互联网网络安全信息通报

2018 年第 657 期（总第 1968 期）

国家计算机网络应急技术处理协调中心广东分中心　2018 年 12 月 5 日

关于一种新型勒索病毒有关情况的通报

12 月 1 日前后，一种新型的勒索病毒在国内开始传播，该勒索病毒要求受害者使用“微信支付”支付赎金。病毒制作者利用 github、CSDN、豆瓣、简书、QQ 空间等网站页面作为下发指令的 C&C 服务器，加密受害者文件并勒索赎金，同时窃取支付宝等软件密码。CNCERT 获得火绒、腾讯报送的信息后，立即开展对 C&C 及下载服务器的协调处置工作。

一、勒索病毒介绍

该病毒采用“供应链感染”方式进行传播，通过论坛传播植入病毒的“易语言”编程软件，进而植入各开发者开发的软件，传播勒索病毒；同时，该病毒还窃取用户的账号密码，包括淘宝、天猫、支付宝、QQ 等。

该勒索病毒在感染用户计算机后不会勒索比特币，而是弹出微信支付二维码，要求受感染用户使用微信支付 110 元，从而获得解密密钥，这也是国内首次出现要求使用微信支付的勒索病毒。目前，微信运营商判定该支付二维码存在违规行为，并表示已无法通过扫描二维码支付赎金解密。

二、措施建议

我中心在此提醒广大用户及时采取如下措施进行防范：

1、安装并及时更新杀毒软件，目前市场主流反病毒软件都已支持针对该勒索病毒的防护与查杀。

2、不要轻易打开来源不明的软件，该勒索病毒通过易语言编写的程序传播，减少使用来源不明的软件可有效预防。

3、如已经感染勒索病毒，可使用相关解密工具尝试解密。目前，许多公司已经针对该勒索病毒开发了解密工具，包括火绒 Bcrypt 专用解密工具、腾讯电脑管家“文档守护者”、360 安全卫士“360 解密大师”等。（解密工具链接附后）

4、已感染勒索病毒的用户，在清除病毒后，尽快修改淘宝、天猫、支付宝、QQ 等敏感平台的密码。

5、定期在不同的存储介质上备份计算机中的重要文件。

附：解密工具

https://www.huorong.cn/info/1543706624172.html（火绒 Bcrypt 专用解密工具）

https://guanjia.qq.com/news/n3/2444.html（腾讯电脑管家“文档守护者”）

http://www.360.cn/n/10496.html（360 安全卫士“360 解密大师”）

联系方式： gd@cert.org.cn