卡巴斯基嵌入式系统安全解决方案

kaspersky

一体化安全防护，专为嵌入式系统而打造（也适用于其他系统）

嵌入式系统遍及我们身边，每天我们都会与其互动。从 PoS 系统、ATM 到医疗设备和自动加油站，我们在很多地方都要依靠嵌入式系统。随着嵌入式系统市场的发展，网络犯罪分子紧随其后，不断磨炼自己的策略、技术和程序，以适应这些分布广泛的系统的细节。

嵌入式安全挑战

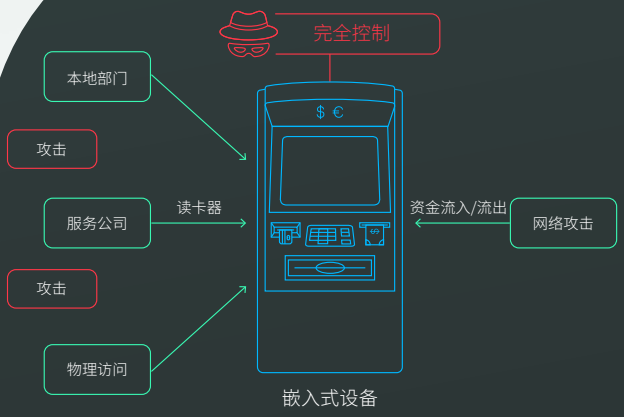
1. **过时且易受攻击的软件。**较长的生命周期可能意味着这些设备运行着不受支持的操作系统和应用程序，其中包含未加修补的漏洞，随时可能被攻击者利用。
2. **无规律的安全更新。**即使软件仍然受支持，也可能存在补丁程序未能及时安装的问题。要更新的多个设备地理位置分散、必须使它们脱机进行更新（从而导致临时拒绝服务）以及在部署更新之前需要测试更新等等有关问题都可能导致补丁程序安装延迟。
3. **流程连续性。**即使是暂时停止使用某些类型的设备（例如医疗设备），也可能造成很大的问题，进一步增加了补丁程序未能及时安装的时长。
4. **公共场所。**许多嵌入式设备都在开放的公共场合中运行，这显著增加了被篡改的风险。网络级防御无法抵御对设备进行的直接物理感染。
5. **其性质存在固有风险。**由于嵌入式设备通常与财务运营直接相关，并处理敏感的个人信息，因此对网络犯罪分子来说尤其具有吸引力。

威胁形势

诸如恶意软件即服务之类的新型犯罪商业模式持续出现，降低了潜在攻击者的技能门槛。尽管 Microsoft 早已不再支持较为陈旧的 Windows 版本，但这些旧版本仍然在使用（Windows XP 依然是嵌入式设备中使用最广泛的操作系统）。数以百万计的嵌入式设备和 PC 继续运行旧版易受攻击的操作系统，出于各种原因，这些操作系统未进行升级。这无异于为黑客敞开了入侵的大门。

与此同时，基于 Linux 的嵌入式系统正在迅速普及，网络犯罪分子正在注意到这一点，调整他们的技术并创建全新的工具以适应基于 Linux 的嵌入式系统的细节。高估 Linux 固有的安全性会很危险 - 虽然攻击者最近才将注意力转向基于 Linux 的嵌入式设备，但他们正在弥补失去的时间。与 Windows 可用的安全产品相比，基于 Linux 的嵌入式设备当前可用的网络安全产品有限，因此无济于事。

如今的企业需要比以往更加精明地采取行动，从而确保系统和数据的安全。卡巴斯基嵌入式系统安全解决方案具有强大的威胁情报、选择加入恶意软件检测和漏洞利用防护、全面的系统强化控制和灵活的管理特性，是专为嵌入式系统设计的一体化安全解决方案。它为大多数网络安全供应商不再支持的旧版系统提供独特的保护级别，现在还可为运行 Linux 操作系统的更加现代的设备提供相同级别的保护。



在针对嵌入式系统的所有成功攻击中，超过半数涉及到员工或第三方服务提供商的“内部人员活动”

物理层攻击

- 黑盒攻击
- PIN 键盘变化/复制器
- 隐藏摄像头
- 爆炸

软件层攻击

- 远程/本地恶意软件安装
- 内存嗅探器/操作系统攻击
- 中间件感染/更改

网络层攻击

- VPN 漏洞
- 暴力破解 RDP
- 允许 RCE 的网络漏洞利用
- 远程安装

嵌入式系统：典型攻击媒介

嵌入式安全挑战

6 **严格规定。**许多嵌入式设备经常会处理财务和个人身份信息，因此需要遵守监管规定，必须采取高度谨慎的安全措施。

7 **内部人员威胁。**根据卡巴斯基的数据，在针对嵌入式系统的所有成功攻击中，有超过 50% 涉及到员工或第三方服务提供商的“内部人员活动”。

8 **Linux 传播。**嵌入式平台的发展极为迅猛，可提供更大的灵活性，并允许使用更广泛的配置。网络犯罪分子正在注意到这一点，与在 Windows 环境中相比，现代专业安全解决方案的选择受到的限制更多。

亮点

为任何嵌入式场景提供最佳保护
卡巴斯基嵌入式系统安全解决方案可提供多层保护，赋予具有不同能力水平和实施场景的设备最佳的安全性。这包括支持基于不同操作系统（例如，Windows 和 Linux）的平台

