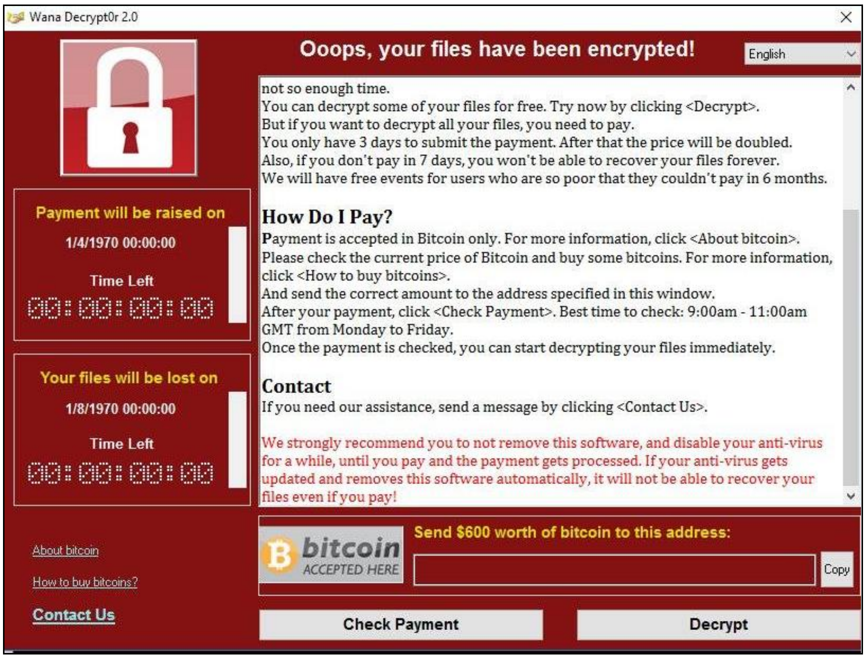
MAY 2017
WWW.BDO.COM.HK

BDO NEWSLETTER

WannaCry/WannaCrypt ransomware

HOW DOES "WANNACRY" WORK?

The "WannaCry" ransomware follows a flow similar to that of other ransomware as it damages a machine. Once a computer has been infected, "WannaCry" will search for files extensions and is capable of encrypting 176 different file types. The ransom note will typically ask user to pay a US$300 in bitcoins, and the payment amount will be doubled after three days if unpaid.



Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Send $600 worth of bitcoin to this address:

WHY IS "WANNACRY" SO VICIOUS?

"WannaCry" was supercharged by incorporating an NSA tool known as Eternal Blue into it's architecture, this allowed the ransomware to spread itself within corporate networks without user interaction through a vulnerability commonly used Windows file-sharing systems. As well as jumping between any linked organisation that may have file-sharing arrangement setup for business purposes.

WHICH SYSTEMS ARE AFFECTED?

Windows 10, Windows 7, Windows XP and Windows Servers.

HOW DID WINDOWS RESPOND?

Microsoft took the unusual steps to release a critical security patch update MS17-010 for its legacy systems such as Windows XP, Server 2003 and Window 8, which further proves the seriousness of the attack. While other more supported version of window operating systems such as Win7, Vista and Win10, would have received update already back in March 2017.

HOW WAS "WANNACRY" DELIVERED?

The malware is delivered as a Trojan through a loaded hyperlink that can be accidentally opened by a victim through an email, an attachment, advert on a webpage or a Dropbox link.

HOW ABOUT DECRYPTING?

Security researchers have indicated that WannaCry uses RSA algorithm for encryption data. A RSA 2048 key has 2^2048 combinations which would take 100,000 billion years for one Computer (capable of one million instructions per second) to go through every single combination. This makes attempting to crack the encryption impractical.

HOW TO PROTECT AGAINST RANSOMWARE ATTACKS?

