简译版

对付挖矿软件的五招

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	5 Steps to Fight Unauthorized Cryptomining		
原文作者	Matt Downing	原文发布日期	2018 年 8 月 1 日
作者简介	Matt Downing 是 Alert Logic 公司首席威胁情报研究员。 https://www.darkreading.com/author-bio.asp?author_id=5019		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/5-steps-to-fight-unauthorized-cryptomining/a/d-id/1332391		
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。 • 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。		

对付挖矿软件的五招

Matt Downing

2018 年 8 月 1 日

挖矿软件看起来只是一种干扰，但它有可能会导致大麻烦。

作为首席信息安全官（CISO）或网络安全专家，有一天你可能会发现“异常情况”——用户的计算机运行速度变慢了。或者，通过调查，你可能会发现企业的电费突然飙升了数百甚至数千美元。

此时，企业网络和/或 web 环境可能已经被挖矿软件感染了。不过，不用惊慌。挖矿软件通常不会窃取敏感数据或故意执行破坏。它们的目的是，利用你的计算资源偷偷挖掘加密货币。

乍一看，这似乎是一种“无害的”犯罪活动。但是，其风险可能与僵尸网络、恶意软件、勒索软件等威胁不相上下。挖矿软件成功感染你的网络或云环境后，会劫持企业付费的资源，这可能会导致企业资源进一步被利用，或者至少能说明企业的网络安全措施存在差距，有被恶意利用的风险。

随着比特币的估值——2017 年 12 月，1 枚比特币的估值高达 2 万美元——不断飙升，犯罪分子对加密货币挖矿愈发感兴趣。即使此后，加密货币的估值出现下降，但是加密货币市场仍然蓬勃发展。预计今年年底，加密货币市场将达到 1 万亿美元，而在 2 月份，这一数值是约 4170 亿美元。

黑客不断“借用”计算能力，是因为他们需要大量的处理能力来运算复杂的数学公式，从而创建数字货币。根据普华永道（PwC）区块链专家亚历克斯·德·弗里斯（Alex de Vries）发布的研究报告，目前全球比特币挖矿至少需要 2.55 千兆瓦的电力，预计今年年底可能会达到 7.67 千兆瓦（作为对比，整个奥地利的电力消耗是 8.2 千兆瓦）。

对电力的贪得无厌，促使黑客感染企业的云环境和网络，而其目的仅仅是为了利用其充足的计算资源。云监控和防御公司 RedLock 的研究人员称，在过去的一年中，黑客已经感染了若干大型公司的亚马逊网络服务（AWS）和 Microsoft Azure 环境，包括英国跨国保险公司 Aviva、全球最大的智能卡制造商 Gemalto、电动汽车和太阳能制造商 Tesla 等。

卡巴斯基实验室称，为了获得企业级的资源使用权限，攻击者会在企业网站中嵌入挖矿软件脚本。这样一来，他们无需在每台计算机上安装恶意软件，就可以利用大量计算机的资源了。他们还在 YouTube 广告中嵌入脚本，通过多个网页和视频传播这些脚本，然后守株待兔。

Bad Packets Report 网站的研究显示，这种做法很普遍——目前有将近 49,000 个网站托管着某种挖矿软件。这其中，超过五分之四的网站托管的是挖掘门罗币(Monero)的 Coinhive 挖矿软件。黑客青睐门罗币的原因是：门罗币的交易几乎无法追踪；而且不同于比特币（需要专门的设备来挖掘），门罗币可以使用商用硬件进行挖掘。

此外，并非所有的挖矿活动都是无害的。今年 5 月份，360 Total Security 公司发现了一个名为 WinstarNssmMiner 的恶意软件，这是一种新型的门罗币挖矿软件，当杀毒软件试图将其删除时会导致系统崩溃。360 Total Security 指出，在 3 天的时间里，他们拦截了超过 50 万次的 WinstarNssmMiner 攻击。

任何存在漏洞的应用程序都将成为挖矿软件的目标，任何不够安全的接口都将被它们利用。幸运的是，只要保持良好的网络安全意识和习惯，就能防止大多数此类攻击。下面，我们将介绍其中的五种方法。

1. 更新病毒特征库和补丁

尽管加密货币挖矿非常“新型”和“热门”，但是此类攻击比较简单。它们的运作方式与传统恶意软件一样——利用稍加修改的商用挖矿软件，然后使用标准协议与挖矿服务器进行通信。如果你的病毒特征库定期更新，就很有可能会检测到此类感染。最安全的做法是，及时给主机打补丁——优先考虑面向外部的主机和被公开披露的漏洞。

2. 使用最新版的软件和应用程序

同样，从供应商处获取最新版的软件和应用程序，也可以提高企业的安全性，使其免受旨在利用旧产品中漏洞的挖矿软件的侵害。

3.避免使用未经身份验证的平台和 API

默认情况下，未经身份验证的平台和应用程序编程接口（API）是不安全的，黑客可以

对它们进行远程管理。例如，我们发现攻击者利用 Alert Logic 公司未经验证的 Docker Daemon API，挖到了 175 枚门罗币，当时总值约为 35,000 美元。因此，请启用身份验证，不要将这些服务直接暴露在互联网上。

4. 不要将云凭证保存在公共 Github 仓库中

攻击者意识到，通过监控 GitHub 可以获得大量的 AWS 密钥。如果你错误地“提交”（commit）了包含凭证的内容，那么攻击者只需几分钟就能搜罗数百个关于帐户凭证的实例。请确保你的开发人员没有使用公共 Github 仓库来生成或测试代码，尤其是云架构的凭证。

5. 监控 Windows 任务管理器

任务管理器会显示你的 CPU 是否过载。对云来说，在运行期间的“正常”CPU 利用率可能高达 80%。但是挖矿软件火力全开，寻求全天候 100%的 CPU 利用率。如果你在企业环境中发现了 100%的 CPU 利用率，基本可以确认遭遇了挖矿软件。

如上文所述，加密货币挖矿攻击并不会让你夜不能寐。到目前为止，此类攻击的影响更多地是干扰和电费增加。但是，这毕竟是一种感染，说明企业的整体网络防御生态系统存在漏洞。通过上述五种方法，你可以向挖矿软件传达这样一个信息：此处无矿可挖，请滚开。

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，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，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，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。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，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“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*