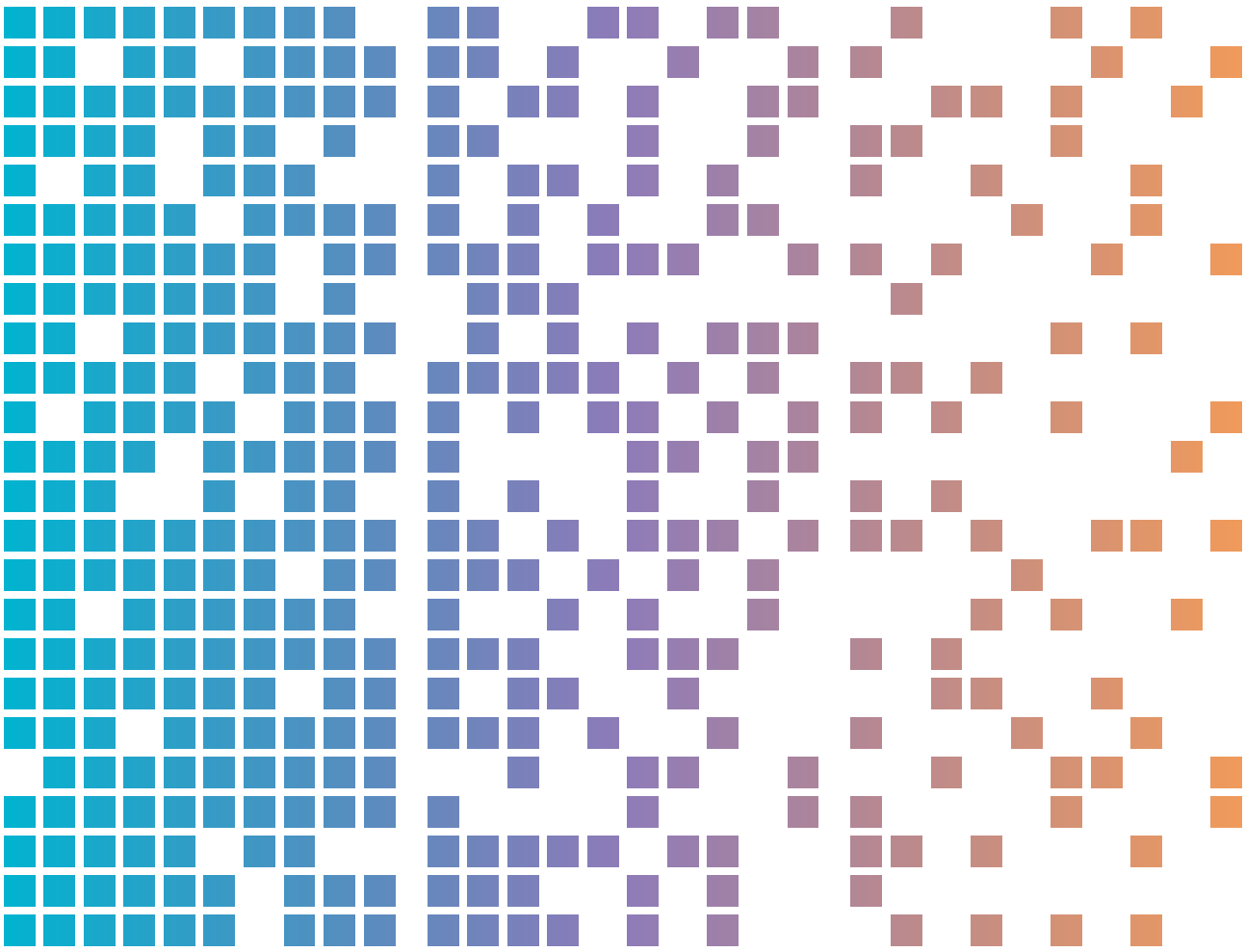
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

