勒索病毒 Ransom:Win32/WannaCrypt 防范及修复指南 – 版本 1

微软安全技术支持组

2017 年 5 月 14 日

Microsoft

目录

版本号	发布日期
1	2017 年 5 月 14 日

Microsoft

1. 什么是勒索软件

勒索软件是过去几年中较为流行的一种恶意软件，主要现象为加密所有当前用户有权限的文件。以下几个因素使这类恶意软件较为特别：

1. 恶意软件作者频繁的进行更新，生成各种新的变种以躲避杀毒软件的扫描。
2. 这些恶意软件对用户文件采用非对称加密，在没有私钥的情况下，无法对文件进行解密。而加密所用的私钥不会保存在被感染计算机上。
3. 这些恶意软件会尝试加密任何当前执行用户有权限的本地或网络共享中的某些文档类型，破坏能力较大。

2. 为什么 Ransom:Win32/WannaCrypt 影响更大

如同其他大多数勒索软件一样，Ransom:Win32/WannaCrypt 通过社会工程学尝试感染目标组织的环境，通常为带有恶意宏的 Office 文档附件的钓鱼邮件。一旦感染环境中的一台计算机后，该变种会尝试在内网中主动传播。这一蠕虫行为是真正让这一变种带来如此巨大影响的原因。

3. 感染以后的症状

当系统被该勒索软件感染后，弹出勒索对话框：

文档被加密，后缀名被更改为 WNCRY。可被加密的文档类型 参考

4. 如何应对

首先，一旦计算机被感染文档被加密，由于无法获取加密所用私钥，从技术角度无法解密这些文档。***唯一的恢复手段是通过已有的备份进行恢复***。确保对关键文档数据进行有效备份是保护数据的最主要方式。

4.1 没有被感染，预防防御办法（非常重要）

(1) 首要任务确定您的反病毒软件更新到最新并可以查杀该勒索软件。Microsoft 反病毒产品病毒库版本 1.243.290.0 及以上可以查杀当前发现的这一变种。如您使用其他反病毒软件，建议与相应厂商确认。
(2) 确保终端用户理解他们不应打开任何可疑的附件，即使他们看到一个熟悉的图标（PDF 或 Office 文档）。用户不应在任何情况下执行附件中包含的可执行文件。如果有任何疑问，请用户联系 IT 管理部门。
(3) 确保 MS17-010 在所有计算机上安装，推荐安装最新的 Microsoft 安全补丁，并将其他第三方软件更新到最新。

- **变通办法**

  如暂时难以完成补丁安装，以下变通办法在您遇到的情形中可能会有所帮助:

  - **禁用 SMBv1**

  对于运行 Windows Vista 及更高版本的客户

  请参阅 Microsoft 知识库文章 2696547

  适用于运行 Windows 8.1 或 Windows Server 2012 R2 及更高版本的客户的替代方法

  对于客户端操作系统：

  1. 打开“控制面板”，单击“程序”，然后单击“打开或关闭 Windows 功能”。
  2. 在“Windows 功能”窗口中，清除“SMB 1.0/CIFS 文件共享支持”复选框，然后单击“确定”以关闭此窗口。
  3. 重启系统。

  对于服务器操作系统：

  1. 打开“服务器管理器”，单击“管理”菜单，然后选择“删除角色和功能”。
  2. 在“功能”窗口中，清除“SMB 1.0/CIFS 文件共享支持”复选框，然后单击“确定”以关闭此窗口。
  3. 重启系统。

变通办法的影响。目标系统上将禁用 SMBv1 协议。

如何撤消变通办法。回溯变通办法步骤，而不是将"SMB 1.0/CIFS 文件共享支持"功能还原为活动状态。

这一方法也可以通过组策略部署注册表的方式进行。组策略配置可参考文档 https://technet.microsoft.com/zh-cn/library/cc753092(v=ws.11).aspx

注册表信息可以在以下文档中找到，您需要重启计算机以使注册表生效。 https://support.microsoft.com/en-sg/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

(4) 如果您使用 Office365，参照以下文档进行邮件过滤 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

(5) 强烈建议不赋予终端用户本地管理员权限。尽量减少域管理员账户的使用，更多关于身份保护的建议参考 http://www.microsoft.com/pth

(6) 启用审核策略以监控可疑行为: http://technet.microsoft.com/en-us/library/dd560628(v=ws.10).aspx or http://technet.microsoft.com/en-us/library/dd772623

(7) 使用文件屏蔽管理保护您的共享文件夹 https://technet.microsoft.com/zh-cn/library/cc732074.aspx

(8) 在您的邮件传输中添加过滤规则，阻止包含可执行文件的压缩包附件。

(9) 如果您使用 Microsoft 反病毒软件，确保您开启行为检测以及 MAPS（基本或高级）

(10) 管理 Office 中的宏功能

大量的感染来自于邮件附件中包含恶意宏的 Office 文档，控制宏的运行有助于防止用户执行造成感染.

