每月热点威胁：数字化敲诈勒索

什么是数字化敲诈勒索？

数字化敲诈勒索是一种网络钓鱼攻击，最终目的是从收件人处骗取钱财。这与预付费欺诈十分相似，比如说：某位银行经理声称有一笔数百万美元的款项等您认领；漂亮的外国女性或帅气的外国男性希望您汇给他们一笔钱，以便他们能远赴千里之外与您见面。许多网络钓鱼攻击试图诱使攻击对象产生一种虚假的安全感和信任感，但是数字化敲诈勒索截然相反：这类攻击通过威胁收件人来骗取钱财。

什么是性勒索？

这是数字化敲诈勒索的一种形式：骗子声称他们入侵了一个色情网站，并表明您（收件人）访问过该网站。他们当时入侵了您的电脑，并控制了您的网络摄像头，不仅录下了您的行为，也录下了您的屏幕。最后，他们声称已盗取您电脑中的所有联系人信息，如果您不通过比特币支付一笔封口费，他们会把（子虚乌有的）“罪证”发给这些联系人。

数字化敲诈勒索有哪些其他类型？

虽然性勒索似乎是数字化敲诈勒索最常见的形式，但是我们也见过一些以收件人生命或其他事物为要挟的攻击。有时，骗子会冒充杀手，受人委托要取收件人的性命。

但是如果收件人愿意付款，他们可以网开一面。其他骗术还包括炸弹威胁（去年 12 月曾在美国和加拿大造成大恐慌），或者声称收件人参与联合作假等等。

延伸阅读

- https://blog.talosintelligence.com/2018/10/anatomy-of-sextortion-scam.html
- https://blog.talosintelligence.com/2018/12/bitcoin-bomb-scare-associated-with.html

这类邮件有没有可能所述为真？

不可能。虽然有些色情网站确实遭到入侵或无意中成为恶意软件的帮凶，但是到目前为止，我们还没有听说过有人因为访问色情网站被黑客入侵，随后被黑客索要财物的例子。同样，杀手恐吓、炸弹威胁和其他勒索形式也没有过前例。考虑到所有这些事实，可以确定这些邮件不过是骗子散播的网络钓鱼邮件。

我该怎么做？

首先，如果您收到这类向您勒索比特币的邮件，请视若无睹。其次，当今大多数反垃圾邮件解决方案应该都能检测并阻止大多数数字化敲诈勒索邮件。在邮件服务器上启用 DMARC 协议也可以帮助过滤掉非法邮件。最后，宣传教育是抵御这类骗术的最有力武器。教用户学会识别这类诈骗邮件是避免受其影响的长久之策。

思科如何为您提供保护？

思科邮件安全	检测数字化敲诈勒索邮件，并阻止其传递到您组织中的收件人手中。
高级网络钓鱼保护	利用高级机器学习技术，进一步增强思科邮件安全解决方案的发件人验证功能。
思科域保护	通过验证 DMARC 合规性，拒绝任何冒充您内部域的欺诈邮件。

CXX-XXXXXX-00 03/19