无声的盗窃：网络犯罪分子使用信息窃取恶意软件入侵企业网络



内容复杂度
中等 ●●○

目录

编制目的

信息窃取恶意软件会窃取用户凭证和系统信息，网络犯罪分子主要利用这些信息谋取经济利益。在针对世界范围内（包括澳大利亚）多个组织和部门的网络攻击中，均有发现信息窃取恶意软件。本出版物为读者提供关于信息窃取恶意软件的网络安全指导，包括威胁行为和针对组织及其员工的缓解建议。

要点

- 信息窃取恶意软件（也称为信息窃取器）是一种专门设计用于从受害者设备中收集信息的恶意程序。这些信息可能包括用户名和密码、信用卡信息、加密货币钱包、本地文件以及浏览器数据（包括Cookies、用户浏览记录和自动填表信息）。
- 网络犯罪分子可能会购买并使用与企业账户相关的被盗用户凭证，以获取对受害者雇主、其客户及其他企业系统设备的初始访问权限。对这些组织的后续影响包括勒索软件攻击、敲诈勒索、商务电子邮件泄露以及知识产权盗窃。
- 澳大利亚信号局下属的澳大利亚网络安全中心（ASD's ACSC）已确认，部分企业网络入侵事件源自员工通过受入侵的个人设备访问工作资源。在多起事件中，网络犯罪分子通过使用被盗的有效用户凭证获得了企业网络的初始访问权限。我们的调查显示，大规模的入侵通常发生在网络犯罪分子成功获取特权用户的账户访问权限之后。
- 允许员工、承包商、受管理的服务提供商或其他实体通过远程方式（包括自带设备BYOD）访问其网络的组织，应意识到信息窃取器的风险，并采取措施来防范这一威胁。网络犯罪分子通过各种技术手段将信息窃取器部署到受害者设备上，包括网络钓鱼邮件、盗版软件下载、搜索引擎优化（SEO）技术、恶意广告或社交媒体平台上的恶意链接等。通常情况下，兼顾工作与个人用途的设备，由于用户行为和安全控制不足，通过这些手段受到感染风险更高。
- 信息窃取器为网络犯罪分子提供了一种有利可图的变现模式，尤其适用于初级网络犯罪分子和技术能力有限的网络犯罪分子。部分网络犯罪分子以“恶意软件即服务”（MaaS）模式销售信息窃取器产品，按月收取订阅费用。

背景

网络犯罪分子使用信息窃取器对澳大利亚组织的安全与福祉构成威胁。信息窃取器感染通常是重大网络安全事件的前兆活动，因为网络犯罪分子会利用它们收集用户凭证。这些用户凭证，特别是可访问面向互联网的远程服务的或特权账户的凭证，之后会被用于获取企业系统和数据的初始访问权限。

注：初始访问权限中间商在网络犯罪生态系统中扮演着专业角色，他们购买并验证被盗的用户凭证。随后，他们将高质量的、针对热门企业环境的用户凭证拍卖给网络犯罪分子，后者会利用这些凭证入侵组织的企业网络。

被盗的有效用户凭证对网络犯罪分子具有极高价值，因为它们可以加快犯罪分子获得企业网络和系统初始访问权限的进程。网络犯罪分子利用被盗的有效用户凭证，可以跳过多种常见的攻击战术与技术，包括：

- 识别并研究目标
- 枚举目标网络中的漏洞
- 构建初始访问路径，例如：
  - 钓鱼内容
  - 利用软件漏洞
  - 攻击远程服务，包括远程桌面协议（RDP）或虚拟专用网络（VPN）服务
  - 对用户凭证进行暴力破解攻击（密码猜测攻击）。

实施这些步骤通常需要投入大量时间并对技术能力有一定要求，这对部分网络犯罪分子而言是一个门槛。那些无法突破企业网络防御的犯罪分子尤其能从信息窃取器感染中获益，因为这些感染可以为他们提供便捷的目标企业用户网络的凭证权限。

