姓名: _____ 日期: _____ 得分: _____

恶意软件分析与威胁缓解指南

木马、勒索软件、间谍软件、Rootkit、虚拟化沙盒、隔离

恶意软件分析学习概览

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恶意软件分析与预防。你将探索间谍软件、木马、勒索软件载荷、逆向工程工具、rootkit 行为和遏制策略。

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/malware/

你的恶意软件防范学习路线图

- 区分木马、蠕虫和 rootkit 恶意软件类型。
- 实施沙箱虚拟化执行，用于代码分析。
- 为活跃的勒索软件载荷设计遏制和清理方案。

恶意软件分析指南说明

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。将所学知识应用于恶意软件缓解。最后完成附加活动: 快速思考。

恶意软件分析与威胁遏制（简介）

木马、蠕虫和勒索软件等恶意代码会对终端和服务器造成高影响威胁。安全团队在虚拟沙盒中分析恶意软件，并迅速执行网络隔离控制，以遏制有效载荷的传播。

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. 特洛伊木马的决定性特征是什么?
   - A. 它伪装成合法软件，诱骗用户运行它
   - B. 它会通过本地网络线路自动复制
   - C. 它感染隔离虚拟沙盒内的文件
   - D. 它拦截互联网服务提供商的流量

2. 哪种类型的恶意软件会加密文件并索要付款?
   - A. 勒索软件
   - B. 间谍软件
   - C. Rootkit
   - D. 广告软件

3. 什么代表间谍软件?
   - A. 旨在秘密监控用户击键和浏览器活动的恶意软件
   - B. 在沙盒虚拟容器内执行的程序代码
   - C. 从数据库注册中心下载的反恶意软件更新
   - D. 自动屏幕亮度调节

4. 恶意软件开发者为什么使用 Rootkit?
   - A. 向操作系统隐藏活动进程和恶意文件
   - B. 提高终端的 CPU 处理速度
   - C. 将数据库文件备份到安全的云保管库
   - D. 延长笔记本电脑的电池续航

5. 在恶意软件分析中，沙盒化是什么意思?
   - A. 在隔离的虚拟保险库中运行可疑文件，以安全地观察其行为
   - B. 将文件哈希值与已知威胁数据库进行比对扫描
   - C. 入侵后恢复数据库备份
   - D. 将本地网络路由器与公共线路断开

检查点 2: 判断正误挑战

6 问题 6

6. 计算机蠕虫需要人类用户交互才能在本地网络中传播。

○ 正确 ○ 错误

7 问题 7

7. 广告软件总是无害的，不会跟踪用户行为或浏览历史。

○ 正确 ○ 错误

8 问题 8

8. 恢复干净的离线备份可让受害者无需支付赎金即可恢复被加密的文件。

○ 正确 ○ 错误

9 问题 9

9. 基于特征码的杀毒软件能够在零日恶意软件的特征码出现之前可靠地阻止它。

○ 正确 ○ 错误

10 问题 10

10. 无文件恶意软件在系统内存中执行恶意脚本，避免向磁盘写入文件。

○ 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. 伪装成安全实用程序的恶意软件是 _____ 。
2. 为勒索钱财而锁定数据库系统的恶意载荷属于 _____ 。
3. 秘密记录密码的键盘记录程序属于 _____ 。
4. 深藏在操作系统内核中需要借助 _____ 。
5. 在隔离的保险库中分析可疑文件，要使用虚拟 _____ 。
6. 阻止活跃的恶意载荷扩散，需要立即对网络进行 _____ 。

词汇词库

遏制隔离　间谍软件　勒索软件　木马病毒　内核后门　沙箱　无文件攻击　WORM

在此写下你的答案:

