关于近日大量学校电脑感染勒索病毒的说明

中国高等教育学会教育信息化分会网络信息安全工作组

2017年5月13日

5月12日，安全工作组接到多所高校报告，反馈大量学校电脑感染勒索病毒，重要文件被加密，类似下图所示。



经过初步调查，此类勒索病毒利用了基于445端口传播扩散的SMB漏洞，部分学校感染台数较多，大量重要信息被加密，只有支付高额的比特币赎金才能解密恢复文件，损失严重。远程利用代码和4月14日黑客组织Shadow Brokers（影子经纪人）公布的Equation Group（方程式组织）使用黑客工具包有关。其中的ETERNALBLUE模块是SMB 漏洞利用程序，可以攻击开放了 445 端口的 Windows 机器，实现远程命令执行。微软在今年3月份发布的MS17-010补丁，修复了ETERNALBLUE所利用的SMB漏洞。目前基于ETERNALBLUE的多种攻击代码已经在互联网上广泛流传，除了捆绑勒索病毒，还发现有植入远程控制木马等其他多种远程利用方式。

根据360公司的统计，目前国内平均每天有不低于5000台机器遭到基于ETERNALBLUE的远程攻击，并且攻击规模还有进一步扩大趋势。

此次利用的SMB漏洞影响以下未自动更新的操作系统：

Windows XP／Windows 2000／Windows 2003

Windows Vista／Windows Server 2008／Windows Server 2008 R2

Windows 7／Windows 8／Windows 10

Windows Server 2012／Windows Server 2012 R2／Windows Server 2016

个人预防措施：

1.未升级操作系统的处理方式（不推荐，临时缓解）：

启用并打开“Windows防火墙”，进入“高级设置”，在入站规则里禁用“文件和打印机共享”相关规则。

2.升级操作系统的处理方式（推荐）：

建议广大师生使用自动更新升级到Windows的最新版本。

建议加固措施：

1.及时升级操作系统到最新版本；

2.勤做重要文件非本地备份；

3.停止使用Windows XP、Windows 2003等微软已不再提供安全更新的操作系统。

参考链接：<https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx>

<https://github.com/x0rz/EQGRP_Lost_in_Translation/>