Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

**HOW DO I PROTECT MY NETWORKS?**

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

- **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
- **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
- **Staff Training:** Have we trained staff on cybersecurity best practices?
- **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
- **Application Whitelisting:** Do we allow only approved programs to run on our networks?
- **Incident Response:** Do we have an incident response plan and have we exercised it?
- **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
- **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?
How do I respond to ransomware?

Implement your security incident response and business continuity plan. It may take time for your organization’s IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization’s essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact PNP ACG or field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

Protecting Your Networks from Ransomware

Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. There are very effective prevention and response actions that can significantly mitigate the risk posed to your organization.

Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization’s reputation.

Ransomware may direct a user to click on a link to pay a ransom; however, the link may be malicious and could lead to additional malware infections. Some ransomware variants display intimidating messages, such as:

“Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine.”

“You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them.”