Seafile 如何保护数据安全

Seafile 拥有数据同步、分享、协作等优化工作流程的功能外，还可以保护数据免受类似 Locky 软件的劫持。使用 seafile 服务保存的所有库以及文件都存储在其服务器上。用户随时可以通过历史版本号，查看对应的文件。

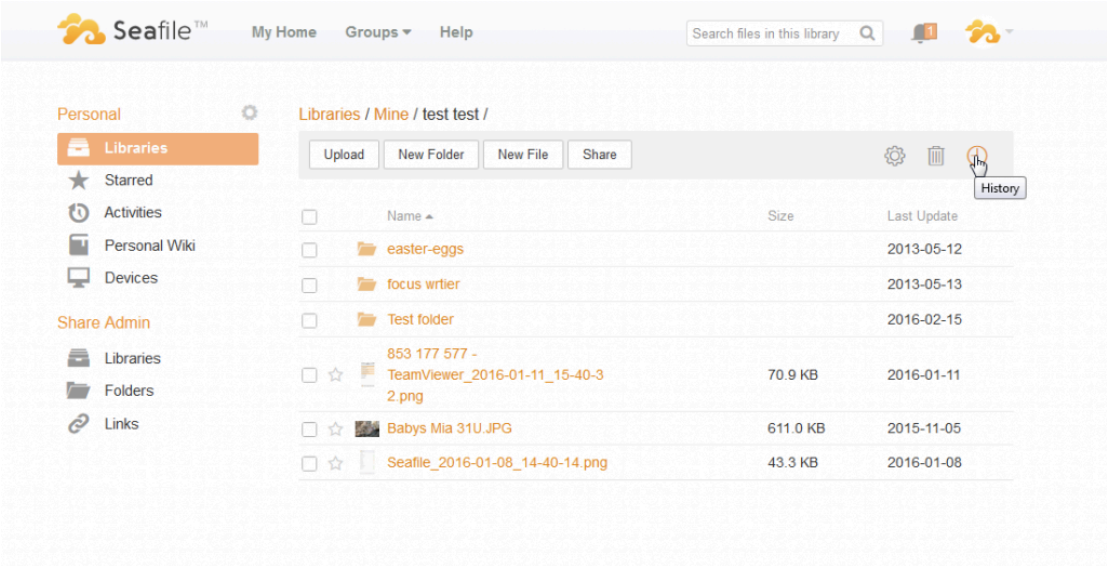
2016 年 2 月，德国好几家医院的 it 系统和德国弗劳恩霍夫研究协会被 Locky 攻击，服务不可用，导致用户像回到无电脑的时代。同样的情况在其它地方也造成了重大的灾难。全世界被计算机病毒感染的机器数量无从得知，但仅在德国，被 locky 攻击的第一个星期后，就有 400000 感染的机器数，并还在以每小时 5000 的数量在增加。粗略估计，大约 20%的垃圾邮件都包含了 Locky 攻击，Locky 传播的越多，感染的机器也越多，这个感染数将是巨大的。同时，Locky 的传播方式也变得越来越有迷惑性，最初只有.zip 文件和恶意宏的文档文件，现在也能通过包含 JavaScript 源码和文本的工具传播。甚至，德国联邦刑事警察办公室发来的邮件（提示含有清除 Locky 的工具）实际也是 Locky 感染源。

那么 Seafile 如何来保护您的数据免于数据劫持呢？您需要在被数据劫持之前就已经使用 Seafile(^_^冷笑话，这是当然的).Seafile 并不解密已被劫持的数据，而是存储了劫持之前的正确数据。这些数据专指存储于 Seafile 服务器的数据。

