

勒索病毒的预防与处置建议

构建防御：防止勒索软件进入系统

与任何形式的在线网络攻击一样，保护入口是关键。以下是防止勒索软件感染企业网络的安全措施列表。

（1）定期备份数据

备份重要文件可将潜在损害降至最低，良好的备份策略可确保所有关键数据保存在安全的位置，以便组织能够在数据丢失的情况下轻松恢复。

（2）部署和实施白名单式的终端防护措施，加强应用程序控制

应用程序控制仅允许在系统上运行非恶意程序。该项措施需要 IT 管理员确定允许哪些应用程序在组织的网络中运行和操作。

（3）正确的实施网络分段和网络安全域的划分

通过策略性地针对资产和资源进行分组，划分安全域。正确的网络分段可以防止攻击时整个网络陷入瘫痪。对于用户的权限设置要遵循最小权限原则，使得犯罪分子更难获得管理权限。

（4）教育用户识别有关社会工程学攻击的危险和标志

为用户提供良好的电子邮件和互联网安全实践培训，例如下载附件、点击网址或仅从受信任的来源执行程序。

（5）及时应用操作系统和第三方供应商提供的软件补丁

未经修补的应用程序和服务器常会被用作将恶意软件（如勒索软件）推入系统的入口。为了解决这个问题，应定期修补和更新软件，仔细检查修补过程，以确定隐患得以消除。

（6）确保安全软件定期更新并执行定期扫描

无论组织为保护网络而构建的防御有多强，网络罪犯只要找到一个破绽即可进入，所以确保所有安全防护产品及时更新并执行定期扫描也同样重要。

中断损伤：检测和阻止破坏产生

从意外点击恶意链接或将受感染文件下载到本地计算机，到显示赎金提示这整个过程可能会在几分钟之内完成。这段时间至关重要，如果在这期

间能够及时检测和阻断勒索软件，就可以将其造成的损害降至最低。以下是一些需要注意的事项。

（1）从网络中识别并隔离受感染的主机

虽然勒索软件行为因为变种和家族不同而不尽相同，但它们都要完成如：建立与 C&C 服务器通信的重要过程，应尽早识别这一行为并将该行为阻断。

当出现异常行为的警报时，IT 管理员应尽快采取行动，尽可能隔离受感染的主机。一旦识别出失陷主机，应立即断开该主机的网络连接，以防止感染到其他主机。

（2）建立实时事件响应小组

实时事件响应小组将监视组织中系统的活动，并接收网络中用户报告的异常通知。虽然用户警报可能意味着加密过程已经开始，但响应小组可以对事件进行控制并防止感染扩散。

（3）鼓励用户向 IT 安全团队报告任何异常的系统行为

IT 管理员应主动教育企业和组织中的网络用户，对所有可能感染的迹象保持警惕。在勒索软件感染过程中，有一些隐藏的物理迹象可以在其完全执行之前显现出来，比如系统运行速度明显减慢说明后台发生了额外的进程，意识到这些迹象可以使 IT 响应团队有足够的时间控制情况。

灾难恢复：从感染中恢复

以下是感染后可参考的处理措施：

（1）查找可用的解密工具

虽然并不是所有的勒索软件加密之后都能够进行解密，比如像 Locky 家族。但还是有很多类型的勒索软件由于在设计和编码过程中出现的缺陷导致其很容易被破解。

为了帮助大家找到一个恢复数据的解决方案，而不需要向勒索软件的创建者支付赎金，我们收集并整理了大量的勒索软件解密工具，可在启明星辰集团 VenusEye 威胁情报中心的勒索病毒专题 <https://lesuo.venuseye.com.cn> 界面搜索病毒名下载工具。

以“微信支付”勒索病毒为例：

VenusEye勒索病毒搜索引擎

超300种勒索病毒家族

输入病毒名、被加密文件名或，或上传被加密文件、勒索提示文件，即可找到解密方法。了解病毒详情

微信支付 文件上传

病毒家族: [勒索支付](#) [已有解密工具](#) [了解病毒详情](#)

查

天镜扫描

防

- 星云防病毒
- 天穹ISM

补

- 建立应急响应流程和预案

检

天阙APT
天玥审计

情报连接 · 赋能安全

安全咨询

以下是由启明星辰应急响应中心VSR、启明星辰初级防御实验室AdLab发布的勒索病毒相关资讯

<

原创



GlobeImposter 2.0勒索攻击预警

VSR

原创



Xbash勒索引擎事件预警

VSR

原创



爱马仕勒索病毒案例

VSR

原创



GlobeImposter勒索样本分析报告

VSR

原创



安全预警利用Redis隧道的攻击勒索

VSR

>

启明星辰威胁情报中心

病毒详情

病毒名称: 微信支付

该病毒目前已提供解密工具, 您可以下载工具尝试解密!

