



网络安全预警通报

2026 年第 10 期（总第 68 期）

西安交通大学网络信息中心 2026 年 10 月 28 日

【预警类型】严重预警

【预警内容】

Weaxor 勒索病毒攻击风险预警通报

一、病毒概述

近日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室依托国家计算机病毒协同分析平台，在我国境内发现多起用户遭遇 “Weaxor” 勒索病毒攻击事件。受害用户的重要文件被加密，文件名被修改并添加 “.weax” 等后缀，攻击者同时在受害主机上留下勒索信，要求用户与其联系并支付赎金。

根据公开披露的信息，“Weaxor” 勒索病毒本身不具备主动传播功能，网络犯罪分子通常先利用弱口令、系统或软件漏洞等方式入侵目标服务器，再通过 PowerShell 脚本、远程控制工具等手段向目标内网投送勒索病毒，实施文件加密和勒索。由于攻击者可能在获得服务器访问权限后手动或自动部署恶意程序，相关攻击具有一定的隐

蔽性，需重点关注互联网暴露资产、远程管理服务及重要业务系统的安全防护情况。

该勒索病毒具备以下特点：

（1）影响操作系统范围广：“Weaxor”具有多个变种，可针对 Windows 和 Linux 等不同操作系统平台投送相应的恶意程序，可能影响个人终端、业务服务器及企业内部信息系统。

（2）攻击入口具有多样性：攻击者主要通过弱口令、系统或软件漏洞等途径入侵目标服务器，并借助 PowerShell 脚本、远程控制工具等方式部署勒索程序，增加了攻击路径排查和溯源难度。

（3）加密文件类型广泛：病毒可对受害主机上的重要文件实施加密，影响数据库文件、办公文档及其他业务数据。根据病毒版本不同，被加密文件可能被添加 “.rox”、“.weax”、“.wxx”、“.wxr”、“.weaxor”、“.roxaew”、“.wax” 等后缀。

（4）采用多层加密机制：根据公开分析，“Weaxor”采用椭圆曲线加密、AES 及 ChaCha20 等密码算法构建文件加密机制，可能显著增加受害者自行恢复数据的难度。

（5）勒索目的明确，业务影响严重：攻击者在受害主机上留下勒索信，要求受害者联系并支付赎金。攻击成功后，可能导致重要业务数据无法访问、业务系统中断，严重时影响单位正常运行。

二、病毒详情

1.技术原理

“Weaxor”勒索病毒主要通过先入侵、后投送的方式实施攻击。攻击者通常不会依靠病毒自身进行主动传播，而是利用目标系统的安全薄弱环节获取访问权限，再部署勒索程序，对目标主机上的重要文件进行加密。

此外，攻击者在部署勒索病毒之前可能已获取目标系统的访问权限，因此即使发现文件加密行为，也应进一步排查此前是否存在异常登录、可疑进程、远程控制工具运行及异常脚本执行等情况，避免仅清除勒索程序而遗漏其他攻击痕迹。

2.涉及病毒详情

病毒名称：Weaxor 勒索病毒

病毒类型：勒索病毒、文件加密恶意软件

威胁等级：严重

影响平台：Windows、Linux 等操作系统

主要攻击目标：企业数据库、OA 办公系统、业务服务器及个人终端

主要入侵方式：弱口令、系统或软件漏洞利用、远程访问服务入侵

主要投送方式：PowerShell 脚本、远程控制工具及其他自动或手动投送方式

加密特征：对受害主机上的重要文件进行加密，并根据病毒版本修改文件后缀

常见文件后缀：.rox、.weax、.wxx、.wxr、.weaxor、.roxaew、.wax 等

勒索行为：在受害主机上留下勒索信，要求受害者联系攻击者并支付赎金

病毒描述：“Weaxor”勒索病毒具有多个版本，攻击者可根据目标操作系统选择相应恶意程序。攻击者通常先利用弱口令或系统、软件漏洞入侵服务器，再通过脚本或远程控制工具投送勒索程序。病毒运行后对目标文件实施加密，并通过修改文件后缀及留下勒索信等方式实施勒索。

需要注意的是，不同版本的“Weaxor”勒索病毒在文件后缀、运行行为及具体加密流程等方面可能存在差异。文件后缀异常可作为排查线索，但不能仅凭后缀判断是否感染，也不能因未发现上述后缀就排除勒索病毒风险。

