“An Email From Microsoft” - HowToCrazy

Dear Customer,

Many organizations around the world were victims of malicious “WannaCrypt” software last week. Seeing businesses and individuals affected by cyberattacks such as this is painful. Our teams have worked relentlessly over the last few days to take all possible actions to protect our customers.

Here are a few things for your reference:

- If you are using Windows Vista, 7, 8.1 & 10: In March, we released a security update which addresses the vulnerability that these attacks are exploiting. Those who have Windows Security Update enabled are protected against attacks on this vulnerability.
  For those organizations who have not yet applied the security update, we suggest you immediately deploy Microsoft Security Bulletin MS17-010.
- Activate Windows Defender: For customers using Windows Defender, we released an update earlier today which detects this threat as Ransom:Win32/WannaCrypt. As an additional “defense-in-depth” measure, keep up-to-date anti-malware software installed on your machines. Customers running anti-malware software from any number of security companies can confirm with their provider whether they are protected.
- If using older version of Windows: Customers running versions of Windows that no longer receive mainstream support may not have received the above mentioned Security Update released in March. Given the potential impact to customers and their businesses, we have released a Security Update for platforms in custom support only. Windows XP, Windows 8 and Windows Server 2003 Security Updates are broadly available for download now (see links below).
- Additional Steps to consider: This attack type may evolve over time, so any additional defense-in-depth strategies will provide additional protections. (For example, to further protect againstSMBv1 attacks, customers should consider blocking legacy protocols on their networks). Some of the observed attacks use common phishing tactics including malicious attachments. Customers should use vigilance when opening documents from untrusted or unknown sources.

More information on the malware is available from the Microsoft Malware Protection Center though the Windows Security blog. We are working with our customers to provide additional assistance as the situation evolves, and will update

this blog with details as appropriate.*https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/*
You may also want to read though the blog posted by Brad Smith, President and Chief Legal Officer, Microsoft, looking at the broader implications of the malicious “WannaCrypt” software attack.

If you have any questions or concerns:

- Webinar: You may want to join the Webinar on Wannacry Attack Q&A, 22nd May, 11am. Join here.
- Email: Please write to us atindiasms@microsoft.com. Our team will respond to you on priority.

Thanks and regards,

Microsoft India Team

Further resources:

Download English language security updates: Windows Server 2003 SP2 x64,Windows Server 2003 SP2 x86,Windows XP SP2 x64,Windows XP SP3 x86,Windows XP Embedded SP3 x86,Windows 8 x86,Windows 8 x64
Download localized versions for the security update for Windows XP, Windows 8 or Windows
Server: http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
Read general information on ransomware: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx
Download MS17-010 Security Update: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

FAQs:

Where can I find the official guidance from Microsoft?
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Is the update available for Windows 2003 & Windows XP as well?

Yes. The link for download of the update is available at the end of this article *https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/*

Will the update run on unlicensed Windows?
It is recommended that the update is run on a licensed version.

What about Windows 2003 R2?
The Windows 2003 update should get applied on Windows 2003 R2 as well.

Will the installation of the patch, prevent the occurrence of ransomware?
No. Applying MS17-010 is just preventing the malware from spreading, not giving protection against the infection itself. Based on reports, this malware is using Social Engineering to target companies.Please warn your users to not open, click or enable macros on email reception.

- *The priority is that your anti-virus can detect the malware.*
- *Verify that you have up-to-date signatures, along with patching the Windows systems*
- *Make sure that users have the level of knowledge required to never click on suspicious attachments even if they are displayed with a familiar icon (office or PDF document). Where an attachment opening offers the execution of an application, users must under no circumstances should accept the execution and in doubt, users should you consult and/or consult the administrator.*
- *Implementation of strong filtering in O365:* *http://blogs.msdn.com/b/tzink/archive/2014/04/08/blocking-executable-content-in-Office-365-for-more-aggressive-anti-malware-protection.aspx*
- *Exchange Online Protection*
  http://TechNet.Microsoft.com/en-us/library/jj723164(v=Exchg.150).aspx
  http://TechNet.Microsoft.com/en-us/library/jj200684(v=Exchg.150).aspx
  http://TechNet.Microsoft.com/en-us/library/jj723119%28V=Exchg.150%29.aspx

Security tips to Protect against Ransomware
https://social.technet.microsoft.com/wiki/contents/articles/29787.microsoft-protection-center-security-tips-to-protect-against-ransomware.aspx

Is the ransomware effective only if the user has administrative rights on the client machine?
No. This piece of ransomware, like most of others, once executed, encrypts all files it

can reach in the context of a user, if the user is an admin on the box the outcome is more devastating. In addition this ransomware also tries to disable shadow copies and make some registry changes in HKLM hive which require administrative privileges.
When it tries to spread it uses a vulnerability, which once exploited gives the malware SYSTEM level access on the target system. All this means that this attack maybe very successful and destructive even if the users don't have admin privileges on their unpatched workstations/servers.

Is only disabling SMB v1 Server (LanmanServer) on all our machines helps us to protect from this vulnerability?
Patch installation would be the first option. To answer the question, Yes. SMBV1 should be removed, but in a planned way. Please refer the below link
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Do we need to disable SMB v1 client (Lanmanworkstation) as well on all our machines?
No. It is only the SMBv1 server component (which means Lanmanserver), on the client machine and not Lanmanworkstation on the client machine.

What is the impact of removing SMBv1?

- *You're still running XP or WS2003 under a custom support agreement*
- *Windows XP will not be able to access shares on a Windows 2003 Server or any other Operating System*
- *Windows Vista and above Operating System will not be able to access shares on a Windows 2003 Member Server or Domain Controller (if you still have them in the environment)*
- *You have some decrepit management software that demands admins browse via the 'network neighborhood' master browser list*
- *You run old multi-function printers with antique firmware in order to "scan to share"*

Please refer the below article for more details
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

If we have to disable smb v1 Server service, what are the registry values to disable it?
When using operating systems older than Windows 8.1 and Windows Server 2012 R2, you can't remove SMB1 – but you can disable it: KB 2696547- How to enable and disable SMBv1, SMBv2, and SMBv3 in Windows Vista, Windows Server 2008,

“An Email From Microsoft” - HowToCrazy

Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012
Please refer to the below link for more details
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

How do we know SMB v1 is active in our environment. Can we proactively check it?
Yes. Please test this, before using in the production environment.
https://blogs.technet.microsoft.com/ralphkyttle/2017/04/07/discover-smb1-in-your-environment-with-dscea/

Windows 2016 and Windows 10 provides a way to audit usage of SMBv1, which can be found here
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Is Windows 10 affected as of now?

https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
The exploit code used by WannaCrypt was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems, so Windows 10 PCs are not affected by this attack as of now.

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
Customers running Windows 10 were not targeted by the attack today.

That being said, Windows 10 systems also need to be patched, because the variants can be developed. In addition to this, it would be recommended to remove SMBv1 from the clients and Windows servers, after doing a complete review of the below mentioned article.

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

“An Email From Microsoft” - HowToCrazy

Microsoft respects your privacy. Please refer to our online Privacy Statement.

If you would prefer not to receive future promotional emails from **Microsoft Corporation** please click on this link. These settings will not affect any newsletters you've requested or any mandatory service communications that are considered part of certain Microsoft services.

To set your contact preferences for Microsoft Communications, click on this link.

Microsoft Corporation (India) Pvt. Ltd.
Level 10, Tower C, Epitome, Building No. 5, DLF Cyber City, Phase 3,
Gurgaon, Haryana 122 002 INDIA