# 有关于“云电脑严重安全问题”的通知

紧急程度：极高

发布日期：2026 年 1 月 11 日
适用对象：所有个人用户

# 概述

据用户于 2026 年 1 月 10 日报告，在使用时，计算机出现了用户密码被改的情况。经管理员重置密码后，用户端出现了加密文件性的勒索软件（图见附件 1），但管理员端未出现问题。文件后缀均被（除 exe、dll、lnk 等系统文件）改为“.WMAN”格式,经过解码软件检查，文件内容均已被修改和加密。据系统记录，发作时间为 2026 年 1 月 5 日下午七时。

据管理员检查，暂未找到病毒源程序，目前找到的疑似病毒源程序“51 吃瓜”未在云沙箱和本地实体机中展现病毒发作的现象和在 360、火绒安全等安全软件下没有检测出病毒，但该软件及其目录下的扩展文件均未被感染。

# 处理方法

我方已经发布和制作了更新版远程系统，并已将软件更新为最新版本，用户应立即联系人工客服进行系统更新和迁移。

我方管理员尝试恢复被加密的数据，但 360 查杀、360 解密、360 电脑急救箱均未找到解决办法，目前正在调查。

目前病毒情况正在进一步调查中。且未在互联网上找到类似的解决办法。

目前我方建议已经感染的用户立刻断开中毒计算机的网络连接和电源连接，待处理方法被发现后进行处理。

# 病毒性质

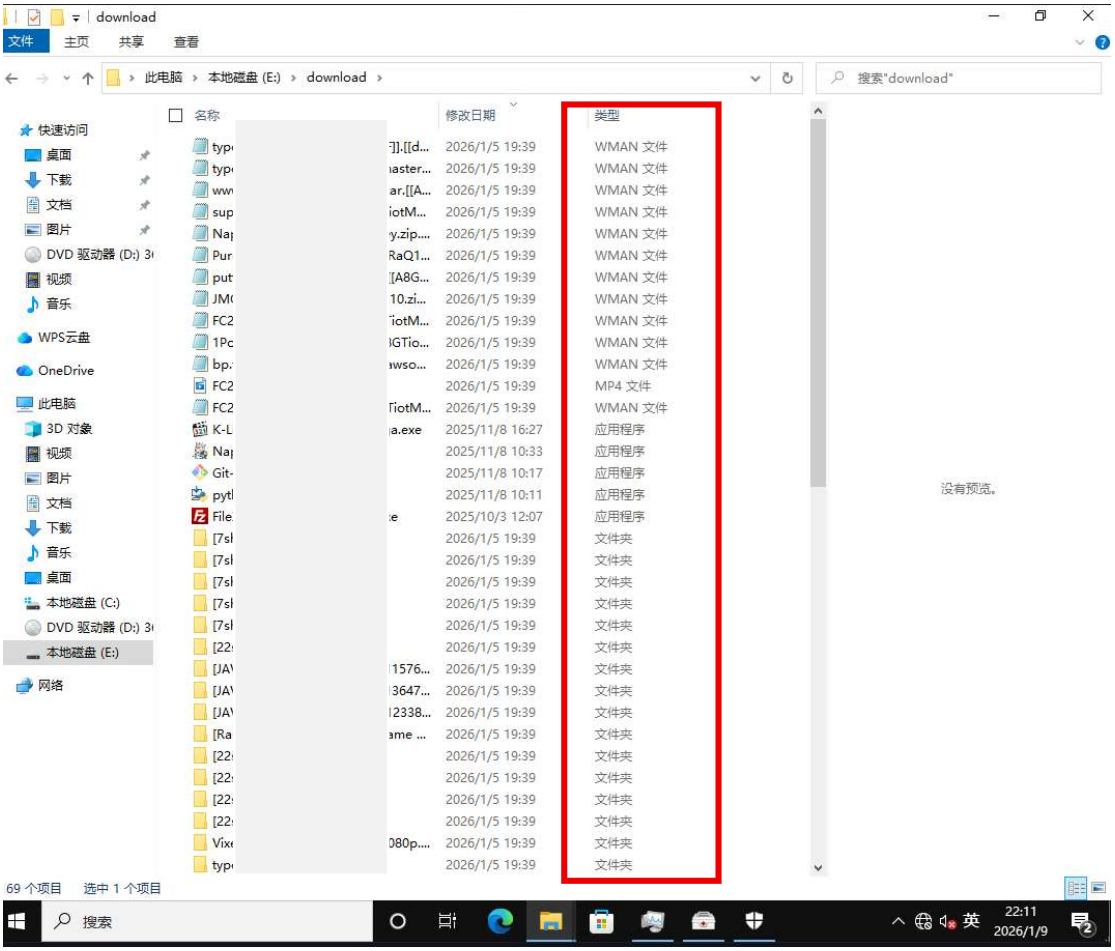
传播：据目前样本所观察，该病毒未有过高的威胁性，暂未找到有关于互联网传播的情况。

