Grant Thornton
An instinct for growth™

Cyber

Ransomware attack

Petya/NotPetya/Petrwrap/exPetr/Goldeneye

Recently a new strain of malware began disrupting computer systems across the world. It is currently unclear if this ransomware is a variation of the 'Petya' ransomware from 2016 or an entirely new strain due to the complex nature of the attack[1]. This malware appears to involve several attack vectors including the 'EternalBlue' exploit used in the 'WannaCry' ransomware attack last month and password capturing techniques in order to infiltrate an organisation and encrypt or lock files on servers to prevent normal business operations.

To date companies across Europe and the US have reported to have been affected with this ransomware. Some of the high profile organisations affected, include the global shipping firm A.P Moller-Maersk, international advertising conglomerate WPP, Russian oil company Rosneft and the Chernobyl nuclear power plant[2].

To guard against this and other similar attacks the following five areas need to be addressed as 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 the IT department with this activity;
3. **system backup and recovery:** ensure that a formal offline backup of IT systems is in place with testing of recovery included;
4. **security management:** ensure that a firewall and vulnerability management solution are in place to ensure emails, websites and systems are protected from malicious software such as this ransomware; and
5. **restrict administrative programs** such as the PSExec utility and Windows Management Instrumentation Command-line (WMIC) that are being utilised by this strain of ransomware to propagate.

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 malware that has been impacting systems across the world since Tuesday 27 June is known variously as 'Petya', 'NotPetya', 'Petrwrap', 'exPetr' or 'Goldeneye'. This malware includes two elements, a propagator and a payload. To date, several attack vectors used to propagate the malware throughout a local network has been detected. It is currently unclear if this is an entirely new malware strain or one built upon old code as it shares some similarities with both the 'Petya' and 'WannaCry' ransomware variants while also using new attack methods unseen before in order to propagate[3].

The propagator of this malware is a worm and there are several ways in which this worm attempts to propagate across the network. The first utilises the 'EternalBlue' exploit seen in the recent 'WannaCry' ransomware attack. This method attempts to exploit a vulnerability within the Server Message Block (SMB) protocol recently patched by Microsoft (MS17-010) in order to spread the malware through other computers. As SMB is typically enabled within an organisation's internal network, this allows the malware to move from computer to computer and infect an entire network.

1 https://blog.kaspersky.com/new-ransomware-epidemics/17314/
2 https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware

3 https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/

Unlike 'WannaCry' this malware also uses password capturing techniques in order to infect patched computers on the network. This malware appears to use custom tools to extract administrator passwords from a systems running memory[4]. With these details, the malware then uses remote administrative tools such as PSExec and WMIC to establish legitimate connections across the internal network via TCP ports 139 and 445. With this administrative access the worm can copy itself across the network, infecting file shares, servers and workstations.

The payload of this malware is an encryption program, which locks the contents of a computer and requires a password to access files. Similar to the 'Petya' ransomware malware, this malware writes to the Master Boot Record (MBR) of an infected computer enabling it to encrypt both the filesystem tables and the files on the drive[5]. The malware then sets the computer to reboot within an hour in order to complete the encryption process. The password must be purchased using bitcoin hence the 'ransomware' title of this kind of malware. The ransom required for this particular malware is $300 in Bitcoin per device. While a small number of payments were seen to have been made to the Bitcoin account early on Tuesday 29 June[6], by midday (CEST) the email address associated with paying the ransom was disconnected by Posteo[7]. This blocks the attackers from gaining access to the emails associated with the Bitcoin account and makes decryption impossible.

With all forms of ransomware, Grant Thornton does not typically recommend paying ransoms to restore access. Although we understand that some businesses may have little other recourse, there is a substantial risk that the recovery password provided on payment will not work and paying the ransom encourages copycat attacks.

Due to the malware being limited to the local network, it is seen to be less infectious than the 'WannaCry' malware. However, the infection has been identified by Microsoft in over 64 countries with Ukraine and Russia being the worst affected. At time of writing, large organisations, such as Ukraine's state telecom, the US pharmaceutical company Merck and the Russian steel and oil companies, Evraz and Rosneft[8].
A reported "vaccine" has been identified by researchers that prevents the malware from infecting files on a computer. As analysis showed that the malware exits its encryption routine if it finds the existence of a certain file on a user's computer, researches have suggested that creating such a file and setting it to read-only would prevent the malware from executing[9]. Additional reports suggest that if a user can prevent the computer from rebooting to complete the encryption process, it may be possible to rescue the files from the infected machine[10].

The source of the malware is still under investigation, with several reports suggesting the malware originated from an infected software supply-chain involving the Ukraine company M.E.Doc, which develops tax accounting software and may have pushed an infected update to their customers[11]. However, the spread of this malware and the use of the 'EternalBlue' exploit suggests that many companies may not have implemented sufficient security measures such as applying the relevant Microsoft patch or blocking unnecessary protocols. At time of writing, the Irish operations of three international companies have been affected by the malware[12].

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 malware exploits a vulnerability in Microsoft Windows. Microsoft released a patch that blocks this vulnerability in March 2017[13]. 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. It is critical that a recent version of the backup is kept in an 'offline' state in order to protect that backup itself from coming into contact with the malware. 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

While it is unclear how this malware is gaining entry to internal networks, the main attack vector for ransomware is through malicious email attachments. As such, firewall controls and email screening or scanning should be implemented. Unlike 'WannaCry' this malware does not appear to gain entry to an organisation's internal network via SMB but instead uses this protocol once it has accessed the local network in order to propagate. It also utilises several administrative tools, PSExec and WMIC, to communicate and with systems that have been patched for the SMB vulnerability.

4 https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
5 https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/
6 http://thehackernews.com/2017/06/petya-ransomware-attack.html
7 https://posteo.de/en/blog
8 https://www.recode.net/2017/6/27/15880024/ransomware-attack-infecting-computers-shipping-oil-companies-worldwide-petya-ukraine-hack
9 https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/
10 https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

11 https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
12 https://www.irishtimes.com/news/ireland/irish-news/global-cyber-attack-hits-operations-of-three-firms-in-ireland-1.3135941
13 https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Therefore, in order to try and prevent the spread of the malware, it is recommended that the SMB protocol and the listed administrative tools be restricted in as much as possible. Other potential entry points include emails to your staff or contractors, via untrusted or backup internet connections.

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, 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[14] 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[15].

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

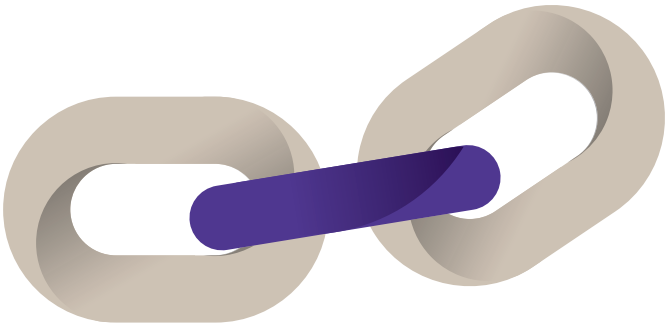
Tommy Maycock
Director, Cyber Security
T +353 1(0) 500 8176
E tommy.maycock@ie.gt.com

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

www.grantthornton.ie

#GTcyber

Grant Thornton Ireland



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

Grant Thornton
An instinct for growth™

grantthornton.ie