

精译版

如何删除类似 WannaCry 的勒索软件

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	How to remove ransomware like WannaCry: Use this battle plan to fight back		
原文作者	Mark Hachman	原文发布日期	2017 年 5 月 13 日
作者简介	PC world 高级编辑,主要专注于微软新闻和芯片科技。 http://www.itnews.com/author/Mark-Hachman/		
原文发布单位	IT News		
原文出处	http://www.itnews.com/article/3169524/security/how-to-remove-ransomware-use-this-battle-plan-to-fight-back.html		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师,本文系出自个人兴趣在业余时间所译,本文原文来自互联网的公共方式,译者力图忠于所获得之电子版本进行翻译,但受翻译水平和技术水平所限,不能完全保证译文完全与原文含义一致,同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系,亦未获得相关的版权授权,鉴于译者及安天实验室出于学习参考之目的翻译本文,而无出版、发售译文等任何商业利益意图,因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献,主要用于安天实验室内部进行外语和技术学习使用,亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿,不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文,因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为,及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的,基于上述问题产生的法律责任,译者与安天实验室一律不予承担。 		

如何删除类似 WannaCry 的勒索软件

常识、备份、主动防御以及自动删除工具是抵御勒索软件祸害的坚实基础。



勒索软件不会像普通恶意软件那样潜入个人计算机，而是突然闯入，直指数据并威胁索要金钱。如果不学会保护自己，勒索事件可能一而再再而三的发生，正如 WannaCry (Wanna Decryptor) 爆发显示的那样。

武装数据盗窃团伙漫步在信息高速公路上，听起来像一场精神紧张的动作电影，但数据证实了这一说法：据 Sonicwall 文章数据显示——甚至在恶意软件攻击数量下降的情况下——勒索软件攻击从 2015 年的 380 万增长到 2016 年的 6.38 亿，一年增长了 166 倍。可以轻易索要现金时，为什么要盗窃数据呢？

旧金山 RSA 安全大会首次举办了一场针对勒索软件的一日研讨会，详细列举了被攻击的对象，造成的损失——更重要的是如何拦截、删除，甚至与扣押数据的骗子谈判。我们获取的大量信息可用于制定反勒索软件策略。

如果勒索软件触到痛点——那么做好准备

三年前，我妻子的电脑被勒索软件入侵了，孩子的照片、纳税文件以及其它私人数据面临丢失的危险。当时心情沉重：心想必须支付数百美元才能避免丢失所有的数据吗？幸亏我们之前听从了专家的大多数防御措施，才能逃过一劫。

第一步：了解你的对手。据英特尔安全 EMEA 业务首席技术官拉杰·萨玛尼所说，全球有 400 多种勒索软件家族——有些甚至针对 Mac OS 和 Linux 操作系统。据数据备份公司 Datto 调查发现，CryptoLocker 通过时间锁定加密抓捕、扣押私人文档，现在最为猖獗。但它们之间也有差异。SentinelOne 首席安全策略官耶利米·格劳斯曼说到，有的控制受害人通过网络摄像头拍摄尴尬镜头，发到网上进行威胁或勒索。

专家说，掌握一些常识可以减少恶意软件和勒索软件攻击的风险：

- 通过 Windows Update 更新电脑。WannaCry 不会攻击 Windows 10 系统，不要选择 Windows XP 和其它老旧 Windows 操作系统。
- 确保配备了活跃防火墙和反恶意软件解决方案。Windows Firewall 和 Windows Defender 勉强足够，最好配备一家可靠的第三方反恶意软件解决方案。虽然可以获取 Windows 8 和 Windows XP 的 WannaCry 补丁。
- 关闭办公软件中的宏（Office 2016 版，确保在信任中心 > Macro 设置关闭或在顶部搜索框键入“macros”，然后打开“Security”框。）

- 不要打开网页尤其是邮件上的可疑链接。勒索软件最常见的感染方式是点击恶意链接。更糟的是，Datto 追踪发现 2/3 的机器出现感染，表明被感染用户点击链接导致更多的机器被感染。

- 同样，远离网络死角。如果不小心，合法网站上的恶意广告仍可能被注入恶意软件，但如果你访问了不该访问的网站风险会增加。

一种有效但不是很完美的防御方法：备份

勒索软件加密、锁定最重要的文件，因此加强保护非常必要。备份就是一种很好的策略。

最好是现在，购买一个永久硬驱——Seagate 1TB 永久硬驱大约只要 55 美元——添加一些不常访问的“存储”。定期备份，隔离拷贝数据。

如果所有的措施都失败了



从 2015 年 12 月到 2016 年 5 月，微软检测到的最常见的勒索软件变种是 Tescrypt。

记住，防护、复制和备份等步骤点只是给你更多的选择余地。如果原始数据存储在其他地方，你需要做的是重置电脑，重新安装应用，恢复备份数据。

不要让这些发生在你身上

我的情况是，我妻子和我发现我们已在云服务和永久硬驱上备份了所有重要的数据。我们损失的不过是晚上几个小时，包括重置她的电脑的时间。

勒索软件感染个人计算机的方法很多：新应用，Flash 游戏网站，意外点击恶意广告。鉴于我们的情况给大家提一个醒，不要随意点击朋友推荐的一些折扣购物网站。我们也给孩子上了一课。

勒索软件是一个令人不安的定时炸弹，随时都可能发生。如果我们把电脑当做家里的一部分来对待——及时清理，维护和隔离外部威胁——会更加舒心，并做好最坏的打算。