ESET Research 发现了第一个内置于即时消息应用程序中的剪贴板劫持木马。

这家网络安全研究公司表示，攻击者正在使用适用于 Android 和 Windows 的木马化 Telegram 和 WhatsApp 应用程序追踪受害者的加密货币资金。

该恶意软件可以将受害者在聊天消息中发送的加密货币钱包地址切换到属于攻击者的地址。一些攻击者使用OCR识别（图像文字识别）从屏幕截图中提取文本并窃取加密货币钱包助记词。除了 Clippers，ESET 还发现远程访问木马与恶意 Windows 版本的 WhatsApp 和 Telegram 捆绑在一起。

Clippers木马（剪贴板劫持木马）是一种窃取或修改剪贴板内容的恶意软件。所有这些都是针对受害者的加密货币资金，其中有几个针对加密货币钱包。

这是 ESET Research 首次发现专门针对即时消息的 Android 剪贴板劫持木马。此外，其中一些应用程序使用光学字符识别 (OCR) 来识别存储在受感染设备上的屏幕截图中的文本，这在 Android 恶意软件中又是首创。

从恶意应用使用的编程语言来看，其背后的运营商似乎主要针对中文用户。因为 Telegram 和 WhatsApp 在中国都被屏蔽了好几年，Telegram 从 2015 年开始被屏蔽，WhatsApp 从 2017 年开始被屏蔽，所以想要使用这些服务的人不得不通过间接的方式获得它们。

攻击者首先设置谷歌广告，引导欺诈性 YouTube 频道，然后将观众重定向到山寨 Telegram 和 WhatsApp 网站。ESET Research 向 Google 报告了欺诈性广告和相关 YouTube 频道，Google 已将其全部关闭。

“我们发现的山寨Telegram主要拦截受害者通信，并将任何发送和接收的加密货币钱包地址替换为属于攻击者的地址。”发现木马化应用程序的 ESET 研究员 Luk tefanko 说。

“除了木马化的 WhatsApp 和 Telegram Android 应用程序，我们还发现了相同应用程序的木马化 Windows 版本。”他说。

尽管服务于相同的通用目的，但这些应用程序的木马化版本包含各种附加功能。所分析的 Android 恶意软件成为第一个使用 OCR 从存储在受害者设备上的屏幕截图和照片中读取文本的 Android 恶意软件实例。

部署 OCR 是为了查找和窃取种子短语，种子短语是由一系列用于恢复加密货币钱

包的单词组成的助记码。一旦恶意行为者掌握了助记词，他们就可以直接从相关钱包中窃取所有加密货币。

在另一个例子中，恶意软件只是将受害者的加密货币钱包地址切换为聊天通信中攻击者的地址，这些地址要么是硬编码的，要么是从攻击者的服务器动态检索的。在另一个例子中，该恶意软件会监控 Telegram 通信中与加密货币相关的某些关键字。一旦识别出这样的关键字，恶意软件就会将完整的消息发送到攻击者的服务器。

ESET Research 还发现了 Windows 版本的钱包地址剪贴板劫持器，以及与远程访问木马 (RAT) 捆绑在一起的 Windows 版 Telegram 和 WhatsApp 安装程序。与既定模式不同的是，其中一个与 Windows 相关的恶意软件捆绑包是由能够完全控制受害者系统的 RAT（远程访问木马）组成。这样，RAT 就能够在不拦截应用程序流的情况下窃取加密货币钱包。

“仅安装来自可信赖和可靠来源的应用程序，例如 Google Play 商店，不要在您的设备上存储包含敏感信息的未加密图片或屏幕截图。如果你认为你有 Telegram 或 WhatsApp 的木马版本，请手动将其从你的设备中删除，然后从 Google Play 或直接从合法网站下载应用程序。” tefanko 建议。

“对于 Windows，如果你怀疑你的 Telegram 应用程序是恶意的，请使用安全解决方案来检测威胁并为你将其删除。Windows 版 WhatsApp 的唯一官方版本目前可在微软商店购买。”