Cutting Through the Cybersecurity Noise

Here's what's important this week: August 30, 2019

Take Action

- Get ready for October's National Cybersecurity Awareness Month. DHS published a bunch of resources and a great 2019 planning toolkit.
  References: https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019 https://niccs.us-cert.gov/sites/default/files/documents/pdf/dhs_ncsam2019_toolkit_508c.pdf?trackDocs=dhs_ncsam2019_toolkit_508c.pdf

Be Aware

- Emotet, a very "popular" type of malware recently began contacting command and control servers again. It was dormant for a few months. Emotet is a banking trojan used to drop other types of malware, like ransomware, onto infected systems. The current theory is the Emotet perpetrators are cleaning up their malware infrastructure and preparing to release a new variant.
  Reference: https://www.bleepingcomputer.com/news/security/emotet-botnet-is-back-servers-active-across-the-world/
- NanoCore v1.2.2, a remote access trojan, is being offered for free on the dark web. This could lead to a rise in attacks targeting passwords, bank details, and other personal information. The malware gives bad guys (even those with limited technical skills) the ability to steal passwords, perform keylogging, and secretly record audio and video using the webcam on Windows systems.
  Reference: https://www.zdnet.com/article/cybersecurity-this-trojan-malware-being-offered-for-free-could-cause-hacking-spike/
- Credential stuffing attacks have been recently hitting the financial services sector hard. It appears the bad guys (with limited technical skills) are using a new tool or service in their attempts to try various account credentials, because they're not throttling their login attempts, causing a denial of service. In other words, the bad guys keep trying to log into user accounts with different passwords, locking out the legitimate users.
  Source: National Cyber-Forensics & Training Alliance threat sharing meeting, August 29, 2019

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.