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

检查点 4: 安全概念配对

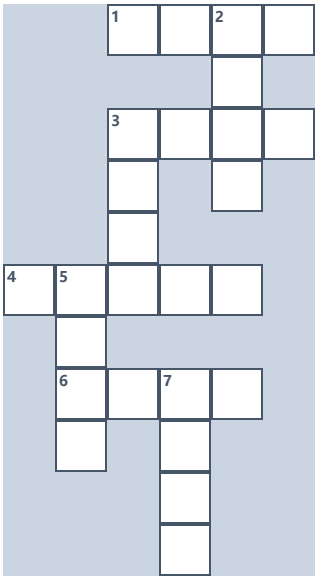
定义配对

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. 木马	**A**	旨在秘密监视并记录用户活动和输入内容的程序。
	2. 勒索软件	**B**	直接在内存（RAM）中运行以躲避磁盘扫描程序检测的恶意软件。（H）
	3. 间谍软件	**C**	限制受感染的终端，以防止威胁载荷扩散。
	4. Rootkit	**D**	伪装成无害或有用的实用程序的恶意软件。（A）
	5. 沙盒	**E**	无需人为操作即可在网络中传播的自我复制恶意软件。
	6. 遏制	**F**	加密系统存储并要求付款才交付密钥的恶意软件。（B）
	7. 蠕虫	**G**	用于安全分析恶意文件的隔离虚拟环境。
	8. 无文件	**H**	深藏在系统内核中以保持管理控制权的隐形恶意软件。

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. 深藏在系统内核中、用于保持管理控制权的隐蔽恶意软件 (4)

3. 在用户不知情的情况下窃取信息的程序 (4)

4. 直接在内存中执行以躲避磁盘扫描程序检测的恶意软件 (5)

6. 对受害者文件加密并索要钱财才肯解锁 (4)

纵向

2. 绕过正常验证、让攻击者能够暗中进入系统的程序 (4)

3. 旨在秘密监视并记录用户活动和输入内容的程序 (4)

5. 用密码学方法把文件变成他人无法读取的形式 (4)

7. 加密系统存储并索要付款才提供密钥的恶意软件 (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: 深藏在系统内核中、用于保持管理控制权的隐蔽恶意软件 (4 字):

3 横向: 在用户不知情的情况下窃取信息的程序 (4 字):

4 横向: 直接在内存中执行以躲避磁盘扫描程序检测的恶意软件 (5 字):

6 横向: 对受害者文件加密并索要钱财才肯解锁 (4 字):

纵向

2 纵向: 绕过正常验证、让攻击者能够暗中进入系统的程序 (4 字):

3 纵向: 旨在秘密监视并记录用户活动和输入内容的程序 (4 字):

5 纵向: 用密码学方法把文件变成他人无法读取的形式 (4 字):

7 纵向: 加密系统存储并索要付款才提供密钥的恶意软件 (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 文 用 连 勒 隧 序 共 器 认 统
系 议 隐 件 墙 全 隧 服 后 安 传 协 系 连 核
务 件 器 安 风 连 问 共 份 门 信 攻 信 件 名
务 软 数 输 内 络 隐 域 览 地 程 访 内 攻 输
无 谍 安 备 名 无 器 名 间 证 门 序 件 谍 保
软 间 墙 密 传 文 问 勒 保 风 管 证 件 谍 设
攻 密 道 公 共 件 用 火 索 址 数 网 数 加 系
程 火 名 程 防 攻 谍 隧 协 软 务 备 证 域 务
序 问 风 份 议 击 设 软 隐 身 件 身 设 理 公
程 道 隧 隐 加 公 件 攻 访 传 据 文 务 共 门
谍 文 件 加 密 记 加 内 文 保 议 连 核 服 内
间 份 务 管 加 间 软 加 浏 数 网 核 险 核 务
防 络 务 攻 密 务 信 私 问 服 理 备 后 证 用
问 传 内 公 勒 信 备 录 户 络 络 门 管 系 份
软 道 谍 设 索 名 传 道 输 码 份 后 数 保 传

词汇列表

无文件攻击 **文件加密** **加密勒索** **勒索软件** **间谍软件** **间谍程序** **后门程序** **内核后门**

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. 无文件攻击
B. 文件加密
C. 加密勒索
D. 勒索软件
E. 间谍软件
F. 间谍程序
G. 后门程序
H. 内核后门

