安全

谋财害命：数字勒索诈骗

Ben Nahorney
2019 年 3 月 14 日 - 0 条评论

自 2018 年年中以来，一种特别有欺骗性的针对性网络钓鱼诈骗活动开始风行起来。思科 Talos 研究人员一直在监控这些诈骗。我们将在下文重点介绍其中几种诈骗。与大多数网络钓鱼诈骗一样，这些网络钓鱼诈骗背后的动机就是为了牟利，但是不再试图用浪漫或财富之类的手段来诱惑人们。相反，网络诈骗者会以损害用户的声誉、人际关系乃至危及生命作为威胁手段。从本质上讲，就是从“利诱”转为“威逼”。

例如，假设某人收到一封邮件，主题行中包含其用户名和密码。这已经够令人吃惊了，然而真正引起此人注意的却是邮件正文。

Bzvgshqw March 2, 2019 at 7:12 PM

bzvgshqw : j38ifUbn

To: j38ifUbn,

Reply-To: Bzvgshqw

j38ifUbn is one of your pass words. Lets get directly to the purpose. No one has paid me to investigate about you. You don't know me and you're probably thinking why you're getting this e mail?

paycxilo bzvgshqw j38ifUbn w bzvgshqw j38ifUbn yuxanob bzvgshqw j38ifUbn qctiem bzvgshqw j38ifUbn kjorothy bzvgshqw j38ifUbn urhqfwuan bzvgshqw j38ifUbn hemagmiji bzvgshqw j38ifUbn pcd bzvgshqw j38ifUbn fuoduybog bzvgshqw j38ifUbn yyoqzj bzvgshqw j38ifUbn

Let me tell you, i setup a software on the adult vids (porn) site and you know what, you visited this site to experience fun (you know what i mean). When you were watching video clips, your browser initiated operating as a Remote control Desktop having a keylogger which gave me access to your display and also cam. Right after that, my software obtained all of your contacts from your Messenger, Facebook, as well as e-mailaccount. and then i made a video. First part displays the video you were viewing (you've got a good taste ;)), and next part shows the view of your cam, & it is u.

pualiiwef bzvgshqw j38ifUbn osgeye bzvgshqw j38ifUbn ew bzvgshqw j38ifUbn vuiago bzvgshqw j38ifUbn zm bzvgshqw j38ifUbn luncyx bzvgshqw j38ifUbn disoxeziw bzvgshqw j38ifUbn pigucijb bzvgshqw j38ifUbn zarrlrlay bzvgshqw j38ifUbn owzwneaku bzvgshqw j38ifUbn

You get a pair of alternatives. We will take a look at each of these possibilities in details:

htizyv bzvgshqw j38ifUbn aiaaso bzvgshqw j38ifUbn veztoe bzvgshqw j38ifUbn bypomurwo bzvgshqw j38ifUbn xypwou bzvgshqw j38ifUbn yiiqo bzvgshqw j38ifUbn emy bzvgshqw j38ifUbn ca bzvgshqw j38ifUbn daalyuexh bzvgshqw j38ifUbn wybepoukf bzvgshqw j38ifUbn

First choice is to ignore this email. Then, i will send your video recording to every one of your personal contacts and then imagine about the humiliation that you receive. and consequently if you happen to be in a romance, just how it is going to affect?

fesiwh bzvgshqw j38ifUbn vuf bzvgshqw j38ifUbn ej bzvgshqw j38ifUbn genevizu bzvgshqw j38ifUbn ilcfeciz bzvgshqw j38ifUbn ziazukvyi bzvgshqw j38ifUbn puaheoiq bzvgshqw j38ifUbn bhiroll bzvgshqw j38ifUbn mdjuq bzvgshqw j38ifUbn wribuipp bzvgshqw j38ifUbn

Number 2 option should be to compensate me USD 997. i will think of it as a donation. Then, i will right away discard your video recording. You can keep going on your way of life like this never happened and you will not hear back again from me.

uilrysma bzvgshqw j38ifUbn doceeky bzvgshqw j38ifUbn qxfakeauf bzvgshqw j38ifUbn zol bzvgshqw j38ifUbn kkikuursu bzvgshqw j38ifUbn ubuoeca bzvgshqw j38ifUbn i bzvgshqw j38ifUbn ekaoyog bzvgshqw j38ifUbn iewzzhnu bzvgshqw j38ifUbn uosi bzvgshqw j38ifUbn

You'll make the payment through Bitcoin (if you don't know this, search for 'how to buy bitcoin' in Google search engine).

