
安全

# 加密货币挖矿：是绵羊还是恶狼？


Ben Nahorney
2018 年 12 月 11 日 - 0 条评论

牟利是攻击者发起威胁的主要动机之一。从出租僵尸网络协助他人实施 DDoS 攻击，到冒充技术支持诱使人们相信自己的计算机存在问题，乃至利用零售终端上的木马病毒盗取信用卡号，我们今天所看到的许多威胁相关活动都是以牟取利益为根本目的。

到目前为止，恶意加密货币挖矿是 2018 年最突出的以牟利为目的的威胁形式。在最近一段时间里，思科 Talos 威胁情报团队就这一主题开展了大量研究。对攻击者来说，恶意加密货币挖矿是近乎完美的犯罪方式：它潜伏在后台，几乎不需要与目标进行交互，就能帮助攻击者牟取暴利。

在深入研究这种威胁之前，我们先来探讨一下加密货币和加密货币挖矿。

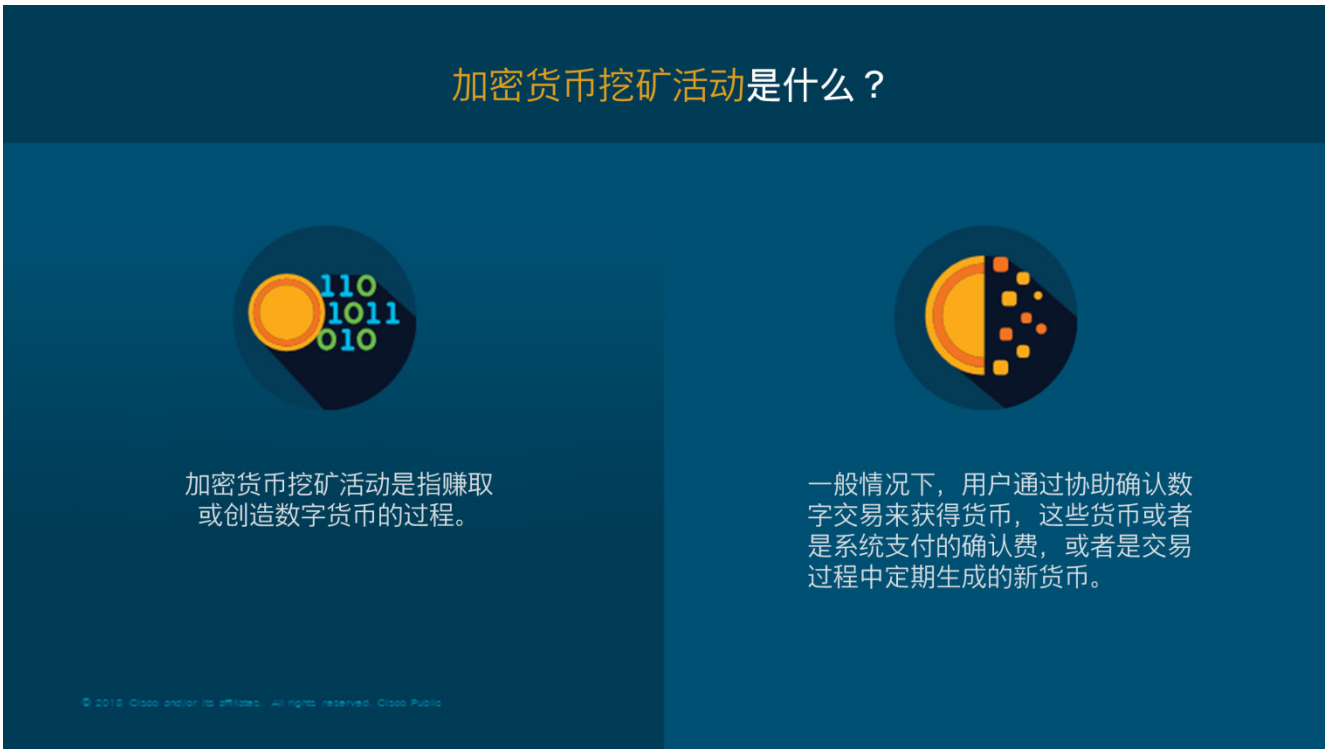
# 加密货币是什么？

按照最基本的定义来讲，加密货币是指未与集中式银行系统（例如全球各个国家/地区或经济区运营的银行系统）关联的数字货币。大约在十年前，比特币的出现让加密货币声名大噪。如今，加密货币市场已充斥着数千种不同的数字货币。

