数智创新
变革未来

网络钓鱼和欺诈检测

目录页

Contents Page

网络钓鱼技术及其演变

网络钓鱼技术及其演变

网络钓鱼技术演变

1. 精鱼式网络钓鱼：针对特定目标个体或组织发动高度定制化的攻击，模仿合法通信的语气、格式和内容，提高可信度和迷惑性。

2. 鱼叉式网络钓鱼：针对特定群体或行业发动定向攻击，通过电子邮件或社交媒体平台发送包含恶意链接或附件的虚假信息，诱骗受害者泄露敏感信息。

3. 语音网络钓鱼：通过电话或语音消息冒充合法机构或个人，诱骗受害者提供个人信息或财务信息。

恶意软件演变

1. 勒索软件：通过加密受害者文件并勒索赎金来破坏数据并敲诈钱财，演变出多种变种，如锁定屏幕、损坏数据、窃取凭证等。

2. 木马病毒：伪装成合法软件，安装后在受害者计算机上远程控制、窃取信息、执行恶意操作，演变出多种变种，如后门、远程访问工具、间谍软件等。

3. 僵尸网络：通过恶意软件控制大量僵尸主机，形成分布式网络，用于发动拒绝服务攻击、发送垃圾邮件、传播病毒或其他恶意活动。

常见的网络钓鱼和欺诈类型

常见的网络钓鱼和欺诈类型

网络钓鱼电子邮件

1. 伪装成来自知名组织（例如银行、科技公司）的电子邮件，要求收件人点击链接或打开附件。
2. 旨在窃取敏感信息，如登录凭证、信用卡信息和个人身份信息。
3. 通常包含语法和拼写错误、未经请求的附件和威胁性语言。

网络钓鱼网站

1. 利用虚假域名或伪造合法网站，诱骗用户输入个人信息。
2. 模仿真实网站的外观和功能，使之难以识别。
3. 通过社交媒体、广告或电子邮件进行推广，以吸引受害者访问网站。

常见的网络钓鱼和欺诈类型

smishing（短信网络钓鱼）和vishing（语音网络钓鱼）

1. 使用短信或语音电话发送欺诈性信息，要求收件人回复敏感信息。
2. 利用升级促销、账户验证或意外通知等诱饵来吸引受害者。
3. 经常从未知号码发送，并包含紧急要求或威胁性语言。

社交媒体网络钓鱼

1. 在社交媒体平台上发布虚假账户、朋友请求或消息，冒充合法组织。
2. 利用平台的信任机制，诱骗用户提供个人信息或访问恶意链接。
3. 可能假装提供客户支持、赠品或优惠，以吸引受害者。

常见的网络钓鱼和欺诈类型

高级持续性威胁（APT）

1. 由国家行为者或网络犯罪分子发起，目标明确的网络攻击。
2. 采用复杂的攻击手法和社会工程技术，绕过传统安全措施。
3. 旨在窃取敏感信息、破坏系统或进行网络间谍活动。

业务电子邮件妥协（BEC）

1. 冒充合法企业与其客户或供应商通信的欺诈性电子邮件。
2. 要求收件人汇款、提供敏感信息或点击恶意链接。
3. 利用对目标组织的了解，进行有针对性的攻击，提高可信度。

基于机器学习的检测方法

基于机器学习的检测方法

基于规则的自学习检测

1. 自动提取特征，通过设定规则进行检测。
2. 利用机器学习算法，自动挖掘数据模式和异常行为，完善检测规则。
3. 持续学习，优化规则，提高检测准确性和效率。

基于聚类的检测

1. 将数据点分组为簇，识别不同行为模式。
2. 分析不同簇之间的差异，发现异常值和可疑事件。
3. 无需事先定义规则，可扩展性高，对未知威胁具有较好检测能力。

基于机器学习的检测方法

基于分类的检测

1. 利用机器学习算法，对数据进行分类，区分正常和异常行为。
2. 训练模型，识别网络钓鱼和欺诈模式，并进行自动分类。
3. 准确率高，响应速度快，适合处理大规模数据集。

基于异常检测的检测

1. 识别与正常模式显著不同的异常数据点。
2. 分析数据分布，发现偏离预期行为的异常值。
3. 不依赖于预定义规则，可检测未知 تهديدات.

基于机器学习的检测方法

基于图的检测

1. 构建网络或图结构，表示数据之间的关系。
2. 分析图结构，识别异常模式和关系链。
3. 适合检测传播广泛的网络钓鱼活动，可视化关联关系。

深度学习检测

1. 利用深度神经网络，自动学习复杂数据模式。
2. 提取高级特征，识别异常行为和未知威胁。