WinXP 的 Wannacry 内存密钥恢复

精译版

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	Wannacry in-memory key recovery for WinXP		
原文作者	GitHub	原文发布日期	2017 年 5 月 19 日
作者简介	GitHub 于 2008 年 4 月 10 日正式上线，除了 Git 代码仓库托管及基本的 Web 管理界面以外，还提供了订阅、讨论组、文本渲染、在线文件编辑器、协作图谱（报表）、代码片段分享（Gist）等功能。		
原文发布单位	Github		
原文出处	https://github.com/aguinet/wannakey		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	• 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。		

Wannakey

警告

据称，该软件仅通过 Windows XP 系统的测试，也就是说只适用于 Windows XP 系统。为了使其生效，您的计算机在感染后禁止重新启动。

还请注意，你需要一些运气来使它起作用（见下文），所以它可能无法在所有情况下生效！

简介

该软件允许恢复由 Wanacry 使用的 RSA 私钥的素数。

该软件通过在 wcry.exe 进程中搜索这些素数来实现。这是生成 RSA 私钥的过程。主要问题是 CryptDestroyKey 和 CryptReleaseContext 在释放相关内存之前不会从内存中删除素数。

这应该不是该勒索软件作者的失误，因为他们能正确使用 Windows Crypto API。实际上，对于我在 Windows 10 下所测试的结果显示，CryptReleaseContext 确实会清理内存（因此这种恢复技术将无法正常工作）。它可以在 Windows XP 下工作，因为在此版本中，CryptReleaseContext 不执行清理行为。

MSDN 指出，对于此功能：“调用此函数后，释放的 CSP 句柄不再有效，此功能不会破坏密钥容器或密钥对。所以，似乎 Windows 下没有干净的跨平台方式来清理这个内存。

如果你幸运的话(与没有被重新分配和擦除的内存有关),这些素数可能仍然在内存中。

这就是这个软件试图实现的功能。

用途

您可以在 bin /文件夹中使用二进制文件。您首先需要通过任务管理器找到 wcry.exe 进程的 PID，并找到 00000000.pky 文件。

一旦获得这个，启动 cmd.exe：

```
> search_primes.exe PID path\to\00000000.pky
```

如果在内存中找到一个有效的素数，那么将在当前目录中生成 priv.key 文件。

然后你可以使用 https://github.com/odzhan/wanafork/ 解密你的文件。

警告：wanafork 现在没有直接在 Windows XP 下工作。这应该很快被修复（希望）！

从源代码编译

可以利用 Visual Studio 2015 express 来编译相关项目。要确保在项目属性中选择 Windows XP 兼容的工具链。

参考

- @wiskitki，在 Windows 10 中发现 CryptReleaseContext 事件（从内存中抹去素数）
- @hackerfantastic，发布了我所使用的样本
- Miasm （https://github.com/cea-sec/miasm），协助提取 DLL 并逆转整个事件
- 针对 Windows RSA 密钥格式 Wine 源代码