Microsoft

WannaCry Seminar for K12 ICT Teachers

Fred Sheu

NTO, Microsoft Hong Kong

What Happened?

- On Friday May 12th 2017, several organizations were affected by a new Ransomware strain.
- The Ransomware used a unpatched Windows SMB v1 vulnerability to spread inside networks.
- The vulnerability was patched by Microsoft in March (MS17-010) for supported versions of Windows.
- Additional patches were released for unsupported versions of Windows (Windows XP, Windows 8 and Windows Server 2003) available on May 13
- The exploit, known under the name ETERNALBLUE, was released in April as part of a leak of NSA tools by Shadow Brokers

How do systems get infected?

- Social Engineering and Phishing email: Some organizations suggest that the initial infection originated from e-mail attachments
- SMB: Affected organizations may have had unpatched Windows vulnerable systems exposed via port 139 and 445.

What happens to the victim?

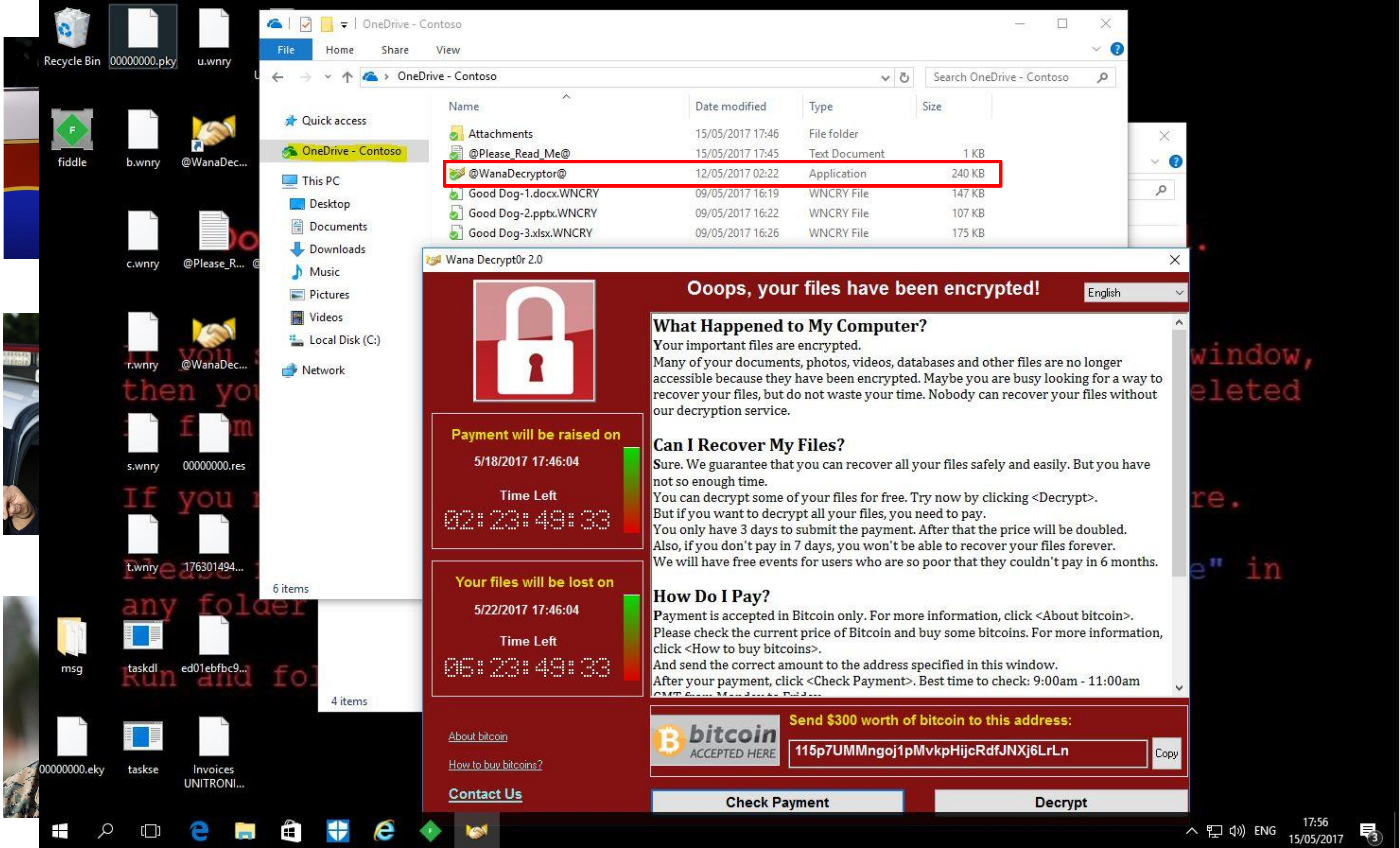
- Files with 176 specific extensions will be encrypted
- Append .WNCRY to the filename of encrypted files
- The victim will see a ransom message asking for approx. $300 Ransomware demands will increase to $600 after 3 days. After 7 days, the files may not longer be recoverable.
- The ransomware will also install a backdoor to access the system remotely via port 445 (Double Pulsar, also part of the NSA tool set) or 139 for older systems.

