Cutting Through the Cybersecurity Noise

Here's what's important this week: July 12, 2019

Take Action

- Block and monitor, please. There have been a number of cybersecurity incidents hitting Arizona entities recently, including a ransomware incident and another where webservers were "phoning home" to a command and control server. Attached is a list of IP addresses I recommend you block. I also want to thank everybody who contributed to this list!!
  Important: The root cause of two incidents was a user clicking on a malicious link in an email. This again proves the importance of the "human firewall." Please continue educating your folks.
  Note: I encourage you to create an ACTIC tip (instructions below) and attach a file containing any indicators of compromise you may see. I'll keep your organization confidential, and your information may help safeguard others. Protecting our organizations is a team sport!
- As always, please patch promptly. Sodinokibi ransomware elevates its privileges on a victim machine by exploiting the vulnerability, CVE-2018-8453 on Windows 7 through 10 and Server editions. So far, this ransomware campaign has hit in Asia and Europe, but expect it to come here. Also, a Sodinokibi campaign has targeted managed and cloud service providers.
  References: https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-exploits-windows-bug-to-elevate-privileges/
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8453
  https://www.secplicity.org/2019/07/08/msps-beware-attackers-targeting-msp-infrastructure-to-install-ransomware/

Be Aware

- Do you know when support for your software ends? Attached is a very good document from the Multi-State Information Sharing and Analysis Center that lists the end of support for all types of software.
- Here's a very good (although a bit technical) article that describes how a fileless malware campaign works. Fileless malware runs the payload directly in memory or leverages legitimate system tools to run malicious code without having to drop executable files on the disk, so they're hard to detect. (Just ignore the article's Microsoft commercial.)
  Reference: https://www.microsoft.com/security/blog/2019/07/08/dismantling-a-fileless-campaign-microsoft-defender-atp-next-gen-protection-exposes-astaroth-attack/

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.