中戏信网[2015]1号

关于加强CryptoLocker恶意软件安全防范工作的通知

各系、部：

近期,在北京有多个单位的计算机感染了Cryptolocker恶意软件病毒，导致大量重要数据无法恢复，给相关单位工作造成严重影响。为进一步加强安全防范工作，防止此类事件发生，请各系、部迅速开展以下几项工作：

  一是迅速开展自查，立即对Cryptolocker恶意软件感染情况进行自查，启用防病毒软件并将防病毒软件升级到最新版本,进行全盘查杀。发现问题，立即报信息网络中心,联系人:张茱萸 联系电话:56620418 邮箱：zxwl@zhongxi.cn

二是提高终端用户的安全防范意识，不轻易打开可疑邮件、点击陌生网站、连接未经认证的无线网络；使用移动存储介质前要进行安全检测。

三是加强重要数据安全保护工作，认真梳理数据目录，加强操作权限管理和记录，尤其是涉及业务系统运行、关键历史记录以及个人敏感信息等重要数据，通过文档保险箱、虚拟磁盘等方式进行加密保护，并开启操作系统的系统保护功能定期实行操作系统和数据备份，对重要数据进一步采取脱机方式进行备份。

四是请各单位于5月29日中午12时前,将恶意软件排查情况通过QQ群(中戏GTO)反馈信息网络中心。

**附件：**CryptoLocker[恶意软件](http://zh.wikipedia.org/wiki/%E6%83%A1%E6%84%8F%E8%BB%9F%E9%AB%94)基本情况及技术防范措施介绍

信息网络中心

                        2015年5月28日

CryptoLocker[恶意软件](http://zh.wikipedia.org/wiki/%E6%83%A1%E6%84%8F%E8%BB%9F%E9%AB%94)基本情况及技术防范措施

一、恶意软件基本情况

CryptoLocker是一种于2013年下半年出现的[特洛伊木马](http://zh.wikipedia.org/wiki/%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A9%AC_(%E7%94%B5%E8%84%91))[恶意软件](http://zh.wikipedia.org/wiki/%E6%83%A1%E6%84%8F%E8%BB%9F%E9%AB%94)，以[勒索软件](http://zh.wikipedia.org/w/index.php?title=%E5%8B%92%E7%B4%A2%E8%BB%9F%E9%AB%94&action=edit&redlink=1)的形式将[Microsoft Windows](http://zh.wikipedia.org/wiki/Microsoft_Windows)操作系统作为目标进行攻击。CryptoLocker会伪装成后缀为.cab、.scr的邮件附件，一旦运行便将扫描用户驱动器上的照片、视频和文档等重要文件，该恶意软件就会使用RSA[公钥](http://zh.wikipedia.org/wiki/%E5%85%AC%E9%92%A5%E5%8A%A0%E5%AF%86)与[AES](http://zh.wikipedia.org/wiki/AES)私钥加密的形式，加密本地与内部网络的特定类型档案；而私钥则存放在恶意软件所控制的服务器上，若用户想要恢复数据，只能向攻击者缴纳赎金。近期，我市发生多起计算机感染勒索软件Cryptolocker病毒事件，造成大量重要业务数据无法恢复。

目前，该病毒已在全球范围内不断升级产生多个变种，可进一步通过门户网站、社交软件、无线网络和多种移动存储介质等途径进行传播，部分变种甚至针对中国计算机用户特点进行恶意行为。由于该病毒采用的加密方式复杂，文件被加密后很难被恢复；赎金的支付又通常以比特币的形式，难以准确追查到攻击源。

二、技术防范措施

为了有效遏制该病毒在我市范围内的进一步传播，避免造成恶劣影响，建议加强以下几方面工作：

1.加强终端用户安全管理工作，经了解国内主流防病毒软件均具备针对该病毒的检测、拦截、清理能力，启用防病毒软件并将病毒库升级到最新，进行全盘查杀；不轻易打开可疑邮件、点击陌生网站、连接未经认证的无线网络；使用移动存储介质前进行安全检测。

2.加强重要数据安全保护工作，认真梳理数据目录，加强操作权限管理和记录，尤其是涉及业务系统运行、关键历史记录以及个人敏感信息等重要数据，通过文档保险箱、虚拟磁盘等方式进行加密保护，并开启操作系统的系统保护功能定期实行操作系统和数据备份，对重要数据进一步采取脱机方式进行备份。