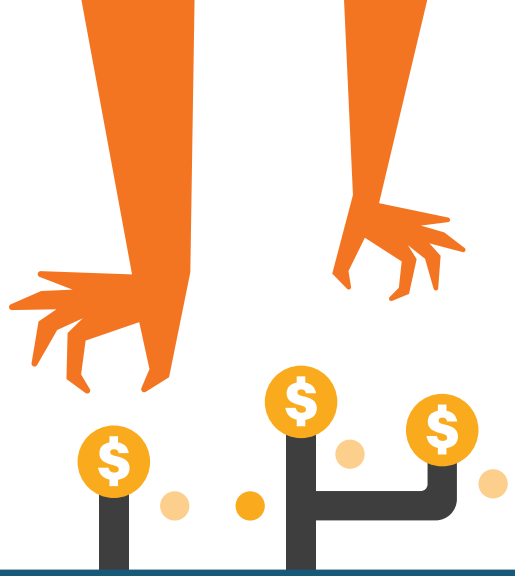
Threat of the Month: 恶意加密货币挖矿



恶意加密货币挖矿是什么？

当今活跃的威胁活动大多是以帮助恶意攻击者牟利为目的。这在勒索软件方面尤其明显：攻击者会锁死受感染的设备，阻止用户使用，向用户索要赎金。但是，感染用户设备并不能保证他们一定会支付赎金。如今，攻击者意识到加密货币挖矿是很好的牟利方法，而且通常情况下，用户甚至不会发现自己已经遭到这种攻击。威胁悄然潜伏，攻击者无需劫持整个系统，就能从中牟利。这种方法简直完美到难以置信：只要威胁未被发现，攻击者就可以坐收渔利，静等加密货币源源不断地流进自己的口袋。

您为何要关注此种威胁？

虽然恶意加密货币挖矿不如勒索软件等威胁那样极具破坏性，但是如果攻击者认为能以这种方式与被攻击者和谐共处，那就大错特错了。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。依据我们的经验，当一款软件占用太多资源时，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资源赚取收益也会造成合规性问题。

加密货币挖矿如何运作？

加密货币挖矿活动是指赚取或创造数字货币的过程。一般情况下，用户通过协助确认数字交易来获得货币，这些货币或者是系统支付的确认费，或者是交易过程中定期生成的新货币。加密货币挖矿有两个途径，一种是在计算机上安装专用于在后台挖掘货币的应用，另一种是通过网络浏览器进行。当用户请求从托管挖矿软件的 Web 服务器打开网页时，服务器会发送一个挖矿数据包，只要打开特定网页，该数据包就会进行货币挖矿活动。

为什么需要重视此类攻击？

挖矿应用本身不一定是恶意的。只要愿意，任何人都可以在自己的计算机上安装挖矿应用。然而，防病毒软件和其他终端技术并不一定能分辨合法挖矿软件和未经批准的挖矿软件。如果您想查明挖矿软件的来源，以及安装后它尝试进行通信的对象，就需要有更加全面的安全解决方案。

延伸阅读

- 使用思科安全产品阻止加密货币挖矿活动
- 保护您的网络免受加密货币挖矿威胁
- https://blogs.cisco.com/security/demystifying-cryptocurrency-mining-threats
- https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

CXX-XXXXXX-00　09/18

我该怎么做？

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，采用高级终端保护。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。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。

思科如何为您提供保护？

下一代防火墙/下一代入侵防御系统	检测并阻止恶意流量，例如与货币挖矿网站的连接。
面向终端的高级恶意软件防护 (AMP)	阻止安装已知的恶意加密货币挖矿应用。
思科 Stealthwatch®	在网络的任何位置（甚至包括在加密流量中）检测加密货币挖矿活动，并隔离受感染的主机（通过思科 ISE 实现隔离）。
思科 Umbrella™	阻止流向分类为“加密货币挖矿”的已知域的流量。