黑客思维

你不知道的事物会伤害你

> **过去和未来的边界已模糊不清；他的过往经历和未来终将经历的融合在一起，除了当下，别无他物。**

— 菲利普 · 迪克 (Philip K. Dick)，
《仿生人会梦见电子羊吗？》

拥抱元宇宙

元宇宙不再是科幻小说里的故事内容。正如我们所说，元宇宙已经发生了微妙的变化，从参加虚拟音乐会和拍卖活动，到使用增强现实家具应用程序，消费者逐渐开始接受元宇宙。

“元宇宙”是由“meta”（意为“超越”）和“verse”（来源于“宇宙”一词）这两个单词组成的新词。它将增强现实和虚拟现实结合在一起，让人们可以在这种交替的数字现实中工作、娱乐和社交。

从本质上讲，元宇宙是下一个新的互联网时代。通过这一激动人心的生态系统，企业可以利用新的方式与客户互动，从而将数字经济提升到新水平。事实上，已经有很多企业正在构建元宇宙的某些部分，并且还有一部分企业已经确立了令元宇宙发挥作用的具体愿景。

最终，元宇宙会将物理世界和数字世界无缝地融合在一起。

然而，将企业扩展到物理世界之外的虚拟世界，是一项庞大而又复杂的迁移工程，会带来一系列新的安全问题。我们需要问的问题是：我们如何为这次迁移做好准备？

虚拟现实 (VR):

全人工环境；完全沉浸式的虚拟环境体验

增强现实 (AR):

虚拟对象叠加到真实环境中；现实世界通过数字对象得到了增强

混合现实 (MR):

虚拟环境与现实世界的结合；彼此交互

扩展现实 (XR)/元宇宙:

以上所有技术的融合

可以确定的是，随着我们过渡到元宇宙，您的企业所面临的攻击面也将显著扩大。虽然我们可以使用现有的防护技术，但可能无法抵御前所未有的新攻击。

随着我们步入元宇宙时代，金融交易不仅涵盖虚拟商品，还将涵盖通过更广泛的渠道（包括 AR/VR 交互）销售的现实世界商品和服务。

在当今的社交媒体营销时代，卖家通过 API 将其系统与社交媒体平台关联，进而销售商品，获得销售收入。元宇宙中开设了近乎无限的虚拟店面，这给数据隐私和身份验证带来了更大的挑战。

在元宇宙时代，安全性意味着要确保虚拟世界中创建的内容的安全性并保护个人数据。因此，像 Akamai 这样有着极高全球边缘平台覆盖率的边缘平台公司将会发挥非常重要的作用。

来自 Akamai 的 Jonathan Singer 根据风险投资家马修 · 鲍尔 (Matthew Ball) 的定义，介绍了元宇宙可能会给首席安全官及其团队带来的挑战。

从本质上讲，元宇宙让您可以在虚拟空间中以数字身份执行各种活动和开展金融交易。它会像智能手机一样逐渐渗入到人们的日常生活中，这也是人类发展的必然趋势。总有一天，它会在不知不觉中成为我们生活的一部分。

在向元宇宙迈进的过程中，您的企业制定了哪些相关计划?

定义	挑战
元宇宙是一个规模庞大的	身份验证、访问策略、恶意软件、加密和安全流量、DNS 安全性、Web 应用程序攻击
互操作网络	正常运行时间、DDoS 攻击、突发的大量访问
由实时	安全性与性能的权衡、API 安全性、流媒体保护、反盗版
渲染的 3D **虚拟世界**组成	欺诈、物理/访问安全性、硬件/物联网安全性、内容完整性
能同步并有效地为**无限数量的用户**提供体验，并让每个用户都有自己的存在感	突发的大量访问、MFA、大规模安全性
同时支持众多数据的连续性，例如身份、	安全注册、凭据调配、授权
历史数据、	加密、PII
授权、	加密、PII、欺诈预防、知识产权、支付安全性
对象、通信	加密、PII、欺诈预防、知识产权
和支付。	加密、PII、欺诈预防、PCI 合规性、标记化、支付风险

游戏安全性 — 我们的元宇宙安全发展蓝图是什么?

