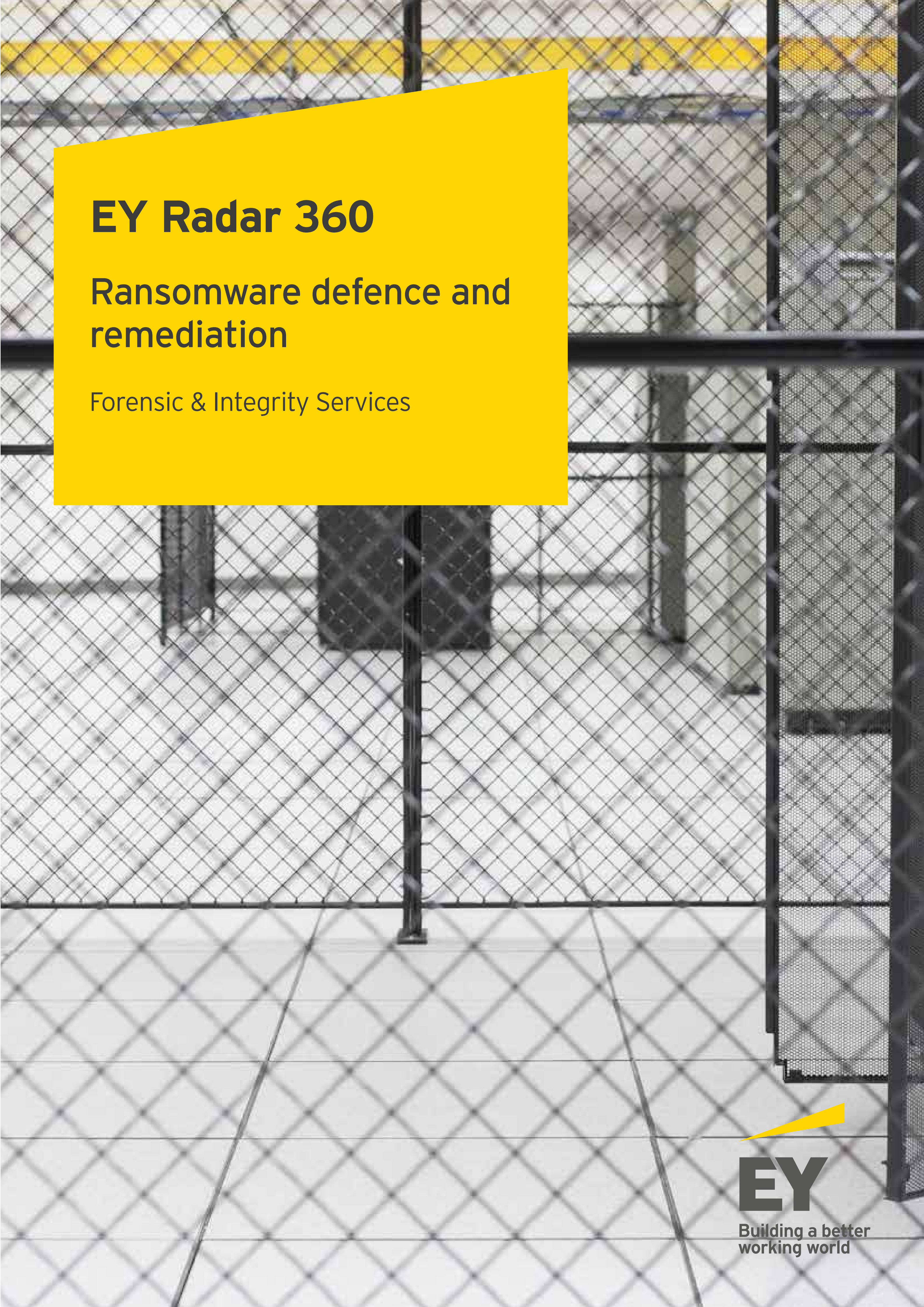
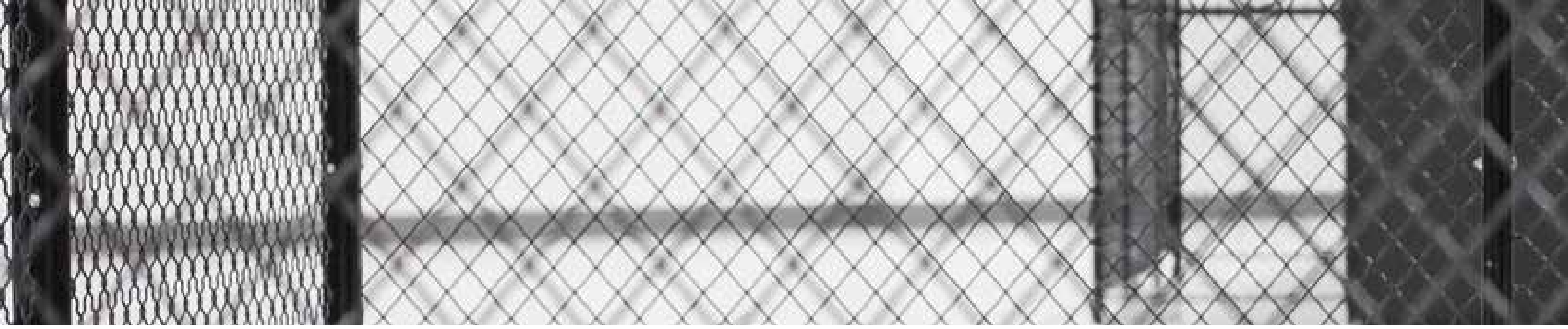