3、主要识别特征

根据公开披露的信息，发现以下情况时应提高警惕：

(1) 重要文件被批量修改文件名，文件名末尾出现“.weax”、“.rox”、“.wxx”、“.wxr”、“.weaxor”、“.roxaew”或“.wax”等异常后缀。

(2) 服务器或终端出现勒索信、异常文本文件，要求受害者与攻击者联系并支付赎金。

(3) 数据库、OA 办公系统或业务服务器上的大量文件突然无法打开，出现集中加密、文件内容异常或业务数据不可用等现象。

(4) 系统中出现来源不明的 PowerShell 脚本、异常远程控制工具、可疑进程或未经授权的程序执行行为。

(5) 服务器存在异常登录、远程访问记录、可疑账号活动或系统、软件漏洞长期未修复等情况。

国家计算机病毒应急处理中心相关平台：

<https://virus.cverc.org.cn>

三、漏洞影响范围

1. 影响范围

目前确认风险主要涉及：

- 使用 Windows 操作系统的个人计算机、办公终端及业务服务器；
- 使用 Ubuntu Linux 等 Linux 发行版的服务器及业务系统；
- 部署企业数据库、OA 办公系统及其他关键业务应用的主机；
- 开放远程登录、远程管理或其他互联网访问服务的服务器；
- 存在弱口令、默认口令、过期账号或身份认证配置不当问题的系统；
- 存在未修复系统漏洞、应用软件漏洞或其他安全缺陷的服务器；
- 通过 PowerShell 脚本、远程控制工具等方式进行日常管理或运维的主机；
- 存储重要业务数据、科研数据、办公文档及数据库备份的终端和服务器；
- 未建立有效离线备份机制、备份数据与生产系统缺乏隔离的业务系统。

需要注意的是，“Weaxor”勒索病毒主要通过攻击者入侵后投送的方式实施攻击，不能仅依靠终端杀毒软件或文件后缀检测判断系统是否安全。

对于互联网暴露资产、远程管理入口、数据库及 OA 办公系统，应重点排查弱口令、漏洞修复、异常登录和可疑程序执行等风险，并核查备份数据是否能够正常恢复。

2. 威胁严重性

攻击成功后，可能造成以下安全影响：

(1) 重要业务数据被加密

攻击者利用勒索病毒对主机上的重要文件实施加密，可能导致办公文档、数据库文件、科研资料及其他业务数据无法正常访问，影响业务连续性。

(2) 业务系统中断

当数据库、OA 办公系统及其他关键业务服务器遭到攻击时，可能导致业务应用无法启动、数据查询失败、办公流程中断或相关服务不可用，影响单位正常教学、科研和管理工作。

(3) 数据恢复成本增加

若受害主机缺乏有效备份，或备份数据与生产环境同时受到影响，可能需要投入大量时间和资源开展系统重建、数据恢复及安全排查。部分被加密文件可能无法通过常规方式恢复。

(4) 服务器及内部网络安全受到威胁

攻击者在投送勒索病毒前通常已获取目标系统的访问权限。如果未及时排查入侵来源、清除恶意程序并修复安全缺陷，攻击者可能继续利用残留账号、远程控制工具或其他持久化机制访问目标系统，扩大安全事件影响范围。

(5) 重要信息及业务连续性面临风险

勒索病毒攻击可能影响重要业务数据的完整性与可用性，并增加业务恢复、事件处置及系统重建的工作量。对于承担重要教学、科研和管理任务的系统，相关影响可能进一步扩展至多个业务环节。

四、处置建议

1.加强系统安全防护：定期排查服务器、数据库及 OA 办公系统的安全风险，及时修复操作系统和应用程序漏洞，清理弱口令及无效账号，严格限制远程管理服务的访问权限。

2.做好重要数据备份：定期备份重要业务数据及系统文件，备份数据应与生产环境有效隔离，并定期开展数据恢复测试，降低勒索病毒造成的数据损失。

3.加强病毒检测与监测：及时更新终端安全防护软件及病毒库，重点关注异常文件加密、文件后缀批量变化、异常脚本执行及可疑远程登录等行为。可通过国家计算机病毒协同分析平台对可疑文件进行检测。

4.及时开展应急处置：发现疑似感染勒索病毒时，应立即隔离受影响主机，保留相关日志及现场证据，排查入侵途径并修复安全缺陷。未经专业评估，不建议直接支付赎金或使用来源不明的解密工具。