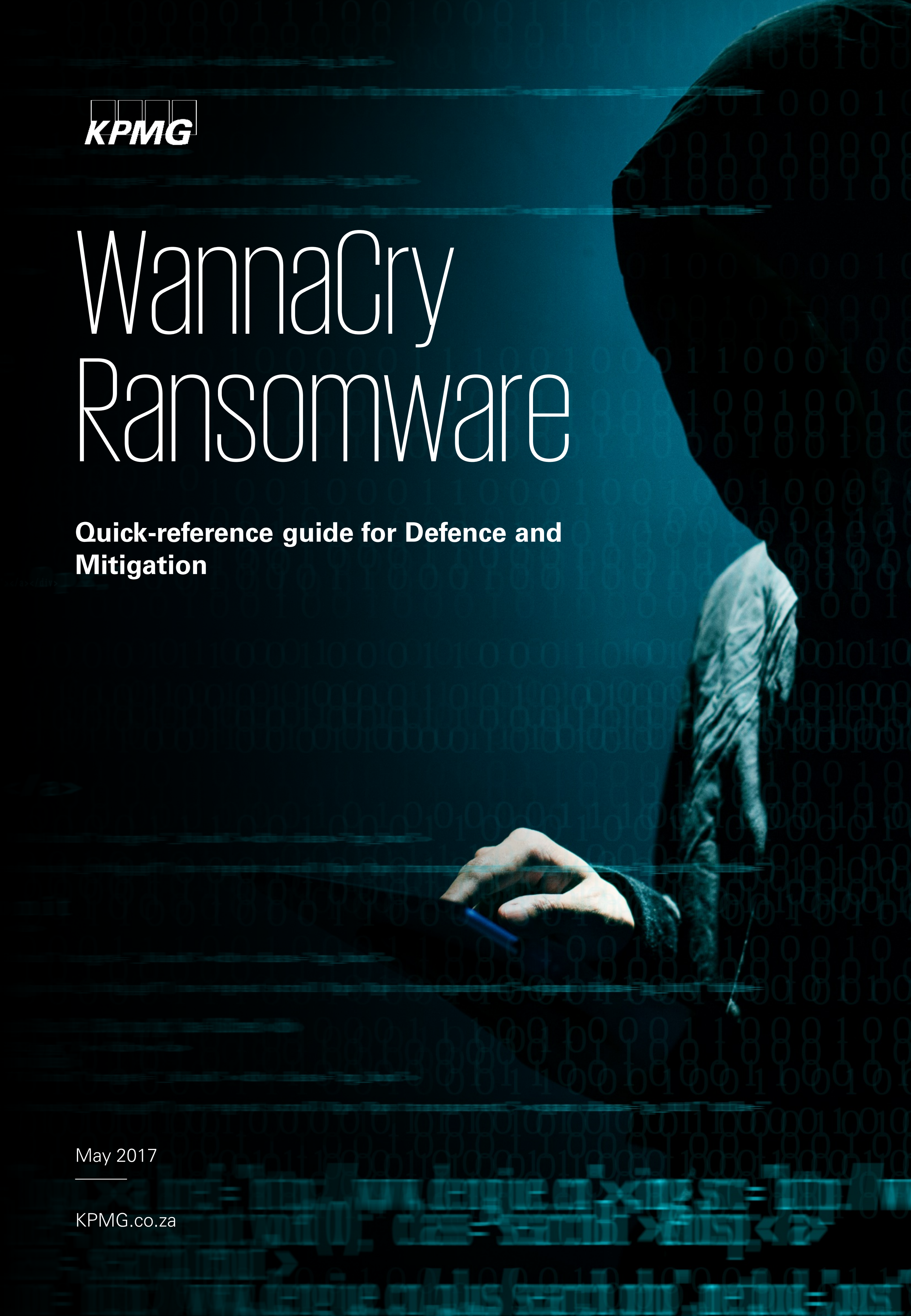

WannaCry Ransomware

Quick-reference guide for Defence and Mitigation

May 2017

KPMG.co.za

WannaCry/WannaCrypt Ransomware

Key Points

This is a quick-reference guide containing some suggestions and actions that you can take to help defend against the WannaCry ransomware. This is a collection of information both available online and compiled by various practices within KPMG Global.

