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?

Two most common sources are phishing emails that contain malicious attachments and website pop-up advertisements. Upon clicking/ downloading such links one's computer can get affected by ransomware.

PROTECTING ORGANIZATIONAL INTELLECTUAL PROPERTY FROM RANSOMWARE

1. Do **NOT OPEN** email attachments from **UNKNOWN SOURCES.**
2. **VERIFY EMAIL ID AGAINST YOUR CONTACTS**. If in doubt, perform a virus scan before downloading and opening the attachment.
3. Enable system **RESTORE POINT, WHICH IS AN IN-BUILT** feature of Microsoft Windows operating system, this could assist in restoring files
4. Enable **VOLUME SHADOW COPY SERVICE** (VSS*) feature of Microsoft that could assist in restoring files
5. **TAKE PERIODIC BACKUP AND ENCRYPT YOUR DATA USING ENCRYPTION TOOLS**
6. Regularly update your **ANTI-VIRUS DEFINITIONS**
7. Set up **END POINT PROTECTION**
8. Use **NETWORK PROTECTION** - Network protection could also help prevent network encryption which could also happen with some crypto Ransomware threats.

RECENT RANSOMWARES SIGHTINGS OBSERVED:

- TorrentLocker
- CryptoWall
- CTB-Locker
- Troldesh
- CRYPVAULT
- Crowti

DELOITTE FORENSIC MALWARE ANALYSIS LAB

At Deloitte Forensic's malware analysis lab, ransomware is analyzed 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 & Head - Forensic Financial Advisory
Tel: +91 22 6185 5180
Email: rmahajan@deloitte.com

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