Cutting Through the Cybersecurity Noise

Here's what's important this week: May 31, 2019

Take Action

- Apply security patches for the EternalBlue (CVE-2017-0144) and BlueKeep (CVE-2019-0708) vulnerabilities, if you haven't already. Recent news articles stated attackers used EternalBlue to spread ransomware throughout the targeted organization making the attack more destructive (and the patch has been available for two years!). ***And even more concerning are reports that threat actors are actively scanning for Windows systems vulnerable to BlueKeep***. It appears that at least one threat actor is investing significant time and effort into compiling a list of vulnerable devices, most likely in preparation for actual attacks.
  References: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
  https://thehackernews.com/2019/05/bluekeep-rdp-vulnerability.html
  https://en.m.wikipedia.org/wiki/EternalBlue
  https://www.ehackingnews.com/2019/05/ransomware-tool-causing-chaos-in.html
  https://blog.erratasec.com/2019/05/a-lesson-in-journalism-vs-cybersecurity.html
- Improve your security awareness program.
  Reference: https://www.welivesecurity.com/2019/05/21/cybersecurity-training-awareness-resources-educators/

Be Aware

- Are you using online file storage technologies like Server Message Block (SMB) file shares, rsync servers, and Amazon Simple Storage Service (S3) buckets? In the past year, Digital Shadows' Photon Research Team found 2.3 billion exposed files. Thankfully, Amazon's new Block Public Access feature has reduced the overall exposure of S3 buckets, and Tripwire recently published a set of AWS best practices.
  References: https://resources.digitalshadows.com/digitalshadows/too-much-information-the-sequel
  https://www.tripwire.com/state-of-security/security-data-protection/secure-information-aws-10-best-practices/

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)

* If links don’t come through, cut and paste all referenced URLs into your browser to access the sites.