在本月初，网络安全公司Proofpoint的研究人员监测到了一起试图传播一种名为“RedLine”的新型恶意软件的垃圾电子邮件活动，主要针对了美国的医疗保健和制造业。

根据Proofpoint研究人员的说法，RedLine是一种信息窃取类恶意软件，目前可以在俄语黑客论坛上购买到，售价分为精简版150美元、专业版200美元以及100美元包月三个档次。

据称，RedLine不仅能够从浏览器中窃取信息（如保存的登录名、密码等），而且还能够收集有关用户及其系统的信息（用户名、国家、硬件配置以及已安装的杀毒软件等）。

此外，最新版本的RedLine似乎还新增了能够窃取加密货币冷钱包的功能。

垃圾电子邮件分析

垃圾电子邮件声称来自美国一家名为“Mobility Research”的康复医疗公司，主题为“Please help us with Fighting corona-virus（请帮助我们对抗冠状病毒）”。显然，攻击者是想要冒用合法公司的名义以及利用当下的社会热点来提高收件人打开电子邮件的概率。

图1.垃圾电子邮件示例

在收件人点击了邮件中的下载按钮之后，一个内嵌RedLine恶意软件的可执行文件

就会从BitBucket（一家源代码托管网站）上下载。

RedLine的推销广告

Proofpoint研究人员在多个论坛上都找到了RedLine的推销广告，有些似乎来自官方卖家（精简版150美元、专业版200美元以及100美元包月），有些似乎是破解版（售价300美元）。

根据官方广告，RedLine的主要功能如下：

- 从浏览器中窃取登录名和密码、cookie、自动填充字段以及银行卡数据（支持的浏览器包括所有基于Chromium的浏览器以及所有基于Gecko的浏览器）；
- 从FTP客户端、IM客户端中窃取数据；
- 按路径、扩展名、子目录爬取指定文件；
- 国家/地区黑名单功能；
- 收集有关受感染系统的信息，包括IP、国家/地区、城市、当前用户名、HWID、键盘布局、屏幕截图、屏幕分辨率、操作系统、UAC设置，用户代理、有关PC硬件的信息（视频卡，处理器）以及已安装的杀毒软件等；
- 窃取加密货币冷钱包的功能。

图2. RedLine的C＆C面板（加载程序任务页面）

图3 .RedLine的C＆C面板（设置页面）

图4. RedLine的C&C面板（日志页面）

恶意软件分析

除上述主要功能外，RedLine还能够执行其他一些任务，如下载并运行其他恶意软件。

图5. RedLine的主函数

图6.负责从基于Chromium的浏览器中窃取银行卡数据的代码

图7.负责从指定网址下载文件，并将其注入另一个文件的代码

结语

RedLine是一种此前从未被公开报道过的新型信息窃取类恶意软件，目前已被不法分子用来攻击美国的医疗保健和制造业。除信息窃取功能外，它还具备其他的一些功能，如下载并运行其他恶意软件。

值得一提的是，RedLine的开发者目前似乎仍在对其进行优化和更新（例如，能够窃取加密货币冷钱包的功能就是在后续版本中新增的），再加上作为恶意软件即服务，这种新型恶意软件或将很快在更多国家出现。