Mirai 僵尸网络仍在肆虐

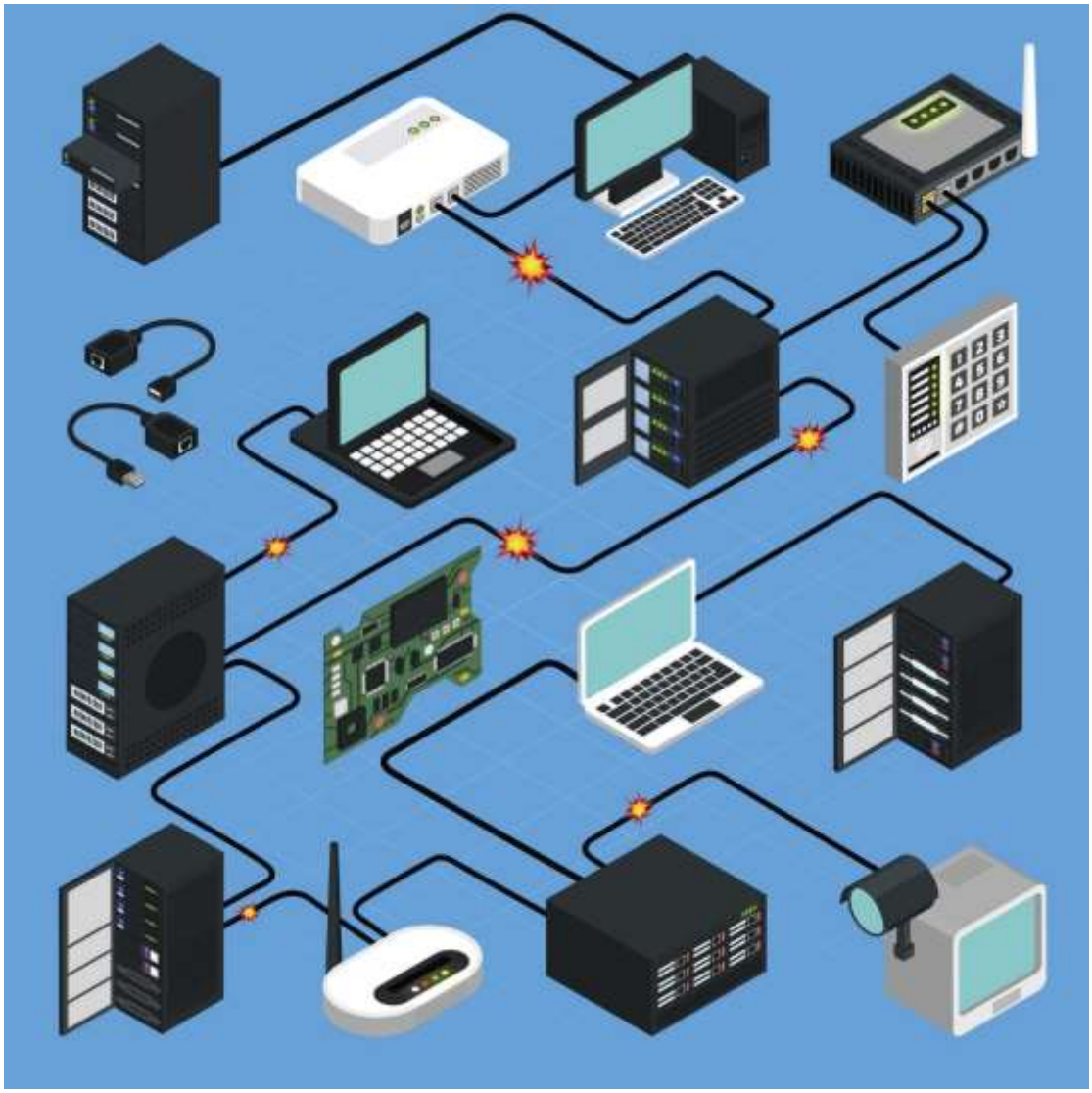
非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	The Botnet That Broke the Internet Isn't Going Away		
原文作者	Lily Hay Newman	**原文发布日期**	2016 年 12 月 9 日
作者简介	Lily Hay Newman 是《连线杂志》安全领域的作者。https://www.linkedin.com/in/lilyhnewman/		
原文发布单位	《连线杂志》		
原文出处	https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/		
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 僵尸网络仍在肆虐