基础信息 截图 解密工具 解决建议 预防措施 关联情报

基础信息

病毒别名: 微信支付 UNNAMLD1969

加密文件后缀:

截图



解密工具

本网站提供的解密工具主要来自于第三方安全厂商, 其安全性已经过验证, 但不保证其对现在或将来的勒索病毒变种都有效, 使用前请务必做好相关文件的备份工作, 并根据实际情况酌情选择!

工具下载: [立即下载](#)

解决建议

1. 隔离机器: 确认机器已感染勒索病毒后, 应断将其断网, 或断电, 切断其与内网其他机器的网络通信, 避免勒索病毒感染其他机器。
2. 全盘杀毒: 使用可靠的杀毒软件全盘扫描, 清除勒索病毒。避免出现二次加密。
3. 解密工具: 可以使用本站提供的第三方解密工具尝试解密, 不过解密工具通常对较新版本的勒索病毒无效。
4. 备份恢复: 如果事先已对关键文件做了备份, 在确保已清除病毒情况下可做数据备份恢复。如果卷影备份未被勒索病毒删除, 可通过卷影备份将系统恢复到未感染勒索病毒的时间点。
5. 专业代付: 不建议向勒索病毒创建者支付赎金。万不得已的情况下, 建议找专业安全团队代付, 以避免出现二次勒索。

预防措施

1. 打补丁: 及时给系统打补丁, 修复漏洞。
2. 装杀软: 安装杀毒软件, 及时更新病毒库。开启防火墙, 并升级到最新版本, 阻止勒索病毒与其C&C服务器通信。
3. 做备份: 定期对重要文件以及数据库做非本地备份。电脑开启系统备份, 并添加保护 (这样可通过卷影备份将系统恢复到被加密之前的状态)。
4. 备份恢复: 如果事先已对关键文件做了备份, 在确保已清除病毒情况下可做数据备份恢复。如果卷影备份未被勒索病毒删除, 可通过卷影备份将系统恢复到未感染勒索病毒的时间点。
5. 改密码: 使用长度大于10位的复杂密码。
6. 加限制: 禁用GUEST来宾用户, 尽量不要使用局域网共享, 或把共享磁盘设置为只读属性, 不允许局域网用户改写文件。尽量关闭不必要的端口, 如: 445、135、139、3389、5900。
7. 防钓鱼: 不要点击来源不明的邮件以及附件, 钓鱼邮件是勒索病毒的重要传播源。

关联情报

<https://mp.weixin.qq.com/s/rFw2eXFAUeo1JR2u7hNeA>

https://mp.weixin.qq.com/s/soOjCXtoMyyXmr0AUw_9g

在使用这些工具之前, 建议先了解这些工具的工作原理, 以确保找到最适合您的解决方案。另外, 请注意, 解密器可能会因为勒索软件的更新而过时, 强烈建议大家除了做好必要的防御措施外, 还需要加强对重要数据进行备份。

感染勒索软件后，赎金窗口一般会说明文件被哪种类型的勒索软件加密了，但有时候也可能没有这方面的提示信息，

（2）实施全面的数据备份和恢复计划

开发全面的备份和恢复计划，可确保组织的重要数据即使在数据丢失时也是完整的（不限于勒索软件感染），通过实施计划组织将能够轻松地恢复正常运作并恢复运营。

（3）进行事件后的感染分析

勒索攻击事件发生之后，我们需要针对事件进行详细的分析，比如对感染的深度和广度进行调查。更重要的是要分析受感染用户是通过什么方式感染的，以确定应该从哪些方面入手对问题进行解决，防止类似的事件再次发生。另外也要对勒索软件行为进行分析，确定勒索软件攻击的指示器，并将这些分析结果用于改进检测防范和防御方法，提升整体安全防护能力。