Cutting Thru the Cybersecurity Noise

Here's what's important this week: September 14, 2018

Take Action

- Federal and defense contractors: Remove all Kaspersky software from your networks by October 1 as required by the National Defense Authorization Act. Why? There are concerns the Russian anti-virus could be used as a Kremlin spying tool or that Kaspersky could be required to turn over customer information to Kremlin officials.
  Reference: https://www.nextgov.com/cybersecurity/2018/09/kaspersky-deadline-approaches-fears-loom-contractors-arent-prepared/151147/

Be Aware

- In last week's Noise I mentioned building your insider threat mitigation program. Tim Casey of Intel, one of the creators of the Threat Agent Library, has created a new Insider Threat Field Guide. These are great resources to help identify risks based on the "bad guys" most likely to harm your organization.
  References: https://www.intel.com/content/dam/www/public/us/en/documents/best-practices/a-field-guide-to-insider-threat-paper.pdf
  https://www.first.org/resources/papers/conference2010/casey-mancini-slides.pdf
  https://www.researchgate.net/publication/324091298/download
- Threat actors, including financial crime gang Cobalt Group, have recently shifted tactics to incorporate lightweight modular downloaders that "vet" target machines for their attractiveness before proceeding with a full-fledged attack. In other words, they're planting hard-to-find malware on your systems to check you out to see if you're worth attacking.
  Reference: https://threatpost.com/bad-actors-sizing-up-systems-via-lightweight-recon-malware/137364/

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)