用友遭遇勒索病毒，被要求支付0.2个比特币，提前转账95折

2022年8月28日至29日，用友畅捷通T+大面积遭受勒索病毒攻击，大量用户计算机文件被.locked后缀的勒索病毒加密。被勒索后，需要支付0.2个比特币（目前大概28011.28人民币）。勒索信如下：

此次攻击从 8 月 28 日 21 时 30 分左右开始大规模爆发，一直持续到 8 月 29 日 1 时左右，截至29日晚，360安全大脑观察到有1986台机器遭到攻击，统计地域分布如下：

关于少量畅捷通T+软件客户遭受勒索病毒攻击的说明

今日有报道多家应用软件公司部分客户遭受勒索病毒攻击，我司少量 T+软件客户也反馈受到勒索病毒攻击。

1、经核实该部分客户的软件服务器为客户自有部署方式，且未做必要的网络安全防护。其中，日常按系统提示进行了数据备份的客户已通过恢复备份数据解决，仅有少数客户受到影响，公司已安排技术工程师和服务商积极协助客户解决问题。

2、畅捷通公司运营的公有云客户及应用了安全策略的专属部署方式的客户均安全运行。

3、建议客户升级到畅捷通公司运营的公有云服务或采用畅云管家等具有安全防护措施的云部署方式。

畅捷通公司是用友集团专注小微企业云服务与软件产品研发与服务的子公司，将全力协助客户做好安全防护工作，并保障公有云的安全运行。

畅捷通信息技术股份有限公司

2022.8.29

但依然有不少用户表示事件没有得到解决：

勒索病毒是一种对企业数据安全的常见威胁。当企业核心生产数据被锁，企业就无法在生产环境中打开该文件，业务便无法继续进行。遭遇勒索的企业常因此损失惨重。

面对勒索病毒的通用解决方案，大部分企业想不到

解决方法很简单，只要将备份数据拷贝出来，重装服务器系统和软件，进行重新恢复就好了。这有两个前提，一个是企业提前将数据进行备份，二是企业的备份数据路径不在被勒索的路径中
（在此次事件中，企业备份路径在用友软件里，那就没有办法了）。

在此次事件中，大部分企业都没有提前部署备份容灾，就算进行备份，也是通过用友的技术将备份路径设置到用友。所以当用友软件遭遇攻击时，企业用户毫无还手之力。

数据安全性问题依然经常被忽略。这是因为中小型企业缺乏此类相关技术人员，对于勒索病毒的敏感性不足。如此次事件中，用友的客户企业，主要都是财务相关，对技术和IT并没有经验，自然很难想到预先防范。

HyperBDR云容灾®，保护企业免受勒索病毒侵扰

提到备份容灾，大部分企业会不由自主地想到传统备份容灾，被繁琐的步骤和庞大的成本劝退。

现在，无论什么企业，都可以利用HyperBDR云容灾®进行云上业务部署。企业可以根据自身需求，在任意云端部署一套完全独立于源端路径的备份容灾体系。

利用HyperBDR云容灾®将数据通过对象存储的方式备份至云端，一年1GB仅需约一元人民币的存储价格。如，将财务系统备份容灾至云端，无灾难时仅做备份，500GB的文件，一年仅需支付500元的存储费用。

当灾难发生时，HyperBDR云容灾®独有的Boot in Cloud®技术可帮助企业一键拉起业务到可用状态，无需手动重装服务器系统和软件，帮企业快速恢复业务连续性，免于遭受损失。

HyperBDR云容灾®采用SaaS化部署，只需三步即可完成容灾部署。无专业备份容灾相关的IT知识或技能，也能轻松完成部署。