在远程办公环境下，一些员工会在个人设备上同时进行工作和私人上网活动。在此过程中，员工可能会将用户凭证存储在网页浏览器的密码存储区域或插件中，或使用网页浏览器的自动填表功能。信息窃取器专门针对这些密码存储区域、身份验证Cookies以及网页浏览器中的其他个人数据。

与企业设备不同，个人设备通常未强制执行企业安全策略，这会对组织构成更高风险。例如，员工可能会因为所进行的活动（比如下载盗版软件或访问高风险网站），从而增加暴露于网络威胁和恶意软件感染的风险。

信息窃取器、分发者、初始访问权限中间商以及勒索软件同盟，现已成为以牟利为核心的网络犯罪生态系统的一个核心组成部分。当网络犯罪分子发展针对攻击链中的特定阶段的专业能力，并将其能力作为“服务”出售给其他犯罪合作方时，该生态系统的效率会提升。

威胁行为

ASD's ACSC正在追踪和监测全球信息窃取器活动增加的状况，该状况对澳大利亚网络构成日益严重的威胁。行业报告指出，在整个2023年，信息窃取器是网络犯罪活动中最常见的恶意软件类型。在暗网市场上出售的被盗数据数量不断增加，而且初始访问权限中间商利用这些数据的活动也在上升，这些现象反映出该趋势正在持续上升，并已在2024年进一步加速。

信息窃取器生态系统

第一阶段：获取恶意软件

信息窃取器通常在网络犯罪市场上以“恶意软件即服务”（MaaS）或“信息窃取即服务”(Stealer-as-a-Service)的形式提供，或作为源代码出售。MaaS是一种商业模式，恶意软件开发者通过网络平台向个人出售其恶意软件的订阅服务，类似于合法的“软件即服务”（SaaS）模式。MaaS模式降低了网络犯罪分子的门槛，它使得没有丰富技术技能的个人也能传播恶意软件并收集被盗信息用于网络攻击。

作为MaaS提供的信息窃取器通常以较低的月费推广，并向网络犯罪分子提供信息窃取器软件管理面板的访问权限。该管理面板可用于生成信息窃取器恶意软件、整理被盗数据并追踪受入侵系统的数量。MaaS提供商会不断推出功能更新、工具和技术支持，以逃避杀毒软件检测，并吸引和保留订阅用户。许多信息窃取器在完成数据外传后具有从受害者的设备自我删除的能力。

第二阶段：传播

分发信息窃取器并从受入侵设备中收集信息的网络犯罪分子被称为“Traffers”（流量分发者）。Traffers 会引导受害者点击恶意链接，从而在大规模活动中传播信息窃取器。大多数攻击活动是不加选择的，依赖于机会性感染。但也有一些攻击是针对特定行业的，会针对特定受害者实施鱼叉式网络钓鱼攻击。Traffers根据买家需求实施这些更有针对性的活动，例如，买家可能希望获取特定高价值组织或行业的访问权限。

Traffers使用多种技术将信息窃取器部署到受害者的设备上，包括：

- **僵尸网络**：由网络犯罪分子控制的受入侵计算机网络，用于发送钓鱼信息或传播恶意软件

- **网络钓鱼**：通过电子邮件或社交媒体、论坛或即时通讯应用程序中的直接信息，以欺骗手段获取敏感信息，这种常见的传播手段降低了网络犯罪分子的进入门槛：
  - 这类信息通常包含恶意链接，而非在邮件中附加恶意软件。
- **恶意搜索结果**：通过搜索引擎优化（SEO）技术将用户引导至提供恶意软件的网站，并且这些恶意软件会被伪装成合法的软件或其他内容
- **恶意广告**：将恶意代码注入合法在线广告中，用于传播恶意软件
- **破解或盗版软件**：通过YouTube视频描述或评论中的恶意链接或不可信下载网站分享的下载内容，包括电子游戏
- **社交媒体广告和帖子**：将用户引导至做好伪装的恶意文件
- **恶意软件更新**：通常伪装成网页浏览器更新的形式