首先您需要禁用 Office 宏自动运行: https://support.office.com/en-us/article/Enable-or-disable-macros-in-Office-documents-7b4fdd2e-174f-47e2-9611-9efe4f860b12?ui=en-US&rs=en-US&ad=US

但该策略不阻止用户在文档打开时点击启用来运行宏。您需要使用 Trusted Location 来只允许用户执行该路径下 Office 文档中的宏 https://support.office.com/en-us/article/Add-remove-or-change-a-trusted-location-7ee1cdc2-483e-4cbb-bcb3-4e7c67147fb4?CorrelationId=cd218d92-02cf-427b-806c-59f6a7c22809&ui=en-US&rs=en-US&ad=US

（11）以下是我们已知的这个恶意软件相关的 IP，建议考虑从防火墙上阻止

a. 154.35.175.225
b. 171.25.193.78
c. 178.162.194.210
d. 192.99.212.139

e. 195.154.165.112
f. 154.35.175.225
g. 171.25.193.78
h. 178.162.194.210
i. 192.99.212.139
j. 195.154.165.112
k. 91.219.236.222
l. 188.166.23.127
m. 193.23.244.244
n. 2.3.69.209
o. 146.0.32.144
p. 50.7.161.218
q. 192.42.113.102
r. 83.169.6.12
s. 158.69.92.127
t. 86.59.21.38
u. 62.138.7.171
v. 51.255.203.235
w. 51.15.36.164
x. 217.79.179.177
y. 128.31.0.39
z. 213.61.66.116
aa. 212.47.232.237
bb. 81.30.158.223
cc. 79.172.193.32
dd. 163.172.149.155
ee. 167.114.35.28
ff. 176.9.39.218
gg. 192.42.113.102
hh. 193.11.114.43
ii. 199.254.238.52
jj. 89.40.71.149

更多相关 IP 可以从 https://otx.alienvault.com/pulse/591608484da25870a4eaf2f6/ 获得。

4.2 如果已经被感染了怎么办

(1) 隔离已感染计算机，在工作域里脱域，拔掉网线，关闭受感染计算机。
(2) 考虑通过 Windows 防火墙阻止 445 端口入站通讯，或禁用 Server 服务
    a. **注意：**此操作将阻止所有的文件共享服务，可能给环境带来较大影响，如未发现已感染计算机不建议进行此项操作

(3) 如果您的反病毒软件暂时无法查杀该变种，您可以使用 Microsoft Safety Scanner https://www.microsoft.com/security/scanner/en-us/default.aspx 对受感染计算机进行完全扫描

(4) 从备份中恢复文件

(5) 同样实施以上防御措施

4.3 如何确认安全更新已经安装成功

1．装完成后必须重启系统。

2．对于 Windows XP/Server 2003, 请手工检查。

3．对于 Windows Vista SP2/Server 2008 SP2 开始的操作系统，可以使用 PowerShell 命令行来验证。

```
Get-hotfix -id kbXXXXXX
```

例如返回以下值，说明安装成功。

```
Source          Description      HotFixID      InstalledBy          InstalledOn
------          -----------      --------      -----------          -----------
CN-JN-2016      Security Update  KB4013429     NT AUTHORITY\SYSTEM  4/15/2017 12:00:00 AM
```

可以修复漏洞的安全更新（文件最小的）是哪些

操作系统	知识库文章号码	安全更新下载链接	安装先决条件	备注
Windows XP	KB4012598	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598	Service Pack 2 或者 Service Pack 3 *Service Pack 2 没有中文版本更新	
Windows 8	KB4012598	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598	无	
Windows Server 2003 SP2	KB4012598	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598	Service Pack 2	
Windows Vista SP2/Server 2008 SP2	KB4012598	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012598	Service Pack 2	
Windows 7 SP1/Windows Server 2008 R2 SP1	KB4012212	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012212	Service Pack 1	2017 年 3 月的仅安全更新

Windows Server 2012	KB4012214	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012214	无	2017 年 3 月的仅安全更新
Windows 8.1/Windows Server 2012 R2	KB4012213	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012213	KB2919355 *需要先安装 KB3021910，然后才能安装 KB2919355	2017 年 3 月的仅安全更新
Windows 10 RTM	KB4012206	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4012606	无	累积安全更新
Windows 10 1511	KB4013198	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013198	无	累积安全更新
Windows 10 1607 | Server 2016	KB4013429	http://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4013429	无	累积安全更新

注意：

1． 对于 Windows 7/8.1/Server 2008 R2/Server 2012/Server 2012 R2，我们从 2016 年 10 月开始每月发布当月的仅安全更新和安全更新汇总。修复漏洞可以从以下任意一种选择：

