姓名: _____ 日期: _____ 得分: _____

勒索软件攻击与业务恢复

载荷执行、文件加密、离线备份、遏制程序和灾难恢复。

勒索软件攻击学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解勒索软件攻击与业务恢复。你将探索载荷执行、文件加密、离线备份、威胁遏制、加密货币支付和灾难恢复计划。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

URL: https://www.vpn.com/cybersecurity/ransomware-attack/

你的勒索软件恢复学习路线图

- 区分木马、勒索软件和间谍软件载荷。
- 在安全的沙盒环境中分析恶意文件。
- 制定快速的网络隔离与遏制流程。

勒索软件攻击指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于勒索软件恢复。最后完成附加活动: 快速思考。

勒索软件攻击与灾难恢复（简介）

勒索软件载荷会以加密方式锁定系统存储，并要求以加密货币支付解密密钥的费用。缓解这一威胁的方法包括网络隔离规则、沙箱化的恶意软件分析以及可靠的物理隔离冷备份。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 勒索软件攻击的主要机制是什么?
   - A. 对用户文件进行加密以拒绝系统访问
   - B. 向表单字段中注入恶意 SQL 命令
   - C. 在公共 Wi-Fi 连接上嗅探网络数据包
   - D. 伪造电子邮件头以绕过 SPF 验证

2. 2. 什么是离线（冷）备份?
   - A. 与网络断开连接的存储副本，以防止恶意软件传播
   - B. 存放在主 Web 服务器硬盘上的备份
   - C. 系统注册表日志的临时缓存
   - D. 用于重置用户密码的管理工具

3. 3. 在勒索软件攻击期间，安全团队应如何隔离受感染的系统?
   - A. 立即断开网线并禁用无线接口
   - B. 升级防病毒特征库
   - C. 关闭主 DNS 服务器
   - D. 重命名被入侵的文件扩展名

4. 4. 安全机构为什么建议不要支付勒索软件的赎金?
   - A. 支付赎金会助长攻击者，且不能保证交付解密密钥
   - B. 它会自动使所有企业保险单失效
   - C. 它自动通过电子邮件通知每一位客户
   - D. 它破坏剩余的系统备份文件

5. 5. 什么是灾难恢复计划（DRP）?
   - A. 系统被入侵后恢复运营和数据的结构化流程
   - B. 映射入站网络端口的防火墙配置
   - C. 列出用户管理权限的数据库架构
   - D. 一种拒绝伪造域名的电子邮件认证协议

检查点 2: 判断正误挑战

6 问题 6

6. 勒索软件载荷很容易传播到连接在网络上的在线备份。

○ 正确 ○ 错误

7 问题 7

7. 支付加密货币赎金能保证文件被成功解密。

○ 正确 ○ 错误

8 问题 8

8. 将受感染的系统与网络断开有助于阻止勒索软件扩散到相邻系统。

○ 正确 ○ 错误

9 问题 9

9. 勒索软件从不使用对称加密来加密系统存储。

○ 正确 ○ 错误

10 问题 10

10. 定期测试数据恢复流程是灾难恢复的关键组成部分。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 拒绝对本地文件的访问使用的是密码学 _____ 。
2. 在系统上执行的活跃恶意代码是 _____ 。
3. 断开连接的异地存储副本属于安全的 _____ 。
4. 阻止恶意软件扩散需要对终端网络进行 _____ 。
5. 网络犯罪分子索要的加密货币付款称为 _____ 。
6. 把可用的运行数据文件还原回来，属于灾难 _____ 。

词汇词库

恶意软件　恶意载荷　隔离　恢复　加密　冷备份　木马　赎金

在此写下你的答案:

1.
2.
3.
4.
5.
6.

