Deloitte.



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

Do **NOT OPEN** email attachments from **UNKNOWN SOURCES**.

VERIFY EMAIL ID AGAINST YOUR CONTACTS. If in doubt, perform a virus scan before downloading and opening the attachment.

Enable system **RESTORE POINT, WHICH IS AN IN-BUILT** feature of Microsoft Windows operating system, this could assist in restoring files

Enable **VOLUME SHADOW COPY SERVICE** (VSS*) feature of Microsoft that could assist in restoring files

TAKE PERIODIC BACKUP AND ENCRYPT YOUR DATA USING ENCRYPTION TOOLS

Regularly update your **ANTI-VIRUS DEFINITIONS**

Set up **END POINT PROTECTION**

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-Locke

Troldesh

CRYPVAULT

Crowt

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

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

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP).

This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTIILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information is not intended on services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect your personal finances or business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained containing professional adviser. No entity in the user access this entire notice and terms of use.

©2016 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339), a private company limited by shares, was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458), with effect from October 1, 2015