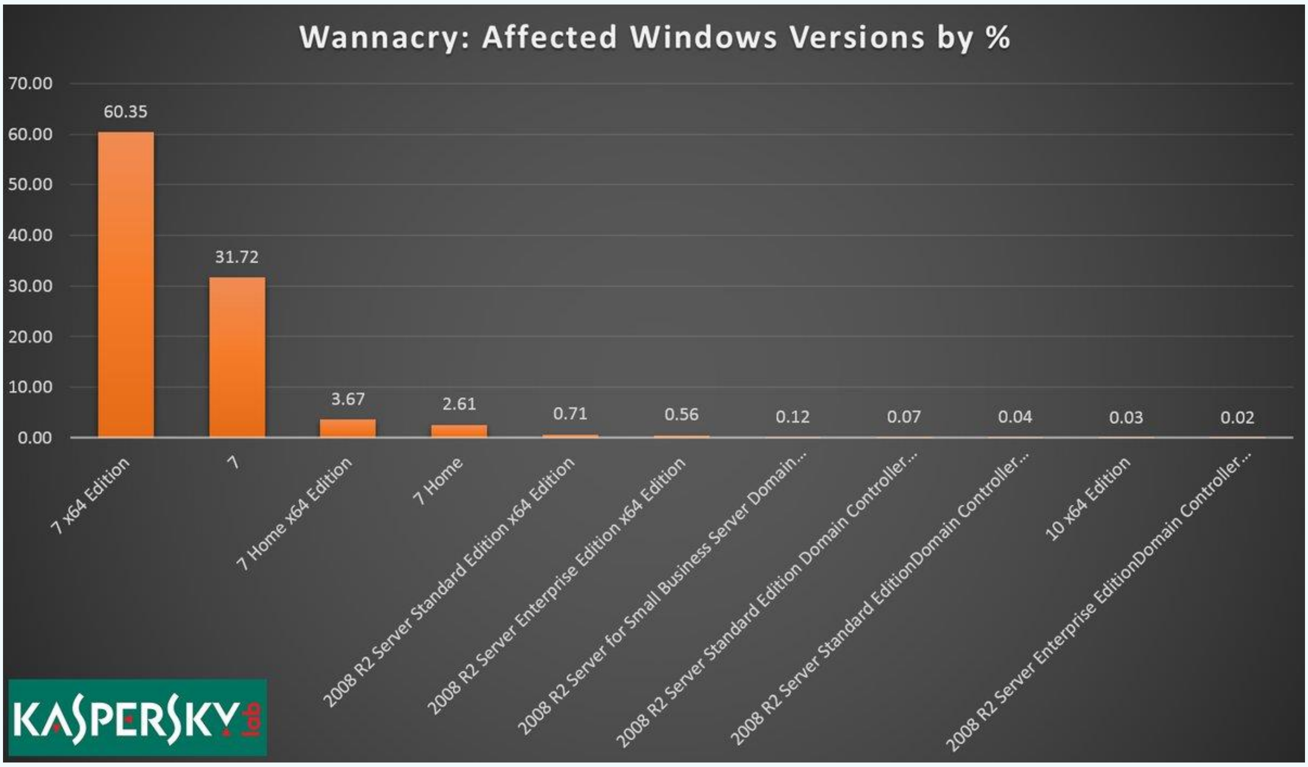
PATCH YOUR SYSTEM

Kaspersky Lab (1) revealed that over 98% of all documented WannaCry infections were running versions of the Windows 7 operating system. The worrying fact is that Microsoft has released a patch for Win7 in March 2017 which if installed could have prevented "WannaCry" attack. New ransomware variants appear on a regularly basis, it is essential to keep your OS, browsers, security and other types of software updated with the latest patches to stay protected.

EDUCATE USERS

One of the most common ransomware delivery channel is through social engineering where users are tricked to download a malicious file or clicking on an executable file. Regular awareness training sessions can help users to detect phishing activities, suspicious websites and other scams.

Reference 1



BACK-UP, BACK-UP AND BACK-UP

Data and system backup is the single most effective way of mitigating the impact of a ransomware infection. This can ensure that critical data can be restored and be accessible for continuous operation despite one set of data has been locked by ransomware. The best practice is to regularly back up important data and store them offsite or a location that will not be hit in case of a network infection. Be sure the backup files are not stored on a mapped drive; some strains of ransomware can even encrypt files over unmapped network shares.

IMPLEMENT LAYERED SECURITY

Installing multiple layers of cybersecurity protection can detect and block ransomware attacks before they happen.

Firewall

Anti-exploit

Antivirus with active monitoring

Anti-malware

Anti-ransomware

DISABLE MACRO

Many ransomware have known to disguise themselves inside attachments such as excel and word documents. If user open the attachment and allow the macro to run, the malware is downloaded and run on the machine. Disabling macro when possible will prevent the malware being executed.

SHOULD YOU PAY A RANSOM?

Different people will have different advice on whether a ransom should be paid. When making your decision, do consider that there is no guarantee that data will be released once the ransom has been paid, and it might also encourage further ransom attacks against your organisation if you choose to co-operate.

HOW CAN BDO HELP?

Our services help organisations build and improve cyber capabilities:

SECURITY ADVISORY

- Cyber / information security audits
- Cyber maturity assessment
- Data privacy compliance assessment

CYBER DEFENSE

- Security program/framework implementation
- Cyber crisis planning

SECURITY TESTING

- Penetration Testing
- Vulnerability and compliance assessment
- Security architecture review
- Social engineering

BDO'S SUPPORT AND ASSISTANCE

25th Floor, Wing On Centre
111 Connaught Road Central
Hong Kong
Tel: +852 2218 8288
Fax: +852 2815 2239
info@bdo.com.hk

RICKY CHENG
Director and Head of Risk Advisory
Tel: +852 2218 8266
rickycheng@bdo.com.hk

RICKY LIU
Senior Manager of Risk Advisory
Tel: +852 2218 3180
rickyliu@bdo.com.hk

BDO Limited, a Hong Kong limited company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO Limited to discuss these matters in the context of your particular circumstances. BDO Limited, its partners, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

www.bdo.com.hk