河南省教育信息安全监测中心

新型勒索病毒“WannaRen”安全预警

2020 年 4 月 9 日

新型勒索病毒“WannaRen”安全预警

事件描述

省教育信息安全监测中心监测到国内多个论坛，贴吧等网站先后有受害者感染新型 WannaRen 勒索病毒并进行求助，其名称与“WannaCry”相似，加密后会追加“.WannaRen”后缀名。

经分析，该勒索病毒通过 KMS 工具捆绑 PowerShell 脚本传播，同时下载另一个 PowerShell 脚本作为载体，下载相关模块文件，其中包括名为“you”的核心加密文件、“WINWORD.exe”白文件和“wwlib.dll”恶意 DLL 文件，使用白文件加载恶意 DLL 文件（俗称白+黑技术）来躲避查杀。勒索信中内容为繁体字，并要求受害者支付赎金完成解密，赎金价格为 0.05BTC（约 2500 元人民币）。目前，被加密的文件在未得到密钥前暂时无法解密。

病毒信息

传播方式	**第三方工具捆绑**
加密文件命名方式	<原文件名>+<原文件后缀名>+.WannaRen
联系方式	WannaRenemal@goat.si
勒索币种与金额	0.05 比特币（约 2500 人民币）
是否有针对性	否
能否解密	暂时不能解密
是否内网传播	是
勒索信界面	

安全防护建议

1、提高网络安全意识，及时进行系统更新和漏洞修复，避免下载非正版的应用病毒、非官方游戏及注册机等；

2、安装具有主动防御能力的终端防护病毒以对勒索病毒提供有效防护；及时备份重要文件，文件备份应与主机隔离；尽量避免打开社交媒体分享的不明来源链接，将信任网站添加书签并通过书签访问；

3、避免使用弱口令或统一的口令；接收邮件时要确认发送来源是否可靠，避免打开可疑邮件中的网址和附件，避免轻易下载来源不明的附件。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052