- 2017 年 3 月的仅安全质量更新 （大小最小，如上表）
- 2017 年 3 月，4 月，5 月的安全更新汇总可以参考下表。

	2017 年 3 月的安全质量汇总	2017 年 4 月的安全质量汇总	2017 年 5 月的安全质量汇总
Windows 7 SP1/Server 2008 R2 SP1	KB4012215	KB4015549	KB4019264
Windows Server 2012	KB4012217	KB4015551	KB4019216
Windows 8.1/Server 2012 R2	KB4012216	KB4015550	KB4019215

2． 安装 **“2017 年 4 月或者 2017 年 5 月的仅安全质量更新”不能**修复漏洞。**（请注意）**

3． **必须**满足**“安装先决条件”**才能安装更新。

- 对于 Windows Server 2012 R2，需要先安装 KB3021910，然后才能安装 KB2919355

- 对于 Windows 7 SP1/ Windows Server 2008 R2, 如果没有安装过任何更新，请先安装 KB3125574 （兼容性已知问题，请参考知识库文章 https://support.microsoft.com/en-us/help/3125574/convenience-rollup-update-for-windows-7-sp1-and-windows-server-2008-r2-sp1）。否则可能需要花费 5 到 6 小时索引系统，才能开始安装安全更新。

当 Catalog 网站访问慢时，怎么下载更新

操作系统	发布日期	CDN 下载链接
Security Update for Windows Server 2003 for x64-based Systems (KB4012598)	5/13/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-chs_68a2895db36e911af59c2ee133baee8de11316b9.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-cht_23a0e14eee3320955b6153ed7fab2dd069d39874.exe
Security Update for Windows 8 for x64-based Systems (KB4012598)	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu
Security Update for Windows 8 (KB4012598)	5/13/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
Security Update for Windows XP SP3 for XPe (KB4012598)	5/13/2017	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-enu_8f2c266f83a7e1b100ddb9acd4a6a3ab5ecd4059.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-chs_41935edbcd6fa88a69718bc85ab5fd336445e7f9.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-embedded-custom-cht_c3696d39aab12713c4bd4e30b8e17f0a03fd8089.exe
Security Update for Windows XP SP3 (KB4012598)	5/13/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe http://wsus.ds.download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-cht_a84b778a7caa21af282f93ea0cdada0f7abb7d6a.exe http://wsus.ds.download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-chs_dca9b5adddad778cfd4b7349ff54b51677f36775.exe

Security Update for Windows Server 2003 (KB4012598)	5/13/2017	http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-enu_f617caf6e7ee6f43abe4b386cb1d26b3318693cf.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-chs_b45d2d8c83583053d37b20edf5f041ecede54b80.exe http://wsus.ds.download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-cht_71a7359d308c8bda7638b4dc4ea305e7e22cc4c2.exe
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	5/13/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-enu_f24d8723f246145524b9030e4752c96430981211.exe
Security Update for Windows Vista (KB4012598) - Windows Vista	3/14/2017	http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-enu_eceb7d5023bbb23c0dc633e46b9c2f14fa6ee9dd.exe
Security Update for Windows Server 2008 (KB4012598) - Windows Server 2008	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
Security Update for Windows Vista for x64-based Systems (KB4012598) - Windows Vista	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598) - Windows Server 2008	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-ia64_83a6f5a70588b27623b11c42f1c8124a25d489de.msu

Security Update for Windows Server 2008 for x64-based Systems (KB4012598) - Windows Server 2008	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
Security Update for WES09 and POSReady 2009 (KB4012598) - Windows XP Embedded	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windowsxp-kb4012598-x86-embedded-enu_9515c11bc77e39695b83cb6f0e41119387580e30.exe http://wsus.ds.download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windowsxp-kb4012598-x86-embedded-chs_8789d2232a3d43c44d4d293dc37b4bc06c997e9b.exe http://wsus.ds.download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windowsxp-kb4012598-x86-embedded-cht_a827a40579d7de4c78efeca91d25ec0762e1c5be.exe
March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
March, 2017 Security Only Quality Update for Windows 7 (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
March, 2017 Security Only Quality Update for Windows Embedded Standard 7 (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu
March, 2017 Security Only Quality Update for Windows Embedded	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

Standard 7 for x64-based Systems (KB4012212)		
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4012212)	3/14/2017	http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-ia64_93a42b16dbea87fa04e2b527676a499f9fbba554.msu
March, 2017 Security Only Quality Update for Windows 8.1 (KB4012213) - Windows 8.1	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x86_e118939b397bc983971c88d9c9ecc8cbec471b05.msu
March, 2017 Security Only Quality Update for Windows 8.1 for x64-based Systems (KB4012213) -Windows 8.1	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu
March, 2017 Security Only Quality Update for Windows Server 2012	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8.1-kb4012213-x64_5b24b9ca5a123a844ed793e0f2be974148520349.msu