r bzvgshqw j38ifUbn hwsfreal bzvgshqw j38ifUbn y bzvgshqw j38ifUbn lup bzvgshqw j38ifUbn qai bzvgshqw j38ifUbn owirfugz bzvgshqw j38ifUbn fieqaikuz bzvgshqw j38ifUbn reafozuar bzvgshqw j38ifUbn ecigymua bzvgshqw j38ifUbn et bzvgshqw j38ifUbn

BTC address: 18z5c6TjLUosqPTEnm6q7Q2EVNgbCy16Td

zoomanai bzvgshqw j38ifUbn zuvola bzvgshqw j38ifUbn cugaismpn bzvgshqw j38ifUbn gh bzvgshqw j38ifUbn ug bzvgshqw j38ifUbn asaktywu bzvgshqw j38ifUbn siwexesqj bzvgshqw j38ifUbn wi bzvgshqw j38ifUbn xuaq bzvgshqw j38ifUbn pytpuhcu bzvgshqw j38ifUbn

[CaSe-sensitive copy & paste it]

toerdcav bzvgshqw j38ifUbn mutqdajom bzvgshqw j38ifUbn imehudysu bzvgshqw j38ifUbn subaev bzvgshqw j38ifUbn pfnvipwec bzvgshqw j38ifUbn fxatykxha bzvgshqw j38ifUbn xogo bzvgshqw j38ifUbn asixajae bzvgshqw j38ifUbn wdkvrn bzvgshqw j38ifUbn mujiekhiq bzvgshqw j38ifUbn

if you are planning on going to the cops, well, this email can not be traced back to me. I have dealt with my steps. i am also not trying to charge you very much, i want to be compensated. in order to%} make the paymen if i do not get the bitcoin, i will definitely send your video recording to all of your contacts including relatives, colleagues, and so on. Nevertheless, if i do get paid, i will destroy the recording right away. If you need proof, reply with Yup and i will send out your video recording to your 10 contacts. This is the non:negotiable offer, that being said do not waste my personal time & yours by replying to this message.

不管这封邮件是谁发送的，发件人声称已经入侵了一个色情网站，发现此人曾经访问过该网站。诈骗者称自己已经控制了此人的显示器和网络摄像头，录下了此人及其访问的色情内容，然后同步了这两个视频流。

似乎嫌威胁力度不够大，诈骗者还声称已经从 Messenger、Facebook 和邮件中收集了此人的所有联系人。最后，诈骗者暗示，如果将视频发送给所有这些联系人，肯定会令此人尴尬万分。

随后诈骗者表示自己不是那么残酷无情，当然可以轻松删掉这些视频。事实上，只要此人支付区区一千美元的比特币，他们就乐意删掉所有这些内容。

如果这听起来有点像勒索，是因为这其实就是勒索。这也是一种欺骗。这种行为与预付费诈骗很像，在此类“性勒索”诈骗中，恶意攻击者会以易受攻击的用户群为目标发起网络诈骗。通过使用群发邮件网络钓鱼活动，他们期望有部分收件人会感到心虚，认为自己可能在某个时刻使用带有摄像头的设备做过邮件中提到的事情。他们利用了这样的心理：部分收件人会受不了羞辱和窘迫，宁愿付钱了事，不管诈骗者所说是否属实。

首先，这些邮件纯属无稽之谈。这是另一系列批量发送的网络钓鱼活动，诈骗者希望能够欺骗足够多的收件人，以此从中牟利。大量此类邮件都是通过 Necurs 僵尸网络分发的，就其非法性而言，堪与“哄抬股价、拉高出货”诈骗、勒索软件以及僵尸网络等已知的其他恶意活动相提并论。

这些邮件还充斥着相当多的专业术语。这并不是说没有办法远程查看人们的桌面或网络摄像头，只是按诈骗者的说法，这不太可能是真的。但是，诈骗者很有可能利用这些邮件触达那些对这一点不知情的用户。正如易受攻击的收件人可能会忽视预付费诈骗中的拼写和语法错误一样，在此类情况下，受害者要么会忽略那些让黑客得逞的技术细节，要么对其不甚了解。

虽然有时成人网站会无意中在其内容中植入恶意广告，但是这些攻击的重点在于攫取欺诈性广告收入，而不是暗中监视个人。当然，如果黑客掌握了足够的资源并且蓄意这么做，并非不可能发起此类攻击。这就引出了一个完全不同的问题：为何攻击者会无所不用其极地以个人为攻击目标？与大多数基于网络的威胁相比，这种攻击耗时较久且相当复杂。