定义与配对字段
1. 加密系统存储并索要付款才提供密钥的恶意软件。
2. 在用户不知情的情况下窃取信息的程序。
3. 深藏在系统内核中、用于保持管理控制权的隐蔽恶意软件。
4. 绕过正常验证、让攻击者能够暗中进入系统的程序。
5. 用密码学方法把文件变成他人无法读取的形式。
6. 对受害者文件加密并索要钱财才肯解锁。
7. 直接在内存中执行以躲避磁盘扫描程序检测的恶意软件。
8. 旨在秘密监视并记录用户活动和输入内容的程序。

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. 攻 件 无 击 文
2. 加 勒 索 密
3. 件 间 软 谍
4. 序 程 后 门
5. 密 文 加 件
6. 软 件 勒 索
7. 程 间 序 谍
8. 内 门 后 核

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	下载安全应用的地方			
2	可能被黑客入侵的设备			
3	你要备份的内容			
4	电子邮件中的警示信号			
5	手机感染恶意软件的迹象			
6	你知道的恶意软件类型			
7	需要谨慎对待的文件类型			
8	恶意软件进入电脑的途径			
9	你今天就可以开始的安全习惯			
10	与网络安全相关的词语			
11	数据泄露后要做的事			
12	更新软件的原因			
13	名称听起来像恶意软件的动物或角色			
14	恶意软件可以窃取的内容			
15	点击了错误链接后要做的事			

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。请制定遏制策略。

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: 无文件恶意软件内存注入

👷

情景: 一名分析师检测到可疑的脚本模式正使用标准管理工具直接在易失性系统内存（RAM）中执行，但磁盘上没有任何恶意文件。

讨论问题: 解释内存分析策略，并指明用于阻止无文件执行的工具。

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

序=1 门=2 行=3 现=4 发=5 后=6 击=7 荷=8 无=9 为=10

加=11 间=12 件=13 意=14 恶=15 密=16 载=17 软=18 终=19 用=20

索=21 文=22 控=23 端=24 勒=25 内=26 程=27 攻=28 监=29 谍=30

20	3	10	29	23		5	4		19	24		15	14	17	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: 什么是恶意软件?

由威胁行为者设计的、用于破坏、劫持或窃取设备和网络上数据的恶意软件。

Q2: 病毒和蠕虫有什么区别?

病毒需要人为操作（如打开文件）才能传播，而蠕虫会在网络间自动传播。

Q3: 特洛伊木马如何感染计算机?

它通过伪装成无害或安全的程序来欺骗用户，并将恶意载荷隐藏在其中。

Q4: 什么是勒索软件?

一种加密目标系统上的文件、并要求支付赎金以换取解密密钥的恶意软件。 [1]

Q5: 什么是间谍软件?

秘密记录用户按键、密码和浏览习惯并发送给攻击者的恶意软件。

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: 沙箱是什么意思?

在安全、隔离的虚拟环境中运行可疑文件，以观察其行为，而不会危及生产系统。

Q7: 什么是无文件恶意软件?

借助合法工具直接在系统内存（RAM）中运行、避免将文件写入磁盘以绕过基础扫描程序的恶意软件。

Q8: Rootkit 如何保护恶意软件?

它会隐藏恶意进程和文件，通常通过颠覆操作系统内核来实现，因此杀毒扫描器可能无法发现它们。

Q9: 什么是动态行为监控?

防病毒扫描会实时监控活动进程，以拦截恶意软件的典型行为，例如批量文件加密。

Q10: 为什么在事件响应中遏制十分紧迫?

隔离被入侵的终端可防止正在运行的恶意软件载荷传播到其他网络设备。

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: 恶意软件开发者如何绕过基于特征码的杀毒扫描器?

它们使用多态技术，每次感染都会改变文件的哈希值和代码结构，而恶意行为保持不变。

Q2: 恶意软件活动中双重用途工具有什么风险?