Lily Hay Newman

2016 年 12 月 9 日



Mirai 僵尸网络在今年 9 月首次出现，它的登场让人惊艳。它利用僵尸物联网设备的流量对一位知名安全记者的网站发动洪泛攻击，通过攻击 Dyn（提供很大一部分的美国骨干网）导致数百万用户无法上网。从那时起，攻击数量不断增加。我们越来越清楚地意识到，Mirai 具有强大的破坏力。

Mirai 是一种自动寻找物联网设备进行感染，并将其纳入僵尸网络（一组可以集中控制的计算设备）的恶意软件。之后，这个物联网僵尸网络可以执行 DDoS 攻击，用大量的垃圾

流量洪泛目标的服务器。在过去的几个星期里，Mirai 破坏了 90 多万德国电信客户的互联网服务，并感染了英国近 2400 个 TalkTalk 路由器。本周，研究人员发布的证据显示 80 个索尼相机型号容易受到 Mirai 的感染。

Mirai 控制了大量的调制解调器和网络摄像头，而且名为“Anna-senpai”的黑客在 9 月公开了它的代码，因此 Mirai 攻击层出不穷。虽然 Mirai 的软件没有什么特别的新奇之处，但是它非常灵活，适应性很强。因此，黑客可以开发不同的 Mirai 变种，来控制新的物联网设备，增加 Mirai 僵尸网络可以利用的设备（和计算能力）。

Qualys 的产品管理副总裁克里斯·卡尔森（Chris Carlson）说：“因为有着广泛开放、无保护的物联网设备，所以 Mirai 正在加速增长，不断地将这些设备纳入僵尸网络。”

僵尸网络

物联网恶意软件的崛起让人联想到困扰早期互联网用户的病毒、蠕虫和垃圾邮件。当时，大多数电脑没有足够的安全措施，争相进入网络泡沫的公司也不一定了解互联网安全的重要性。现在也是如此，但是目标从电脑转向网络摄像头和路由器。

然而，如今的技术时代有着明显的不同之处，即：用户如何与被感染的设备交互。被感染的电脑通常会出现故障，运行速度减慢或弹出通知（通过操作系统安全警报或通过恶意软件本身[类似勒索软件的情况下]）。所有这一切都鼓励人们采取措施。标准做法是在企业 PC 上安装安全软件，反病毒软件也很受家庭用户的欢迎。

一些物联网设备，如路由器，能够通过最少的用户交互无限期运行。Mirai 很难控制的一个原因是它潜伏在设备中，并且通常不会显著地影响它们的性能。普通用户（更有可能是小企业）压根想不到他们的网络摄像头可能沦为了僵尸网络的一部分。即使能够确定，他们也基本无计可施，没什么直接的方法来修复被感染的产品。

网络安全防御公司 Digital Shadows 的战略副总裁瑞克·霍兰德（Rick Holland）说：“这类似于 21 世纪初的网络安全状况，设备缺乏安全性。漏洞设备的数量不会下降，而是会增加。”

很难清除

Mira 并不是唯一的物联网僵尸网络。越来越广泛的物联网设备安全问题不容易解决，

数十亿设备面临各种恶意软件的攻击。

但是现在 Mirai 是最主要的僵尸网络，因为它容易获得，可以调整，能够用不同的变种执行不同的活动。霍兰德指出，Digital Shadows 研究人员发现越来越多的 Mirai 用户寻求帮助（有时恶意行为者也需要技术支持！），彼此提供提示和建议。

消费者可以采取一些预防措施来提高其个人物联网的安全性。通过评估家中使用的物联网设备，消除无需任何理由直接访问互联网的多余“智能”产品，人们可以减少攻击风险。此外 对于提供可访问接口的设备 您可以更改默认密码和下载固件更新以获得更好的保护。

正如关键基础设施技术研究所发布的报告一样，在物联网安全全景中，Mirai 终将成为一个“阶段性威胁”。有了新玩具，黑客就会对 Mirai 失去兴趣，受 Mirai 感染的设备数量也会减少。

不过，这一天来得不会太快。Mirai 已经有足够的资本来维持几年，而且更易受感染的产品每天都会出现。正如报告所说，Mirai “激发了物联网漏洞利用的复兴”。在此期间，也会出现更多的混乱。

霍兰德说：“谁知道今年结束之前会出现什么呢。但是能够肯定的是，Mirai 不会很快消失。”