令加密货币广受欢迎的一项功能便是区块链技术，即利用公共数字化账本来验证货币和交易的技术。区块链技术在本质上是一个使用加密货币确保交易安全的加密型分布式系统，因此它很难被修改或篡改，这也是它的主要优势。

# 加密货币挖矿是什么？

无论它是被称为货币挖矿或加密货币挖矿，还是简称为“挖矿”，都是指生成或赚取新货币的过程。虽然不同货币之间存在细微差异，但挖矿主要是指在区块链系统中验证交易的过程，执行该验证过程的用户将会获得一笔费用作为报酬。具体而言，用户可以通过帮助验证区块链和其中包含的交易账本来赚取货币。



对某些加密货币来说（例如比特币），当区块链中添加了新交易区块时，也会生成新币。比特币的例子很好地说明了如何通过在区块链中验证交易来 “挖掘” 新币。

# 加密货币挖矿有什么坏处吗？

事实上，这没有什么坏处。无论是加密货币，还是加密货币挖矿，本身都不具备任何恶意性质。现今有不少人是出于正当的目的来使用加密货币和从事加密货币挖矿活动的。要区分正当的日常加密货币挖矿活动和我们所称的恶意加密货币挖矿活动，一个重要的因素是看是否获得用户的许可。

通常，用户自行安装的加密货币挖矿软件与恶意攻击者安装的加密货币挖矿软件之间并无太大差异。事实上，在许多情况下，二者是完全相同的。唯一的不同点在于，恶意加密货币挖矿软件是在所有者不知情的情况下进行挖矿活动的。任何在设备所有者不知情的情况下运行的软件都会让人感到不安。

# 恶意加密货币挖矿是如何成为主流威胁的呢？

在恶意加密货币挖矿出现之前，恶意攻击者惯用的牟利手段是勒索软件。但是，随着用户越来越了解恶意软件锁定计算机所用的技术，企业也能越来越好地防止勒索软件带来的灾难，恶意攻击者开始另寻他法。

与之前的牟利方法相比，恶意加密货币挖矿还有一些明显的优势。勒索软件并不能保证设备用户一定会支付赎金。他们可能会定期备份，或者受感染设备上的文件对他们无关紧要。而且无论是哪种情况，只要通过重镜像恢复设备就能解决问题。

与此同时，世界各地的执法机构开始打击勒索软件攻击者，这增加了他们面临的风险。随着与勒索软件相关的逮捕事件日益增加，越来越多的网络攻击者倾向于采用风险更小的攻击方法：恶意加密货币挖矿软件。

在过去几年和 2018 年上半年，加密货币的价值不断攀升。正如其他任何与软件相关且有价值的事物一样，加密货币也引起了恶意攻击者的关注。另一方面，勒索软件的效果却大不如从前，这进一步促使攻击者转向加密货币。

恶意加密货币挖矿的发展还得益于其他几项独特优势。其中吸引人的一项优势是，加密货币挖矿是一种游走于灰色地带的威胁。由于合法加密货币挖矿和恶意加密货币挖矿之间只有细微的差异，所以许多用户在被后者攻击时，并不如当他们发现系统中存在其他威胁时那么担忧。如果它只是在后台挖矿，而不实施任何恶意活动，那有什么要担心的呢？这便是攻击者十分看重的一项优势，他们可以悄无声息地窃取利益，而不会引起受害者的关注。

# 披着羊皮的狼仍然是一匹狼

经过更加深入的思考，我们有充分的理由认为恶意加密货币挖矿值得高度关注。

与计算机上的任何其他软件一样，加密货币挖矿也会占用资源。而当一款软件占用太多资源时，它便会对整体系统性能产生负面影响。不仅如此，使用的资源越多，耗电就越多。就单个系统而言，电力成本的增加可能并不明显。但如果将其乘以组织中终端的数量，电力成本将会显著增加。