此外，为什么当他们明明可以只通过网络钓鱼邮件欺骗其目标用户，却要如此大费周章呢？

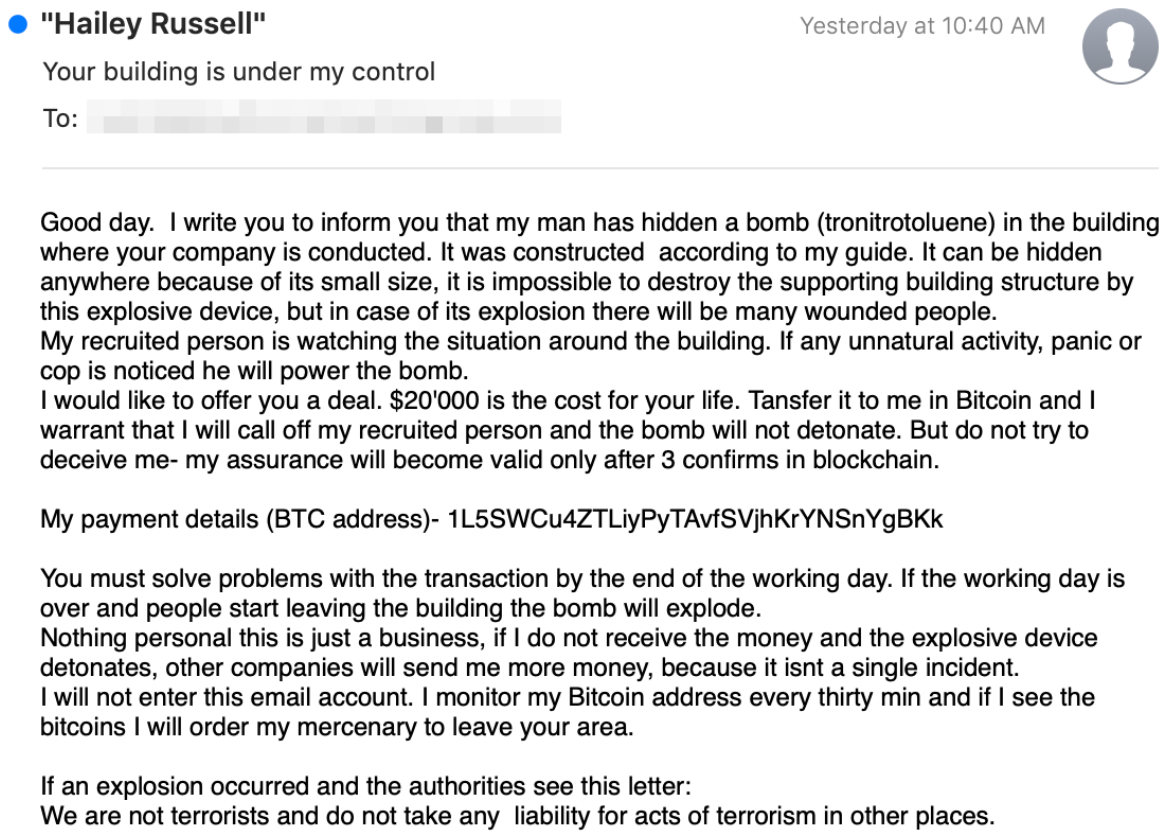
这都是为了发起持续的攻击活动。Talos 在 10 月份首次公布的调查结果中指出，诈骗者持续分发数字勒索诈骗。根据 Talos 的最新研究，Talos 开展的调查中提到的 “Aaron Smith” 性勒索攻击活动在 3 月初的某一天占到所有垃圾邮件的 5%。

值得注意的是，鉴于这些攻击活动的一贯特点，即使收件人选择支付赎金，他们似乎也不会全额支付。根据 Talos 对许多攻击活动中使用的比特币钱包的分析，所分析的钱包中只有一小部分有比特币余额。其中许多余额远远低于诈骗者要求的数千美元。即便如此，Talos 分析的两次攻击活动的最终报酬是一个六位数的总和。

鉴于这些以性勒索为主题的骗局取得了一定的成功，数字勒索诈骗者已经扩展到其他更暴力的主题 - 通常会威胁杀掉收件人。在一个此类变体中，诈骗者声称自己是一名杀手，已接到杀死收件人的合同。只是出于 “良知”，他们改变了初衷。如果收件人可以通过特币支付一笔固定的金额，他们愿意忘掉整个合同。

