Cybersecurity Advisory for SamSam Ransomware	**Cyber Advisory**
Criticality:Medium-High:Yellow:	**03/29/2018, Noon**

Summary	Recently there have been several, high-profile, ransomware incidents targeting government entities. The threat actors may expand their attacks to all sectors.
Criticality	Criticality is ***medium-high***, based on current events and potential for impact. Note: See below for criticality criteria.
Details	Here's how the attack works. The threat actors • Scan the internet for new, internet-accessible servers that have port 3389 open for Remote Desktop Protocol (RDP) • Gain access to the system by brute-forcing the RDP service password • Once in the system, perform reconnaissance on the system, traverse the network, and attempt to destroy any backup files, then • Manually deploy SamSam ransomware. It appears the threat actors may be part of a criminal enterprise looking for financial gain. There have been no reports of data exfiltration.
Recommended Actions to Secure RDP	Listed below are recommended actions provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC) to secure RDP and cloud-based virtual machines (VMs). • Verify that all cloud-based VM instances, with a public IP, do not have open RDP ports, unless there is a valid business reason to do so. Note: Some cloud service providers enable RDP by default when a cloud-based VM is created and assigned a public IP address. • Assess the need to have RDP open on systems and, if required, limit connections to specific, trusted hosts. • Place any system with an open RDP port behind a firewall and require users to VPN in through a firewall. • Perform regular checks to ensure RDP, port 3389, is not open to the public internet. • Enable strong passwords and account lockout policies to defend against brute-force attacks. • Apply two-factor authentication, where possible. • Enable network-level authentication where possible. • Enable logging, ensuring the logs are kept for a minimum of 90 days and reviewed regularly to detect intrusion attempts. • When creating cloud-based VMs, follow the cloud provider's best practices. • Ensure third-parties that require RDP access are using cybersecurity best practices, including those described above for RDP connections.

Recommended Actions to Secure Networks and Systems	Listed below are recommended actions provided by the MS-ISAC to secure networks and systems. • Perform regular backups of all systems to limit the impact of data loss. Store the backups offline as some ransomware is able to encrypt backup files if they are connected to the network. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Verify the backups are operational. • Know what is connected to and running on your network. • Keep all hardware, operating systems, applications, and software up-to-date and patched. • Use antivirus programs with automatic updates of signatures and software. • Apply the Principle of Least Privilege and consider implementing network segmentation. • Consider the use of a proxy server for internet access. • Implement software restriction policies or other controls to prevent unauthorized programs from executing, especially when stored in locations frequently used by malware, such as temporary folders. • Ensure that staff know where and how to report suspicious emails and possible infections.
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 Criteria	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.