第三阶段：数据收集

一旦信息窃取器在受害者的设备上运行，它就会开始从受入侵的设备中收集敏感数据。除了窃取用户凭证外，如果信息窃取器是僵尸网络的一部分，网络犯罪分子还可以远程控制受入侵设备，通过发送配置命令激活其他功能或投送其他恶意软件。一般而言，信息窃取器能够窃取以下内容：

- 用户名和密码，尤其是保存在网页浏览器多重身份验证（MFA）用户会话或令牌中的用户名和密码
- 身份验证Cookie
- 网页浏览器自动填表信息
- 电子邮件凭证、内容和联系人信息
- 网页浏览记录
- 用户文档
- 信用卡信息
- 桌面通讯应用的聊天记录
- 系统信息
- 加密货币钱包
- VPN或文件传输协议（FTP）凭证。

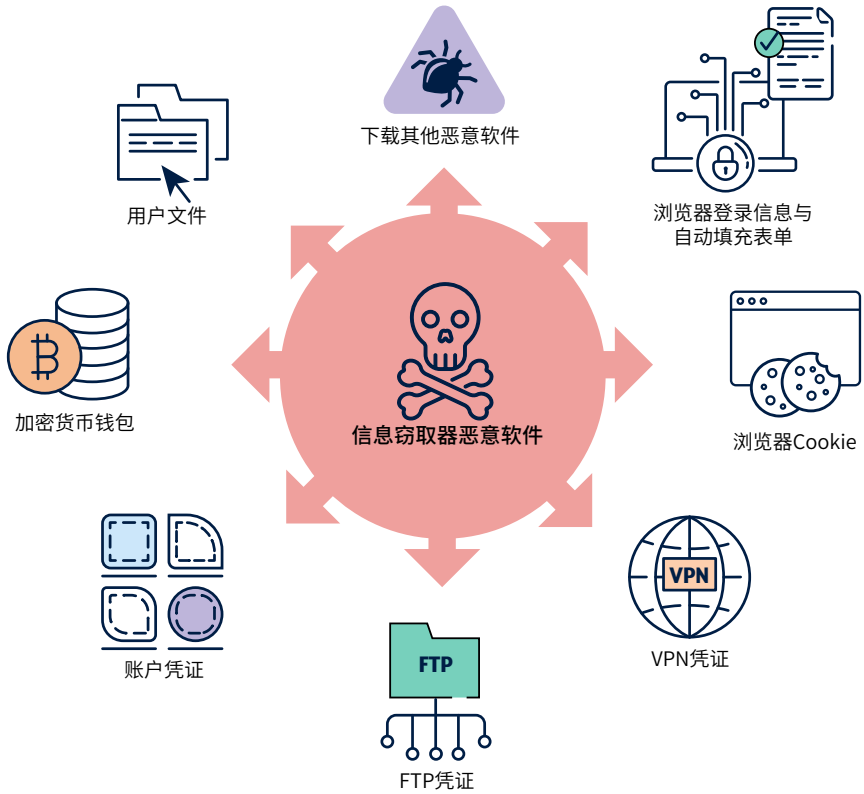


图1. 信息窃取器能力

某些网页浏览器身份验证Cookie能让用户一次登录账户或服务后，在几天内保持登录状态，因此用户无需重新进行身份验证。一旦这些身份验证Cookie被窃取，网络犯罪分子就可以绕过MFA要求，从而访问受害者的账户、企业网络和企业系统。

第四阶段：数据整合与变现

信息窃取器被配置为将受害者信息（称为“日志”）外传至恶意的命令与控制（C2）服务器。通常，信息窃取器会利用热门的通讯应用程序（如Telegram和Discord），将日志推送给网络犯罪分子。

