ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT
Ransomware
July 2019

Why are we issuing this alert?

We received information that some government entities' computer systems and data have been encrypted and made inaccessible by ransomware. Ransomware is malicious software (malware) hackers use to encrypt and deny access to systems or data until a ransom is paid. Recovery from a ransomware attack can be difficult if adequate protection is not in place. This alert outlines how entities can safeguard against ransomware and take appropriate action if they fall victim to it.

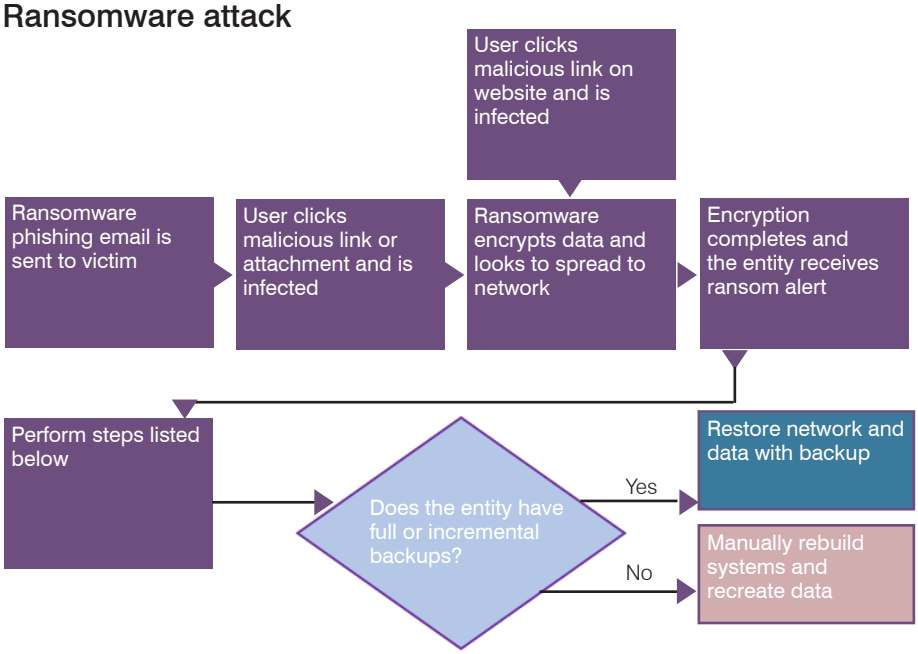
What is ransomware?

Ransomware is an increasingly common form of malware that typically involves encrypting or locking digital data and then demanding a ransom. Like most malware, ransomware often infects a system through email attachments, downloads, web browsing, and system vulnerabilities. Attackers use 2 main strategies to infect the victim's computers with malware. The first and most common approach involves the attacker sending fraudulent email to an organization (see textbox for information about phishing or spear phishing emails). The email contains malicious code hidden in a legitimate-looking link or attachment, but clicking the link or opening the attachment infects the computer. The second approach involves fraudsters adding malicious code to legitimate websites. On legitimate websites, malicious code can be hidden in links or files. By visiting the website and clicking on links or opening files, the victim's computer can be infected. In either approach, once a computer is infected, the malware begins encrypting systems and data, which may include data backups and other computers on the same network. After the ransomware is in place, the victim receives a ransom alert demanding compensation in exchange for a decryption key. Paying the ransom does not guarantee an organization will get a decryption key to recover the data. However, there are very effective prevention and response actions that can significantly lower the risk posed to your entity.

Phishing—Typically involve mass communications (i.e., email, social media) where the communication appears to come from a legitimate and often trusted source and requests the receiver to divulge private information or perform certain actions that could potentially lead to data or financial loss.

Spear phishing—Similar to phishing except direct communication is personalized with the victim's information.

