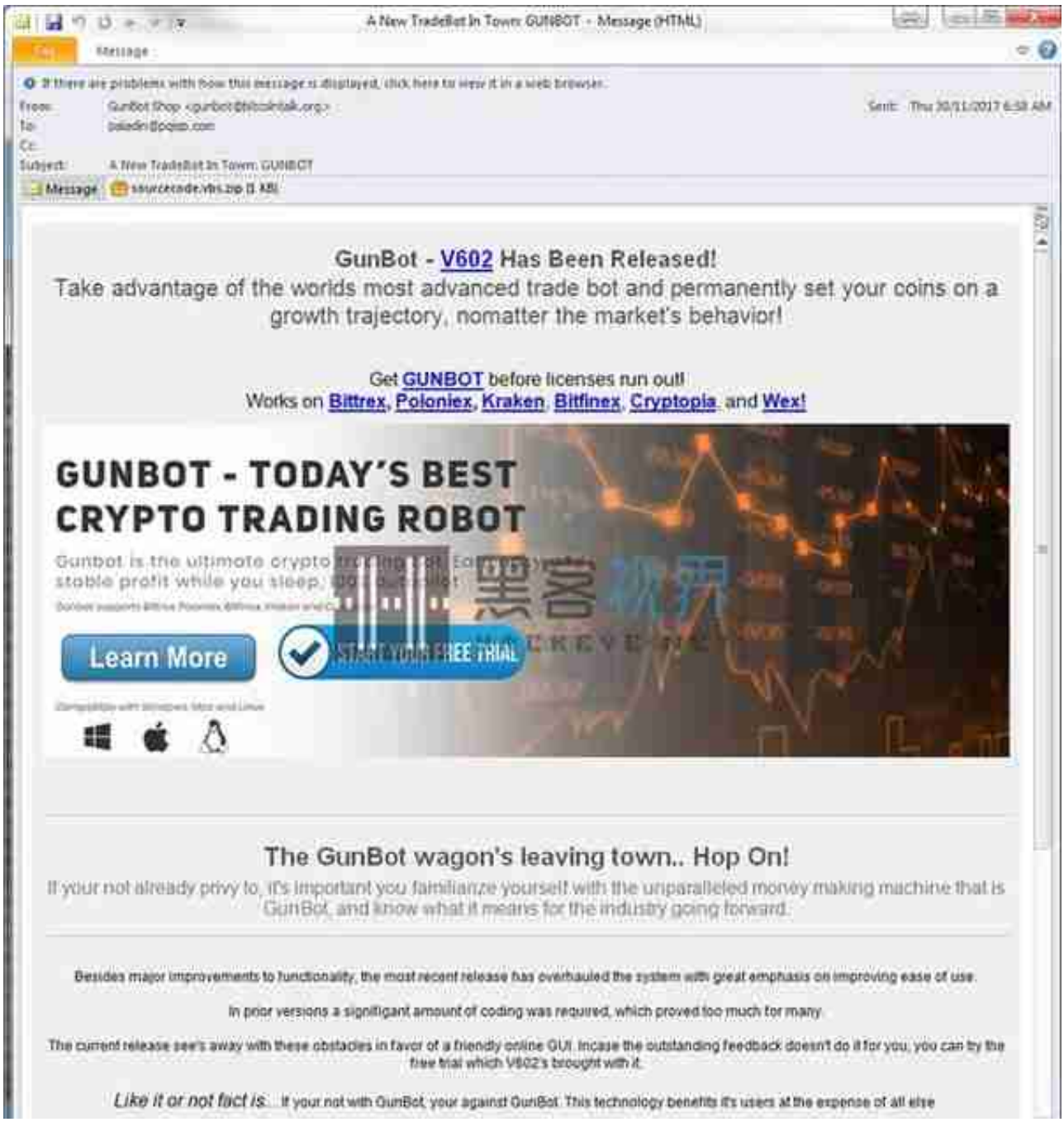

从邮件的内容来看，它似乎用于推销由GuntherLab或Gunthy开发的名为“Gunbot”的新型比特币交易机器人。

邮件附件中包含了一个名为“sourcode.vbs.zip”的压缩文件，其中包含一个简单的VB脚本，用于下载一个伪装成JPEG图像文件的PE格式二进制文件。根据Fortinet的说法，攻击者并没有试图掩盖他们的意图，要么是因为他们原本就不想这么做，要么是因为他们缺乏相关的混淆技术。

这个二进制文件被证明是一个名为TTJ-Inventory System的开源库存系统工具的木马化版本，即Orcus RAT。硬编码密钥用于将编码后的代码解密为另一个可直接加载并执行到内存的.NET PE可执行文件。

Orcus RAT的运作原理

该可执行文件在其资源中还包含三个嵌入式PE可执行文件，可以找到实际的Orcus RAT服务器。

- M - Orcus RAT服务器
- PkawjfiajsVIOefjsakoekAOEFKasoefjsa-持久性监督
- R-RunPE模块