此外，加密货币矿工利用公司网络赚取收益也会造成合规性问题。对金融业的组织而言则更是如此，因为无论相关负责人是否知晓此类活动，使用公司资源创造收益的行为都受到严格的限制。

不过，也许最令人担忧的问题是，用户并不知道系统被恶意加密货币挖矿软件感染，他们在不知情的情况下运行网络时，这些恶意软件可能会导致网络配置或整体安全策略出现安全漏洞。而此类漏洞很容易被攻击者利用，谋取其他利益。那么，如果发现网络被加密货币挖矿软件感染，可以采取哪些基本措施来阻止其他恶意威胁利用相同的漏洞来进一步实施恶意活动呢？

# 恶意加密货币挖矿软件是如何感染设备的呢？

造成感染的方法有很多，而且大多数方法都并不新奇。植入恶意加密货币挖矿软件的方法与植入其他恶意威胁的方法并无差别:

- 利用终端和基于服务器的应用中存在的漏洞
- 利用僵尸网络将加密货币挖矿软件散播到新设备和以前曾受过感染的设备
- 发送包含恶意附件的邮件
- 利用 JavaScript 脚本使设备可通过网络浏览器进行加密货币挖矿活动
- 利用恶意广告软件安装浏览器插件，进行加密货币挖矿活动


这些只是恶意加密货币挖矿软件感染设备的几种较为常见的方式。当然，与其他任何威胁一样，只要有入侵系统的方法，攻击者便会进行尝试。

# 如何预防恶意加密货币挖矿威胁？

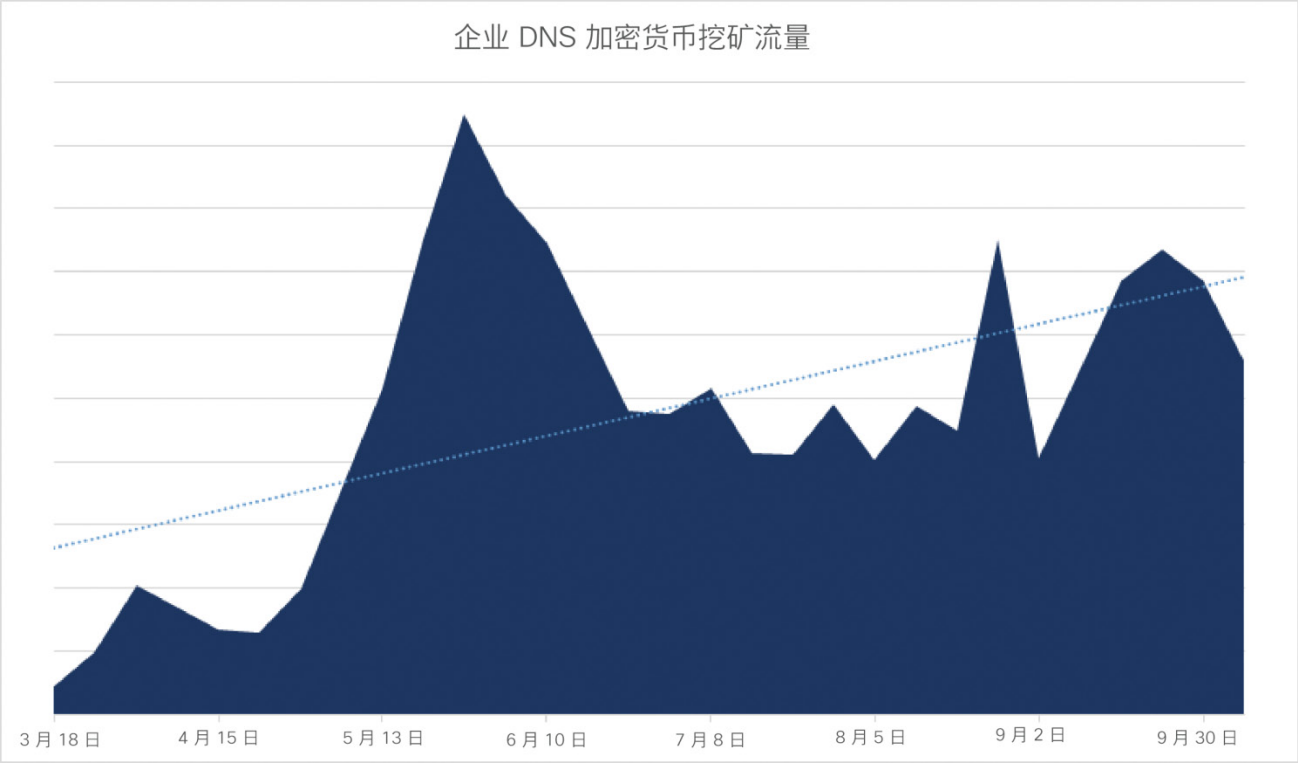
与对待其他与威胁相关的事物一样，良好的安全防护部署能够很好地将恶意加密货币挖矿软件拒之门外。

