精译版

# xDedic 市场数据对企业造成威胁

**非官方中文译文·安天技术公益翻译组 译注**

| 文档信息 | | | |
|---|---|---|---|
| 原文名称 | xDedic Marketplace Data Spells Danger for Businesses | | |
| 原文作者 | Kelly Sheridan | 原文发布日期 | 2017 年 4 月 25 日 |
| 作者简介 | Kelly Sheridan 是 Dark Reading 的副主编。http://www.darkreading.com/author-bio.asp?author_id=837 | | |
| 原文发布单位 | Dark Reading | | |
| 原文出处 | http://www.darkreading.com/threat-intelligence/xdedic-marketplace-data-spells-danger-for-businesses--/d/d-id/1328721? | | |
| 译者 | 安天技术公益翻译组 | 校对者 | 安天技术公益翻译组 |
| 分享地址 | 请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块 | | |
| 免责声明 | • 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。<br>• 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。<br>• 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。<br>• 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 | | |

# xDedic 市场数据对企业造成威胁

Kelly Sheridan

2017 年 4 月 25 日

**xDedic 是暗网上的热门市场，它销售 RDP（远程桌面协议）服务器的访问权限，帮助犯罪分子攻击政府和公司。**

xDedic 是暗网上最大和最具破坏性的市场之一。六个月前，商业风险情报公司 Flashpoint 发现它拥有一个数据库，其中包含超过 8.5 万个组织的信息。

网络犯罪分子在 xDedic 市场上购买受感染的 RDP 服务器的访问权限，这样一来，他们就能轻松进入在线系统，特别是具有远程 IT 人员的公司。RDP 是微软的专有协议，它允许用户通过网络连接到其他机器，使管理员能够远程控制服务器和 PC。

Flashpoint 研究总监维塔利·克雷莫斯（Vitali Kremez）表示，Flashpoint 监控 xDedic 市场至少两年了。该市场自 2014 年投入运营，在网络犯罪分子之间建立了很好的声誉，这些犯罪分子攻入企业的 RDP 服务器，然后在该市场上转售凭证。

克雷莫斯解释说，黑客通常先扫描网络，寻找连接到微软远程桌面协议的特定端口。在确定了具有开放端口的服务器之后，他们会通过暴力破解的方式来测试用户名和密码组合，直到找到匹配项。

一旦他们获得 RDP 服务器访问权限，就会在 xDedic 市场上销售访问凭证并更新管理员权限。任何购买凭证的人都能够进入企业网络，进而窃取数据、提升权限、启动外部攻击、部署勒索软件、植入恶意软件、操纵网络设置以及控制账户。

克雷莫斯指出，对于简短而弱效的服务器密码来说，黑客的暴力破解非常有效。但是，他们很难破解更长更复杂的密码。然而，即使服务器的凭证很强大，大型僵尸网络仍然可以帮助攻击者获得 RDP 服务器访问权限。

克雷莫斯解释了以攻击医疗机构而闻名的威胁源“The Dark Overlord”是如何利用 xDedic 数据库来执行攻击的。医疗机构经常被攻击，这是因为一旦犯罪分子能够访问开放的 RDP 服务器，就能够窃取有价值的数据。

“我们一直在调查针对医疗机构的攻击行为”，他继续说，“我们发现，很多医院被攻击的原因是其 RDP 服务器凭证泄露了。”

但是，医疗机构并非头号目标。

xDedic 数据库包含超过 8.5 万台服务器的信息，能够帮助我们了解黑客最喜欢攻击的行业。数据分析显示，最常被攻击的行业包括教育、医疗、法律、航空和政府。美国，德国和乌克兰是最常被攻击的国家。

克雷莫斯说：“教育机构是最不安全的，最容易受到伤害。”他指出攻击者能够很容易地通过暴力攻击进入大学网络。然而，大学和医疗机构都有信息共享社区，他们可以通过这些社区共享攻击信息，并改进其信息安全程序。

克雷莫斯认为，xDedic 的威胁还会继续增长，特别是在 Shadow Brokers 发布漏洞利用工具之后。如果犯罪分子继续开发工具包并利用这些漏洞，扩展对其他网络的访问权限，那么他们将会造成更大的伤害。他指出，虽然这些漏洞并非零日漏洞，但它们仍然是很危险的。

克雷莫斯建议企业不要将服务器连接到外网并采取适当的访问控制措施。虽然对技术人员和网络程序来说，将服务器连网更加方便，但这是很危险的，因为网络犯罪分子通常会暴力破解这些连网的 RDP 服务器的访问凭证。

他还建议采取密码预防措施。“经常更改密码，并使密码尽可能复杂。”他继续说，“至少，这样能够阻止 xDedic 攻击者。”