# EY Radar 360

## Ransomware defence and remediation

Forensic & Integrity Services

Building a better
working world

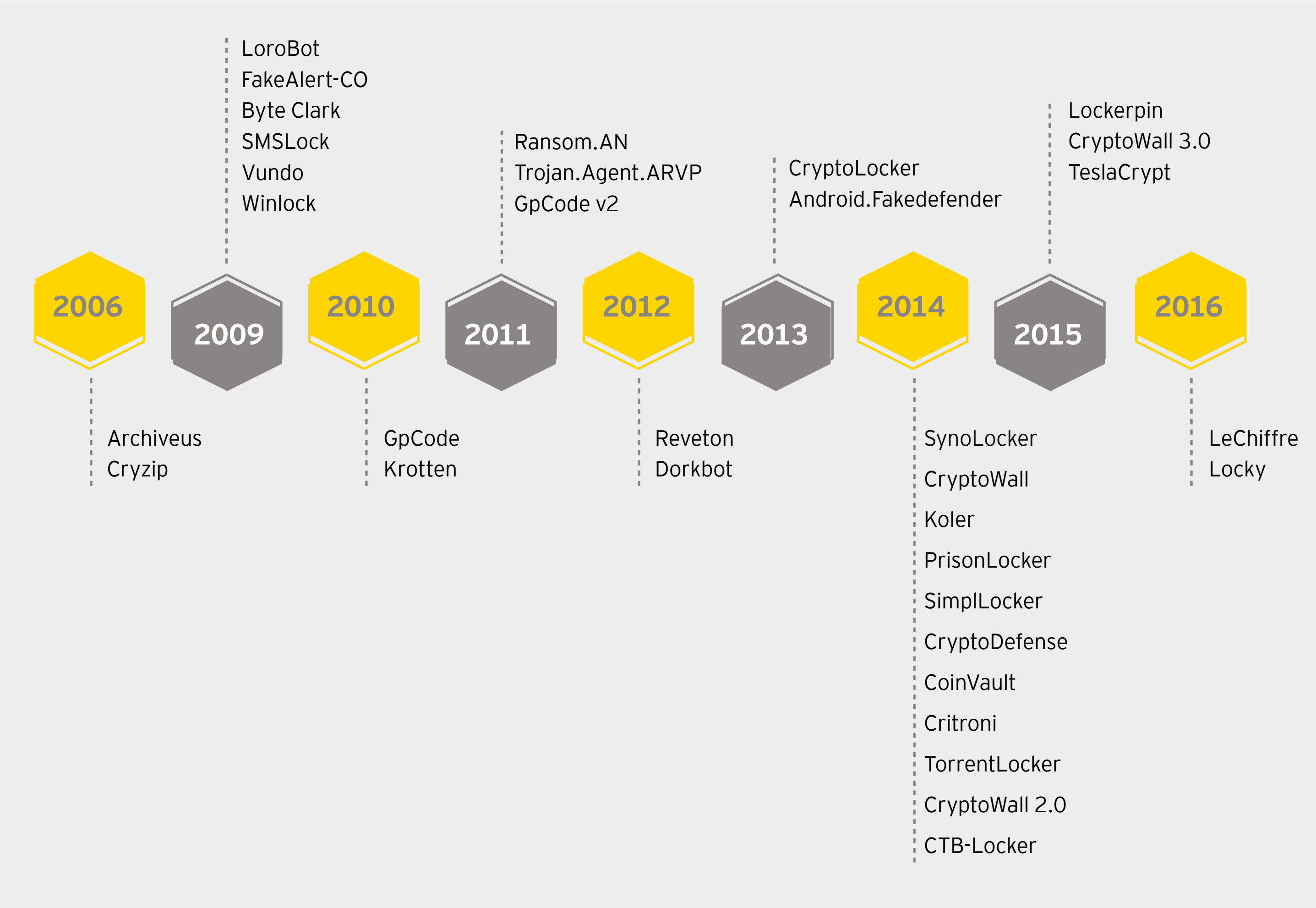


Ransomware is a sophisticated malware that bypasses the traditional layers of security and makes the user's computer files inaccessible, by either locking them up or encrypting them. The user is then asked to pay a "ransom" to the cybercriminals to regain access to the data. Unlike other malware, ransomware does not even require elevated or administrative credentials, making it even difficult to control.