There has been an outbreak of ransomware WCry, also referred to as WNCry, WannaCry, WanaCrypt0r or Wana Decrypt0r, which is rapidly spreading globally. So far, it is understood that the malware is associated with the following events:

— Locks all the data on a computer system

— Provides instructions on what to do next, which includes a demand of ransom (typically US$300 - $600 ransom in bitcoins)

  - Demand includes paying ransom in defined period of time otherwise the demand increases, leading to complete destruction of data

— The encryption is carried with RSA-2048 encryption which makes decryption of data extremely difficult (next to impossible)

How is it spreading? :

Like most of the ransomware attacks this is coming through attachments on email and initial assessments are showcasing that once infected, the ransomware spreads through a remote code execution vulnerability in Microsoft Windows computers: MS17-010. The vulnerability MS17-010 is also known as **ETERNALBLUE**, for which a patch is available.

What to do:

The below are suggestions and guidelines only, please ensure that you also perform the necessary research and threat intelligence to adequately safeguard against the malicious software outbreak.

People

Users: If not already done, management should ensure that a communication is sent to all users within the organisation in order to make them aware of the situation and what to do in the event of suspicious email coming through.

— Email communication should include details of the virus name, how to identify suspicious email from unknown senders, especially ones that demand immediate action.

— Users should be made aware to not click on or open suspicious links and attachments from unsolicited emails.

— Users should also be made aware to immediately disconnect from the network if a suspected case of infection is identified, in order to help contain the infection.

— All users should be informed to ensure that anti-virus software is updated.

WannaCry/WannaCrypt Ransomware

What to do (continued)

Network Team/Info Security Team: Ensure that technical teams are made aware of the situation and are briefed on the appropriate technical countermeasures. In addition, management should ensure that the technical teams are adequately trained and made aware of how to deal with and contain instances of infection.

Technology

The below points highlight some countermeasures that can be taken - these are by no means exhaustive and existing incident response and information security procedures within your organisation should also be consulted where necessary. These are only suggestions and you should identify the suggestions that would work best in your environment – some measures are more extreme than others.

- Consider blocking all *.onion sites at edge firewalls
- **Consider blocking ports TCP 445/139 at edge firewalls** and perform external scanning of all internet facing ranges to confirm ports are blocked.
- **Push out MS17-010 pacth to every machine as a matter of priority.** https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- For Windows XP/2003 machines consider using the inbuilt firewall to block ports TCP 445/139 (however this will have severe repercussions for domain joined machines)
- **Disable SMBv1** – guidance on this is provided at the following link: ttps://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
- For systems without patches, consider isolating these from the network as much as possible (strict VLAN's and Firewalls with strict ACL's (for example only allow 139/445 to FileServer and DC)
- Consider turning off attachments in email (painful but until it "dies down") – this is an extreme measure.

Process

- Ensure that all devices running outdated versions of Microsoft Windows XP, 2003 and other unsupported versions are identified. Check if the MS17-010 has been made available (for extended support contracts) and apply workarounds and scanning of devices to detect possible instances of infection.
- Ensure that all anti-virus and anti-malware software is updated with the latest signatures to assist in defending against infection from the ransomware.
- Monitor your network, system, media and logs for any malicious software, possible ex-filtration of data, abnormal behaviour or unauthorized network connections.
- Ensure that you have performed recent backups of key business data and perform recovery testing in order to determine whether backups can be successfully restored.

Contact Us

Feel free to contact us should you require further information or require assistance in this regard. For technical information on some of the Indicators of Compromise, please contact us.

Marcelo Vieira *(Associate Director: Information Protection and Business Resilience)*
E: Marcelo.Vieira@kpmg.co.za
C: 082 718 8485

Kaspar Euvrard *(Senior Manager: Information Protection and Business Resilience)*
E: Kaspar.Euvrard@kpmg.co.za
C: 082 576 3588

Judy Allen *(Manager: Information Protection and Business Resilience)*
E: Judy.Allen@kpmg.co.za
C: 082 719 6514

Brent Cairney *(Director: Technology Advisory Cape Town)*
E: Brent.Cairney@kpmg.co.za
C: 083 299 8757

Shamit Govind *(Director: Technology Advisory Durban)*
E: Shamit.Govind@kpmg.co.za
C: 082 719 1389

Paul van de Haar *(Senior Manager: Eastern Cape)*
E: Paul.VandeHaar@kpmg.co.za
C: 081 841 9143

We can, amongst other:

— Help you develop your incident response capability

— Help you to exercise and test those capabilities using credible scenarios

— Help you improve your cyber security defences and understand current security posture and capability

— Help you test those defences using our ethical hacking teams

kpmg.com/socialmedia

kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

16729MC