检查点 4: 安全概念配对

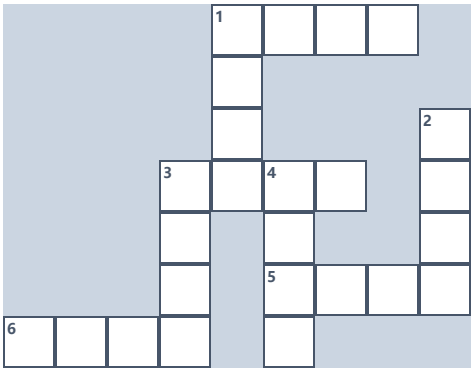
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. 加密	**A**	断开受感染的网络系统。
	2. 有效载荷	**B**	伪装成干净文件的恶意文件。（H）
	3. 冷备份	**C**	对文件进行加密锁定。（A）
	4. 隔离	**D**	重大系统中断事件。（G）
	5. 赎金	**E**	执行恶意软件。
	6. 恢复	**F**	已断开连接的离线副本。
	7. 灾难	**G**	从备份中恢复数据库。
	8. 木马	**H**	加密密钥付款请求。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

1. 执行恶意软件 (4)

3. 用密码学方式锁定文件 (4)

5. 加密受害者文件并索要赎金的恶意程序 (4)

6. 从备份中还原数据库 (4)

纵向

1. 旨在破坏系统或窃取数据的有害程序 (4)

2. 重大的系统中断事件 (4)

3. 把丢失或被加密的文件找回来 (4)

4. 对受害者文件加密并索要钱财才肯解锁 (4)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

1 横向: 执行恶意软件 (4 字):

3 横向: 用密码学方式锁定文件 (4 字):

5 横向: 加密受害者文件并索要赎金的恶意程序 (4 字):

6 横向: 从备份中还原数据库 (4 字):

纵向

1 纵向: 旨在破坏系统或窃取数据的有害程序 (4 字):

2 纵向: 重大的系统中断事件 (4 字):

3 纵向: 把丢失或被加密的文件找回来 (4 字):

4 纵向: 对受害者文件加密并索要钱财才肯解锁 (4 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 域 道 安 息 恶 用 连 意 隧 灾 共 器 认 统
系 议 隐 件 墙 全 隧 服 文 安 传 协 系 连 复
务 荷 器 安 风 连 问 共 份 件 信 攻 信 件 名
务 载 数 输 恢 络 隐 域 览 地 恢 访 恢 攻 输
文 意 安 备 名 文 器 名 索 证 事 复 件 载 保
软 恶 墙 密 传 件 问 勒 保 风 管 证 件 载 设
攻 密 道 公 共 加 用 火 索 址 数 网 数 加 系
荷 火 名 荷 防 密 载 隧 协 软 务 备 证 域 务
件 问 风 份 议 设 软 隐 身 身 件 设 理 公 道
事 隧 隐 加 公 件 攻 访 传 据 恶 务 共 事 记
难 恶 意 软 件 加 恢 恶 保 议 连 复 服 份 数
灾 务 管 索 加 软 加 浏 数 网 复 险 务 据 防
络 务 攻 务 密 信 私 问 服 理 备 证 恢 用 问
传 恢 公 信 勒 备 录 户 络 络 管 复 系 份 软
道 载 设 名 索 传 道 输 码 份 难 数 保 传 索

词汇列表

文件加密 **恶意软件** **加密勒索** **勒索软件** **恶意载荷** **灾难事件** **文件恢复** **数据恢复**

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 文件加密
B. 恶意软件
C. 加密勒索
D. 勒索软件
E. 恶意载荷
F. 灾难事件
G. 文件恢复
H. 数据恢复

定义与配对字段
1. 对受害者文件加密并索要钱财才肯解锁。
2. 从备份中还原数据库。
3. 用密码学方式锁定文件。
4. 执行恶意软件。
5. 加密受害者文件并索要赎金的恶意程序。
6. 把丢失或被加密的文件找回来。
7. 旨在破坏系统或窃取数据的有害程序。
8. 重大的系统中断事件。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 加 文 密 件 _____

