TIP SHEET:

HAVE YOU BEEN HIT WITH RANSOMWARE?

LMG SECURITY

HERE'S WHAT TO DO NEXT

- **Don't Panic.**
- **Assess the situation.** Identify affected systems as quickly as possible and make a list.
- **Quarantine affected systems if at all possible, to prevent the ransomware from spreading.** If the computer is already encrypted, unplug it from the network and keep the power on. It may be possible for examiners to recover the key from memory if you keep it plugged in. If the ransomware is actively encrypting files but has not fully encrypted everything, the best course of action is typically to unplug the computer and remove battery backup. This will preserve any files that have not yet been encrypted. For Virtual Machines: take snapshots while running, then suspend the VM.
- **Reset passwords for all cloud accounts and local domain services** as quickly as possible.
- **Check your backups** and evaluate what data may be recoverable, and what has not been backed up. Determine the most recent viable backup date and time.
- **Make sure you have an offline backup.** If your backups are online, take them offline and make a copy immediately, to minimize the risk that they could be overwritten by ransomware (this happens frequently).
- **Preserve evidence,** including network logs, server logs, antivirus alerts, IDS/IPS, malware and any other data that can help you identify the source of the compromise, determine precisely which systems are affected, and figure out what the attackers did while they were in your network. Make sure to save a copy of the malware itself. Often, logs are automatically deleted from systems after a certain amount of time, so it's important to export this evidence quickly and save it offline.
- **Proactively check for any other signs of suspicious activity,** in order to identify any other infected systems.
- **Do not respond to the criminals.** Call a professional ransom negotiator for assistance.
- **Activate your existing crisis management, disaster recovery or business continuity plans** as needed. Be sure to address communications needs, as well as technical needs.
- **Check your insurance coverage.** You may have coverage for ransom payments, incident response services, public relations support, or other relevant services.
- **Notify your insurer, if appropriate.** In many cases, insurance will only cover ransom payments or support services if the insurer has been notified in accordance with your policy.
- **Call an experienced cyber attorney.** Ransomware may trigger state or federal breach notification requirements. Ensure that you are meeting your obligations by involving a qualified attorney right away.

- **Be aware that all of your written communications, including emails and text messages, may ultimately be discoverable** if a lawsuit occurs.
- **Use phone and in-person communication methods** whenever practical. Attackers may be monitoring your email.
- **Communicate carefully.** Release a statement with general information for your community that is in line with your public relations strategy. Typically, affected organizations state that they are experiencing technical difficulties or an unexpected maintenance window, and do not disclose that there is a security issue or ransomware unless there is a clear need.
- **Document, document, document.** Write down details about what happened, including suspicious activity, and make sure to keep a record of all actions taken in response. In a ransomware case, things move quickly, and the triage stages can seem like a blur later. Having a written record will help you later on in your recovery process.

COMMON QUESTIONS AT THIS PHASE

How did the attackers get in?
You want to know this so that you can ensure that your network is secure going forward.

Are the attackers still in our network?

Did the attackers view or take any data?
If so, precisely what data was at risk?

YOUR NEXT STEPS

During the next days and weeks, you will need to clean the ransomware out of your network, restore your data, and resume operations. You should:

☑ RECOVER FROM BACKUPS

If you have intact backups, you may be able to restore your data and remove the need to purchase a decryptor or attempt to bypass encryption.

Consider calling a ransomware expert to assist with decryption and guide you through the ransomware recovery process.

☑ ASSESS DECRYPTION OPTIONS

If you cannot restore all of your data from backups, you have two options: check for an available decryptor, or negotiate and pay the ransom.

★ CHECK FOR AN AVAILABLE DECRYPTOR

Many ransomware strains have publicly available decryptors. The site "nomoreransom.org" is an excellent resource. If the decryptor for your strain is not available, a ransomware expert may be able to work with law enforcement or other parties to find a privately available decryptor. Note that decryptors do not always recover 100% of your data.

★ NEGOTIATE AND PAY THE RANSOM

It is wise to involve an experienced ransom negotiator at this stage.

- *Proof of Life.* Before paying any ransom, you should request "proof of life"—in other words, make sure that the criminal is capable of decrypting your files. At this stage, you will need to provide an encrypted sample file, typically a small image, which will be uploaded to the ransomware contact. The criminals will demonstrate that they are capable of decrypting the file.
- *Payment.* Typically the criminals will require payment in cryptocurrency. A professional ransomware expert can manage this process for you, so that you only need to provide a credit card or bank account.

☑ TESTING

Once the criminals provide a decryption key and supporting utilities, it's important to carefully check their software for additional malware in a laboratory environment. Professional ransomware experts can take care of this for you.

☑ RESTORATION

The process of decrypting data typically takes between 1-2 weeks. The precise amount of time that it takes depends on the volume of data and the encryption methods used by the criminals. Once your data is decrypted, it should be scanned for malware prior to restoration in a production environment.

Remember that you are not alone. Ransomware is a challenge for every affected organization. There are many people who can help you at each stage of the process.

If you need assistance at any time, please contact us, we can help.

LMG SECURITY

145 W FRONT STREET
MISSOULA, MT 59802
www.LMGsecurity.com

WE ARE HERE TO HELP
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855
E-mail: info@LMGsecurity.com

REFERRING A CLIENT
To refer a client to LMG Security, please email info@LMGsecurity.com