Deloitte.

WHAT IS RANSOMWARE ?

Ransomware is a malware that restricts or limits users from accessing their system through 3 ways:

- User screen lockdown
- User file encryption
- Remote access and control of victim system through a command & control Centre

In many cases Ransomware victims may have to pay a 'Ransom' or 'release fee' through a digital payment gateway in order to re-gain access to their systems. However, **in our experience there is no guarantee of regaining system access even after the ransom money is paid.**

WHAT IS THE SOURCE OF RANSOMWARE ?

Most common sources of ransomware are phishing emails that contain malicious attachments, website pop-up advertisements and infected system in the network. Upon clicking/downloading such links one's computer can get affected by ransomware.

While many ransomware infections require a victim to open an email attachment or click a link, **recent attacks are notable for its ability to copy itself between vulnerable machines without user intervention.**

PROTECTING ORGANIZATIONAL INTELLECTUAL PROPERTY FROM RANSOMWARE

1. Regularly update your Operating System/Software for security patches.
2. Take **periodic backup and encrypt your data** using encryption tools. **Store the backup copy offline**, as it helps in preventing the backup copy getting infected by the malware.
3. Regularly update your **anti-virus/anti-spam-ware/anti-ransomware definitions.**
4. **Do not open** email attachments from **unknown sources**.
5. The moment you **suspect any system(s) is infected**, disconnect it from your computer network and **shut it down.** This can prevent the ransomware from spreading in your network and encrypting more of your data and mapped drives.
6. **Verify email id against your contacts**. If in doubt, perform a virus scan before downloading and opening the attachment.
7. Enable system **restore point, which is an in-built** feature of Microsoft Windows operating system, to assist in restoring files.
8. Enable **Volume Shadow Copy Service (VSS*)** feature of Microsoft that could assist in restoring files.
9. Set up **End point protection**.
10. Use **network protection** - Network protection could also help prevent network encryption which could also happen with some crypto Ransomware threats.
11. **Use Software Restriction Policies** to prevent or restrict the primary attack vectors, i.e. deny execution of user that can write/create privileges on business critical systems.

DELOITTE FORENSIC MALWARE ANALYSIS LAB

At Deloitte's Forensic Malware Analysis Lab, we can:

- Attempt to perform recovery of the deleted data to the extent possible.
- Attempt to identify the source of infection.
- Check if any malicious files were downloaded or dropped in the system for infection.
- Check if any malicious file(s) are left in the system.

We analyse ransomware through a root-cause oriented approach.

Our malware exploration framework is focused on reverse engineering the malware to provide insight on micro grained code and application modules compromised. The malwares decoded are further tested in an automated environment across all operating systems and digital devices. We can help assess whether other malware may have been also installed that could compromise the systems, or whether other systems may have been similarly affected.

For more details, please contact

Rohit Mahajan
APAC Leader, Partner and Head
Forensic - Financial Advisory
T: +91 22 6185 5180
E: rmahajan@deloitte.com

Jayant Saran
Partner
Forensic- Financial Advisory
Tel: +91 124 679 3607
Email: jsaran@deloitte.com