病毒预警

2019 年 1 月 3 日

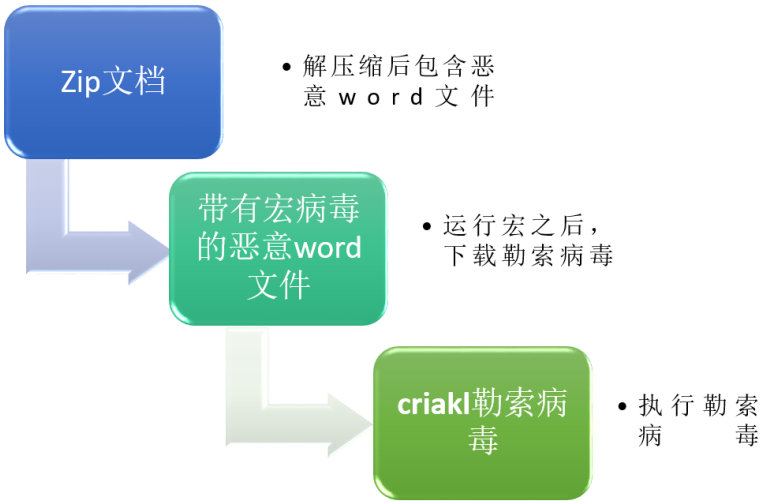
criakl 勒索病毒预警

事件描述

新年伊始，亚信安全截获最新 criakl 勒索病毒变种，该病毒利用社会工程学，通过钓鱼邮件附件进行传播，一旦用户运行附件文件，病毒会加密用户系统中的文件，亚信安全将其命名为：Ransom.Win32.CRYAKL.AMR。由于该病毒一直处于非活跃状态，而在 2019 年伊始出现变种，值得我们广大用户警惕，避免造成大规模爆发。

criakl 勒索病毒分析

criakl 勒索病毒最早可以追溯到 2014 年，该病毒一直不温不火，鲜有变种出现，本次亚信安全截获的最新变种是通过钓鱼邮件附件进行传播，其攻击流程如下：



- 邮件附件是 zip 压缩包，该压缩包里面包含带有宏病毒的 word 文件（亚信安全已经拦截该病毒，并将其命名为 Trojan.W97M.POWLOAD.AA）；
- Word 恶意文件实际上是病毒下载器，运行该文件中包含的恶意宏之后，其会链接 http://vallyxs0.{block}tech/1.exe 下载恶意文件；

- 下载并执行恶意文件，该文件即为 criakl 勒索病毒。

解决方案

- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 不要随意点击邮件中的链接；
- ✓ 不要启用 office 宏功能。如果非必要，建议关闭 Office 的宏功能；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案：

- ✓ 亚信安全病毒码版本 14.725.60 (云病毒码版本 14.725.71，全球码版本 14.727.00)及以上版本已经可以检测，请用户及时升级病毒码版本。

总结：

criakl 勒索病毒最早可以追溯到 2014 年，该勒索病毒一直不温不火，很少出现变种，2019 年伊始，该病毒出现新的变种，异常活跃，亚信安全提醒广大用户小心防范，避免大规模爆发。