How to Prevent Infection?

- Supported Windows versions (Windows Vista, 7-10, Windows Server 2008-2016) can be patched with MS17-010 released by Microsoft in March.
- Microsoft released (on May 12) a patch for older systems going back to Windows XP, Windows 8 and Windows 2003.
- Confirm that patch is installed (suggest auto-update)
- Install run the latest Microsoft anti-virus software
  - Windows Defender for Windows 8.1 and Windows 10, or Windows Security Essentials for Windows 7 and Windows Vista (definition 1.243.290.0 or above)

Sights of Affected Systems

- Encrypted files will have the "wncry" extension.
- Systems will scan internally for port 445.
- Ransom message will be displayed.
- Note that Microsoft anti-malware has signatures now for WannaCry.



Name	Date modified	Type	Size
Attachments	15/05/2017 17:46	File folder	
@Please_Read_Me@	15/05/2017 17:45	Text Document	1 KB
@WanaDecryptor@	12/05/2017 02:22	Application	240 KB
Good Dog-1.docx.WNCRY	09/05/2017 16:19	WNCRY File	147 KB
Good Dog-2.pptx.WNCRY	09/05/2017 16:22	WNCRY File	107 KB
Good Dog-3.xlsx.WNCRY	09/05/2017 16:26	WNCRY File	175 KB

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/18/2017 17:46:04

Time Left

02:23:49:33

Your files will be lost on

5/22/2017 17:46:04

Time Left

06:23:49:33

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 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

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

About bitcoin

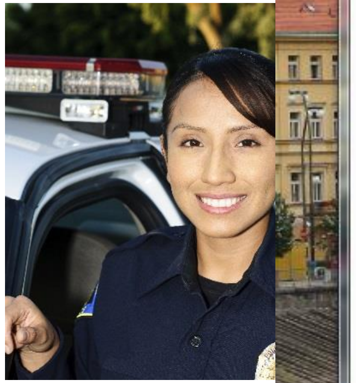
How to buy bitcoins?