R2 (KB4012213) -Windows Server 2012 R2		
March, 2017 Security Only Quality Update for Windows Embedded 8 Standard (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x86_5e7e78f67d65838d198aa881a87a31345952d78e.msu
March, 2017 Security Only Quality Update for Windows Embedded 8 Standard for x64-based Systems (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu
March, 2017 Security Only Quality Update for Windows Server 2012 (KB4012214)	3/14/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/02/windows8-rt-kb4012214-x64_b14951d29cb4fd880948f5204d54721e64c9942b.msu
Most current Windows 10 cumulative updates - May 2017		
Windows 10		
2017-05 Cumulative Update for Windows 10 for x64-based Systems (KB4019474)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019474-x64_4ed033d1c2af2daea1298d10da1fad15a482f726.msu
2017-05 Cumulative Update for Windows 10 for x86-based	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019474-x86_259adeed4a4037f749afab211ff1bc6a771ff7f6.msu

Systems (KB4019474)		
Windows 10 Version 1511		
2017-05 Cumulative Update for Windows 10 Version 1511 (KB4019473)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019473-x86_5e2b7bce2f1b116288b4f1f78449c66ecc7c7a53.msu
2017-05 Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB4019473)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019473-x64_c23b6f55caf1b9d6c14161b66fe9c9dfb4ad475c.msu
Windows 10 Version 1607 & Windows Server 2016		
2017-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4019472)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x64_dda304140351259fcf15ca7b1f5b51cb60445a0a.msu
2017-05 Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB4019472)	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x64_dda304140351259fcf15ca7b1f5b51cb60445a0a.msu
2017-05 Cumulative Update for Windows 10 Version 1607 for x86-based	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4019472-x86_9bf106e898b57c20917cd98fd8b8d250333015a5.msu

Systems (KB4019472)		
Windows 10 Version 1703		
2017-05 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4016871) -Windows 10	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4016871-x64_27dfce9dbd92670711822de2f5f5ce0151551b7d.msu
2017-05 Cumulative Update for Windows 10 Version 1703 for x86-based Systems (KB4016871) -Windows 10	5/9/2017	http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows10.0-kb4016871-x86_5901409e58d1c6c9440e420d99c42b08f227356e.msu

5. Q&A 问答

1) 问：如果有任何相关问题， 需要紧急联系微软，找谁？
答：请随时联系贵司对应的微软客户经理。

2) 问：对于 MS17-010，里面包含 2 个安全更新号码 4012215 和 4012212，是都需要打还是只要打一个 4012212 就可以呢？
答：KB4012215 是 2017 年 3 月的安全质量更新汇总，涵盖了 KB4012212，因此两者任选一个安装，都能修复漏洞。

3) 问：安装时提示此更新不适用于您的计算机，怎么办？
答： 请确认系统满足了先决条件再安装。例如 Windows Server 2008 R2, 必须在 Service Pack 1 安装完成后，才能安装这次涉及到的安全更新。

4) 问：如何判断是否已经安装了正确的补丁？
答：首先重启系统。然后对于 Vista SP2/Server 2008 SP2 开始的系统，可以使用 PowerShell 命令 Get-hotfix 来确认。

5) 问：即使安装了 MS17-010 还有可能中招，如果中招了是否可以杀毒，还是必须重装？此时系统还会传播勒索软件吗？
答：请参考指南“**如果已经被感染了怎么办**”这一部分。安装更新并不阻止系统发送恶意请求。此时环境中没有安装安全更新的系统将处于高危阶段。

6) 问：是否会跨网段传播？
答：会。

7) 问：如果 Windows Server 2008 SP2 安装重启后，安全更新被回退了，怎么办？
答：请联系 Premier 热线服务电话，开启案例分析解决。
大陆 Premier Primary 8008201859
香港 Premier Primary 800966770
Premier backup 800938384
General backup 28044299
澳门 Premier Primary 0800948
台湾 Premier Government 0800-003033
+886-2-3725-3333
Premier All 0800-003525
+886-2-3725-3525

8) 问：SMB V1 如果停止了会有什么影响？
答：SMB v1 是从 Windows Vista SP2/Windows Server 2008 SP2 开始引入的。如果停止掉，Vista/Server 2008 之前的系统（XP/Server 2003）就无法访问共享。Computer Browser 服务也会受到影响。如果系统上有较多应用依存于 SMB v1 的话，这些应用可能无法使用。

9) 问：如果要重新安装系统，只格式化 C 盘就可以了还是需要全盘格式化？
答：如果没有专业的分析，不可决定是否需要所有磁盘格式化 。