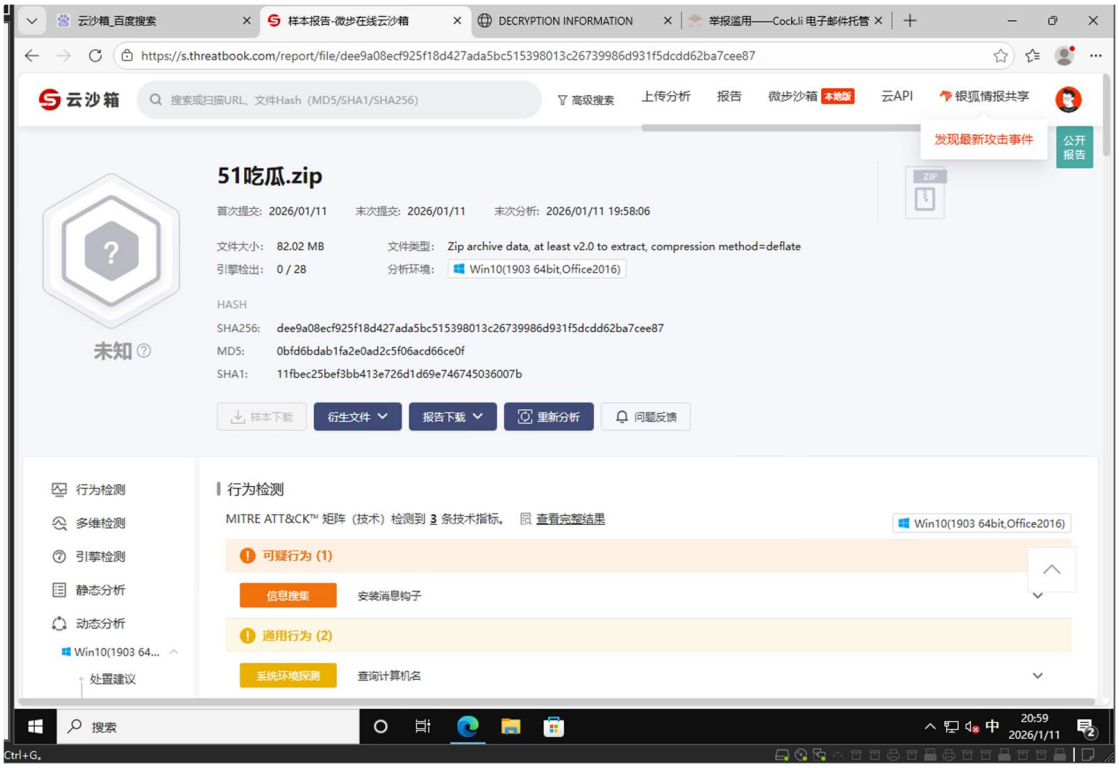
加密性：就目前所看，该病毒只加密了设有初始密码的“User”（即用户使用的账户），但远程端无法连接的“Admin”(即管理员使用的账户)未被病毒所感染。

据以上推测，该病毒是只感染个人用户的一种广泛的勒索性质的软件。

# 附件 1


你的电脑被加密了!
解密请联系我们: dawsones@cock.li
联系我们时，请务必在邮件头部注明此标识符: A8GTiotMRaQ1F
1. 发生了什么?
由于安全漏洞，您电脑上的所有文件都被加密，文件结构未受损，我们已尽一切可能防止这种情况发生。
2. 我该如何找回我的档案?
如果您想恢复文件，您需要通过写信 dawsones@cock.li 来支付我们的工作费用，并讨论交易价格。
3. 我该如何支付?
我们只接受比特币加密货币支付，如果您不知道如何自行补充比特币，您所在国家有许多中介机构随时准备为您提供帮助。
4. 文件恢复的速度有多快?
解密速度取决于您与我们的联系速度以及我们能多快就价格达成一致。
5. 文件恢复保证
如果您不尝试自行解密，我们保证您所有文件都会归还。
crypted!
r our work by writing
to us at and discussing the price of the transaction.


download
文件 主页 共享 查看
此电脑 › 本地磁盘 (E:) › download ›
搜索"download"
名称
修改日期
类型
没有预览。
69 个项目 选中 1 个项目
搜索
英
22:11
2026/1/9


云沙箱_百度搜索
样本报告-微步在线云沙箱
DECRYPTION INFORMATION
举报滥用——Cock.li 电子邮件托管
https://s.threatbook.com/report/file/dee9a08ecf925f18d427ada5bc515398013c26739986d931f5dcdd62ba7cee87
云沙箱
搜索或扫描URL、文件Hash（MD5/SHA1/SHA256）
高级搜索
上传分析
报告
微步沙箱 本地版
云API
根狐情报共享
发现最新攻击事件
公开报告
51吃瓜.zip
首次提交: 2026/01/11
末次提交: 2026/01/11
末次分析: 2026/01/11 19:58:06
文件大小: 82.02 MB
文件类型: Zip archive data, at least v2.0 to extract, compression method=deflate
引擎检出: 0 / 28
分析环境: Win10(1903 64bit,Office2016)
HASH
SHA256: dee9a08ecf925f18d427ada5bc515398013c26739986d931f5dcdd62ba7cee87
MD5: 0bfd6bdab1fa2e0ad2c5f06acd66ce0f
SHA1: 11fbec25bef3bb413e726d1d69e746745036007b
未知
样本下载
衍生文件
报告下载
重新分析
问题反馈
行为检测
多维检测
引擎检测
静态分析
动态分析
Win10(1903 64...
处置建议
行为检测
MITRE ATT&CK™ 矩阵（技术）检测到 3 条技术指标。
查看完整结果
Win10(1903 64bit,Office2016)
可疑行为 (1)
信息搜集
安装消息钩子
通用行为 (2)
系统环境探测
查询计算机名
搜索
20:59
2026/1/11
Ctrl+G。