勒索病毒防护（二）


勒索病毒
防护知识系列
勒索病毒攻击流程
NO.01
探测侦察阶段
① 收集基础信息
攻击者利用弱口令、远程代码执行等网络产品安全漏洞，攻击入侵用户内部网络，获取管理员权限，进而主动传播勒索病毒。目前，攻击者通常利用已公开且已发布补丁的漏洞，通过扫描发现未及时修补漏洞的设备，利用漏洞攻击入侵并部署勒索病毒，实施勒索行为。

② 发现攻击入口

攻击者通过漏洞扫描、网络嗅探等方式，发现攻击目标网络和系统存在的安全隐患，形成网络攻击的突破口。此外，攻击者同样可以利用网站挂马、钓鱼邮件等方式传播勒索病毒。

NO.02 攻击入侵阶段

① 部署攻击资源

根据发现的web应用漏洞、系统漏洞、远程桌面弱口令等问题，在向系统突破口部署响应的攻击资源，例如MetaSploit、CobaltStrike管理工具或FRP等隧道代理工具。

② 获取访问权限

采用合适的网络攻击工具，通过软件供应链攻击、远程桌面入侵等方式，获取攻击目标网络和系统的访问权限，并通过使用特权账户、修改域策略设置等方式提升自身权限，攻击入侵组织内部网络。

NO.03 病毒植入阶段

① 植入勒索病毒

攻击者通过恶意脚本、动态链接库DLL等部署勒索病毒，并劫持系统执行流程、修改注册表、混淆文件信息等方式规避安全软件检测功能，确保勒索病毒成功植入并发挥作用。

② 扩大感染范围

攻击者在已经入侵内部网络的情况下，通过实施内部鱼叉式网络钓鱼、利用文件共享协议等方式在攻击目标内部网络横向移动，或利用勒索病毒本身类蠕虫的功能，进一步扩大勒索病毒感染范围和攻击影响。

NO.04 实施勒索阶段

① 加密窃取数据

攻击者通过运行勒索病毒，加密图像、视频、音频、文本等文件以及关键系统文件、磁盘引导记录等，同时根据攻击目标类型，回传发现的敏感、重要的文件和数据，便于对攻击目标进行勒索。

② 加载勒索信息

攻击者通过加载勒索信息，胁迫攻击目标支付勒索赎金。通常勒索信息包括通过暗网论坛与攻击者的联系方式、以加密货币支付赎金的钱包地址、支付赎金获取解密工具的方式等。

勒索病毒处置措施

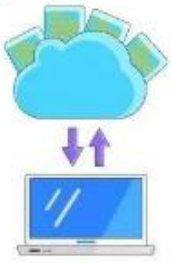
NO.01 物理隔离

物理隔离被感染主机，最好是直接拔网线，云环境及时修改安全组策略，将被感染的机器隔离，确保被感染的机器不能和内网其他机器通信，防止内网感染，如果被勒索的机器和未被勒索的机器存在相同的登陆口令，及时修改未感染机器的登陆口令。

NO.02 防止扩散

保障被感染主机，与内网其他主机进行隔离。及时关闭未感染机器远程桌面、共享端口，例如22、135、139、445、3389、3306、1521等高危端口。

NO.03 及时备份



对于未感染的机器进行备份，备份后及时物理隔离开备份数据，如：硬盘或者u盘备份后需要及时拔掉。

NO.04 排查业务系统

在已经隔离被感染主机后，应对局域网内的其他机器进行排查，检查核心业务系统是否受到影响，生产线是否受到影响，并检查备份系统是否被加密等，以确定感染的范围。

NO.05 不要轻易联系黑客

在不了解勒索病毒的情况下，不要直接联系黑客，容易钱财两空。

NO.06 不要破坏被勒索的服务器环境

对于十分重要、无备份且不能恢复的机器，应禁止杀毒、关机、重启、修改后缀等操作，最好保持原封不动，在不了解的情况下，任何动作都可能导致数据永远无法恢复。应尽快联系专门的安全公司及数据恢复公司进行处理。

对于有备份，或者实在不能恢复的机器，最好重装系统，或者将业务迁移到其他服务器上。

内容来源：智慧通大