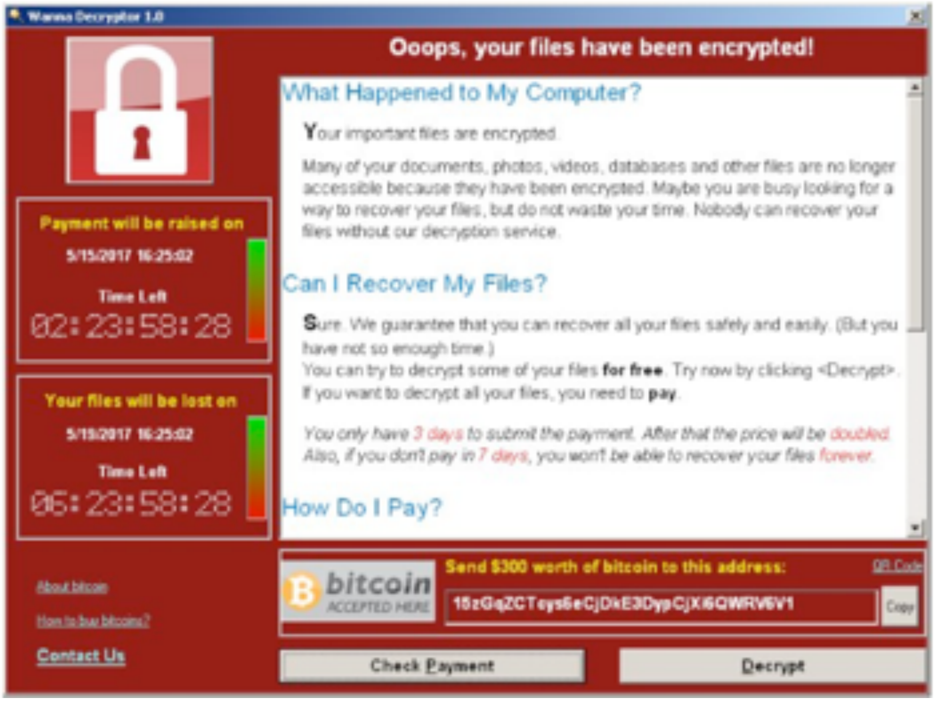
WBM Client Community Briefing : WannaCry Ransomware

WannaCry ransomware spreads aggressively across networks, encrypts files and demands a ransom payment.

Many of you will have seen the news regarding a global outbreak of a virulent new strain of ransomware known as WannaCry (Ransom.Wannacry). This virus has hit hundreds of thousands of computers worldwide since its emergence on Friday, May 12, 2017.

WannaCry is far more dangerous than other common ransomware types because of its ability to spread itself across an organization's network by exploiting a critical vulnerability in Windows computers, a patch for which was issued by Microsoft in March 2017 (Critical Security Bulletin MS17-010).

This dangerous malware exploit, known as "Eternal Blue" was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group. Security experts say unknown hackers took advantage of tools stolen from the US National Security Agency to create the virus, as portions of the spy agency's sophisticated cyber arsenal have been leaked online in recent months.



Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
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.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

What Does WannaCry Ransomware Do?

WannaCry searches for and encrypts 176 different file types and appends .WCRY to the end of the file name. It ask users to pay a US$300 ransom in bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted.

How does the malware enter the computer?

The cyber weapon involved in the attack is malware known as Wanna Decryptor or WannCry. It infiltrates computers by way of web links and attachments in spam emails.

Who is impacted?

This attack does not have a specific target (everyone is a target). Any unpatched Windows computer is potentially susceptible to WannaCry. Organizations are particularly at risk because of its ability to spread across networks and a number of organizations globally have been affected, the majority of which are in Europe. The highest-profile organization to fall victim to this cybercrime was Britain's National Health Service, which uses the 15-year-old Windows XP operating system on its computers. Windows XP is so old that Microsoft was no longer offering free software updates for it. Microsoft announced on Sunday that it was reversing that policy.

Am I protected?

Our commitment to the WBM client community is to ensure that you are the most protected business community possible, and that includes this most recent strain of Ransomware.

In 2015, WBM launched a systematic initiative toward protecting our business community, including the Connection 2015 Security Summit to bring awareness to this emerging threat, the acquisition of Agilysis, a Calgary based leader in security solution management to ensure competency and capacity relating to the issue, and the 2016 launch of the WBM Ransomware protection system, including end user briefings, and an affordable, subscription based 3 Stage Security Solution for small and medium business. In addition, we have leveraged cloud based technologies such as Office365 to drive cost savings and remote workforce, eliminate vulnerable stand alone systems, and deliver increasingly powerful security, anti-spam, and redundancy measures.

WBM Automated Patch Management

As a WBM Managed Services Solutions client, you receive automated patching of your devices. As Microsoft releases patches, the WBM technical team tests the patches for possible compatibility issues, and once approved, the patches are automatically pushed out to all visible devices.

The patch MS17-010 (which fixes the vulnerability that WannaCry is now exploiting) was approved by the WBM Technical team and pushed out to WBM client devices on March 28th, 2017 (7 weeks ago today). Because systems that are offline will not receive the patch, it is not uncommon for some systems to be missed. In these cases, the WBM team will continue to attempt to patch the device (generally 5 times in a row) during off hours, prior to 'forcing' the patch during daytime hours to ensure all devices have been updated.

As this patch was pushed out many weeks ago now, it would be difficult for active devices to miss all 5 attempts and the forced update, but it is certainly possible for a computer to have missed all attempts (could be powered off or out of service for example). We are currently working to identify any computers that may have been missed, and will be actively pushing the patch where required.

WBM 3 Stage Security System

In addition to having an automated patching process, all members of the WBM client community who have opted into the 3 stage security protection program are assured of having current technology in place to detect a possible infection, the ability to decrypt and inspect incoming data, and, in a worst case scenario, have the added protection of being able to restore to a previously un-infected state.

Your firewalls are attached to a Global Management Subscription, continuously updating your systems to protect against emerging threats. The Sonicwall Next Generation Firewalls were updated to inspect and block attempts to exploit the vulnerability used by WannaCry on April 24th, 2017, well in advance of the outbreak that impacted hundreds of thousands of businesses.

WBM Client Community Firewall Intrusion Data
Top 5 Gateway Viruses Blocked Since May 12th 2017 WannaCry Outbreak

1. UPX packed executable file (ExePacker)	Overall Counts	3329
2. PECompact2 packed executable file (ExePacker)	Overall Counts	220
3. Password-protected ZIP file	Overall Counts	130
4. Downloader.PDF_2 (Trojan)	Overall Counts	118
5. File containing VBA macros	Overall Counts	92
6. All known Wannacry Signatures	Overall Counts	0

http://blog.sonicwall.com/wp-content/uploads/2017/05/WannaCrypt-Signatures.png

While we can never provide a 100% assurance of immunity to any possible scenario, we want to provide comfort that we are actively monitoring the situation and to date we have not seen a breach across the WBM client community in western Canada.

This does not mean that we shouldn't all do our part to protect ourselves and be as aware as possible in watching for any suspicious content. As a helpful reminder, we are including the previously published 2016 end user guide to ransomware, which we encourage everyone to post or distribute accordingly.

If you have any further questions, or would like to confirm that your organization has the complete WBM Security System in place, please do not hesitate to contact us, we are here to help. Questions can be directed through your WBM Relationship Manager, or directly to our Security Solutions Team:

Bill Sullivan Security Practice Business Development
WBM Technologies 3602 Blackfoot Trail SE, Calgary, AB. T2G 4E6
1.888.275.4926 toll free bsullivan@wbm.ca