Cutting Through the Cybersecurity Noise

Here's what's important this week: June 14, 2019

Publication Notes

- Unless something urgent happens, I will not be publishing Noise next week, June 21 due to a schedule conflict.
- Unless something urgent happens, I will not be publishing Noise July 5. I'll be too busy recovering from my annual 1776 sing-along.

Take Action

- Help cutdown on malicious email from spoofed addresses by implementing Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC). Reminder – Verizon's 2019 Data Breach Investigation Report found that email was responsible for 94% of all malware attacks across all sectors.
  References: https://www.csoonline.com/article/3402016/3-email-security-protocols-that-help-prevent-address-spoofing-how-to-use-them.html
  https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Be Aware

- The GoldBrute botnet is scanning the internet searching for poorly protected Windows machines with Remote Desktop Protocol (RDP) enabled. If you don't actively need RDP for business purposes, please disable it. Bad guys have been breaking into systems via RDP and easily cracked passwords for a while now. This botnet is just the latest example.
  Reference: https://www.bleepingcomputer.com/news/security/new-goldbrute-botnet-is-trying-to-hack-15-million-rdp-servers/
- Here are six ways malware can bypass your controls and infect your devices.
  Reference: https://www.csoonline.com/article/3400860/6-ways-malware-can-bypass-endpoint-protection.html
- This is nice. Cloudflare provides its full set of security services (mainly DDOS protection) to any politically or artistically important organizations at no cost so long as they are either non-profits or small commercial entities.
  Reference: https://blog.cloudflare.com/project-galileo-fifth-anniversary/

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.