攻击者使用合法的管理工具（如 PowerShell 或 Sysinternals）混入正常的网络流量，使检测变得困难。

Q3: 进程镂空如何执行恶意载荷?

它以挂起状态启动一个合法的系统进程，用恶意软件替换其内存中的代码，然后恢复执行。

Q4: 命令与控制 (C2) 服务器起什么作用?

黑客操作的远程服务器，用于向被入侵机器上运行的恶意软件发送指令和负载。

Q5: 键盘记录为什么难以发现?

基础键盘记录器占用的 CPU 资源极少，并将其进程隐藏在合法的用户空间实用工具中。

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: 代码混淆如何延缓恶意软件分析?

它会加密或重新排列源代码，使分析工具和安全扫描器无法读取。

Q7: 引导区病毒的功能是什么?

一种感染引导过程（MBR、引导扇区或 UEFI 固件）的 rootkit，因此在操作系统加载之前就会运行。

Q8: 启发式扫描如何识别零日威胁?

它扫描可疑的代码模式和管理命令，而不是查找匹配的数据库哈希值。

Q9: DLL 劫持有什么威胁?

通过将恶意动态链接库（DLL）放入应用程序的目录路径，迫使合法应用程序加载它。

Q10: 自动化恶意软件分析流水线如何使用虚拟化?

它们在多个操作系统虚拟机中运行可疑文件，自动生成行为日志和网络 PCAP 文件。

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

特洛伊木马仍是常见的感染方式，因为它们把恶意代码隐藏在看似无害的程序中。

2. 安全洞察

FBI 的 IC3 在 2025 年收到超过 3,600 起勒索软件投诉，报告的损失超过 3,200 万美元。 [3]