Telegram和暗网上均有专门用于日志的出售与交易的市场。网络犯罪分子通过多种方式将日志变现，包括：

- 在黑市出售日志，包括出售给初始访问权限中间商
- 通过身份盗窃和敲诈勒索直接利用受害者
- 利用信息获取对企业网络的初始访问权限，以实施勒索软件攻击。

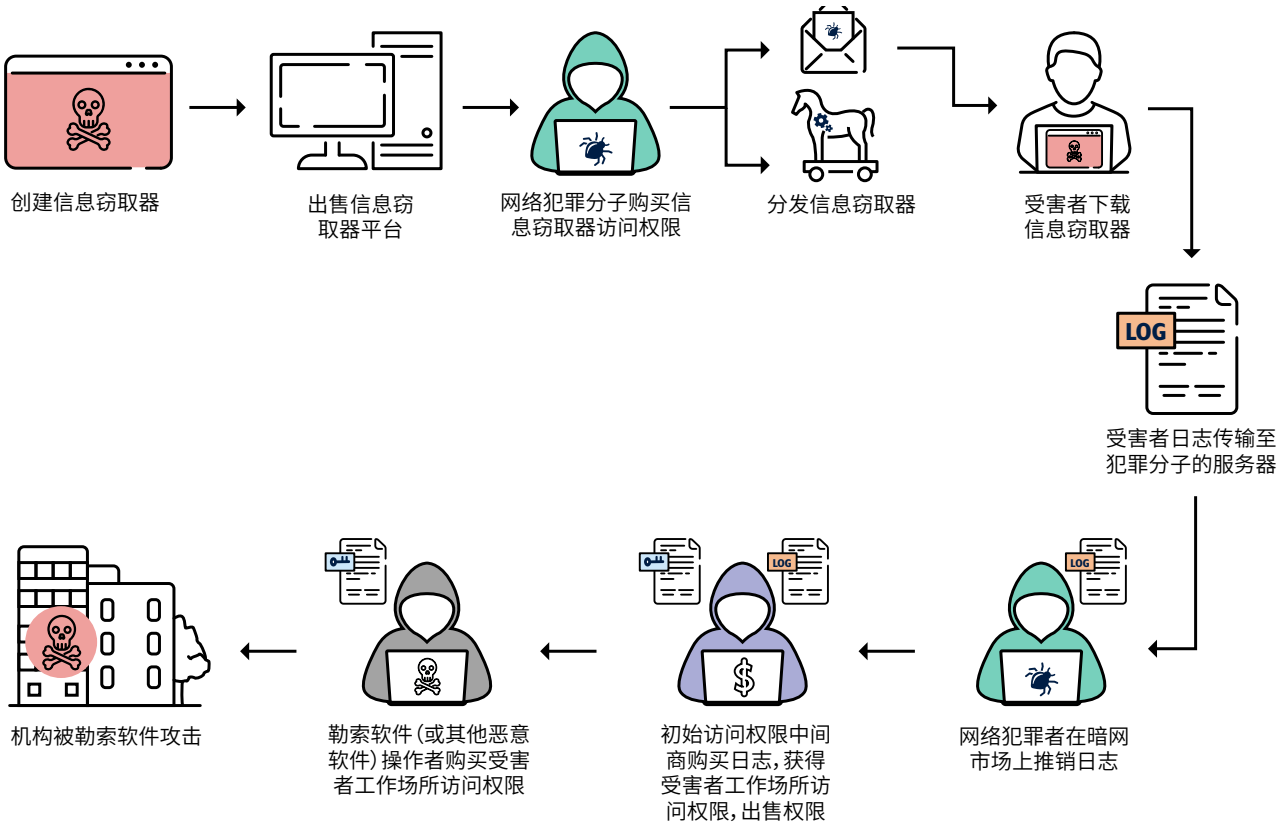


图2. 信息窃取器生态系统与可能对组织造成的影响

影响

信息窃取器可能对个人和组织造成严重影响。当信息窃取器收集到用户凭证后，网络犯罪分子可能利用这些用户凭证，通过有效用户帐户访问企业网络或企业系统，这通常会延迟系统所有者的检测。

