KPMG

WannaCry/WannaCrypt Ransomware

Important Information

15th May 2017

Key Points on the Malware

Name: WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY

Affected Systems: Windows – Vista SP2, Windows 2008 R2, Windows 7, Windows 8.1, Windows 2012 R2, Windows 10, Windows Server 2016 (other Windows versions affected by ETERNALBLUE *may* be vulnerable)

Vector: It uses ETERNALBLUE (SMBv1) MS17-010 to propagate. *Microsoft released patches for Windows XP, Server 2003, and Windows 8 on Friday, 12 May 2017.*

Ransom Amount: between $300 to $600. There is code to 'rm' (delete) files in the virus. Seems to reset if the virus crashes.

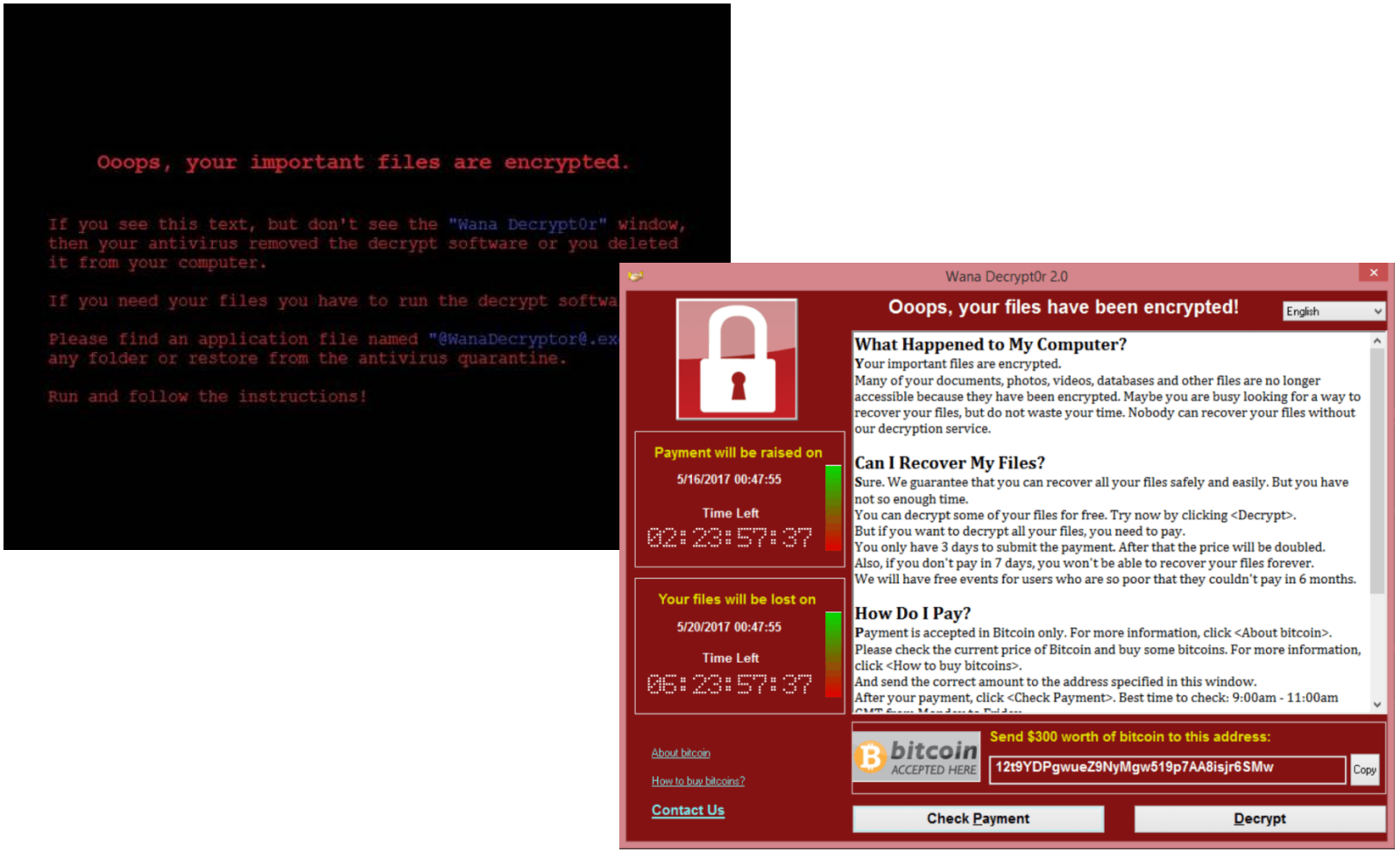
Persistence Techniques: Malware loops through every open RDP session on a system to run the ransomware as that user (using tscon.exe equivalent as SYSTEM). Various reports that variants also install the in-memory DOUBLEPULSAR backdoor.