Ransomware attack



To help protect systems and data from ransomware, IT standards and best practices recommend:

- **Performing regular data backups—**A backup is a secondary copy of data used to restore the original if data is lost, such as to ransomware (see textbox for information on backup types). Frequent system and data backup is essential and aids in recovering a system. While online backups could be beneficial for quick recovery from system disruption or failure, offline backups could provide the best recovery from a ransomware attack. Full or incremental backups should be stored offline, not connected to or accessible from the network, or at an alternative site that cannot be accessed through the network. Mirror backups, or data replication, do not protect against or help recover from a ransomware attack because the data in one server encrypted by ransomware is replicated in real-time to another server and will therefore also be encrypted.
- **Testing backups periodically—**To ensure that backups can be used to restore a system to a previous version, backups should be tested periodically to verify their integrity, which would include ensuring that the backups include all necessary system data and files and that the restoration process using the backups will work effectively if a ransomware attack were to occur.

Backup types:

Full backups—A full or complete copy of data. While full backups could provide the best recovery from a ransomware attack, frequently performing full backups often requires a large capacity of disk or tape storage space.

Incremental backups—Only makes copies of data that has changed since the previous full backup, which helps to decrease the amount of storage space required for backups.

Mirror/replication backups—Process of copying data in real-time from one server to another server, including the cloud. Mirror backups are sometimes viewed as an appropriate stand-alone method for performing a data backup. While mirror backups can increase system availability, it should not fully replace a data backup. Some mirror/replication backup solutions support snapshots or continuous data protection, which could help entities recover from a ransomware attack by restoring files to a version prior to encryption, but standard backups should be included as part of a holistic backup solution.

- **Implementing system-level protections—**System protections such as intrusion detection systems, antimalware, and email filtering can be used to detect and sometimes block ransomware attacks before data can be compromised. Entities should run security scans regularly to help detect threats.
- **Maintaining updated systems—**Hardware and software vendors periodically issue updates or patches for their products to correct security vulnerabilities and other system flaws they have identified to improve their products' security, usability, and performance. It is important to keep systems and applications updated with the latest patches to reduce the number of exploitable entry points available to an attacker because vulnerable systems are often the targets of most attacks.
- **Requiring security awareness training for employees—**Employees should complete security awareness training during onboarding and at least annually thereafter. Security awareness training helps to ensure that employees understand the risks associated with information security, the importance of complying with security policies, and how to recognize security threats, such as phishing emails with suspicious links or attachments.
- **Restricting unnecessary permissions—**Users' permissions to install and run software on their work computers should be limited to the minimum permissions needed to perform their work. Disable administrative rights for regular users and restrict write permissions on network file shares for users who do not require them. Restricting permissions may help prevent malicious software from running on systems and can limit its ability to spread on a network.

Even with adequate security controls, such as those mentioned above, there is always a possibility that ransomware could still occur. If a system is compromised by ransomware, consider the following:

- **Isolate the compromised system(s)—**Remove the compromised system(s) from the network immediately. To protect other computers, the network, and shared drives, shut down the system(s) believed to be compromised.

- **Immediately secure backup data or systems by taking them offline—**Ensure that backup data is not connected to or accessible from the network.
- **Change passwords—**Change any compromised account and network passwords after removing the system from the network.
- **Notify the authorities—**Contact the Phoenix field office of the Federal Bureau of Investigation (FBI) and request assistance. This is strongly encouraged by the United States Government as the FBI has valuable tools, relationships, and experience related to cybercrimes.
- **Contact your liability insurance provider—**Your liability insurance provider should have policies and procedures to protect the entity from computer fraud and should be contacted if ransomware attacks the computer system.
- **Implement disaster recovery or contingency plans—**After the malware has been removed from the system, implement any applicable steps in the entity's formal disaster recovery or contingency plan to bring the system back to working order.

Helpful cybersecurity and cybercrime links:

National Institute of Standards and Technology—https://www.nccoe.nist.gov/projects/building-blocks/data-security

U.S. Department of Homeland Security Ransomware Publication—https://www.us-cert.gov/security-publications/Ransomware

FBI Cyber Crime—https://www.fbi.gov/investigate/cyber

U.S. Department of Justice, Criminal Division—https://www.justice.gov/criminal-ccips