为了迎接元宇宙的到来，以及应对在此之前出现的各种挑战，我们建议各行业的所有首席信息安全官都来先熟悉一下游戏行业的受众群体和安全挑战。

元宇宙现有的基础技术很大一部分来自游戏行业，并且深受其影响。

随着大量技术不断融合到一个相互关联的社交/技术领域，视频游戏显然已成为铺平前进道路的关键驱动行业之一。游戏业开创了技术和互动模式，其应用范围并不局限于视频游戏本身。

元宇宙现有的基础技术很大一部分来自游戏行业，并且深受其影响。不仅是技术，游戏行业的业务模型也广泛应用于各行各业。

在十年前，帐户的主要价值在于信用卡号，以及任何可能帮助犯罪分子入侵银行账户的信息。

时至今日，游戏帐户本身就是一笔财富，因为玩家在其中投入了游戏时间并积攒了游戏道具。这些投入了玩家大量时间和积攒了众多装备的帐户一旦被盗，即可让其购买者不费吹灰之力便能够在游戏中达到高段位水平。游戏道具也可以在第三方市场出售，换取真金白银。

这种形式的虚拟价值已经反映在投资界，从人们购买 NFT 代币便可窥见一斑。随着整个世界和您的企业朝着元宇宙迈进，保护帐户和访问权限仍将是企业的首要任务。

当所有公司都将业务运营迁移到元宇宙之后，公司与用户和员工围绕帐户安全开展合作将成为客户体验和品牌关系的重要组成部分，同时也将扩大安全性在企业中的作用。

Akamai 对于游戏领域的问题知之甚深。我们发布的报告包括《犯罪分子针对游戏行业的攻击方式和原因》，以及近期发布的两份有关游戏安全性的互联网现状报告：《保障安全岂能单打独斗》和《疫情下的游戏行业》。

每一篇文章都从几个方面分析了，在攻击者接连不断的攻击下，应该如何保持系统在线和正常运行。

《保障安全岂能单打独斗》报告中还介绍了 Akamai 与国际游戏会议组织 DreamHack（现称 ESL Gaming）针对硬核玩家合作开展的一项调查的结果，旨在更好地了解玩家对游戏安全性的感受，以及在涉及到保护自己的游戏帐户时他们认为个人应承担多大的责任。

如果不谈谈 Roblox，任何关于疫情期间元宇宙和游戏业的讨论都是不完整的。尽管由于疫情全球肆虐，孩子和父母都曾困在家里，但是 Roblox 为儿童和青少年参与社交、发挥创造力和接收教育提供了途径。据估计，Roblox 上发布的游戏数量在 52 万至 4000 万之间。似乎选择范围有点宽泛，但确实如此。

Roblox 正在发展成为一家全球化实体，它需要为开发人员、玩家等人群交付安全一致的体验，无论他们身处何地。糟糕的用户体验，例如加载速度慢或断网，可能会导致企业收入损失。

Roblox 寻求 Akamai 的帮助，以确保成功打造性能优异的在线多人游戏和游戏创作体验。

借助 Akamai 产品，这家公司能够为世界各地的开发人员和玩家提供安全、一致的体验。

了解详情：

Roblox 面向全球玩家交付高性能游戏体验

点击阅读

Chun Chat 与文明黑客的对话

Chun Han　　Alex Leung

Chun Han 是 Akamai 的解决方案工程设计经理，喜欢与 Akamai 的很多安全专家交流。

这次他的访谈对象是 Alex Leung，Alex 是一名获得认证的文明黑客和高级企业架构师，他一直在非传统地点开展安全评估工作。Alex 分享了他认为勒索软件无孔不入的原因。

Chun: 您最近都在忙些什么?

Alex: 我一直在针对大型网络活动（例如，最近举办的东京奥运会）开展网络安全评估和媒体流咨询工作。

Chun: 在您看来，黑客目前都对哪些领域感兴趣?