Contact Us

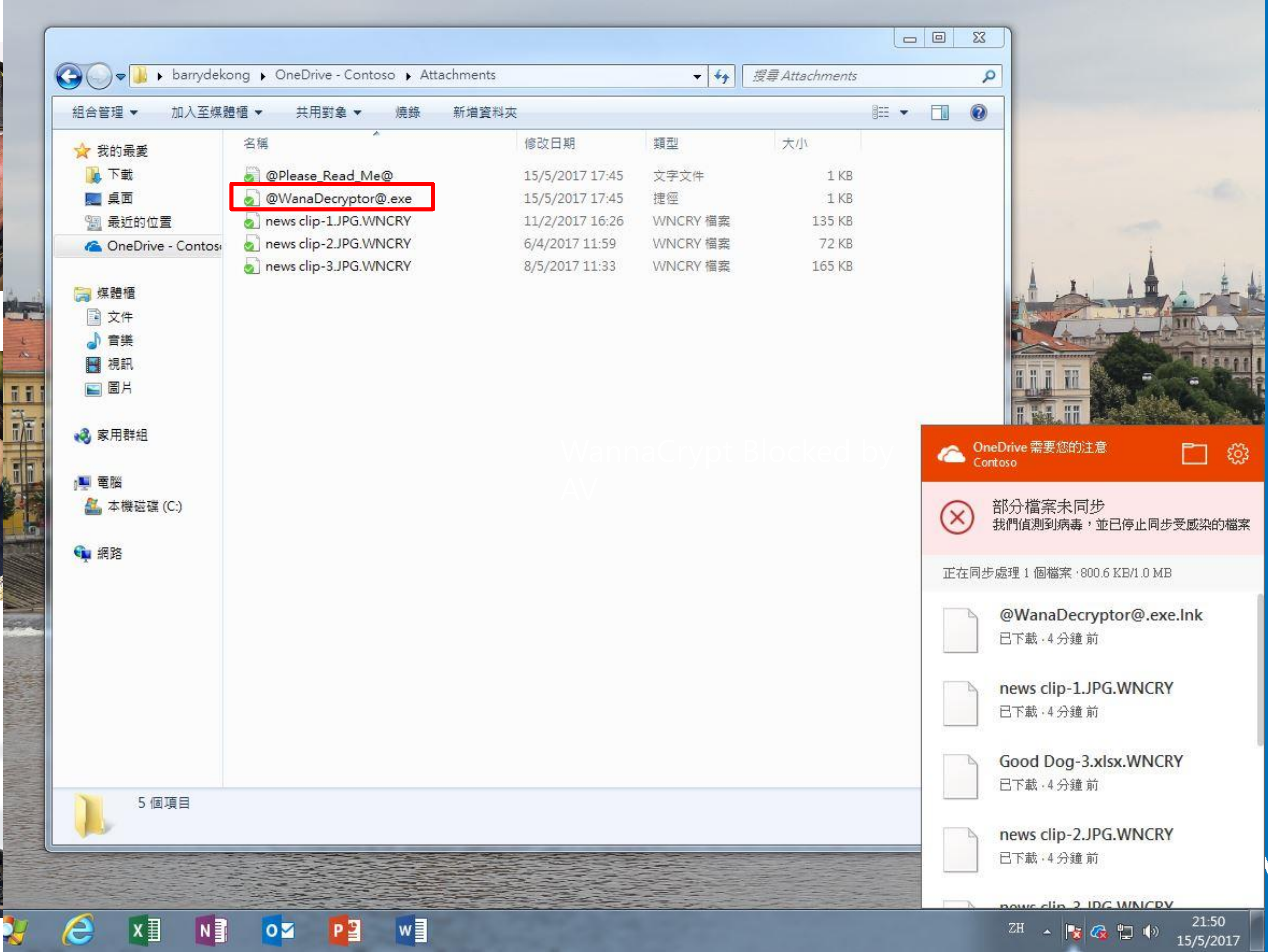
Check Payment

Decrypt

ft



WannaCrypt Blocked by AV



名稱	修改日期	類型	大小
@Please_Read_Me@	15/5/2017 17:45	文字文件	1 KB
@WanaDecryptor@.exe	15/5/2017 17:45	捷徑	1 KB
news clip-1.JPG.WNCRY	11/2/2017 16:26	WNCRY 檔案	135 KB
news clip-2.JPG.WNCRY	6/4/2017 11:59	WNCRY 檔案	72 KB
news clip-3.JPG.WNCRY	8/5/2017 11:33	WNCRY 檔案	165 KB

