勒索：Locky

出品：美国国家安全局

翻译：樊山

什么是 Locky

Locky 是一个多级勒索限制访问被感染的系统文件直到支付赎金。网络行为诱使受害者开启和点击社会工程垃圾邮件的附件。在许多情况下，这些电子邮件包含获得受害者的凭据并收集来自受害人主机上的个人信息的能力。Locky 的主要传送机制是通过微软 Word，Excel 或 Outlook 附件。

已知 Locky 目标包括各种普通公民，医院和政府网络。针对医院的研究技术包括通过虚假单据引诱收件人点击附件并提示用户启用宏。一旦执行，它会指挥和控制服务器产生一个传送勒索支付到主机。然后，被感染的主机上的文件被加密，并提供有关如何支付赎金的说明。

增长和外部事件

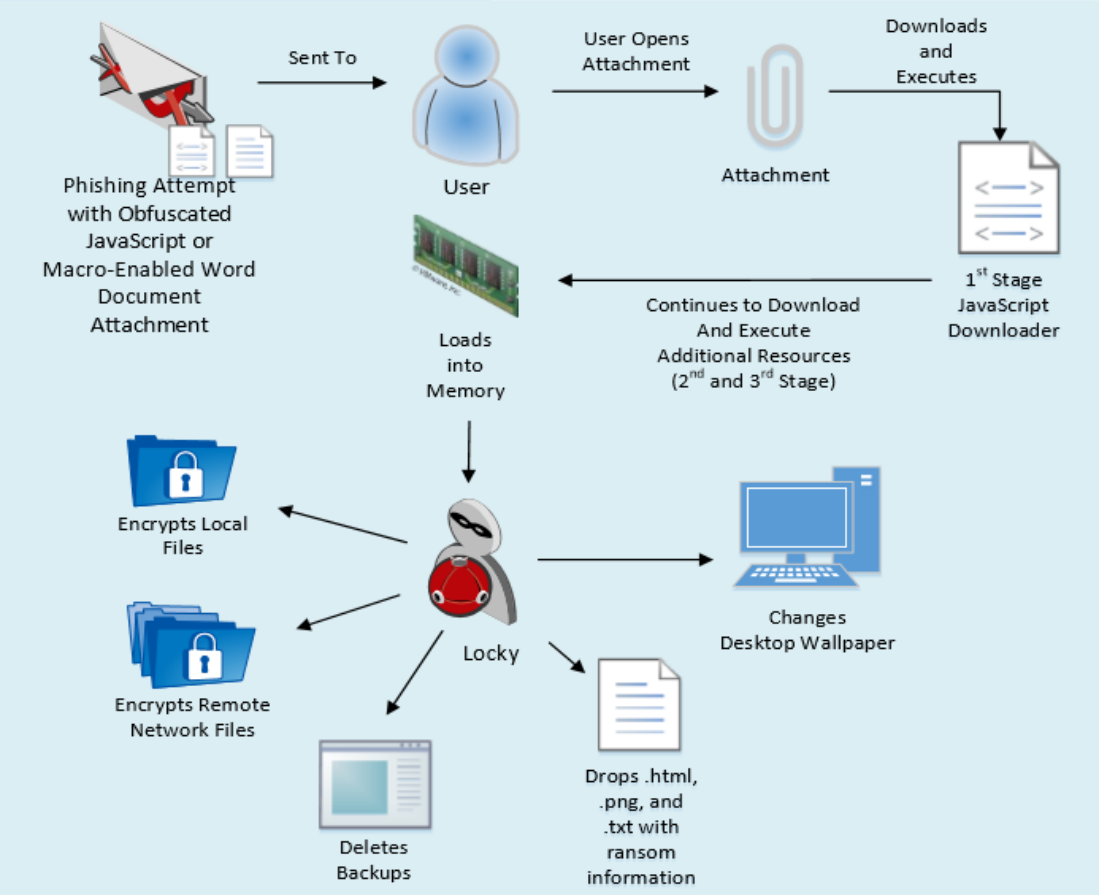
Locky 攻击持续弹性对抗措施通过更新施，代码更正并增加新的功能。观察分析在研究的每个阶段显示计划阶段攻击周期停顿同时每个阶段持续呈指数级增长。据 Trustwave 报道，在过去的 7 天内，有针对性的邮件数量增长了 200,000，在此期间发送的电子邮件中 Locky 垃圾邮件占近 18%。在感染的顶点，每小时 1000 设备进行回拨 C2 服务器。目前，每天约有 1,000 台设备被发现。

Locky 通过针对医院揭示勒索的 TTP 一个显著变化。已感染的几家医院以很可能包括密歇根州的弗林特，在洛杉矶的好莱坞长老会医疗中心，三德医院和

加拿大至少一所医院。好莱坞长老会支付 40 比特币的赎金（$17,000 名美元）重新获得网络功能。据报道在德国的两家医院已经支付赎金，而密歇根州的弗林特医院和一个德国医院得以通过包括设备的成功重新映像功能快速缓解恢复。