- 要检测并阻止恶意加密货币挖矿活动，您需要拓展防御策略，将高级终端保护作为其中的一项内容。
- 您可以运用网络安全分析来发现组织中可能会出现加密货币挖矿活动的位置。
- 要防止加密货币挖矿应用找到落脚点，您应该阻止您的网络连接到已知涉及加密货币挖矿活动的网站。
- 部署 DNS 层安全策略也能极为有效地阻止加密货币挖矿活动，防止挖矿交易被发回到恶意攻击者的设备。

总而言之，如果您实施分层安全防护措施，采用由新一代防火墙、终端、安全分析和 DNS 层构成的有效安全防线，就能更好地检测和阻止加密货币挖矿软件感染您的网络。

# 此类攻击的现状和长期前景如何？

从其发展历史来看，加密货币市场经历了巨大的波动。根据我们观察到的情况，恶意加密货币挖矿活动的起落与加密货币价值的激增和暴跌是同步的。以思科在 DNS 层上观察到的加密货币挖矿相关总体流量为例，虽然存在走势陡峭的波峰和波谷，但整体看来，随着时间的推移，加密货币挖矿活动呈上升趋势。




值得注意的是，在同一时期，许多常见加密货币的价值都出现下滑，整体呈跌落趋势。其中一个例子是门罗币，这是恶意加密货币挖矿活动中常用的一种虚拟货币。


造成这一差异的原因可能有很多。最简单的原因可能是，由于恶意加密货币挖矿软件部署简单且被捕的风险较小，恶意攻击者不断推出此类恶意软件，并且只要用户未发现此类恶意软件或者根本不在乎设备上是否有此类恶意软件，它们就能够长期潜伏在设备内，不断为攻击者赚取收益。

或者，有可能正是由于加密货币价值下滑，才导致加密货币挖矿活动整体增长。因为随着加密货币价值出现下滑，攻击者通过感染设备赚取的收益也会下降，为了维持收入，他们需要让恶意加密货币挖矿软件感染更多的设备。

# 结论

从过去到未来，牟利一直是恶意攻击者的主要动机。从许多方面来看，恶意加密货币挖矿都是一种能让攻击者以极小的代价来牟取暴利的手段，而且与其他

威胁相比，受害者不会过于担心这种威胁可能带来的后果。尽管如此，这种威胁造成的间接损失依然是不可忽视的问题，应当予以重视。

有关详细信息，请阅读我们发布的如何保护您的网络免遭加密货币挖矿活动侵害白皮书。如果您准备采取应对措施，请了解思科 DNS 安全解决方案的功能，并申请 14 天免费试用。我们一如既往地欢迎您在下方的评论区留言。

**喜欢这些类型的文章？请订阅 Threat of the Month 博客，及时获得我们针对新威胁发布的通告。**

*更新：我们的 Talos 威胁情报团队新近完成了两篇博客文章，介绍读者可能感兴趣的加密货币挖矿活动相关状况。Nick Biasini 的博客文章详述了 2018 年加密货币挖矿活动历程，包括值得关注的攻击策略以及他对 2019 年攻击活动的预测。他们还分析了三个值得注意的加密货币挖矿团伙（Rocke、8220 挖矿团伙和 Tor2Mine）的活动。*

标签:

- 比特币
- 加密货币
- 加密货币挖矿活动
- 安全
- 安全思想领袖
- 威胁情报
- Threat of the Month