



## 2018 年趋势：勒索软件革命

哈尔滨安天科技集团股份有限公司



David Harley

2018年3月7日

实际上，这是我[近三十年前](#)职业生涯开始的地方。我提供咨询服务的第一起恶意软件疫情是波普博士（Dr. Popp）编写的“艾滋木马”（[AIDS Trojan](#)），该木马使得受害者无法访问数据，除非进行“软件续订租约”付款。此后很长一段时间，都没有出现可以称为勒索软件的威胁，除非把针对企业的持续性 [DDoS（分布式拒绝服务）](#) 攻击算在内。

### 实在太像拒绝服务攻击

在世纪之交，利用僵尸网络（由被僵尸程序感染的 PC 构成）放大的 DoS 攻击成为一个值得注意的问题，但是在过去几年中，DDoS 勒索威胁与勒索软件威胁齐头并进。一些受害企业不愿透露攻击事件可能会影响统计数据，出于[政治动机](#)（而非[单纯的经济动机](#)）的 DDoS 攻击也出现了增长。然而，各种恶意软件之间还存在复杂的交互：在一些[案例](#)中，勒索软件变种包含了 DDoS 僵尸程序；最近，Mirai 僵尸网络的模仿者对 WannaCryptor 的“域名开关”（kill switch）



执行 [DDoS 攻击](#)，使休眠的恶意软件副本再次苏醒。

## 蠕虫功能

当然，被 ESET 称为 [Win32/Filecoder.WannaCryptor](#) 的恶意软件比 Mirai 更加复杂。虽然没有像我们在千禧年的头十年所看到的一些蠕虫攻击那样猛烈（部分原因是它的传播依赖于已经被广泛修复的漏洞），但勒索软件和蠕虫的结合加速了它的传播。然而，其对重要企业的经济影响引起了全球媒体的关注。

## 支付赎金也无济于事

WannaCryptor 的一个特点是，即使受害者支付赎金，也不太可能解密所有的数据。当然，在这方面它不是唯一的：在很多勒索软件案例中，犯罪分子因不完整的编码或[从来没有打算恢复数据](#)，而无法恢复[部分](#)或[所有](#)数据。例如，Ranscam 和 Hitler 只是简单地删除了文件，没有进行加密，因此犯罪分子也不可能帮助受害者恢复数据。幸运的是，它们似乎并没有特别广泛地传播。也许[最臭名昭著的例子](#)是 Petya（ESET 将其命名为 [DiskCoder.C](#)），它确实对数据进行加密。考虑到它的执行能力，没有恢复机制似乎并非是意



外，而是一种“拿了钱就跑”的计策。

## 擦除程序

DiskCoder.C 有时被称为 NotPetya，这清楚地说明它不会作为勒索软件获取赎金，但其他“擦除程序”显然有不同的打算，例如最近卷土重来的 Shamoon 恶意软件。这个针对乌克兰的恶意软件具有擦除功能，包含 KillDisk 组件([与 BlackEnergy 相关](#)) 和 [Industroyer](#) 部署的其中一个载荷。

## 从这些趋势中学到了什么？

劫持用户数据并勒索赎金是攻击者赚钱的一种简便方法，而出于其他原因（如政治动机）破坏数据的事件似乎也在增加。与其猜测关于数据劫持的所有可能的变化，我们不如来看看一些能够[降低风险的方法](#)。

1. 即使受害者知道支付赎金会鼓励犯罪分子，他们仍然会[支付赎金](#)来恢复数据，我们理解这种做法。但是，在支付赎金之前，请与你的安全软件厂商确认：（a）不支付赎金，是否有可能恢复数据；（b）支付赎金是否也无法恢复数据。

2. 主动保护数据比依赖犯罪分子的能力和诚信更靠谱。请定期备份所有有价值的数 据，在安全的物理环境中（最好



是多个位置)，使用不会遭勒索软件和其他恶意软件感染的存储媒体，保存离线备份。显然，备份能够防御勒索软件和其他恶意软件破坏数据，因此应该成为灾难恢复计划的一部分。

3. 如今，很多个人和企业对用光盘和 U 盘这样的物理媒体备份数据的关注程度比不上云存储——当然，云存储很可能是非现场 (offsite) 的。但是，如果云存储“一直开启”，那么其内容可能会像本地和其他联网存储一样易受勒索软件感染。非现场存储需要注意：

- a. 不要一直开启
- b. 当远程设备在线时，保护备份的数据免受自动和悄无声息的修改或被恶意软件覆盖。
- c. 保护早期的备份数据不受损害，这样，即使恶意软件感染了最新的备份，你至少可以保住一部分数据，包括当前数据的早期版本。
- d. 通过说明提供者的法律/合同责任、如果提供者停业会发生什么情况等问题来保护客户。