Alex: 由于疫情原因，底层 IT 基础架构已经发生了结构性转变。随着员工开始远程办公，内部系统被推到风口浪尖，攻击面也因此骤然扩大到整个互联网。Microsoft Exchange 服务器攻击与突如其来的攻击面扩大有关。

首席信息安全官以前能够进行系统分类，并访问公司办公室的物理边界。随着越来越多的公司迁移到云端，这一边界已逐渐变得模糊不清。疫情是压垮骆驼的最后一根稻草，疫情期间，几乎没有人还在原来的边界内，最终表明基于边界的安全模式是有缺陷的。

因此，首席信息安全官现在更倾向于采用 Zero Trust 网络访问 (ZTNA) 设计，除非得到确认，否则一切皆被视为可疑行为。

Chun: 您认为哪些领域易受攻击?

Alex: 自 2013 年以来，供应链攻击一直是恶意黑客的目标。和公司一样，黑客也关心投资回报率 (ROI)。也就是说，网络犯罪分子更感兴趣的是找到最薄弱的环节，而不是攻克那些无懈可击的部分。

因此，每当我听到首席信息安全官谈论某款卓越的网络安全工具时，我都会对潜在盲点表示担心。对恶意黑客来说，网络安全优势与他们的攻击策略无关，他们总是在寻找最薄弱的环节。

过去，很多勒索或勒索软件活动都会涉及每秒千兆的大规模 DDoS 攻击。在疫情期间，网络犯罪分子可以利用大量常见漏洞和风险 (CVE)，以及实施过程中的缺陷。只需通过零日漏洞发起一次隐秘但却有效的漏洞利用攻击，就可以植入勒索软件，而无需会触发 WAF 警报的强大攻击手段。投资回报率看起来非常高。

Chun: 说得很对。传统的黑客通过容积攻击来击溃本地安全设备，并窃取所需信息。而现在，偷偷侵入并保持“正常”状态不仅可以降低成本，而且让您几天甚至几年都很难发现有攻击的存在。您认为勒索软件受害者应该支付赎金吗?

Alex: 如果您的公司收到了勒索信，Akamai 建议不要支付赎金，因为即便支付，也不能保证对方会停止攻击。此外，支付赎金只会加强犯罪集团的财务实力。

Chun: 是的，我见过一些支付赎金的案例，结果不难想象。攻击者没有遵守诺言；加密数据也没有完全恢复。在一些案例中，攻击者发起了二次攻击，另外还提出了赎金要求。不过，我们能否通过访问暗网来主动防范此类攻击?

Alex: 正如孙子所说，“知己知彼，百战不殆。”要制定防御策略，必须要了解恶意黑客的战术和心态。

我建议首席信息安全官订阅 Akamai 的《互联网现状》(SOTI) 报告，我们会在这些报告中详细介绍网络安全趋势，以及在暗网中观察到的一些值得注意的情报。例如，我们了解到，被盗账户的售价可能低至 1.30 美元。这有助于推断出攻击者发起一次撞库攻击的经济成本。

了解遇到勒索软件攻击时可主动采取的措施：

勒索攻击卷土重来

点击阅读

> “知己知彼，百战不殆。”
>
> — 孙子

Chun: 是的，我看到过这类内容，如果帐户与信用卡详细信息一致，则售价会提高 10 倍。我之前参与过网络安全攻防项目，知道攻击者被拦截时会变得更加兴奋。他们会不断尝试新的战术，可能从晚上 9 点一直持续到凌晨 3 点。这就是黑客们的心态吗？喜欢玩刺激的胜负游戏？

Alex: 是的，我们在实时流量中抵御攻击时，的确会刺激到他们的肾上腺素。然而，不论好坏，最终结果很大程度上都取决于我们在危机发生前冷静时所做出的决定，即准备、演习和监控。

Chun: 英雄所见略同。如果让您给首席信息安全官们一条建议，会是什么？

Alex: 我建议定期重新审视我们的假设。恶意黑客比大多数文明黑客更务实，也更谦卑。他们会定期审视自己的假设，并以批判性的方式评估什么做法有效、什么做法无效。这让他们得以不断发展和调整策略。这样做还有助于我们发现自身的盲点。

观看 Chun Han 对话 Alex Leung 的采访视频（英文版）

Chun 热衷于提供快速、可靠且安全的数字化体验。

如果您想了解更多有关 Akamai 与我们提供的解决方案，请

联系我们