Reducing the Risk of Ransomware

Taking robust and preventive measures to counter ransomware
The recent wave of cyber attacks is proof that cyber criminals are becoming more aggressive and sophisticated, simultaneously targeting all kinds of interconnected organizations across the globe.

A cyber criminal’s greatest ally is complacency.

Jason Yuen
Malaysia Cybersecurity Leader, EY
Background

On 12 May 2017, a massive ransomware cyber attack caused major business impact across the globe, affecting organizations in almost every sector.

This ransomware attack has rapidly spread and caused outage to over 200,000 systems across 150 countries and is expected to escalate further.

Most security researchers, including EY, anticipate that new variations are likely to surface in the very near future. Such looming IT security threats call for robust and preventive measures to mitigate the risk of potential attacks.

What is WannaCry ransomware?

- WannaCry ransomware is a type of computer malware, typically spread by phishing emails, that encrypts files and disks and locks computers. The hacker then demands a ransom for decryption, which has to be paid within a stipulated timeframe in the form of electronic currency called bitcoins.

- Ransoms of approximately US$300 to US$600 are requested to be paid to one of three bitcoin accounts within three days.

- This type of ransomware normally spreads via a windows protocol called SMB (the Server Message Block protocol operating over port 445 and 139), typically used by Windows machines to communicate with file systems over a network.

- Once successfully installed, this ransomware scans for and propagates to other at-risk devices. This version of ransomware exploited a weakness in older versions of the Microsoft operating system. Microsoft released an emergency security patch to address this weakness called MS17-010 and most anti-virus companies have updated their signatures.

- WannaCry ransomware leverages zip files sent over emails and also checks to see if backdoors (like DoublePulsar) are already installed on previously infected machines. Both DoublePulsar and the ExternalBlue exploit that target the SMB vulnerability were made public by the Shadow Brokers in April 2017.
## How to reduce the risk of ransomware attack?

### 10 Checkpoints

**Reducing the Risk of Ransomware**

<table>
<thead>
<tr>
<th>Checkpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure vulnerability management (including patch management) is a robust and mature enterprise program</td>
</tr>
<tr>
<td>2</td>
<td>Maintain an effective enterprise incident response and Business Continuity Plan (BCP) that are tested and measured for effectiveness against ransomware, as well as updated to reflect the current cyber threat environment</td>
</tr>
<tr>
<td>3</td>
<td>Maintain backups that account for all critical data and the rate of data generation</td>
</tr>
<tr>
<td>4</td>
<td>Align timeline and procedures for restoring system backups with your Business Continuity Plan (BCP)</td>
</tr>
<tr>
<td>5</td>
<td>Review the organization’s incident response and disaster preparedness plans to verify that they adequately address recovery from a ransomware event</td>
</tr>
<tr>
<td>6</td>
<td>Implement endpoint monitoring, giving your team visibility into malicious behavior occurring at that level</td>
</tr>
<tr>
<td>7</td>
<td>Identify and confirm critical systems and data are not unnecessarily connected to internet</td>
</tr>
<tr>
<td>8</td>
<td>Ensure the organization has a security awareness training program in place with proactive testing</td>
</tr>
<tr>
<td>9</td>
<td>Ensure the testing of the security program with “red team” services and active hunting campaigns</td>
</tr>
<tr>
<td>10</td>
<td>Maintain proactive security monitoring of the entire environment</td>
</tr>
</tbody>
</table>

**Note:**

1 A red team is an independent group that challenges an organization to improve its cyber defense systems.
What to do when WannaCry strikes?

Post-attack: 6 Actions

- **Disconnect infected machines** from the network and take all backups offline as they could become encrypted if left connected to the network.
- **Activate your incident response plan** and do not treat the investigation as merely an IT issue or exercise. Ensure there is cross-functional representation in the investigation team, including legal, compliance, information security, business, public relations, human resources and other departments.
- **Identify and address vulnerabilities in your connected ecosystem.** Ensure adequate security updates, malware detection and anti-virus detection to complicate attackers’ efforts to get back in; enhance detection and response capabilities for future attacks; and prepare for virus eradication events.
- **Ensure IT systems are patched** before powering up PCs. Keep systems up to date with a robust enterprise-level patch and vulnerability management program. This should include a formal, repeatable life cycle to manage vulnerabilities based on risks as they evolve, and a comprehensive asset model that focuses on the exposure of assets to these risks, including any connectivity to other assets.
- **Activate business continuity plans.** Prepare data based on varying requirements for regulatory reporting, insurance claim and dispute, litigation, threat intelligence and/or customer notification.
- **Collect and preserve evidence** in a forensically sound manner so that it is conducive to investigation, and reliable and usable in civil or regulatory matters.

**Ramifications of WannaCry Attack**

- The infection can spread if not mitigated quickly.
- Data could be lost if not preserved and the decryption process fails.
- Adversaries routinely leave behind malware even after the data is decrypted.
- Ransomware infections could trigger regulatory or statutory requirements.
- Careful consideration should be given as to when and how to engage law enforcement.
- Negotiations with an adversary should be conducted by experienced professionals who have done it before.
Questions to ask your IT function

**Pre-attack Questions**

- Is my company’s IT operating system (OS) updated with the latest security patches?

- What contingency or disaster recovery plans are in place to mitigate the risk of complete information lockdown?

- Is there a network-wide alert system in place to ensure all staff are aware of and vigilant against the risk of contagion?

- What is the risk of cyber virus contagion from my vendors, suppliers and partners?

- What IT governance policies are in place to protect my company’s existing data backup?

> It is not advisable to pay the ransom as there is no guarantee that your data will be unlocked.

Susanna Lim
Malaysia Advisory – Risk, EY

**Post-attack Measures**

Who to report to immediately – your IT department, local authorities and payment processor (if relevant)?

How to isolate the infected computer unit to ensure it does not affect your entire IT network?

“WannaCry” ransomware
Malware outbreaks such as WannaCry require companies to respond in a comprehensive and defensible manner.

Even after the data is restored, companies sometimes face allegations that sensitive personnel-related or other business information had been compromised in the ransomware attack.

Third parties and other stakeholders may require the company to demonstrate forensically that, even if the data was accessed, it was not stolen.

Joyce Lim Wan Cheak
Malaysia Fraud Investigation and Dispute Services (FIDS) Leader, EY
EY Contacts

Chow Sang Hoe
Malaysia Advisory Leader, EY
Asean Advisory Leader, EY
Tel: +603 7495 8696
sang-hoe.chow@my.ey.com

Susanna Lim
Malaysia Advisory - Risk, EY
Tel: +603 7495 8773
susanna.lim@my.ey.com

Jason Yuen
Malaysia Cybersecurity Leader, EY
Tel: +603 7495 8789
jason.yuen@my.ey.com

Joyce Lim Wan Cheak
Malaysia FraudInvestigation and Dispute Services (FIDS) Leader, EY
Tel: +603 7495 8847
wan-cheak.lim@my.ey.com

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 organisation, 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 organisation, please visit ey.com.

©2017 Ernst & Young Advisory Services Sdn. Bhd.
All Rights Reserved.

APAC no. 07000965

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/my