ORION INVESTIGATIONS

RESPONDING TO A RANSOMWARE ATTACK

Author – Andrew Smith - Director of Computer Forensics Services

8th February 2023

When a company becomes a victim of a ransomware attack they will often contact Orion to ask if we can recover their encrypted data. In almost every case the answer is going to be no as we will not have access to a recovery key to decrypt the data. Therefore, it is vital that the company maintains up to date backups of their data.

The number of ransomware attacks continue to rise year on year. According to the Verizon 2022 Data Breach Investigation Report there was a 13% increase in ransomware attacks and ransomware was involved in 25% of all breaches.

One of the trends now employed by the attackers is the double extortion method. The attackers gain access to the network and steal the confidential data. They will then encrypt the data on the network and demand a ransom to be paid to decrypt the data. If the victim has the data backed up and refuses to pay the ransom, the attackers will then threaten to release the data online.

When a company falls victim to a ransomware attack the natural response is to wipe the infected machine and restore the data in order to get up and running again as quickly as possible. As a result, attackers will often use ransomware as a way to destroy any evidence of a data breach after they have extracted the data from the network.

It is therefore important for the company to conduct a thorough investigation even if the encrypted data cannot be recovered.

The purpose of the investigation is to preserve potential evidence in order to:

- Identify how the system came to be infected with ransomware
- Identify if any confidential data has been extracted from the system
- Provide answers to the regulatory authorities and show you have taken reasonable steps to prevent a repeat
- Preserve the data in case decryption keys are released at a later date

If you become a victim of a ransomware attack, how should you respond?

- Do not shut down the infected devices
- Disconnect the infected devices from network
- Preserve logs such as Firewall, VPN, anti-virus logs or any other logs which can be saved
- Document all information pertaining to the ransomware attack
    - Photo or copy of the ransom demand note/splash screen
    - Ransomware variant name if known
    - The file extension of encrypted files
    - The date and time of the attack
    - The file naming scheme for the ransom note/readme file left by attacker
    - Any email addresses or URL or other method provided by the attacker for communications
    - Required payment method/bitcoin addresses provided by the attacker
    - Ransom amount demanded if known

What information will the investigators need to know from you?

- Number of devices affected
- Type of devices, make, model, size of hard drive
- What OS is on the devices
- Is there encryption on devices and If so what encryption and can IT provide a recovery key?
- Location of devices
- Timeline of events
- Details of ransomware

It is important to respond quickly and get the investigators onsite as soon as possible so that they can begin the process of preserving potential evidence from the infected devices. This will include not only the data from the hard drives and logs but also volatile data such as RAM memory which can provide a wealth of information such as network connections, open ports and destination IP addresses.

We would therefore recommend that you do not wait until you become a victim of a ransomware attack before deciding which investigation company you wish to work with. Do your research, due diligence and complete the vendor onboarding process before an attack occurs. This will ensure a quick response and prevent the loss of any potential evidence.

