Grant Thornton
An instinct for growth™

Cyber

Ransomware attack 'WannaCry'

Ransomware infections from 10 May 2017

The virus that has been impacting systems across the world this last week is known as "WannaCry". This virus infiltrates an organisation and encrypts or locks files on servers preventing normal business operation. Very high profile organisations have been affected including: UK National Health Service (NHS), Telefonica among many others.

To guard against this and other similar attacks the following four areas need to be part of an organisations cyber controls:

1. **user awareness:** cyber security awareness activity across all levels of the organisation;
2. **patch management:** ensure that IT systems are regularly patched with security updates and that the culture exists within the organisation to assist IT in this activity;
3. **system backup and recovery:** ensure that a formal backup of systems is in place with testing of recovery included; and
4. **firewall management:** ensure that a firewall and vulnerability management solution is in place to allow for emails, websites and systems to be protected from malicious software such as 'WannaCry'.

For a more in-depth analysis and more detailed technical view see details below. Please email **cyber.security@ie.gt.com** with any queries you have and we will revert in due course.

Detailed technical analysis

The virus that has been impacting systems across the world this last week is known variously as 'WanaCry', 'WanaDecryptor', 'Wanna Crypt' or 'WanaCryptor'. This virus includes two elements, a **propagator** and a **payload**. The propagator of this virus is a worm, which communicates with other computers over **Server Message Block (SMB)**. As SMB is typically enabled within an organisation's internal network, this allows the virus to move from computer to computer and infect an entire network.

The payload of this virus is an encryption program, which locks the contents of a computer and requires a password to access files. The password must be purchased using bitcoin, hence the 'ransomware' title of this kind of virus.
The ransom required for this particular virus is $300[1] in Bitcoin per device. It has been estimated that as of 16 May, only $7,000[2] has been paid to the bitcoin wallets referred to in this virus (approximately 23 payments). Grant Thornton does not recommend paying ransoms to restore access. Although we do understand that some businesses may have little other recourse, there is no guarantee that the recovery password provided on payment will work and paying the ransom encourages copycat attacks.

The effectiveness and rapid spread of this ransomware has surprised many in the cyber security community. Within 72 hours, over 200 countries had reported infections, which included large organisations, such as the UK NHS, Telefonica, KPMG and others[3], though the largest proportion of infections seem to have been in Russia[4]. The virus has been temporarily slowed, through the unusual inclusion of a 'kill-switch' within the virus source code. A security researcher activated the kill switch[5], though it is only a matter of time before a new variant of this virus is released without this particular 'flaw'.

1 http://www.independent.ie/irish-news/one-of-the-biggest-attacks-in-history-six-things-you-need-to-know-about-the-worldwide-ransomware-hit-and-what-it-means-for-ireland-35710624.html
2 https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/#more-39367
3 https://arstechnica.co.uk/security/2017/05/what-is-wanna-decryptor-wcry-ransomware-nsa-eternalblue/
4 Matthieu Suiche: https://twitter.com/msuiche/status/864022459854487552
5 https://arstechnica.co.uk/information-technology/2017/05/wanna-decryptor-kill-switch-analysis/

The source of the virus is still under investigation, however it makes use of a bug or vulnerability within the Microsoft Windows operating system. The vulnerability originally affected all versions of Windows, up to version 8 (version 10 is not affected) and details were included amongst the NSA documents which recently were published by the 'ShadowBroker' team. The ethics of the US government having knowledge of a flaw which would allow attackers to compromise many computers globally is beyond the scope of this article, Microsoft issued a statement decrying the practice[6]. There has been some discussion of lawsuits and damage claims, yet the terms of the software license agreement with Microsoft and the sovereign immunity principle as it applies to the NSA will most likely render these impotent.

There have been reports that only 20 Irish IP addresses[7] had been identified in the infected traffic, indicating that Irish organisations have largely been spared the impact however, some organisations such as the HSE, have disconnected from the internet in order to prevent impacts on service. As this virus continues to exist and copycats start to spring up, we may not continue to be so lucky.

In order to reduce your chances of being infected, there are a number of concrete steps you can take.

Patching and where you can't patch, protect

This virus relies upon a vulnerability in Microsoft Windows. Microsoft released a patch that blocks this vulnerability in March 2017[8]. Those organisations that have not yet patched their systems should do so as a matter of urgency.

Not all systems can be patched or kept up to date due to compatibility issues with other programs, licensing concerns, or they are embedded versions. Where this is the case, additional protections should be considered. It may be possible to isolate the affected system to its own network segment or even completely remove it from the network and physically isolate it. Disabling unnecessary services, such as SMB version 1 may reduce the attack surface.

Backups and recovery

The most comprehensive security measure for ransomware attacks such as this is a recent, reliable backup. In the event of a ransomware attack you can scrub your existing systems and restore from backup. This is obviously the 'nuclear option' and can cost a great deal in time and resources however, it is the most conclusive defence against ransomware attack.

Firewalls and other controls

Preventing this virus from entering your organisation in the first place is of course the preferred option. This particular virus communicates over the SMB protocol. Blocking this protocol on your firewalls will prevent this particular virus from entering your network via the internet. Other potential entry points include emails to your staff, contractors via untrusted or backup internet connections. Additional controls, such as email screening or scanning or disabling the SMB protocol where it is not necessary reduce the chances of infection.

Incident response

One of the key defences in your arsenal for attacks such as this is your incident response capability. The ability to quickly identify an infection and to contain and eradicate the infection are key to your organisation's defences. Incident response should now consider the steps of identification, containment, eradication, recovery and prevention[9] and consider the reporting requirements that may exist under regulations.

Cyber security awareness

Ultimately, as this issue has clearly demonstrated, cyber security is a clear business risk. Awareness at all levels of the business, in particular the board level, of the cyber security risks and implementation of an appropriate cyber security programme are essential to safeguard your organisation[10].

Contact

Please email **cyber.security@ie.gt.com** or a member of our team with any queries you have and we will revert in due course.

Mike Harris
Partner, Cyber Security
T +353 (0)1 436 6503
E mike.harris@ie.gt.com

Gary McPartland
Associate Director, Cyber Security
T +353 (0)1 500 8158
E gary.mcpartland@ie.gt.com

Over 1,000 people operating from offices in Dublin, Belfast, Cork, Galway, Kildare, Limerick and Longford.

www.grantthornton.ie

#GTcyber

Grant Thornton Ireland

6 https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0002ryord1599e79s6r1×d-7joquye
7 http://www.irishtimes.com/business/technology/just-20-irish-ip-addresses-hit-by-global-cyber-attack-1.3083514
8 https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

9 https://www.grantthornton.ie/insights/publications/cyber-security-incident-response/
10 https://www.grantthornton.ie/insights/imagazine/why-you-need-to-be-cyber-secure/