Cybersecurity Advisory — Ban Crypto Mining	**Cyber Advisory**
Criticality:Low:Green:	**5/4/2018 3:00 PM**
Summary	As mining cryptocurrency continues to grow as a way to make money, the ACTIC recommends organizations update their Acceptable Use Policies to forbid using organization resources for cryptocurrency mining. This is especially important for organizations that provide public-accessible internet access.
Criticality	Criticality is ***low***, based on current events and potential for impact. Note: See below for criticality descriptions.
Definition and Risk: Cryptocurrency Mining	Cryptocurrency mining is the process of verifying cryptocurrency transactions and adding them to the public ledger, known as the blockchain. Anyone with access to the internet and suitable hardware can participate in mining and get paid for it. Cryptocurrency mining uses a lot of computing resources. It increases device CPU and network bandwidth consumption, slowing system response times (sometimes severely). Because performing crypto mining is so resource intensive, it could damage devices due to overheating.
Recommended Actions	Listed below are recommended actions. **Prevent** • Update your internal and external Acceptable Use Polices to ban cryptocurrency mining. While most acceptable use policies have a statement that forbids using organization resources for personal use that consumes excessive system resources, the ACTIC recommends adding a line explicitly forbidding cryptocurrency mining. Note: Contact ActicCybersecurity@azdps.gov if you want a sample acceptable use (or other cybersecurity) policy. • Communicate the policy update. **Detect** • Monitor system performance and network traffic for excessive resource use. **Respond** • Ensure incident response processes are up-to-date and alert key players to the potential risks.

To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)
Criticality Descriptions	Listed below is a general description of the criticality rating. The rating is subjective based on information currently known and the analyst's experience. • **High / Red**: The potential incident may impact or breach critical business, systems, and/or services without immediate intervention. There may also be indications that an attack is currently in process. • **Medium / Yellow**: The potential incident does not place an organization's business, systems, and/or services in immediate risk but may pose an unacceptable risk if not addressed in a timely fashion. • **Low / Green**: The potential incident does not pose unacceptable risk, but may indicate trends or patterns that might suggest a future impact. • **Informational / White**: There no current potential incident. Information is for awareness.
Disclaimer	This alert contains raw intelligence that has not been analyzed. It is provided for your situational awareness to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.
References	http://www.chelanpud.org/about-us/newsroom/news/2018/04/03/pud-board-acts-to-halt-unauthorized-bitcoin-mining https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/bitcoin-mining-security-risks/