保护新旧版本的系统
卡巴斯基嵌入式系统安全解决方案经过优化，可在 Windows XP、7、8、10 和 11 中全功能运行。在可预见的未来，卡巴斯基将继续支持 Windows XP，让客户有足够的时间在准备就绪后进行升级。卡巴斯基嵌入式系统安全解决方案还支持运行 Windows 或 Linux 操作系统的最新架构。

低资源消耗，高保护级别
即使是在低端硬件上，卡巴斯基嵌入式系统安全解决方案也能有效地运行。

ATM 和 PoS 攻击增加
根据卡巴斯基研究数据，针对 ATM 和 PoS 系统的攻击数量在 2022 年大幅增长，并且还在继续增长中，与 2020 年相比增长 19%，与 2021 年相比增长 4%。

关键功能

系统强化（安全控制）。这些系统安全强化技术由应用程序、设备和更新控制组成，仅允许使用受信任的应用程序、外围设备和更新来源。这可防止未经授权启动和运行程序，包括恶意软件以及可能被恶意使用的应用程序。

选择加入反恶意软件功能。选择加入安全层，使用在本地或云端运行的威胁情报、启发式模型和机器学习模型，通过精确的检测逻辑检测已知、未知和高级威胁。

漏洞利用预防[1]。防止正在运行的Windows系统组件和第三方应用程序中的漏洞被利用，帮助抵御更高级的攻击，包括旨在避开默认拒绝模式应用程序控制机制的攻击，以及使用无文件技术的攻击。

网络威胁防护。防止对操作系统的任何入侵，防范端口扫描和暴力破解攻击，以及利用网络相关漏洞侵害目标设备的网络攻击。这样，您就可以阻止针对嵌入式系统的主要攻击媒介之一。

完整性监控与合规性支持。对指定注册表项、文件和文件夹执行文件完整性和注册表访问监控上标跟踪，并可以阻止任何不需要的更改。这不仅有助于检测通过恶意软件发起的入侵，还有助于检测对关键资源的直接访问/离线修改。这些通常都是数据保护法规中特别推荐的对策 – 支持它们有助于确保合规性。

支持功能较少的系统和旧版系统。甚至支持使用陈旧硬件和不受支持的操作系统（最低支持 Windows XP SP2）的低功率嵌入式系统。您可以继续安全地运行旧款设备或旧版桌面，直到准备好升级。

日志检查[1]。根据对 Windows 事件日志的监测和检查来检测可能的安全破坏行为。当应用程序检测到显示网络攻击企图的异常行为时，它会通知管理员。

灵活的管理 – 本地或云端。根据您的需求，您可以通过本地管理服务器、Kaspersky Security Center SaaS 云控制台来管理企业嵌入式系统的安全性，以及其他卡巴斯基解决方案。虽然本地管理在要求严格保证隐私的情况下非常有用，但由供应商运行的云端 SaaS 控制台有助于降低资本支出和运营支出，能够快速启动安全的工作流程，同时减少维护烦恼。

防火墙管理。您可以直接从 Kaspersky Security Center 配置操作系统的防火墙，从而通过单个、统一的控制台方便地进行本地防火墙管理。如果嵌入式系统未加入域，并且无法集中配置 Windows/Linux 防火墙的设置时，这项功能尤为重要。

耐受连接性差的情况。由于许多类型的嵌入式设备通常位于远程位置，因此蜂窝覆盖范围不佳、近距离无线电来源的干扰等因素导致连接性差的情况并不罕见。卡巴斯基嵌入式系统安全解决方案即使在非常低的带宽下也能保持稳定，这样即使长时间没有连接也能保持可靠的保护功能。

[1] 仅限 Windows 操作系统

专家服务和高级支持

正确维护安全解决方案的生命周期需要付出很多努力，而嵌入式设备的特殊性使其与常规端点存在差别，因此维护嵌入式系统安全性可能特别费力。Kaspersky Professional Services 可在整个生命周期中提供帮助，包含从部署和更新、配置和性能优化直至迁移到更新型硬件的每一个阶段。我们的高级支持保证优先、专业地解决事件，并由专职技术客户经理提供无与伦比的专业知识支持。

相关产品和服务

卡巴斯基威胁情报： 多样的服务选择，结合情报源、威胁数据源和内部研究，由我们的安全专家进行分析，从而全面地了解针对贵组织的网络威胁。

支付系统安全评估： 对 ATM 和 POS 设备进行的全面分析让您清楚地了解当前的安全级别，使您能够进一步提高安全性、优化其配置并消除任何安全漏洞。

卡巴斯基网络安全解决方案： 全球知名的端点保护平台，利用经过最多测试、屡获殊荣的安全特性保护您的端点、服务器、工作站和移动设备。全部通过单个控制台管理。

行业

- 金融服务
- 交通和旅游（票务）
- 零售
- 餐厅和酒店
- 医疗
- 政府和非商业
- 娱乐业

设备

- 自动取款机
- 售票机
- 加油机
- 结帐
- 销售点
- 医疗设备
- 传统端点
- 投币式自动售货机和游戏机

使用嵌入式设备的行业

网络威胁新闻：securelist.com
卡巴斯基技术：kaspersky.com/technowiki
IT 安全新闻：business.kaspersky.com
中小企业的 IT 安全：kaspersky.com/business
企业的 IT 安全：kaspersky.com/enterprise

www.kaspersky.com.cn

我们屡获殊荣。我们独立自主。我们透明可信。我们致力于建立更安全的世界，让技术改善我们的生活。我们保护世界安全的目的，是让地球上的每个人都能享受它带来的无限机会。确保网络安全，创造更安全的**明天**。

有关更多信息，请访问：kaspersky.com/about/transparency

Proven.
Transparent.
Independent.