itbigtec
艾体宝

艾体宝Morphisec技术解析

移动目标防御技术

“计算机网络和系统的静态特性使它们很容易受到攻击，因此很难防御。”

—下一代网络基础设施(NGCI)顶点计划

为什么要关心移动目标防御？

下一代自动化网络安全，用于在运行时在内存中阻止勒索软件、供应链攻击、零日、无文件和其他无法检测到的攻击。非常适合增强NGAV、EDR和XDR，不需要额外的员工，也不会对终端或服务器造成性能影响。

移动目标防御（MTD）原理说明

尽管大幅增加了对网络安全的投资，但网络攻击造成的损失继续以前所未有的速度上升，预计到2025年将达到10万亿美元以上。如果现有的解决方案有效，勒索软件和供应链漏洞就不会发生，并造成如此多的财务损失、品牌侵蚀和业务损失。今天的解决方案显然没有对抗威胁参与者的高级攻击。

下一代防病毒(NGAV)、终端保护平台(EPP)以及终端检测和响应(EDR和XDR)解决方案可通过可识别的签名和行为模式阻止已知攻击。但它们通常不会检测或阻止组织今天正在经历的更具破坏性的高级攻击-无法检测到的攻击，如零日、恶意软件变体或导致勒索软件的供应链攻击。Gartner认可的一项新技术已被证明可以阻止Windows和Linux系统上的高级威胁，使预防优先的安全成为现实：移动目标防御(MTD)，也称为自动移动目标防御(AMTD)。

什么是移动目标防御？

MTD可防止勒索软件、供应链攻击、零日攻击、无文件攻击、内存攻击和其他高级威胁。它使用内存中的系统多态，以一种不可预测的方式向对手隐藏操作系统和应用程序目标。这大大减少了攻击面，降低了安全运营成本。

Gartner

“假设一个行窃专家能够撬开任何一扇门的锁。MTD的目标不是建造更好的锁。毫无疑问，改善大门安全的一个值得称赞和必要的目标，但这项任务留给了其他安全解决方案。相反，MTD安全策略的目标是让小偷很难或不可能找到门和门锁。”

通过减少攻击者的机会窗口并增加他们探测和攻击的成本，跨多个网络和系统维度的受控变化增加了攻击者的不确定性和复杂性。

为什么需要移动目标防御技术?

几乎所有的恶意软件都用于使用硬盘或操作系统(OS)上的可执行文件。这些可执行文件留下了它们存在的证据。防病毒(AV)、NGAV、EPP、EDR和XDR等工具的发展是为了发现恶意软件部署的迹象，如攻击模式和签名。然后，它们将在威胁造成真正的破坏之前将其隔离。

但老练的攻击者对传统的网络安全工具很了解。攻击链越来越多地劫持合法的系统进程以达到恶意目的，或者在运行时将目标设备内存作为目标，而不是硬盘或操作系统。被劫持的合法系统进程和内存中的威胁几乎没有提供要检测的签名或要分析的行为模式。

合法的系统进程在运行时必须在内存中工作，但这种环境对目前的网络安全工具来说大多是看不见的。为了抓住正在进行的攻击，它们需要在应用程序运行时多次扫描设备内存，并监听正确的触发操作以发现恶意模式。但在一个典型的应用程序的运行环境中，可能有4GB的虚拟内存。即使设置到最积极的警报设置，也不可能足够频繁地扫描这一数据量。至少在不降低应用程序速度的情况下，使其几乎无法使用。

为了确保可用性，内存扫描器只能在特定的内存位置和特定的时间线触发器上寻找高度特定的参数。在最好的情况下，一个以扫描为重点的解决方案可能会扫描一小部分应用程序的内存。但是，现在的威胁也使用多态性来混淆它们的存在，所以在如此小的设备内存样本中捕捉到恶意活动将是奇迹。