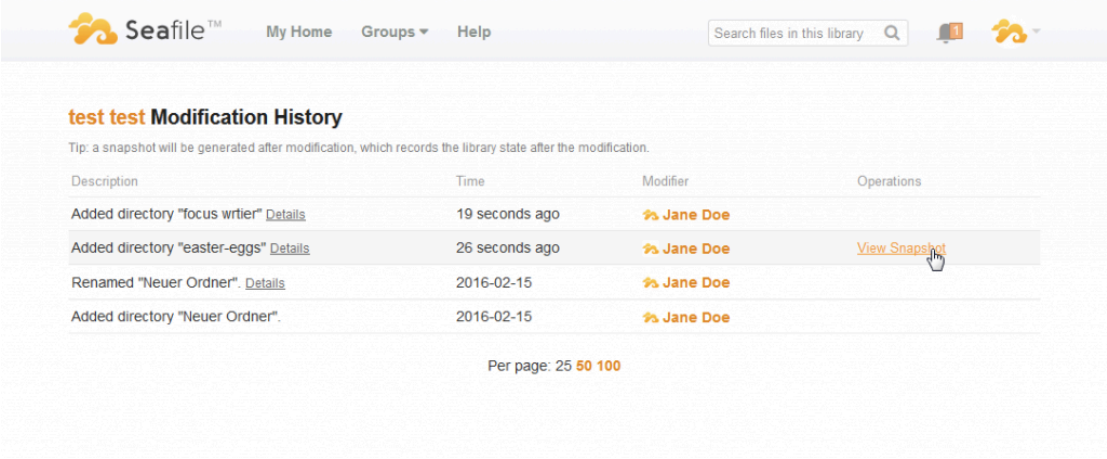
Seafile 会保存所有文件和库的历史。如果一个文件或库改变，Seafile 会将这些改变作为一个新版本来保存（对应单独文件）。在理论上，你可以随时回到 Seafile 文件和库的任何一个版本。因此，如果劫持软件来加密 Seaflie 数据，比如所有文件被重命名为.Locky，Seafile 会将之保存为一个新的版本。您所需要做的，就是将文件恢复到前一个正确版本。

具体操作如下：

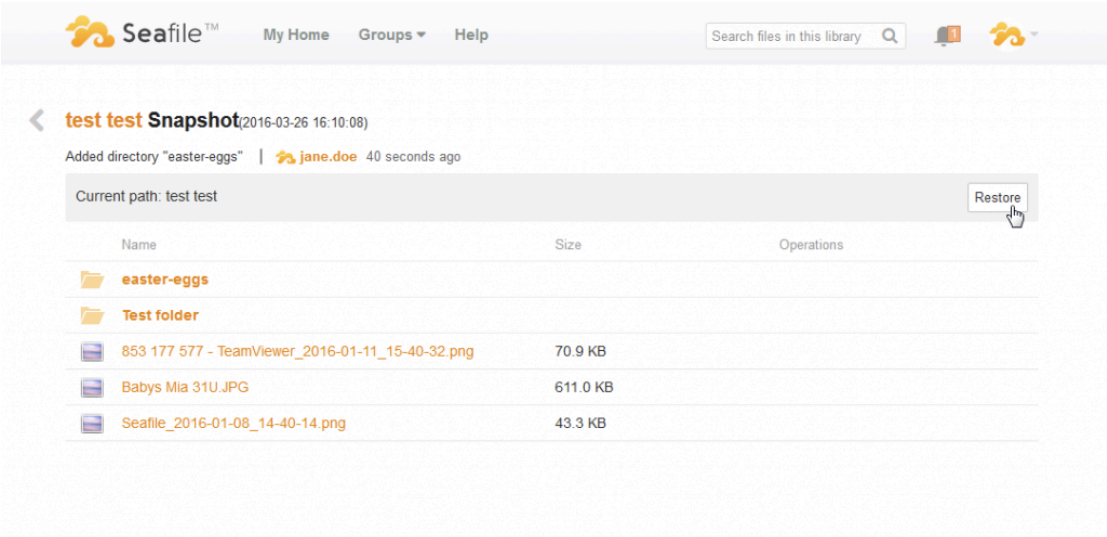
点击 Seafile Web 界面（Seahub）的库名字，然后点击右上方的小钟符号来获取访问库的权限，这样就能看到这个库的所有变更。在每行的右边有“Operation”（操作）部分。



点击“View Snapshot”（查看快照）来访问要恢复的版本。



检查这个库的数据是否正常，如果没有，可以选择一个较早版本的快照。找到需要恢复的快照，点击右上角的“Restore”（恢复）按钮。



所有数据将会恢复完整。