Mirai 开始攻击 Windows 系统

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	Lovely. Now someone's ported IoT-menacing Mirai to Windows boxes		
原文作者	John Leyden	**原文发布日期**	2017 年 2 月 10 日
作者简介	John Leyden 是 The Register 记者，主要关注安全领域。 https://uk.linkedin.com/in/joleyden		
原文发布单位	The Register		
原文出处	https://www.theregister.co.uk/2017/02/10/windows_mirai_bot/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
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。 • 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。 • 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。 • 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。		

Mirai 开始攻击 Windows 系统

John Leyden

2017 年 2 月 10 日

你打开了电子邮件，这全是你的错.....Windows PC 现在也能传播 Mirai 了。

劫持了数十万物联网设备（小工具和路由器等）的 Mirai 恶意软件现在也能够感染 Windows 系统了。

Mirai 是在 2016 年 8 月被发现的，它感染了全球大量不安全的 Linux 设备，然后对目标（主要是 DNS 提供商 Dyn）发起 DDoS 攻击。许多家庭用户依赖 Dyn 的服务器来支持他们的网站和在线服务；在 2016 年 10 月的攻击中，很多网站和服务被迫下线，导致大量用户无法上网。

受影响的设备包括很多个人数字录像机，网络摄像头等。Mirai 扫描具有开放端口的机器，然后使用默认或硬编码的密码登录，从而控制这些机器。

本周，俄罗斯安全软件制造商 Dr Web 的研究人员发现了 Mirai 僵尸程序的 Windows 版本，该版本首先感染微软主机，然后扫描存在漏洞的物联网设备。这意味着，如果公司网络上的 Windows 客户端和服务器遭到感染，则相邻的存在漏洞的设备也会遭到攻击。

该 Windows 版本用 C++编写，被命名为 Trojan.Mirai.1，它使用 IP 地址和密码列表来扫

描网络中的设备并尝试登录这些设备。如果 Trojan.Mirai.1 通过 Telnet 进入 Linux 机器，就会在受感染的机器上下载并运行 Linux.Mirai，从而继续传播。如果它在网络上找到了 Windows 机器，就会利用 WMI（Windows 管理规范）和 IPC（进程间通信）在计算机上启动一个新的进程来感染它，从而继续传播。

2017 年 1 月底，研究人员首次在微软系统上发现了 Mirai，它使用 MS SQL Server 事件服务，作为管理员执行命令并安装恶意软件。

该木马如何在公司网络上创建据点呢？这取决于它的主要工具，例如，利用电子邮件附件作为诱饵。如果你的 Windows PC 和服务器被未经授权的软件感染，你最先想到的可能是你的物联网设备。话虽如此，该恶意软件只需要成功感染一个或两个 Windows 机器，就能够在企业的 Linux 设备中传播。

加利福尼亚州 DDoS 缓解公司 Nsfocus IB 的技术专家理查德·麦尤斯（Richard Meeus）说，Mirai 的最新变种对企业带来了更大的风险。

麦尤斯说："Mirai 能够利用 Windows 机器传播意味着，它已经建立了一个进入私人网络的途径。以前，我们认为没有直接连网的物联网设备面临的风险不那么大。鉴于许多家庭和企业都在使用 Windows 设备，Mirai 现在能够感染更多的设备了。"