5 個項目

OneDrive 需要您的注意
Contoso

部分檔案未同步
我們偵測到病毒，並已停止同步受感染的檔案

正在同步處理 1 個檔案 · 800.6 KB/1.0 MB

@WanaDecryptor@.exe.lnk
已下載 · 4 分鐘 前

news clip-1.JPG.WNCRY
已下載 · 4 分鐘 前

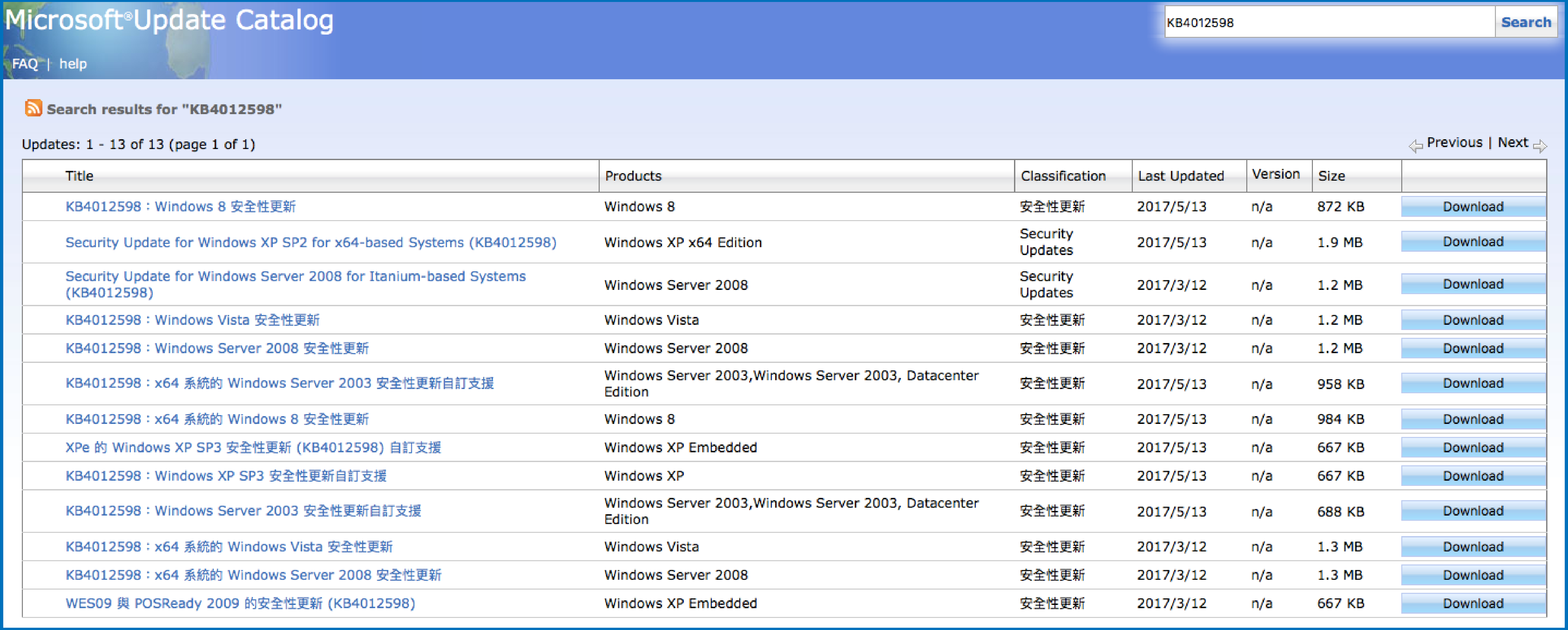
Good Dog-3.xlsx.WNCRY
已下載 · 4 分鐘 前

news clip-2.JPG.WNCRY
已下載 · 4 分鐘 前

What if you are suspected to be infected

- Disconnect from network
- Disable port 139, 445 and SMBv1
- Backup the unlocked files
- Update patches MS17-010 or security patch for older systems
- Run anti-virus software
- Contact HKCERT 8105-6060 or Microsoft Hotline 2388-9600 for support