自这种诈骗活动从 2018 年年中出现以来，后面出现了更多这类诈骗的变种，其中包括引诱式攻击威胁和 “我知道你在骗人” 式的邮件诈骗。然而，在 12 月，数字勒索诈骗愈演愈烈，一跃成为全国性的新闻头条。这一轮的邮件诈骗中包含炸弹威胁，导致整个美国和加拿大的学校、报纸、运输系统和各种各样的企

业撤离。在这种情况下勒索的金额要高得多，达到约 20,000 美元，但截至上次调查，与该攻击活动相关的比特币钱包中都没有余额。



"Hailey Russell" Yesterday at 10:40 AM

Your building is under my control

To:

Good day. I write you to inform you that my man has hidden a bomb (tronitrotoluene) in the building where your company is conducted. It was constructed according to my guide. It can be hidden anywhere because of its small size, it is impossible to destroy the supporting building structure by this explosive device, but in case of its explosion there will be many wounded people.
My recruited person is watching the situation around the building. If any unnatural activity, panic or cop is noticed he will power the bomb.
I would like to offer you a deal. $20'000 is the cost for your life. Tansfer it to me in Bitcoin and I warrant that I will call off my recruited person and the bomb will not detonate. But do not try to deceive me- my assurance will become valid only after 3 confirms in blockchain.

My payment details (BTC address)- 1L5SWCu4ZTLiyPyTAvfSVjhKrYNSnYgBKk

You must solve problems with the transaction by the end of the working day. If the working day is over and people start leaving the building the bomb will explode.
Nothing personal this is just a business, if I do not receive the money and the explosive device detonates, other companies will send me more money, because it isnt a single incident.
I will not enter this email account. I monitor my Bitcoin address every thirty min and if I see the bitcoins I will order my mercenary to leave your area.

If an explosion occurred and the authorities see this letter:
We are not terrorists and do not take any liability for acts of terrorism in other places.

令人庆幸的是，反垃圾邮件解决方案将通过使用黑名单和其他过滤器捕获大多数的数字勒索邮件。在邮件服务器上启用 DMARC 协议也可以帮助过滤掉非法邮件。但是，诈骗者似乎也发现了这一点并采取措施试图逃避垃圾邮件过滤器。例如，Talos 最近发现，有邮件使用 base64 编码和邮件正文中呈现白色的垃圾 HTML 文本，这对于在白色背景下阅读邮件的用户来说是不可见的。（请参阅第一个示例邮件。）

在其他情况下，诈骗者编造了邮件内容，对文本进行了截图，然后只需将图片粘贴到邮件正文中即可发起攻击。当然，这给受害者带来了更多不便，因为他们无法再复制并粘贴相当复杂的比特币钱包地址。诈骗者显然考虑了这一点，并且出于便捷性考虑，他们开始提供 QR 码，从而方便收件人支付赎金。

因此，如果这完全是一个骗局，诈骗者是如何获得密码的呢？很有可能，他们设法获得了包含人们邮件和密码的数据泄露记录列表。您可能是包含大量邮件地址和密码组合的名单中的一员。如果该密码确实是您目前使用的密码，请立即更改此密码，并避免在其他位置使用该密码。如果您想了解您的邮件地址是否已被泄露，请查看 Have I Been Pwned 等服务，该服务将列出是否可能发生泄露以及可能发生泄露的地点。

另外，请考虑采用以下产品或功能：

- **思科邮件安全**包括高级威胁防御功能，可以更快地检测、阻止和修复传入邮件中的威胁。同时，它可以保护组织的品牌，防止数据丢失，并通过端到端加密在数据传输过程中保护重要信息。
- **思科高级网络钓鱼防护**可进一步增强思科邮件安全中已有的发件人身份验证和 BEC 检测功能。它集成了机器学习，将本地身份和关系建模与行为分析相结合，以防止基于身份欺骗的威胁。

归根结底，教育才是最好的武器。培训用户识别此类诈骗可以大大减少其影响。最后，如果一件事情听起来好得（坏得）难以置信，那么它也许真的不可信。

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

喜欢这篇博客吗？请订阅每月热点威胁博客系列，并在下一篇博客发布时收到提醒。

标签:

- #安全#
- 高级恶意软件防护
- 思科邮件安全
- 邮件
- 邮件安全
- 专题
- 安全思想领袖
- 威胁情报
- 每月热点威胁
- totm