Anna-Senpai 是何方神圣？

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	Who is Anna-Senpai, the Mirai Worm Author?		
原文作者	Brian Krebs	原文发布日期	2017 年 1 月 17 日
作者简介	Brian Krebs 是《华盛顿邮报》的一名记者。https://krebsonsecurity.com/about/		
原文发布单位	Krebs on Security		
原文出处	https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/?winzoom=1		
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。		

Anna-Senpai 是何方神圣？

Brian Krebs

2017 年 1 月 17 日

2016 年 9 月 22 日，我的网站遭到了恶意软件 Mirai 的攻击，被迫下线了将近 4 天。Mirai 利用不安全的物联网设备（如无线路由器和监控摄像头）创建僵尸网络，执行大型网络攻击。大约一个星期后，该攻击的幕后黑手“Anna-Senpai”公布了 Mirai 的源代码，此后便出现了数十个模仿者。

经过几个月的调查，KrebsOnSecurity 确定了 Anna-Senpai 的真实身份，以及至少一个帮助编写和修改该恶意软件的同伙的身份。

2016 年 9 月 30 日，Anna-Senpai 公布了 Mirai 的源代码。

在继续分析之前，我先做出两点声明。首先，这是我写过最长的博文，因为我想捋一捋这几个月的调查过程。这些信息有助于读者了解 Mirai 的经济动机和之前的僵尸网络活动。其次，我在博文中提及了很多名字和术语，因此我编写了一个词汇表。

本文基于几百个小时的研究结果。有时候，我迫切地寻找看似无关的人和事件之间的缺失链条；有时候，我被大量的信息（其中大部分是虚假或误导性的信息）淹没，努力地去伪存真。如果您不理解为何只有极少数网络犯罪分子被绳之以法，我可以告诉您，在网络时代，要想弄清楚谁对谁执行了什么攻击，需要非凡的耐心和大量的调查资源。

在之前的文章中，我介绍过类似 Mirai 的僵尸网络，它们以天为单位攻击个人、企业、政府机构和非营利组织，导致他们无法上网。在这些“分布式拒绝服务（DDoS）攻击”中，

攻击者利用数千个被感染的系统，向目标发送大量的垃圾流量，导致目标无法处理合法的请求。虽然 DDoS 攻击通常针对单个网站或主机，但是通常会导致广泛的互联网服务中断。

大量 DDoS 活动源于所谓的“压力测试”(booter/stresser)服务。这些服务本质上是 DDoS 租赁，能够帮助技能拙劣的用户执行重大攻击。我们将会看到，非法 DDoS 租赁行业的激烈竞争导致一些人剑走偏锋。

线索

我发现 Mirai 是一个被广泛使用了将近 3 年的物联网僵尸网络家族的最新变种，至此，我终于找到了确定 Anna-Senpai 身份的线索。

2016 年夏天，我的网站遭到了几次大型攻击，攻击者利用了被一个僵尸网络家族感染的物联网系统，我们认为该僵尸网络家族就是 Mirai 的前身。该恶意软件有好几个名字，包括“Bashlite”，“Gafgyt”，“Qbot”，“Remaiten”和“Torlus。

所有相关变种都以类似蠕虫的方式 (从一个主机传播到另一个主机) 感染新系统。被感染的系统进行网络扫描，试图找到能够加入僵尸网络的其他设备。有时候，这些扫描太过猛烈，会在不经意间对家庭路由器、网络摄像头和 DVR 造成 DDoS 攻击。这种行为类似于早些年的 Morris，NIMDA，CODE RED，Welchia，Blaster 和 SQL Slammer。

被感染的物联网设备不断扫描网络，希望找到其他可以感染的设备，特别是使用出厂默认设置和密码的设备。然后，被感染的设备被迫参与 DDoS 攻击 (讽刺的是，Mirai 和类似的物联网蠕虫最常感染的正是监控摄像头)。

Mirai 的前身有很多名字，每个名字都对应着一个变种，这说明它在不断改进。在 2014 年，一个名为“lelddos”的攻击团伙公开使用了该家族的代码，发动了大规模的持续攻击，导致很多网站下线。

Lelddos 团伙最常攻击的是托管游戏《我的世界》的网络服务器。(《我的世界》是微软销售的一款非常流行的计算机游戏，可以在任何设备和任何网络上运行。)

《我的世界》是一款带有生存冒险元素的建造类游戏，整个游戏世界由各种方块构成，玩家可以破坏它们 ,也可以用自己的方块随意建造东西。该游戏听起来可能有些简单和无聊，但是颇受欢迎，尤其是受男孩欢迎。微软已售出超过 1 亿份副本，任何时候都有超过 100

万人在线玩这个游戏。玩家可以建造自己的世界，也可以登录最喜欢的服务器与朋友一起玩。

Minecraft.net

每天有超过 1000 个玩家登录的大型服务器每月可轻松盈利超过 5 万美元，主要的赢利点是：玩家租用服务器上的空间构建自己的世界，购买游戏装备和特殊能力。

不足为奇，收入最高的《我的世界》服务器最终吸引了勒索者（如 lelddos 团伙）的注意。Lelddos 团伙知道，服务器下线一天，其运营商就会少赚几千美元，因此他们对服务器发起大规模 DDoS 攻击，进而勒索赎金。

更糟糕的是，如果被攻击的服务器无法及时上线，很多忠实客户就会选择其他的服务器。

ProxyPipe 是一家专门保护《我的世界》服务器的公司，罗伯特·科埃略（Robert Coelho）是该公司的副总裁。

科埃略表示："《我的世界》行业竞争相当激烈。如果你是一名玩家，你最喜欢的服务器下线了，你可以切换到另一个服务器。但是对于服务器运营商来说，最重要的就是玩家数量和强大的服务器。登录服务器的玩家越多，运营商赚得就越多。如果服务器下线，运营商就会迅速流失客户，也许会永远失去这些客户。"

2014 年 6 月，ProxyPipe 公司遭到了 lelddos 团伙的 DDoS 攻击，攻击流量达到 300 Gbps。该团伙还在 Twitter 上公开嘲讽 ProxyPipe。