Old versions of Microsoft Patches



Search results for "KB4012598"

Updates: 1 - 13 of 13 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	
KB4012598：Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	872 KB	Download
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	2017/5/13	n/a	1.9 MB	Download
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：x64 系統的 Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	958 KB	Download
KB4012598：x64 系統的 Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	984 KB	Download
XPe 的 Windows XP SP3 安全性更新 (KB4012598) 自訂支援	Windows XP Embedded	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows XP SP3 安全性更新自訂支援	Windows XP	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	688 KB	Download
KB4012598：x64 系統的 Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.3 MB	Download
KB4012598：x64 系統的 Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.3 MB	Download
WES09 與 POSReady 2009 的安全性更新 (KB4012598)	Windows XP Embedded	安全性更新	2017/3/12	n/a	667 KB	Download

Other measures

1. Educate users
2. Check backup availability
3. Update machines and software
4. Avoid the use of accounts with the Domain Administration right
5. Manage macros in Office (and OLE packages)
6. Enable "File Screening Management" if you use File Server
7. Enable AppLocker (or SRP Software Restriction Policy on XP)
8. Implement Strong Filtering in Office 365
9. Exchange Online Advanced Threat Protection
10. Put in place URL Filtering
11. Windows Device Guard and Credential Guard to protection
12. Microsoft SCCM and SCOM for patch and security management

Additional Links

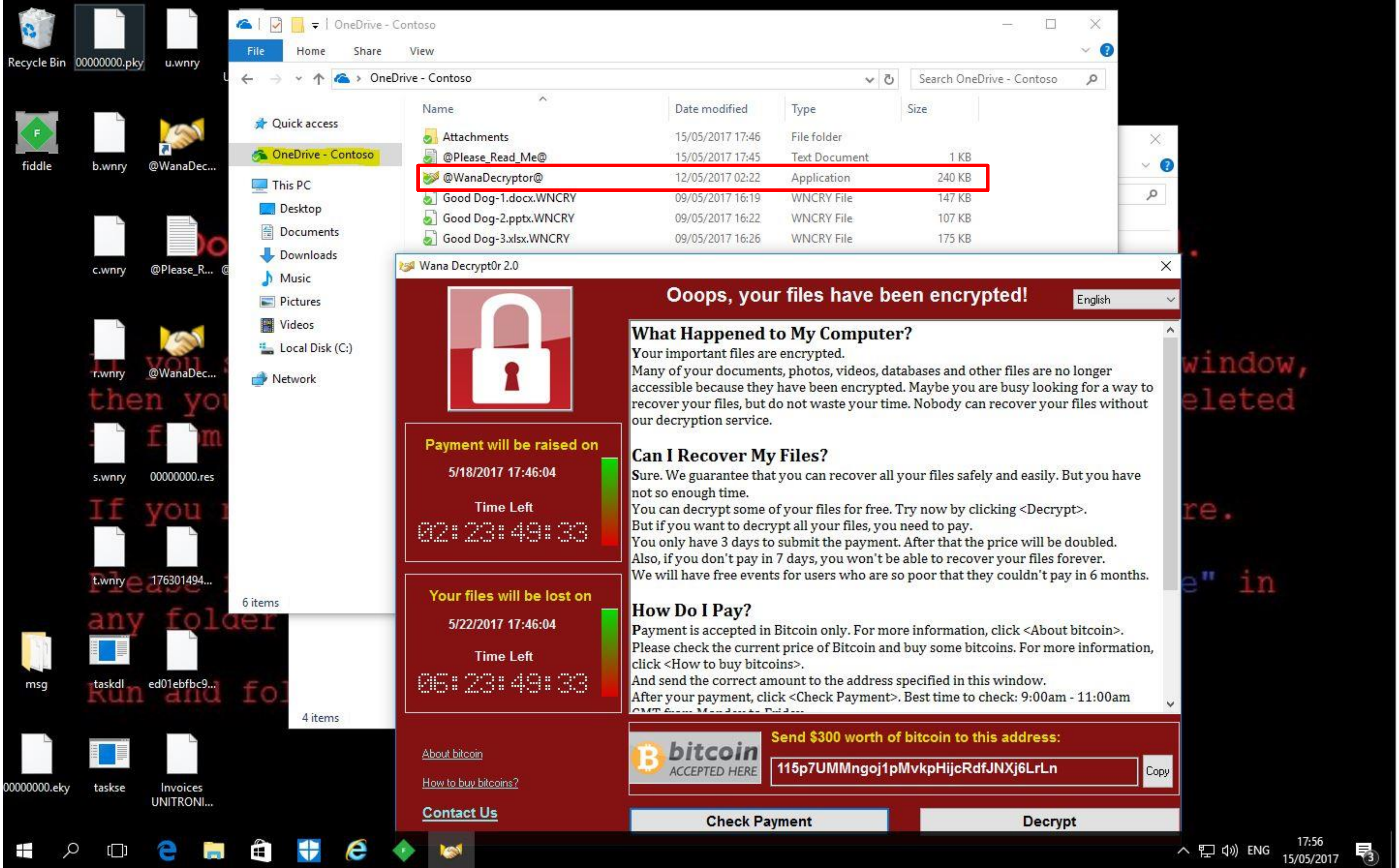
- Microsoft Customer Guidance for WannaCrypt Attack https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Microsoft Security Bulletin MS17-010