对于受信息窃取程序影响的**组织**，后果可能包括：

- 勒索软件
- 数据泄露
- 商务电子邮件泄露
- 知识产权被盗
- 敏感信息被盗。

对于受信息窃取器影响的**个人**，后果可能包括：

- 个人电子邮件或社交媒体账户被未经授权访问
- 身份被盗风险增加
- 网络钓鱼攻击风险上升
- 财产损失或金融账户被未经授权访问
- 隐私丧失。

案例分析：

本案例分析已进行匿名处理，以便公开发布。本案例基于多个影响澳大利亚实体的网络安全事件，这些事件已向ASD's ACSC报告。受影响实体在下文中称为“该组织”。本案例分析中所提及的人员姓名均为虚构，为保护受害者的身份，部分细节已被省略。

该组织是一家澳大利亚企业，允许员工通过个人设备访问企业系统。Alice 是该组织的一名远程工作员工。

在居家办公时，Alice使用个人笔记本电脑远程访问其所在组织的企业网络。Alice在她的**个人笔记本电脑**上，从一个她认为合法的网站**下载**了Notepad++（一种记事类软件）的某个版本。一个**信息窃取器**伪装成Notepad++安装程序。

当Alice尝试安装该软件时，信息窃取器被激活，并开始从她的笔记本电脑中**收集用户凭证**。这包括她的工作用户名和密码，这些凭证已保存在她的网页浏览器的登录信息中。随后，信息窃取器将这些用户凭证发送到一个由网络犯罪团伙控制的远程命令与控制服务器。

被盗日志与其他数据一起打包，然后通过暗网市场**出售给网络犯罪分子**。

一个名叫Bob的网络犯罪分子购买了Alice的用户凭证，并识别出其中与其组织网络服务相关的用户凭证。Alice所在的组织**没有为这些服务配置MFA**，这使得Bob可以仅凭盗取的用户凭证就成功**通过验证并访问**企业网络。

Bob使用被盗的**有效用户凭证**在未被发现的情况下访问了Alice所在组织的企业网络。Bob能够在企业网络内横向移动，识别属于该组织的敏感数据并将其外传，以便对企业实施勒索。

在窃取敏感数据之后，Bob对组织的**数据库和文件系统**进行了**加密**，使其无法被访问。

缓解措施

组织可能无法对其连接到企业网络的设备强制执行控制措施，尤其是员工远程工作时使用的个人设备。ASD's ACSC建议组织重点实施控制措施，以保护自身免受针对用户凭据的信息窃取器带来的风险。这些缓解措施包括：

为员工提供网络安全意识培训

- 通过为员工提供有效培训，防止成功的有针对性的社会工程攻击和恶意文件下载。
- 提高对信息窃取器、其传播方法以及对组织的钓鱼威胁的认识。

保护企业账户安全

- 实施MFA：
- 在外部和内部服务、系统以及敏感数据存储库（特别是针对网络邮件、虚拟专用网络(VPN)和访问关键系统的特权用户账户）中实施MFA。最佳方式是在所有账户上实施防钓鱼的MFA。
- 当用户账户不再需要时，禁用用户账户。
- 限制管理员权限：
- 仅使用专用的锁定工作站（如安全的管理工作站）执行网络管理和其他特权任务。
- 遵循最小权限最佳实践方法，要求管理员使用特权用户账户管理系统，使用标准用户账户执行非管理任务。
- 阻止特权用户账户（明确授权访问在线服务的除外）访问互联网、电子邮件和网络服务。
- 考虑为系统和应用程序实施即时管理。
- 强制管理和审计特权用户账户。
- 定期更新密码，特别是那些面向外部的远程访问账户。
- 对会话令牌和Cookie强制执行生命周期超时和日落策略。