Locky 行为

Locky 已被观察到使用相同的僵尸网络传输机制进行勒索，如 Dridex。变体通常采用多级负载降低系统设计恶意软件传送模块化，模糊分析并躲避典型的企业 AV 防御。几乎所有的变种采用含模糊 JavaScript，或者放置启用宏的 Word 文档，然后执行第一阶段的 JavaScript 下载邮件附件。当第二阶段的窗口可执行文件被下载并执行时，一个可执行文件从第二阶段可执行文件资源段解压并进一步执行。一些变体将在第三阶段以可执行文件的形式下载额外的资源。下面的图表凸显 Locky 变异的常见功能。



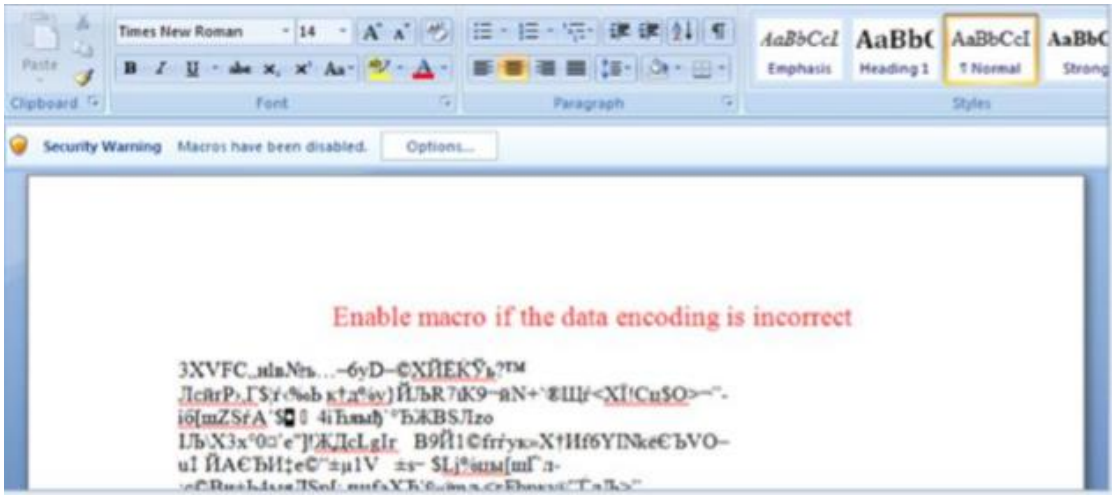
Locky 本身加载到内存中，设置持久性机制，加密文件和文档同时用自定义扩展其重命名，删除 VSS 快照，并改变桌面墙纸。

缓解措施

- 为了减少攻击面，确保正确的本地网络分段。
- 教育用户有关常见鱼叉式网络钓鱼战术和如何识别，以及预防感染。保持用户对不良安全性做法负责。
- 定期执行备份和保留异地副本：Locky 有加密您的基于网络的备份文件的能力；因此，建议每个系统不仅备份在域内而且应场外存储复制。
- 确保可靠的应用程序白名单（AWL）策略，包括防止任何程序从用户可写文件位置的规则，特别是%TEMP%位置（例如 C：\用户\ * \应用程序数据\本地\ TEMP）。大多数 AWL 产品有从允许执行阻止%TEMP%目录中的“默认”规则，而且组织也应保证被列入白名单的任何位置也防止用户写入这些文件夹。
- 确保 HIPS 规则拒绝运行未知的可执行文件，精心调校，并设置阻拦。例如，McAfee 的 HBSS 规则 3905 和 2297 拒绝来自常见的恶意软件的位置（例如临时目录）执行。规则 7010，7011，7035 和是与美国国防部的环境中额外的优化类似的规则。自定义规则可以创建拒绝注册表项“HKEY_CURRENT_USER\ SOFTWARE \ Locky”的创建。
- 如果允许，实施一个注册表访问保护规则下阻止注册表键/值创建“HKCU\Software\locky”
- 确定被感染的网络用户：如果在网络共享显示.locky 扩展名的文件，查找文件所有者的每个文件夹中的“_Locky_recover_instructions.txt”文件。这将有助于确定感染的用户。
- 在电子邮件附件禁用宏：在过去感染的发生率到极高后，微软特意将自动禁止对 Word 文档的宏作为一项安全措施。不要打开它。

主机系统破坏前后

截图是如果用户启用了受感染 Word 文档的宏时的展示，它会自动破坏主机系统。应当注意的是，破坏主机的附加方法包括发送已设计逃避 AV 检测 JavaScript 文件附件。



犯罪分子希望你点击[选项...]，打开宏。不这样做！

“Locky”设置你的墙纸，以确保你知道下一步该怎么做

IAD 操作融合和分析产品-IAD 可扩展运营缓解措施缓解措施指导意见