2. 加 勒 索 密 _____

3. 荷 恶 载 意 _____

4. 复 恢 文 件 _____

5. 件 恶 软 意 _____

6. 软 件 勒 索 _____

7. 事 灾 件 难 _____

8. 数 复 恢 据 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	你绝不应分享的信息			
2	可能被黑客入侵的设备			
3	不支付赎金的原因			
4	你今天就可以开始的安全习惯			
5	你知道的安全工具			
6	保护账户的方法			
7	电脑被感染的迹象			
8	保存备份的地方			
9	你绝不想丢失的文件			
10	勒索软件传播的途径			
11	攻击发生后第一个小时要做的事			
12	攻击期间要联系的人			
13	勒索软件可以锁定的内容			
14	与网络安全相关的词语			
15	经常成为攻击目标的机构			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 企业勒索软件载荷的遏制

👷

情景: 一个企业局域网遭到活跃的勒索软件入侵。 关键文件服务器已开始显示 .locked 文件扩展名。

讨论问题: 详细说明隔离步骤，并概述数据恢复协议。

案例研究 2: 评估离线备份架构

👷

情景: 一家企业想设计一种数据备份策略，以降低备份被攻破的风险，即使主要本地网络被勒索软件完全控制。

讨论问题: 设计一个安全的离线备份存储库系统。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

文=1 网=2 恶=3 难=4 索=5 据=6 冷=7 统=8 系=9 备=10

软=11 络=12 码=13 勒=14 件=15 从=16 意=17 服=18 份=19 事=20

载=21 恢=22 密=23 全=24 复=25 荷=26 灾=27 数=28 加=29 安=30

16	7	10	19	22	25	29	23	28	6	9	8

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是勒索软件?

勒索软件是一种恶意软件，旨在阻止访问计算机系统或文件，直到支付赎金为止。

Q2: 勒索软件如何传播?

通过钓鱼邮件附件、未打补丁的软件漏洞和被入侵的远程访问系统。 [1]

Q3: 为什么要求用加密货币付款?

比特币等加密货币提供相对的匿名性，使执法部门难以追踪资金。

Q4: 杀毒软件能拦截勒索软件吗?

是的，但基于特征码的杀毒软件可能无法防御新出现的零日勒索软件载荷。

Q5: 什么是物理隔离备份?

与主网络没有物理或逻辑连接的备份副本，可防止扩散。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 什么是双重勒索?

攻击者不仅加密文件，还窃取敏感数据，以便在不付款时威胁公开泄露。

Q7: 什么是解密器?

包含将被锁定文件恢复为明文所需加密密钥的软件工具。

Q8: 如何及早发现勒索软件?

通过监控文件系统中突然出现的大量文件修改和重命名活动。

Q9: 保险起什么作用?

网络保险有助于承担恢复成本，但保障条款和赎金支付规则因保单而异。

Q10: 我应该重启被感染的系统吗?

不要，重启可能会破坏易失性内存证据；应改为将其与网络隔离。 [1]

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: 勒索软件如何使用非对称加密?

它使用嵌入在恶意软件中的公钥来加密文件，需要攻击者的私钥才能解密。

Q2: 为什么还要使用对称加密?

对称加密（如 AES）速度快，可在几分钟内锁定庞大的数据库，而非对称密钥则用来保护 AES 密钥。

Q3: 什么是逻辑分段?

将网络划分为相互隔离的区域，防止恶意软件从工作站节点横向传播到核心服务器。

Q4: 什么是 WORM 存储?

一次写入多次读取（Write-Once, Read-Many）介质，可防止备份数据被勒索软件载荷编辑、覆盖或删除。

Q5: 什么是卷影副本?

Windows 创建的本地备份快照；勒索软件通常会先使用管理员工具将其删除。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: 凭据被盗如何助长勒索软件攻击?