强化企业移动性

- 执行企业移动风险评估并实施企业移动强化指南。
- 如果您允许员工使用个人设备进行工作，请实施“自带设备 (BYOD)”政策，因为企业管理的设备比未受管理的个人设备更安全。

审查和评估访问您的网络的供应商（包括“软件即服务”(SaaS)供应商和受管理服务提供商）带来的供应链风险。如何管理与受管理服务提供商合作时的安全性。

保护您的企业网络

- 保持应用程序和操作系统为最新版本。
- 应用本地安全策略，通过严格的允许列表强制执行应用程序控制。
- 实施网络分区，根据角色和功能分离网络区块。
- 审计和监控用户活动，特别是远程员工的活动。
- 监控特权账户可以揭示对敏感数据的未经授权访问或异常数据传输活动，例如向外部网络上传大量数据。
- 实施防数据丢失策略和工具，以防止未经授权的数据传输。

成为澳大利亚信号局网络安全中心(ASD's ACSC)网络合作伙伴并加入其网络威胁情报共享(CTIS)服务

- 网络威胁情报共享(CTIS)是一个双向共享平台，使政府和行业合作伙伴能够接收和共享有关恶意网络活动的信息。
- ASD's ACSC正在追踪信息窃取器活动，并通过网络威胁情报共享(CTIS)平台共享活跃的命令与控制基础设施的详细信息。
- 注册成为合作伙伴，保护您的组织和客户数据免受网络犯罪威胁。

为入侵做好准备

- 制定网络安全事件响应计划，以便在信息窃取器入侵事件发生时使用。确保员工了解如果他们怀疑自己下载了可疑文件，应该做什么以及联系谁。

实施ASD's ACSC的"基本八项"

- 除上述缓解措施外，ASD's ACSC强烈建议实施其"基本八项"的其余部分。

给远程工作员工的建议

- 保护您的个人设备上的信息
  - 培养良好的上网习惯，不要点击可疑链接或弹出窗口，也不要从未知或不受信任的来源下载文件或软件。
  - 为工作账户和个人账户使用不同的密码。在可能的情况下，为个人账户使用MFA。
  - 除非您的雇主明确批准，否则请勿将您的工作凭证存储在个人密码管理器中。这包括您的网页浏览器的密码管理器。**如有疑问，请要求您的雇主提供企业支持的密码管理器。**
  - 请勿从共享或公共工作站登录您的工作账户。
  - 注意您的网页浏览器自动填表功能中存储的内容。信息窃取器针对浏览器保存的用于自动填充表单的数据。在填写网页表单时，请考虑手动输入敏感数据，例如信用卡号，而不是将其保存到您的网络浏览器的自动填表功能中。
  - 在上网活动结束后，从所有在线服务中登出并清除网页浏览器Cookie，以减少信息窃取器可获取的信息。
  - 确保您的操作系统的内置杀毒功能已启用。如果您使用第三方杀毒解决方案，请确保其保持最新版本，并且是来自信誉良好的供应商。

帮助

受信息窃取器入侵影响或需要帮助的澳大利亚组织，可以通过**1300 CYBER1 (1300 292 371)**或访问cyber.gov.au/report提交报告联系澳大利亚信号局网络安全中心 (ASD's ACSC)。

即使事件被认为已得到控制，ASD's ACSC仍鼓励各实体报告与信息窃取器相关的可疑网络活动和入侵指标。我们利用您提供的信息来加深对网络威胁行为者战术、技术和程序的理解，这有助于我们向以相同方式受到攻击的其他澳大利亚组织发出警告。

免责声明

本指南中的材料具有一般性，不应被视为法律建议或在任何特定情况或紧急情况下可依赖的帮助材料。在任何重要事项上，您都应该根据自己的情况寻求恰当的独立专业建议。

对于因依赖本指南中包含的信息而导致的任何损害、损失或费用，联邦政府不承担任何责任或义务。

版权所有

如需了解更多信息或报告网络安全事件，请联系我们：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

该号码仅可在澳大利亚境内拨打。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre