HongKe 虹科

针对Linux安全

Linux终端、服务器、工作负载&OT安全的演变

从攻击者的角度来看，Linux是一个完美的目标。这是一个长寿的操作系统，拥有稳定可靠的界面。它托管组织中最关键的静态数据，以及保持业务运行所需的应用程序服务。因为它在历史上被广泛认为是安全的，所以许多组织并没有太过认真地考虑Linux的安全性。但近年来，Linux恶意软件攻击迅速升级，仅在2022年就增长了50%。

Linux安全风险包括：

- 通常用于托管企业最关键的静态和动态数据；
- 倾向于长期处于“ 设置并忘记 ”的状态，这使得安全漏洞无人关注；
- NGAV、EPP和EDR/XDR存在安全漏洞，因为它们是概率性的，而不是确定性的。而且它们不会改变底层系统，因此攻击者可以随时随地训练和攻击；
- 安全漏洞和错误配置在云和内部部署中很普遍，一旦投入生产，就很难修补和加固，尤其是关键任务系统和遗留系统。

核心能力

定期随机化系统级APIs

内核变形：系统范围的保护确保不会出错

只有受信任的代码才能运行；其他所有代码都被捕获以进行取证分析

在运行时自主重写内存中的低级受信任应用程序代码

安全优势

运行时利用漏洞防御

针对受信任应用程序的深度防御

减少传统系统和保护不足系统的攻击面

可忽略的误报警报

运营优势

保护本地和云中的虚拟机和裸机服务器-包括空隙服务器

内存和CPU占用空间可以忽略不计。可以在Raspberry PI、物联网设备和关键金融交易管理服务器上运行。

不需要额外的人员编制--“ 安装即可忘记 ”

维护成本极低，无需更新

结论

阻止各种早期阶段MITRE ATT&CK的战术和技术

在运行时停止供应链和其他高级攻击

阻止较难捕获的Linux操作系统/本机远程代码执行(RCE)和权限提升(PE)，而不会生成误报警报

识别并阻止多变的防御规避和其他高级战术

Gartner 说：“ 自动移动目标防御是一种新兴的改变游戏规则的技术，用于改善网络防御。 ”

Gartner

自动移动目标防御：终端安全的下一步发展

虹科摩菲斯 Linux是一款主动式安全解决方案，通过在内存中随机化API、在运行时阻止供应链攻击和其他用漏洞，保护您最关键的资产免受复杂攻击。

虹科摩菲斯通过自动移动目标防御(AMTD)技术和攻击面减少机制实现了独特的预防能力组合，从而发现了这一点。

虹科摩菲斯Linux是一种有效且全面的解决方案，可缓解Linux平台上基于本地代码的攻击。

MDSec

Supports:

AlmaLinux 8.x、9.x、Amazon Linux 2、CentOS 7.x、8.x、Oracle Linux 7.x、8.x、Red Hat Enterprise Linux (RHEL)6.x及以上版本、Rocky 8.x、9.x、SuSE Linux 12.x及15.x、Debian 9.x及以上版本、Ubuntu 14.04及以上版本。至少使用Intel x86或AMD64体系结构的裸机或虚拟机对于基于ARM的64位架构，我们支持Debian 11、Raspberry PI OS和Ubuntu 22.04 ARM64b，它们都运行长期支持(LTS)内核版本2.6.x、3.x、4.x或5.x。

关于虹科摩菲斯

虹科摩菲斯针对最高级的威胁提供预防优先的安全，以阻止从终端到云的其他攻击。虹科摩菲斯的软件由自动移动目标防御(AMTD)技术提供支持，这是网络安全的下一步发展。AMTD可阻止勒索软件、供应链攻击、零日攻击和其他高级攻击。Gartner研究表明，AMTD是网络的未来。AMTD提供超轻量级深度防御安全层，以增强NGAV、EPP和EDR/XDR等解决方案。我们在不影响性能或不需要额外工作人员的情况下，针对无法检测的网络攻击缩小他们的运行时内存安全漏洞。超过5,000家组织信任虹科摩菲斯来保护900万台Windows和Linux服务器、工作负载和终端。虹科摩菲斯每天可以阻止联想、摩托罗拉、TruGreen、Covenant Health、公民医疗中心等数千次高级攻击。

HongKe 虹科

www.hocyber.com
hocyber@hkaco.com
(+86)135 3349 1614

(+86)400-999-3848
各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港 | 日本 | 韩国 | 新加坡 | 美国硅谷

联系我们