Example of affected organisations: NHS (UK), Telefonica (Spain), FedEx (US), University of Waterloo (US), Russia interior ministry & Megafon (Russia), Сбера bank (Russia), Shaheen Airlines (India), Neustadt station (Germany), University of Milan (Italy) amongst others….

Spread so far: Over 100,000 attacks in over 150 countries

Kill switch: Initially, the 'kill-switch' domain was sinkholed, stopping the spread of the worm. However, multiple security researchers have claimed that there are more samples of WannaCryout there, with different 'kill-switch' domains and without any kill-switch function, continuing to infect unpatched computers worldwide.

What you see...



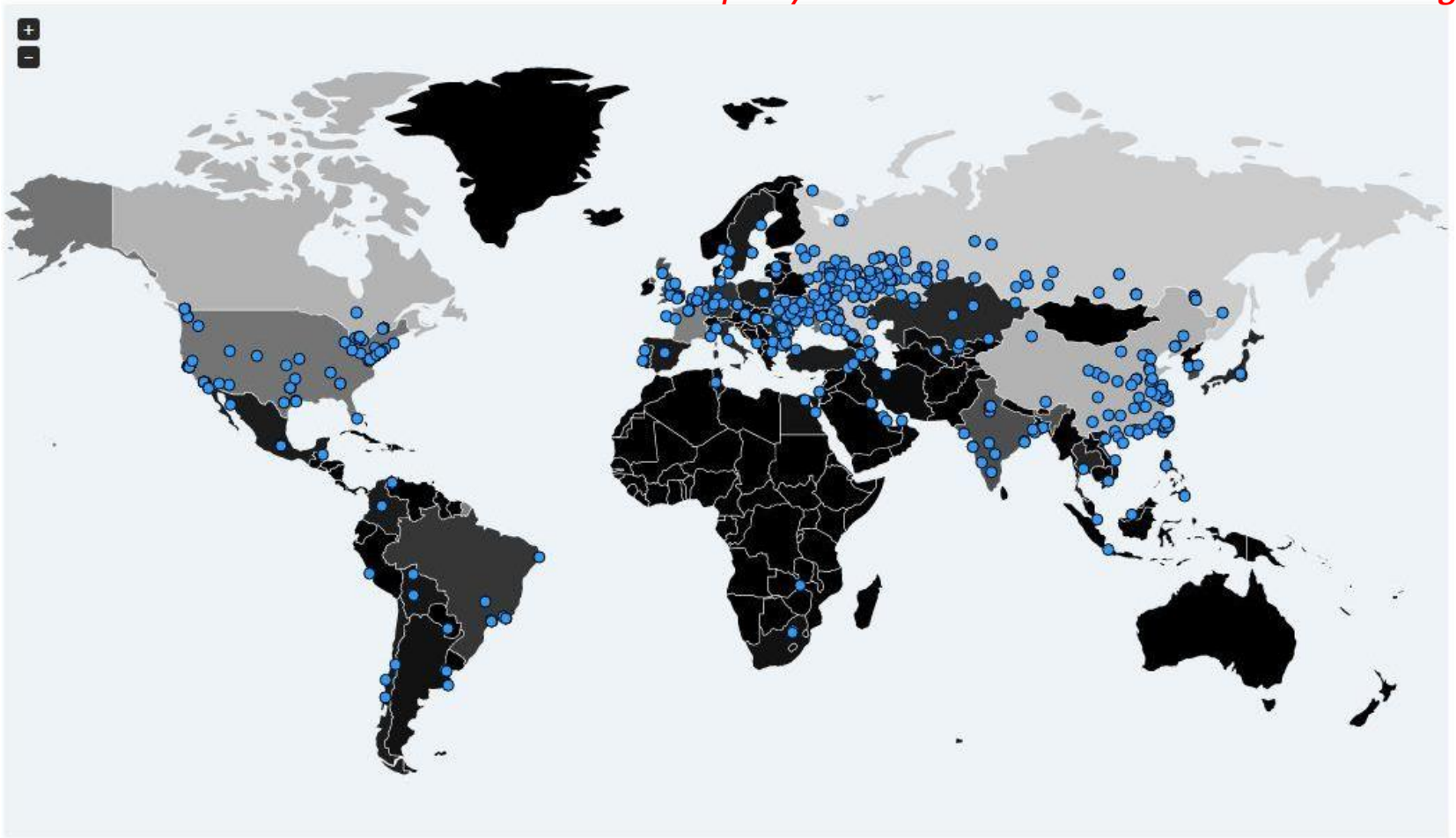
International Coverage

Following languages by default:

Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, Vietnamese

Infection Patterns (Current Status)

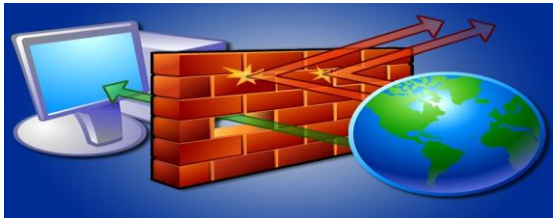
The number of affected countries has rapidly increased to over 150 and still rising.



Is it time to....

Mitigation Steps

- There are also mitigation steps that can be taken – these are by no means exhaustive
  - Block all *.onion sites at edge firewalls
  - Turn off attachments in email (painful but until it “dies down”) - email without attachments is better than no email at all!
  - **Block 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 to every machine as a matter of priority**
  - 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**! https://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
  - Update AV/SIEM/IPS/Everything!
  - Start monitoring for IoC’s if you have a SOC
  - Upgrade all end of life machines as a matter of priority.
  - For systems without patches isolate from the network as much as possible (strict VLAN’s and Firewalls with very very tight ACL’s (for example only allow 139/445 to FileServer and DC)



How KPMG can Help you

- We can help you to develop a robust incident response capability for times such as this;