3. 安全洞察

蠕虫可利用未打补丁的协议漏洞（如 SMB 中的 EternalBlue）在网络中迅速传播。

4. 安全洞察

无文件恶意软件很难被检测，因为它通过合法工具在内存中运行，在磁盘上留下的痕迹很少。

5. 安全洞察

分析沙盒通常在每次运行后恢复到干净的快照，以便每次测试都从已知状态开始。

6. 安全洞察

Rootkit 可以修改内核系统调用，向反恶意软件扫描程序报告虚假的诊断结果。

7. 安全洞察

代码混淆使用加壳工具来压缩并隐藏恶意软件真实的二进制载荷结构。

8. 安全洞察

多态恶意软件每个新副本都会改变自身代码，进而改变文件哈希值，以规避特征码检查。

9. 安全洞察

DLL 劫持利用 Windows 等标准操作系统中的搜索顺序配置。

10. 安全洞察

安全厂商每天都会发现大量新的恶意软件样本，因此特征库需要不断更新。

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

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

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

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

特洛伊木马的决定性特征是什么？ → 它伪装成合法软件，诱骗用户运行它

2 问题 2 正确答案: A

教学提示

哪种类型的恶意软件会加密文件并索要付款？ → 勒索软件

3 问题 3 正确答案: A

教学提示

什么代表间谍软件？ → 旨在秘密监控用户击键和浏览器活动的恶意软件

4 问题 4 正确答案: A

教学提示

恶意软件开发者为什么使用 Rootkit？ → 向操作系统隐藏活动进程和恶意文件

5 问题 5 正确答案: A

教学提示

在恶意软件分析中，沙盒化是什么意思？ → 在隔离的虚拟保险库中运行可疑文件，以安全地观察其行为

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** 正确答案: 错误

教学提示

错误: 蠕虫会自我复制，无需任何用户操作即可在网络间传播。

7 **问题 7** 正确答案: 错误

教学提示

错误: 广告软件并不总是无害的；其中很多会追踪浏览行为以定向投放广告。

8 **问题 8** 正确答案: 正确

教学提示

正确: 干净的离线备份可以在不支付赎金的情况下恢复被加密的文件，不过被窃取的数据仍可能泄露。

9 **问题 9** 正确答案: 错误

教学提示

错误: 特征码扫描器需要已知样本，因此全新的零日恶意软件可能绕过它们。

10 **问题 10** 正确答案: 正确

教学提示

无文件恶意软件在系统内存中执行恶意脚本，避免向磁盘写入文件。

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

D 1. 木马	F 2. 勒索软件	A 3. 间谍软件	H 4. Rootkit
G 5. 沙盒	C 6. 遏制	E 7. 蠕虫	B 8. 无文件

检查点 3: 答案 – 关键术语

1 木马病毒	2 勒索软件	3 间谍软件	4 内核后门
5 沙箱	6 遏制隔离		

检查点 6 替代活动: 答案 – 词语配对

1 D – 勒索软件	2 F – 间谍程序	3 H – 内核后门	4 G – 后门程序
5 B – 文件加密	6 C – 加密勒索	7 A – 无文件攻击	8 E – 间谍软件

教师讨论提示

关键术语:
检查学生能否用自己的话解释木马、勒索软件和间谍软件，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	文	用	连	勒	隧	序	共	器	认	统
系	议	隐	件	墙	全	隧	服	后	安	传	协	系	连	核
务	件	器	安	风	连	问	共	份	门	信	攻	信	件	名
务	软	数	输	内	络	隐	域	览	地	程	访	内	攻	输
无	谍	安	备	名	无	器	名	间	证	门	序	件	谍	保
软	间	墙	密	传	文	问	勒	保	风	管	证	件	谍	设
攻	密	道	公	共	件	用	火	索	址	数	网	数	加	系
程	火	名	程	防	攻	谍	隧	协	软	务	备	证	域	务
序	问	风	份	议	击	设	软	隐	身	件	身	设	理	公
程	道	隧	隐	加	公	件	攻	访	传	据	文	务	共	门
谍	文	件	加	密	记	加	内	文	保	议	连	核	服	内
间	份	务	管	加	间	软	加	浏	数	网	核	险	核	务
防	络	务	攻	密	务	信	私	问	服	理	备	后	证	用
问	传	内	公	勒	信	备	录	户	络	络	门	管	系	份
软	道	谍	设	索	名	传	道	输	码	份	后	数	保	传

填字游戏答案



填字游戏答案教师指南

横向

1 横向: 内核后门 深藏在系统内核中、用于保持管理控制权的隐蔽恶意软件 (4 字)

3 横向: 间谍程序 在用户不知情的情况下窃取信息的程序 (4 字)

4 横向: 无文件攻击 直接在内存中执行以躲避磁盘扫描程序检测的恶意软件 (5 字)

6 横向: 加密勒索 对受害者文件加密并索要钱财才肯解锁 (4 字)

纵向

2 纵向: 后门程序 绕过正常验证、让攻击者能够暗中进入系统的程序 (4 字)

3 纵向: 间谍软件 旨在秘密监视并记录用户活动和输入内容的程序 (4 字)

5 纵向: 文件加密 用密码学方法把文件变成他人无法读取的形式 (4 字)

7 纵向: 勒索软件 加密系统存储并索要付款才提供密钥的恶意软件 (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. 攻件无击文 — **无文件攻击**
2. 加勒索密 — **加密勒索**
3. 件间软谍 — **间谍软件**
4. 序程后门 — **后门程序**
5. 密文加件 — **文件加密**
6. 软件勒索 — **勒索软件**
7. 程间序谍 — **间谍程序**
8. 内门后核 — **内核后门**

秘密密码挑战答案

“用行为监控发现终端恶意载荷”

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。请制定遏制策略。
- 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: 无文件恶意软件内存注入

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位分析师检测到可疑的脚本模式正使用标准管理工具直接在易失性系统 RAM 中执行，但磁盘上并不存在恶意文件。
- 推荐策略与解决方案: 先隔离受影响的终端并获取内存镜像。检查 PowerShell 和 WMI 日志，用 AppLocker 阻止未经批准的脚本，然后重启以清除恶意载荷。