Cybercriminals tend to target companies that have highly confidential or critical data, as they are more susceptible to pay the ransom to retrieve their data.

**Malware** (**mal**icious soft**ware**) is a software code that disrupts, steals or damages computer systems and data. Malware can be computer viruses, worms, Trojan horses, spyware, adware or any other program with malicious content.

## Evolution of ransomware



2006
- Archiveus
- Cryzip

2009
- LoroBot
- FakeAlert-CO
- Byte Clark
- SMSLock
- Vundo
- Winlock

2010
- GpCode
- Krotten

2011
- Ransom.AN
- Trojan.Agent.ARVP
- GpCode v2

2012
- Reveton
- Dorkbot

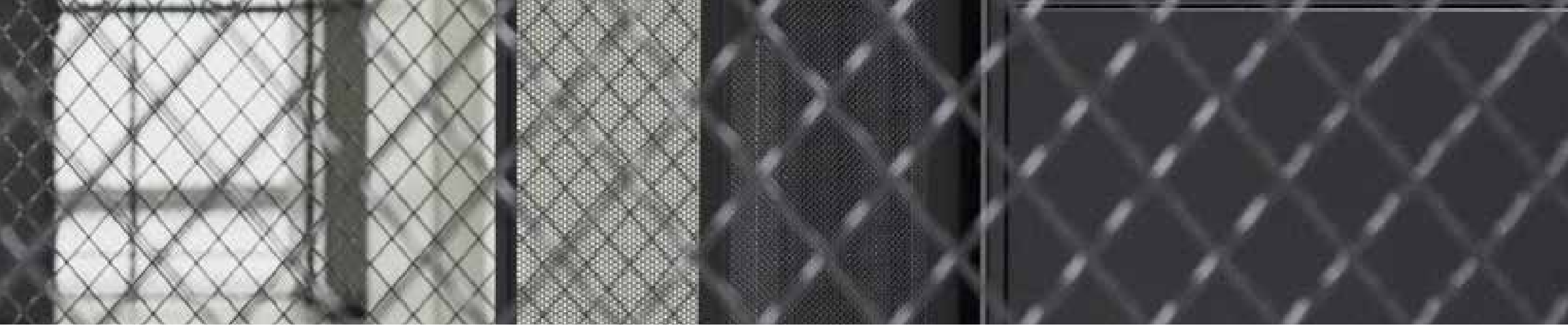
2013
- CryptoLocker
- Android.Fakedefender

2014
- SynoLocker
- CryptoWall
- Koler
- PrisonLocker
- SimplLocker
- CryptoDefense
- CoinVault
- Critroni
- TorrentLocker
- CryptoWall 2.0
- CTB-Locker

2015
- Lockerpin
- CryptoWall 3.0
- TeslaCrypt

2016
- LeChiffre
- Locky

*Data collated from various sources*



## Modus operandi

**Enter**

Enters the system though malicious websites or email attachments (human error) or by exploiting a vulnerability

**Exploit**

Exploits additional vulnerabilities in the system to gain more control of specific file locations or user accounts

**Execute**

Executes and installs itself on the compromised system and then synchronizes it with a command and control server

**Encrypt**

Encrypts or locks data and files on the system

**Extort**

Demands ransom in exchange for a decryption key for unlocking the system

## Severity of the problem

**US$500**

The typical "first offer" ransom demand per computer for regaining access to the computer and files. This demand can go up significantly.

**2,275**

ransomware complaints from businesses and individuals collectively submitted between 1 June, 2014 and 31 March, 2015. This is as per Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the non-profit, National White Collar Crime Center.

**US$325 million**

damages due to just one family of ransomware called "CryptoWall" according to an October 2015 report of Cyber Threat Alliance

**230**

different types of computer files that could be targeted by ransomware. These are up from 70 in 2013, according to Bromium Inc., an information-security firm.

**250,000**

new ransomware samples reviewed by Intel Security, a unit of Intel Corp, in 4Q14 (up by 155% from the previous quarter)

**23%**

of recipients open phishing messages used to transmit ransomware and other malware, according to Verizon Communications Inc.