攻击者购买泄露的管理员登录凭据，通过远程桌面登录，在网络中手动执行勒索软件。

Q7: 什么是演练式恢复测试?

定期将备份数据库恢复到隔离的测试环境中，以验证恢复速度和数据完整性符合灾难恢复指标。

Q8: 终端检测与响应 (EDR) 如何阻止勒索软件?

通过分析进程行为（例如快速加密），并迅速挂起异常应用。

Q9: 什么是勒索软件即服务 (RaaS) 模式?

一种特许经营模式，恶意软件开发者将勒索软件构建工具租给下属，以换取一定比例的赎金分成。

Q10: 未打补丁的 RDP 如何引发勒索软件?

暴露在外且未打补丁的远程桌面协议网关使攻击者能够暴力破解登录并手动启动恶意软件。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

勒索软件攻击者常使用 vssadmin.exe 等工具删除 Windows 卷影副本，阻止本地恢复。 [1]

2. 安全洞察

对称 AES-256 密钥通常用于加密文件负载，然后再用公共 RSA 密钥将其锁定。

3. 安全洞察

从一次得逞的勒索软件攻击中恢复可能需要数周时间，因此经过测试的离线备份非常重要。

4. 安全洞察

FBI 不支持支付赎金，并警告说支付赎金并不能保证你能取回任何数据。 [2]

5. 安全洞察

灾难恢复计划 (DRP) 应定义恢复时间目标 (RTO) 和恢复点目标 (RPO)。

6. 安全洞察

FBI 建议使用加密且不可变的备份，即无法被更改或删除的备份。 [3]

7. 安全洞察

勒索软件开发者利用先进的混淆技术来绕过传统的基于特征码的杀毒扫描器。

8. 安全洞察

网络分段限制横向移动，有助于阻止勒索软件扩散到第一台受感染主机之外。 [3]

9. 安全洞察

暴露在外且安全防护不足的远程服务（如远程桌面协议 RDP）是常见的勒索软件入口。 [1]

10. 安全洞察

CISA 建议将加密备份保存在离线状态，因为许多勒索软件变种会搜寻并删除可访问的备份。 [1]

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[1] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

答案: 检查点 1 – 单项选择

1 问题 1

正确答案: A

教学提示

勒索软件攻击的主要机制是什么？ → 对用户文件进行加密以拒绝系统访问

2 问题 2

正确答案: A

教学提示

什么是离线（冷）备份？ → 与网络断开连接的存储副本，以防止恶意软件传播

3 问题 3

正确答案: A

教学提示

在勒索软件攻击期间，安全团队应如何隔离受感染的系统？ → 立即断开网线并禁用无线接口

4 问题 4

正确答案: A

教学提示

安全机构为什么建议不要支付勒索软件的赎金？ → 支付赎金会助长攻击者，且不能保证交付解密密钥

5 问题 5

正确答案: A

教学提示

什么是灾难恢复计划（DRP）？ → 系统被入侵后恢复运营和数据的结构化流程

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** 正确答案: 正确

教学提示

勒索软件载荷很容易传播到连接在网络上的在线备份。

7 **问题 7** 正确答案: 错误

教学提示

错误: FBI 警告说，付款并不能保证你能拿回任何数据。

8 **问题 8** 正确答案: 正确

教学提示

正确: CISA 建议拔掉受感染的主机或使网络下线，以遏制扩散。

9 **问题 9** 正确答案: 错误

教学提示

错误: 勒索软件通常使用 AES 等快速对称加密算法加密文件。

10 **问题 10** 正确答案: 正确

教学提示

定期测试数据恢复流程是灾难恢复的关键组成部分。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

C 1. 加密	E 2. 有效载荷	F 3. 冷备份	A 4. 隔离
H 5. 赎金	G 6. 恢复	D 7. 灾难	B 8. 木马

检查点 3: 答案 – 关键术语

1 加密	2 恶意载荷	3 冷备份	4 隔离
5 赎金	6 恢复		

检查点 6 替代活动: 答案 – 词语配对

1 C – 加密勒索	2 H – 数据恢复	3 A – 文件加密	4 E – 恶意载荷
5 D – 勒索软件	6 G – 文件恢复	7 B – 恶意软件	8 F – 灾难事件

教师讨论提示

关键术语:
检查学生能否用自己的话解释加密、有效载荷和冷备份，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

