最近，一种名为“WannaRen”的新型比特币勒索病毒正大规模传播，在各类贴吧、社区报告的中招求助人数更是急剧上升，真可谓闹得满城风雨！不幸感染“WannaRen”勒索病毒的用户，重要文件会被加密并被黑客索要0.05BTC赎金（约等于2580rmb）。

在检测异常的第一时间，360安全大脑率先出击，首家发现“WannaRen”勒索病毒来源并且
关联到幕后黑客团伙，
并首家分析出真正的勒索攻击代码。
经360安全大脑分析确认，“WannaRen”勒索病毒的作者正是此前借“永恒之蓝”漏洞祸乱网络的“匿影”组织。

此次“匿影”组织一改借挖矿木马牟利的方式，变换思路通过全网投递“WannaRen”勒索病毒，索要赎金获利。
不过，广大用户不必太过担心，360安全大脑极智赋能下的360安全卫士已第一时间发现并支持对“WannaRen” 新型勒索病毒的拦截查杀。

谁是“匿影”组织？

“加密币挖掘机”变身“勒索病毒投递者”

从360安全大脑追踪数据来看，“匿影”家族在加密货币非法占有方面早有前科。早在以往攻击活动中，“匿影”家族主要通过“永恒之蓝”漏洞，攻击目标计算机，并在其中植入挖矿木马，借“肉鸡”（被非法控制电脑）挖取PASC币、门罗币等加密数字货币，以此牟利发家。

在攻击特征上，“匿影”黑客团伙主要利用BT下载器、激活工具等传播，也曾出现

过借“永恒之蓝”漏洞在局域网中横向移动扩散的情况。“匿影”黑客团伙在成功入侵目标计算机后，通常会执行一个PowerShell下载器，利用该加载器下载下一阶段的后门模块与挖矿木马。

（PowerShell下载器部分代码）

而此次新型比特币勒索病毒“WannaRen”的扩散活动中，从表面看与此前的“WannaCry”病毒类似，都是病毒入侵电脑后，弹出勒索对话框，告知已加密文件并向用户索要比特币。但从实际攻击过程来看，“WannaRen”勒索病毒正是通过“匿影”黑客团伙常用PowerShell下载器，释放的后门模块执行病毒。

（“WannaRen”勒索病毒攻击全过程）

旧瓶装新毒：

“匿影”家族后门模块下发WannaRen勒索病毒

正如上文所述，“匿影”组织转行勒索病毒，但其攻击方式是其早期投放挖矿木马的变种。唯一不同，也是此次“WannaRen”扩散的关键，就在于PowerShell下载器释放的后门模块。

从360安全大脑追踪数据来看，该后门模块使用了DLL侧加载技术，会在“C:\ProgramData”释放一个合法的exe文件WINWORD.EXE和一个恶意dll文件wwlib.dll，启动WINWORD.EXE加载wwlib.dll就会执行dll中的恶意代码。

后门模块会将自身注册为服务，程序会读取C:\users\public\you的内容，启动如下

图所示的五个进程之一并将“WannaRen”勒索病毒代码注入进程中执行。

（后门模块注入的目标）

在注入的代码中，可以看到是此次勒索病毒的加密程序部分：

完整的攻击流程如下面两图所示：

（“匿影”Powershell下载器释放并启动后门模块）

（“匿影”后门模块注入svchost.exe并加密文件）

WannaRen勒索病毒具备“横向传播”能力

360安全大脑强力截杀

追踪过程中，360安全大脑还发现“匿影”组织下发的PowerShell下载器中，包含了一个“永恒之蓝”传播模块。该模块会扫描内网中的其他机器，一旦有机器未修复漏洞就会惨遭感染，成为又一个“WannaRen”勒索病毒受害者。

（PowerShell下载器中的“永恒之蓝“传播模块）

（PowerShell下载器释放的永恒之蓝漏洞利用工具）

除此之外，PowerShell下载器还会在中招机器上安装一个名叫做的everything后门，利用everything的“HTTP 服务器”功能安全漏洞，将受害机器变为一台文件服务器，从而在横向移动时将木马传染至新的机器中。

（everything后门模块）

通过修改everything配置文件把机器变为文件服务器

不难看出，企业用户一旦不幸中招，“WannaRen”勒索病毒则可能在内网扩散。不过广大用户无需过分担心，360安全卫士可有效拦截此勒索病毒。面对突袭而来的“WannaRen”勒索病毒，360安全大脑再次提醒广大用户提高警惕，并可通过以下措施，有效防御勒索病毒：

1、及时前往weishi.360.cn，下载安装360安全卫士，查杀“匿影”后门，避免机器被投递勒索病毒；

2、对于安全软件提示病毒的工具，切勿轻信软件提示添加信任或退出安全软件运行；

3、定期检测系统和软件中的安全漏洞，及时打上补丁。