- We can help you exercise and test incident response capabilities using credible scenarios;
- We can help you improve your cyber security defences; and
- We can help you test cyber security defences using our ethical hacking teams!

KPMG Cyber Security Services Overview

Prepare	Protect	Detect & Respond	Integrate
Helping clients understand and improve their current state of preparedness against cyber-attacks, including services such as;	Helping clients design and implement their cyber defense infrastructure, including services such as;	Helping clients maintain visibility of their cyber weaknesses and respond to cyber-attacks, including services such as;	Helping clients embed cyber security into culture and decision making of the organization including services such as;
• Cyber Readiness Assessment • Cyber Strategy and Transformation • Cyber Governance and Resilience • Data Governance and Privacy • Emerging Technology Risk Management • Threat Modeling • Cyber Defense Architecture Design	• Identity and Access Governance • Cloud Service and Cloud Provider Assessments • Vulnerability Management • Secure Application Development Services • Data Leakage Prevention Services • Critical Infrastructure Services • Secure SDLC	• Cyber Operations and Incident Response • Vulnerability and Penetration Testing • Platform and Network Security Assessments • Threat Detection and Intelligence Services • Cyber Asset Inventory Services • Post Breach Investigation	• Cyber Security Awareness • Cyber Incident Simulation • Red Team / Blue team Exercises • Cyber in the Boardroom Services

Cyber Assurance Services incl. ISO, ISAE, PKI/NIST, etc.

Contact

If you have any further questions or feedback, please contact KPMG Nigeria Cyber (KPMGCyberSecurity@ng.kpmg.com) or;

Joseph Tegbe
Partner and Head, Technology Advisory
+234 803 402 0989

John Anyanwu
Associate Director, Technology Advisory
+234 803 975 4061

Samuel Asiyanbola
Manager, Technology Advisory
+234 806 042 7195

kpmg.com/socialmedia

kpmg.com/app