

简译版

如何远程操控服务器并将其“变砖”

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	How to Remotely Brick a Server		
原文作者	Kelly Sheridan	原文发布日期	2018 年 12 月 19 日
作者简介	Kelly Sheridan 是 Dark Reading 的编辑。 https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/application-security/how-to-remotely-brick-a-server/d/d-id/1333531		
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	<ul style="list-style-type: none"> 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。 		

如何远程操控服务器并将其“变砖”

Kelly Sheridan

2018 年 12 月 19 日

研究人员演示了如何远程操控服务器并将其“变砖”，服务器“变砖”会对企业带来严重且不可逆转的后果。

研究人员报告称，如果攻击者能够访问公司的服务器，那么整个公司就是他们的囊中之物了——他们会滥用这种访问权限，远程将服务器变砖。

大多数人认为，固件攻击和其他造成永久性损害的攻击都是物理攻击。然而，Eclypsium 公司的研究人员演示了如何利用基板管理控制器（BMC）和系统固件中的漏洞，远程将服务器变砖和破坏基础设施。对企业来说，这将是一场灾难。

Eclypsium 的工程副总裁约翰·卢瑟戴斯（John Loucaides）表示，将系统变砖的想法并不新鲜。虽然这个概念已经出现了一段时间，安全专家也发现了可能导致此类攻击的漏洞，但是很少有人演示攻击过程。现在，Eclypsium 发布了研究报告，希望提高人们对此类远程攻击的认识——此类攻击能够大规模执行，造成巨大的破坏。

“服务器变砖会造成相当严重的影响，”卢瑟戴斯指出。如果受到恶意软件感染，我们可以擦除受影响的系统并恢复备份数据。但是，如果服务器变砖，我们需要去机房现场打开每个受影响的服务器，重新刷固件。卢瑟戴斯解释说，这是一个缓慢的技术过程，超出了大多数 IT 人员和当前企业系统的能力。“在这方面，传统网络安全缺乏对策。”他说。

他指出，攻击者并不需要多么高超的技术，就能执行此类攻击。许多人认为这是国家级别的攻击，其实并不是。互联网上存在很多开源工具包，攻击者可以利用这些工具包访问和操控目标系统，导致系统无法运行。Eclypsium 在演示中首次使用了这种方法，并强调称，成功执行此类攻击的门槛并不高。

卢瑟戴斯指出，类似的威胁已经出现。例如，攻击者用已经损坏或无效的固件来替换服务器组件。Eclypsium 演示的攻击方法基于其之前对 BMC 的研究，即通过远程利用 BMC 漏洞将服务器变砖。（译者注：BMC 是独立于服务器的计算机，用于远程配置系统，不需依赖主机操作系统或应用程序。BMC 采用传感器来远程监控服务器、计算机以及其他硬件设备

的物理运行状态：包括但不限于供电电压、风扇速度、湿度、温度，减轻管理员的工作量，提升管理效率，降低维护成本。)

攻击演示效果是如何达成的

第一步是进入公司网络。“首先，我们需要通过某种方法感染公司网络。”卢瑟戴斯解释道，例如利用恶意软件感染公司系统、窃取凭证等。

随后，研究人员使用常规更新工具将恶意固件映像发送给 BMC。他们在一篇博客中指出，这一步不需要身份验证或凭证。固件更新包含额外的代码，一旦这些代码被触发，就会擦除 UEFI 系统固件和 BMC 固件的基本组件。

为什么将 BMC 作为攻击目标呢？卢瑟戴斯说，服务器的任何部分都可以作为攻击目标，而且会得到类似的结果，但是攻击 BMC “最容易理解、效果最明显”。而在勒索软件攻击或其他重大攻击场景中，BMC 用于恢复系统。

在第三步中，BMC 接收并启动映像。BMC 负责系统管理和恢复，因此它可以在系统的任何部分安装组件。研究人员利用他们在 BMC 中安装的恶意功能来破坏系统固件；通过破坏 BMC，他们就切断了系统操作员的恢复路径。

卢瑟戴斯解释说，第三步完成后，在执行第四步之前，攻击者会执行恶意代码。一旦攻击者通过窃取凭证获得访问权限，他们就可以执行恶意代码了；或者他们可以在 BMC 中安装一个组件并将其保留任意长的时间。“这些不需要同时进行，”他补充道。最终的载荷可以由定时器或外部 C&C 触发。

第三步和第四步的间隔时间取决于攻击者的目标。卢瑟戴斯说，如果他们想要造成最大程度的损害和破坏，他们会尽可能感染更多的组件，然后同时将它们变砖。在第五步中，BMC 重启服务器，但是服务器已经不可用了。

如何应对攻击

卢瑟戴斯表示，现有的安全措施并未关注固件或硬件，但是有一些方法可以阻止此类攻击。首先，我们可以通过基本的网络安全措施来防止初始感染，例如保护凭证、使用多因子身份验证等。

“我们无法完美地解决所有问题，”他承认道，“总有地方会出错。我们的诀窍是：评估

系统中不同组件的完整性。”

他指出，在应用程序和操作系统层面，人们都很关注更新。但是，在固件层面，并没有多少人关注更新。安全团队应该定期扫描和监控基础设施，以便及时发现和阻止异常情况。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>