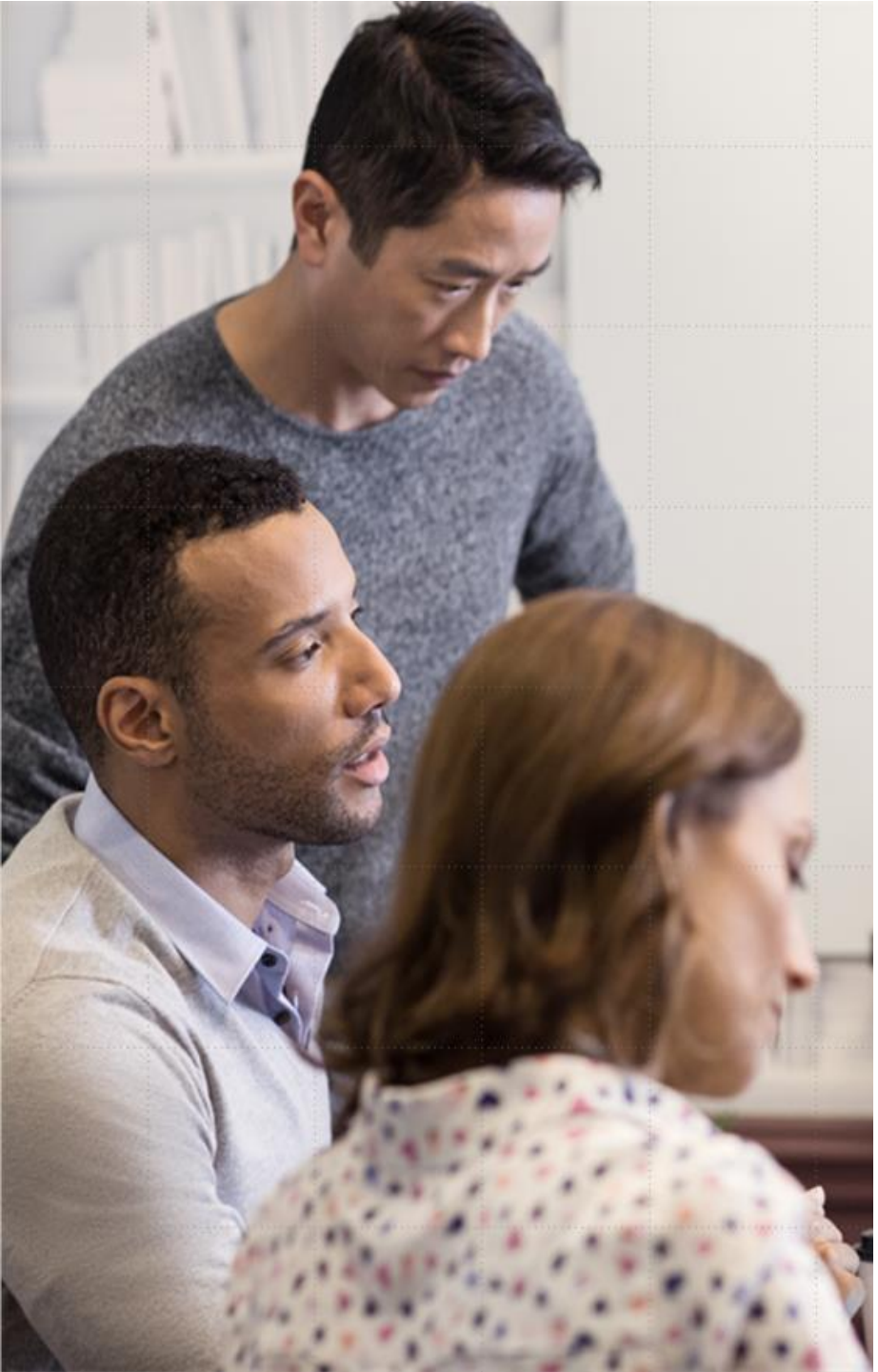
- Bounty as a tool to engage research
- New vulnerability class with industry wide impact
- Up to $250,000 USD for qualified find
  - New classes of speculative execution
  - Bypasses of our mitigations
  - Missed variants
- Commitment to share bounty finds with industry partners

aka.ms/bugbounty



Cloud pivots

- Established Cyber Defense Operations Center
  - Bring all SOC and Threat Intelligence teams together
- Working together with Amazon & Google to curb abuse through common reporting format & sharing
- Sharing expertise through workshops on Azure forensics



PSIRT Framework

- Forum of Incident Responders and Security Teams (FIRST) initiative
- Microsoft is 1 of 21 organizations contributing
- Creating framework for how to setup and run Product Security Response
- Best Practices spread over small to medium to large organizations

Big Questions Remain

- With shared components, how do we coordinate?
- How should industry engage with researchers?
- Right time to broaden disclosure?
- What about government disclosure?

Security Response as Investment

- Fluid engagement, not a static standard
- Realize that human is capital
- Engage even when we don’t always agree
- Legal engagement should not be tool of first choice
- Champion customer outcome
- Give back to the community
- Be part of the community

Thank you

© 2018. Copyright Microsoft Corporation. All rights reserved.

phillipm@microsoft.com
@phillip_misner

Photo Credits

- Dubai at Night, Photo by Trey Ratcliff, https://www.flickr.com/photos/stuckincustoms/