Cutting Through the Cybersecurity Noise

Here's what's important this week: May 10, 2019

Take Action

- Keep doing that voodoo that you do so well.

Be Aware

- A new round of tech support scams is hitting around the country. Business email compromise (BEC) scams continue to be popular – especially fake invoices and payroll diversions. There are also a new wave of Emotet-infected malicious emails and a new ransomware campaign, called RobbinHood, that's actively targeting US government networks.
- A new version of Qakbot (aka Qbot) has a new technique to avoid detection. After infecting a device, the downloader grabs two files containing encrypted data from one of the hijacked domains used by the attackers. Then Qakbot re-assembles the decrypted data from the two files with the help of a specially-crafted batch file. Filenames seen are (randalpha)_1.zzz and (randalpha)_2.zzz.
  Reference: https://www.bleepingcomputer.com/news/security/qakbot-assembles-itself-from-encrypted-halves-to-evade-detection/
- Wipro customers, be aware that their trusted networks and systems were used to launch cyberattacks against the company's customers. Brian Krebs publicly spanked them for being a bad example on how to handle a breach. This is a good case study for all.
  Reference: https://krebsonsecurity.com/2019/04/how-not-to-acknowledge-a-data-breach/
- On May 2, 2019, President Trump issued the Executive Order on America's Cybersecurity Workforce to get more cybersecurity folks. But the good news is that we are now officially "strategic assets" and "guardians of our national and economic security."
  Reference: https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

Reminders

The Arizona Counter Terrorism Information Center (ACTIC) and Urban Area Security Initiative issue this product to increase Arizona's awareness and cyber resilience. It's up to you to make sure you take the proper steps to secure your networks and devices. Although vendors, products, and/or services may be mentioned, we do not endorse any specific one.

Contact ACTICCybersecurity@AZDPS.GOV with any questions, to provide feedback, or to be added/removed from this distribution. Please note that this email address is not monitored 24x7.

Report potential, suspected, and/or confirmed cyber threats to the ACTIC via:

- https://www.azactic.gov/Tips/
- ACTIC@AZDPS.GOV
  - (602) 644-5805 or (877) 2 S A V E A Z (272- 8329)