  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Security update for unsupported Windows

  http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
- Microsoft Malware Protection (WannaCrypt)

  https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

Microsoft



Name	Date modified	Type	Size
Attachments	15/05/2017 17:46	File folder	
@Please_Read_Me@	15/05/2017 17:45	Text Document	1 KB
@WanaDecryptor@	12/05/2017 02:22	Application	240 KB
Good Dog-1.docx.WNCRY	09/05/2017 16:19	WNCRY File	147 KB
Good Dog-2.pptx.WNCRY	09/05/2017 16:22	WNCRY File	107 KB
Good Dog-3.xlsx.WNCRY	09/05/2017 16:26	WNCRY File	175 KB

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/18/2017 17:46:04

Time Left

02:23:49:33

Your files will be lost on

5/22/2017 17:46:04

Time Left

06:23:49:33

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 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

About bitcoin

How to buy bitcoins?

Contact Us

bitcoin ACCEPTED HERE

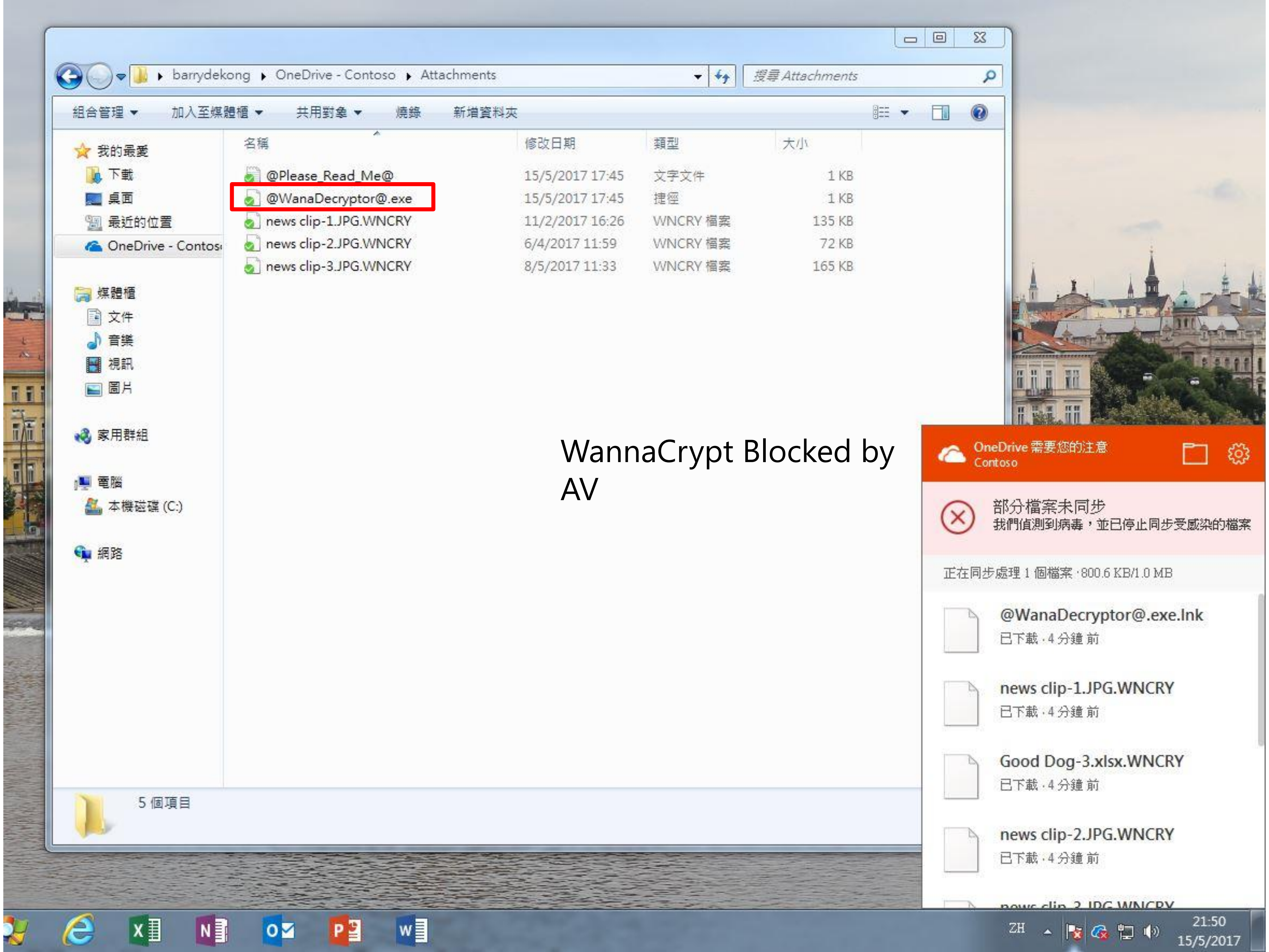
Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

Check Payment

Decrypt



名稱	修改日期	類型	大小
@Please_Read_Me@	15/5/2017 17:45	文字文件	1 KB
@WanaDecryptor@.exe	15/5/2017 17:45	捷徑	1 KB
news clip-1.JPG.WNCRY	11/2/2017 16:26	WNCRY 檔案	135 KB
news clip-2.JPG.WNCRY	6/4/2017 11:59	WNCRY 檔案	72 KB
news clip-3.JPG.WNCRY	8/5/2017 11:33	WNCRY 檔案	165 KB