4. 不要低估非可重写/可重用备份媒体的有用性。如果你不能修改写入其中的内容，那么勒索软件也不能。定期检



查，以确保你的备份/恢复操作（仍然）能够正常工作，你的存储媒体（只读，禁止写入或允许写入）仍然可读（允许写入的媒体不一定可写入）。此外，请备份你的备份。

5. 当然，不能只依靠备份而不使用安全软件。但要记住，使用安全软件删除活跃的勒索软件与恢复数据绝不是一回事：删除勒索软件然后决定支付赎金，意味着即使犯罪分子配合，数据也可能无法恢复了，因为解密机制是恶意软件的一部分。另一方面，你当然不希望将你的数据恢复到勒索软件仍然处于活动状态的系统中。幸运的是，如果恶意软件能够规避安全软件，备份也可以保护你的数据。

## 未来预测

计算机科学家丹尼尔·德尔伯特·麦克拉肯（[Daniel Delbert McCracken](#)）曾说过：“不要对可以在你一生中检查的计算做出预测”。尽管如此，我们仍然可以根据勒索软件的近期演变做出一些推断，以便对其未来的演变提供一些见解。

## 针对性

AIDS 木马的目标非常具体。即便在当时，也没多少人



对研究它的细节感兴趣，用光盘传播木马的成本相对较高，而且赎金支付机制对攻击者没什么好处。（当然，在 1989 年，波普博士没有加密货币或暗黑网络，也没有简单的方法利用西联汇款[419 诈骗者的最爱]或者[裸照获利](#)。）攻击本身是“经典的”勒索软件，因为它导致受害者无法访问数据。之后，DoS 和 DDoS 攻击使得企业无法通过他们提供的服务受益：当客户无法使用这些服务时，服务提供商可能会支付赎金。但是，随着互联网的非企业化、个人化使用不断扩展，攻击面和潜在目标的范围也在扩展。这可能会影响到大多数现代勒索软件的传播。

### 非针对性

当高知名度或高价值的受害者（医疗机构、学术机构、电话服务提供商、互联网服务提供商）被披露后，媒体和安全产品营销人员往往会感到兴奋，但认为这些机构就是攻击目标是不正确的。我们并不总是知道攻击活动的感染途径，因此我们不能说“它永远不会发生！”但是，看起来勒索软件团伙做得相当不错，他们首先攻击大型机构的员工，成功感染员工的帐户后在机构网络中进行横向运动，迫使机构支付大笔赎金。例如，英国医疗服务机构 NHS Digital 否认医疗机构是勒索软件的特定目标——我也这样认为，但它同时



承认医疗机构的网站经常沦为受害者。

### 这种情况会改变吗？

目前，似乎还有企业准备支付相当大笔的赎金。在某些情况下，这是一个合理的“备用战略”，即在技术防御失败的情况下保留支付赎金的选项。在其他情况下，公司可能认为相比于建立复杂的、并不总是有效的防御措施，支付赎金更具成本效益。这可能会吸引犯罪分子攻击“软柿子”公司或有能力支付大笔赎金的公司（金融机构、赌场等）。擦除攻击和即使支付赎金也无法恢复数据的勒索攻击的增加可能会减轻这种不健康的趋势，但是那些不太可能增强防御措施达到最佳效果的企业可能会面临更严重的攻击风险。毕竟，相比于攻击随机用户，攻击大型企业能够获得更多的赎金，且速度更快。

### 数据 vs 设备

对智能手机和其他移动设备的攻击往往不太注重数据，更多的是导致用户无法使用设备和服务。这种情况很糟糕，如果用户不支付赎金，则可能会丢失设置和其他数据，尤其是现在更多的人选择使用移动设备而不是 PC 和笔记本电脑，



这样可能会威胁到更广泛的数据。随着联网设备越来越多，攻击面越来越大，联网设备和传感器嵌入到更多的物品和环境中——从路由器到冰箱到智能电表，从电视到玩具，从发电站到加油站和起搏器。随着所有物品变得越来越“智能”，可能被恶意软件破坏的服务（无论是否要求赎金）的数量也越来越多。在过去的几年中，我们讨论过我的同事 Steff Cobb 所说的“勒索物联网”（[Ransomware of Things](#)）的可能性。到目前为止，相比于所引发的关注，这种威胁的实例远少于预期。然而，这很容易改变，特别是如果更多的传统勒索软件作为赚快钱的手段变得不再那么有效。不过，我并不确定这会很快发生。

另一方面，物联网安全跟不上物联网的发展速度。我们已经看到很多黑客利用物联网的不安全性赚钱。这并不像媒体报道会影响到大量物联网设备的恶意软件那样简单，所以没有理由恐慌，但是我们应该低估网络犯罪分子的坚韧和震惊世界的能力。