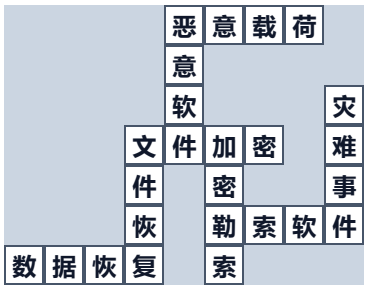
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	域	道	安	息	恶	用	连	意	隧	灾	共	器	认	统
系	议	隐	件	墙	全	隧	服	文	安	传	协	系	连	复
务	荷	器	安	风	连	问	共	份	件	信	攻	信	件	名
务	载	数	输	恢	络	隐	域	览	地	恢	访	恢	攻	输
文	意	安	备	名	文	器	名	索	证	事	复	件	载	保
软	恶	墙	密	传	件	问	勒	保	风	管	证	件	载	设
攻	密	道	公	共	加	用	火	索	址	数	网	数	加	系
荷	火	名	荷	防	密	载	隧	协	软	务	备	证	域	务
件	问	风	份	议	设	软	隐	身	身	件	设	理	公	道
事	隧	隐	加	公	件	攻	访	传	据	恶	务	共	事	记
难	恶	意	软	件	加	恢	恶	保	议	连	复	服	份	数
灾	务	管	索	加	软	加	浏	数	网	复	险	务	据	防
络	务	攻	务	密	信	私	问	服	理	备	证	恢	用	问
传	恢	公	信	勒	备	录	户	络	络	管	复	系	份	软
道	载	设	名	索	传	道	输	码	份	难	数	保	传	索

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 恶意载荷 执行恶意软件 (4 字)

3 横向: 文件加密 用密码学方式锁定文件 (4 字)

5 横向: 勒索软件 加密受害者文件并索要赎金的恶意程序 (4 字)

6 横向: 数据恢复 从备份中还原数据库 (4 字)

纵向

1 纵向: 恶意软件 旨在破坏系统或窃取数据的有害程序 (4 字)

2 纵向: 灾难事件 重大的系统中断事件 (4 字)

3 纵向: 文件恢复 把丢失或被加密的文件找回来 (4 字)

4 纵向: 加密勒索 对受害者文件加密并索要钱财才肯解锁 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 加文密件 — **文件加密**
2. 加勒索密 — **加密勒索**
3. 荷恶载意 — **恶意载荷**
4. 复恢文件 — **文件恢复**
5. 件恶软意 — **恶意软件**
6. 软件勒索 — **勒索软件**
7. 事灾件难 — **灾难事件**
8. 数复恢据 — **数据恢复**

秘密密码挑战答案

“从冷备份恢复加密数据系统”

案例研究答案

A 案例研究 1: 企业勒索软件载荷的遏制

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一个企业局域网遭到活跃的勒索软件入侵。关键文件服务器上的文件扩展名开始显示为 .locked。
- 建议策略与方案: 将所有受影响的服务器与局域网断开。终止活动的管理会话。从安全的、写保护的离线备份系统中恢复未被入侵的文件。

B 案例研究 2: 评估离线备份架构

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一家企业想设计一套数据备份策略，即使主本地网络被勒索软件完全劫持，也能降低备份被攻破的风险。
- 推荐策略与解决方案: 实施一次写入多次读取（WORM）存储。通过断开备份系统与所有网络的连接来构建逻辑气隙，并执行每日物理介质轮换。