积极的警报设置也会导致大量的假阳性警报，需要额外的资源来分析。如果大量的警报和误报对使用当前网络安全工具的组织来说不是一个问题，那么他们的警报设置可能太低。他们几乎肯定错过了最具破坏性的高级攻击。

这就是企业需要MTD的原因。

自动移动目标防御技术使运行时的内存环境变形，以创造一个持续变化的、不可预测的攻击面。这意味着，即使威胁行为者在极不可能的情况下找到了他们的目标，他们也无法在另一台设备上重复使用这种攻击，甚至以后在同一台设备上也是如此。MTD使用一个超轻量级的代理来确定地阻止未经授权的进程，而不是以概率的方式。这意味着MTD很少产生假阳性警报，也不会明显影响系统性能。它可无缝集成到技术栈中，通过深度防御增强NGAV、EPP、EDR和XDR，以阻止内存、无文件、零日、供应链攻击和其他高级威胁。

移动目标防御：创新和颠覆性技术

移动目标防御使用与攻击者类似的技术，如多态性、欺骗性和逃避性。它通过随机化应用程序内存运行时间来混淆目标，因此威胁行为者无法准确识别他们的目标。

想象一下，在一条有路标的岔路口。在一个方向是一个充满财富的豪宅。另一个方向则是一个危险的峭壁。MTD会切换路标所指向的方向。

走这条假想路的威胁者会被转移到峭壁上。同时，合法的交通仍然被送往豪宅。员工可以完成工作，而威胁者则被拒绝进入。

移动目标防御的好处是什么?

长期以来，网络安全的主流范式一直侧重于检测和响应。这种方法本质上是被动的，并把创新优势让给了威胁者。

MTD改变了保护关键系统的计算方式。它是一个主动的、预防为主的系统。它打断了网络攻击的进展，并阻止了威胁者在目标组织中获得持久性的能力。

美国国土安全部将移动目标防御定义为："在多个网络和系统维度上控制变化，通过减少攻击者的机会之窗和增加他们的探测和攻击努力的成本来增加不确定性和复杂性"。

自动移动目标防御通过减少 "假阳性 "安全警报、IT支持票和分析师警报分流时间，降低了IT和安全团队的成本和努力。

它通过多态性和规避来保护关键系统，而这些多态性和规避正是对手在过去10年中所使用的巨大效果。它为防御者提供了一种主动的方法，而不是等待威胁者入侵他们的系统并找到漏洞。它使企业能够在勒索软件传播和实施之前防止终端上的违规行为。

主动防御,而不是被动防御不会等到攻击者入侵后才起作用

多态防御隐藏漏洞,免受多态攻击

阻止攻击者获得持久性的能力

虚拟补丁保护漏洞，直到补丁发布

大幅削减成本、误报警报和所需的IT资源

移动目标防御技术如何工作

其他终端保护解决方案必须首先检测到攻击，才能阻止它。Morphisec通过拆除它们的传输机制和杀伤链来防止高级攻击；检测永远不会出现在其中。移动目标防御将内存变形，使攻击无法找到它们的目标。即使是最先进的规避式攻击和无文件的恶意软件也会被立即阻止。

Morphisec入侵预防平台使用专利的零信任执行技术来主动阻止规避性攻击。它通过以下三个步骤来实现这一目标。

第1步：变形和隐藏

当一个应用程序加载到内存空间时，Morphisec会对进程结构进行变形，使内存对攻击者来说始终是不可预测的。

第2步：保护和欺骗

合法的应用程序代码内存被动态更新以使用变形的资源；应用程序照常加载和运行。原有结构的框架被作为一个陷阱留下。

第3步：防御和揭露攻击

攻击以原始结构为目标，由于找不到他们期望和需要的资源而失败。攻击会被立即防御，被困住，并记录下完整的取证细节。

艾体宝科技有限公司

www.itbigtec.com
sales@itbigtec.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼

T (+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

版本：V1.0 - 22/11/14

网络安全与监控方向
(T: 135 3349 1614)

网络安全交流2群

获取更多资料

itbigtec.com