5 個項目

WannaCrypt Blocked by AV

OneDrive 需要您的注意
Contoso

部分檔案未同步
我們偵測到病毒，並已停止同步受感染的檔案

正在同步處理 1 個檔案 · 800.6 KB/1.0 MB

@WanaDecryptor@.exe.lnk
已下載 · 4 分鐘 前

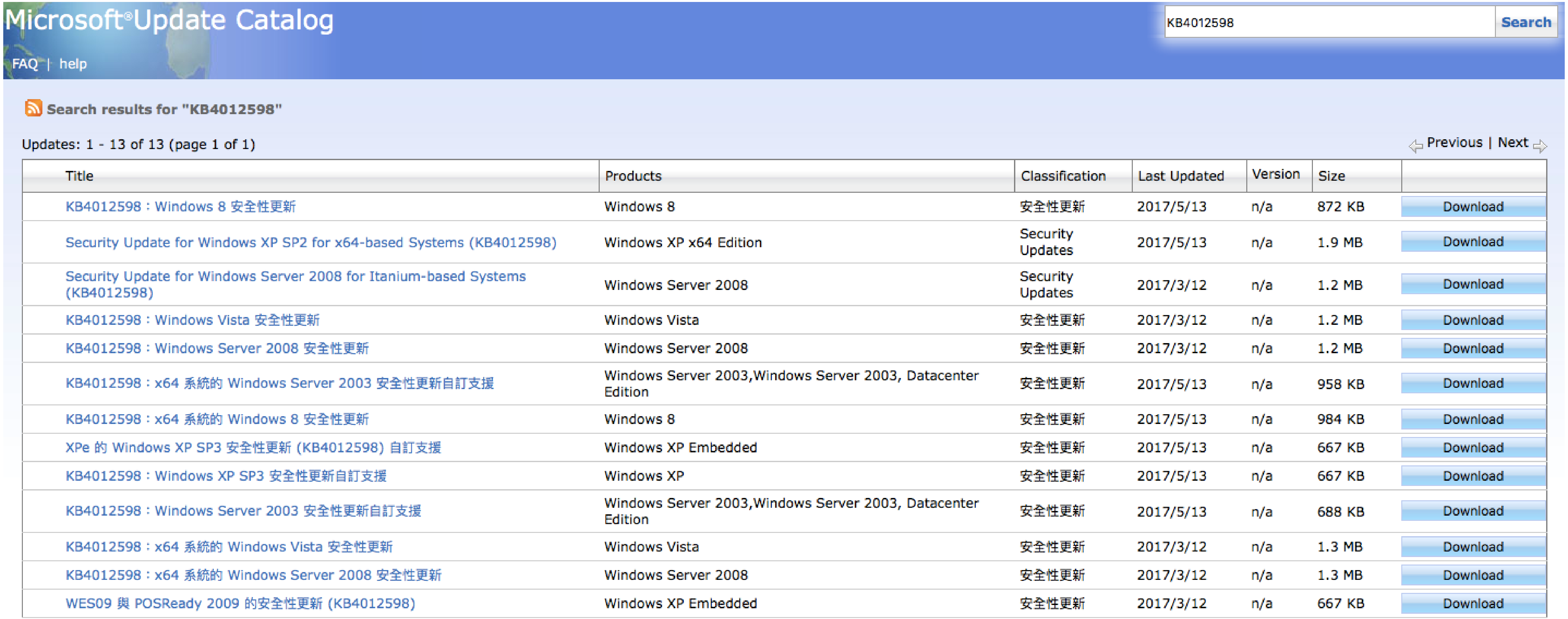
news clip-1.JPG.WNCRY
已下載 · 4 分鐘 前

Good Dog-3.xlsx.WNCRY
已下載 · 4 分鐘 前

news clip-2.JPG.WNCRY
已下載 · 4 分鐘 前

news clip-3.JPG.WNCRY

舊系統Microsoft Patches



KB4012598

Search results for "KB4012598"

Updates: 1 - 13 of 13 (page 1 of 1)

Previous | Next

Title	Products	Classification	Last Updated	Version	Size	
KB4012598：Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	872 KB	Download
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	2017/5/13	n/a	1.9 MB	Download
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：x64 系統的 Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	958 KB	Download
KB4012598：x64 系統的 Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	984 KB	Download
XPe 的 Windows XP SP3 安全性更新 (KB4012598) 自訂支援	Windows XP Embedded	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows XP SP3 安全性更新自訂支援	Windows XP	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	688 KB	Download
KB4012598：x64 系統的 Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.3 MB	Download
KB4012598：x64 系統的 Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.3 MB	Download
WES09 與 POSReady 2009 的安全性更新 (KB4012598)	Windows XP Embedded	安全性更新	2017/3/12	n/a	667 KB	Download