*Data collated from various sources*

Recently, there are reports of ransomware incidents being on the rise in India.

## Impact on business

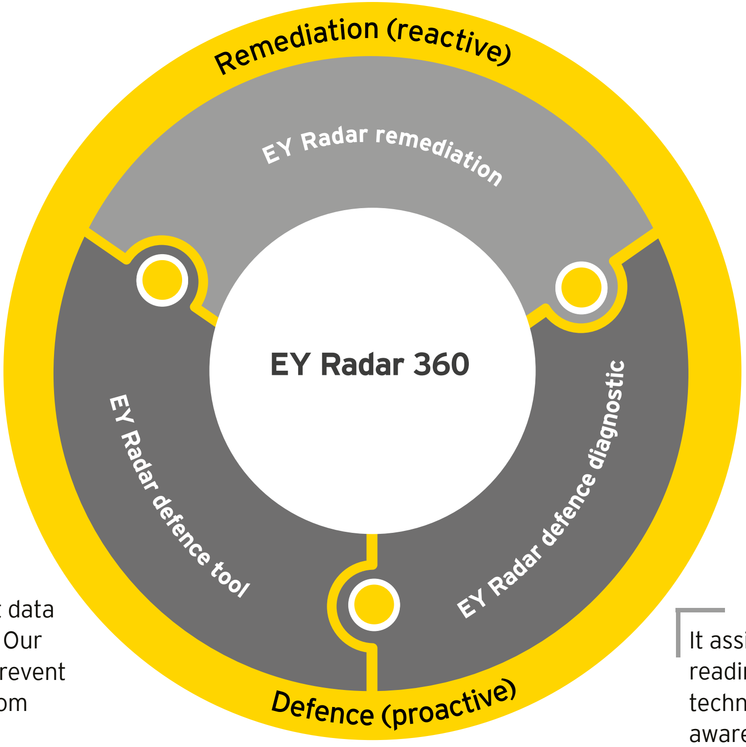
- Financial and operational loss
- Reputational damage
- Data breach
- Increased vulnerabilities due to the proliferation of digital technology
- Disrupting business continuity

## Our solution - EY Radar 360

### Helping companies defend and remediate a ransomware attack

Ransomware incidents are rising at a rapid pace, catching many companies unprepared to deal with this new and unprecedented problem. The existing anti-virus and anti-malware tools seem to be ineffective against ransomware. Our solution, EY Radar 360 is created to help clients deal with this menace. It has both reactive and proactive components.

We use our proprietary EY Radar 360 ransomware remediation toolkit and forensic procedures to salvage data in case of a successful ransomware attack, without the need for paying any ransom to the hackers. Our success rate increases if we are called in as close to the incident as possible.



It helps proactively protect data from ransomware attacks. Our tried-and-tested tool can prevent damages to critical data from many known and unknown ransomware and malware.

It assists in analyzing the maturity and readiness of clients' procedures, technology controls and employee awareness to deal with potential ransomware infections. The procedures and guidelines suggested can help strengthen the defences of our clients against ransomware and malware. If implemented, they significantly increase the success of a remediation attempt during the reactive phase.

## Case study

### Company

A global medical equipment manufacturer

### Case

- Critical data on company computers and main enterprise resource planning (ERP) server was infected by the LeChiffre ransomware
- A ransom of US$1,000 in virtual currency was demanded per computer for the release of data
- EY was brought in to assist in incident response and remediation

### Approach

- A quick triage revealed other systems with a similar infection
- Infected systems were isolated from the network
- The EY Radar toolkit was used on the infected systems to recover data and remediate the infected systems
- The compromised systems were forensically examined for the source and the spread of the malware
- Subsequently, the compromised systems were disinfected
- Major loopholes and technical vulnerabilities were identified and fixed to prevent any future incidents

### Conclusion

- EY was able to recover critical data from all the infected systems
- The source of the malware was identified as an email containing a malicious attachment and vulnerability on an internet-facing terminal server
- The source of the email was traced to an IP address
- Critical functionality of the ERP was restored

EY | Assurance | Tax | Transactions | Advisory

**About EY**
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

**About EY's Forensic & Integrity Services**
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority — no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYIN1606-051

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

## Contacts:

**Arpinder Singh**
Partner and Head – India and Emerging Markets
Direct: + 91 12 4443 0330
Email: arpinder.singh@in.ey.com

**Harshavardhan Godugula**
Partner
Direct: + 91 40 6736 2234
Email: harshavardhan.g@in.ey.com

**Ranjeeth Bellary**
Associate Partner
Direct: + 91 22 6192 0172
Email: ranjeeth.bellary@in.ey.com