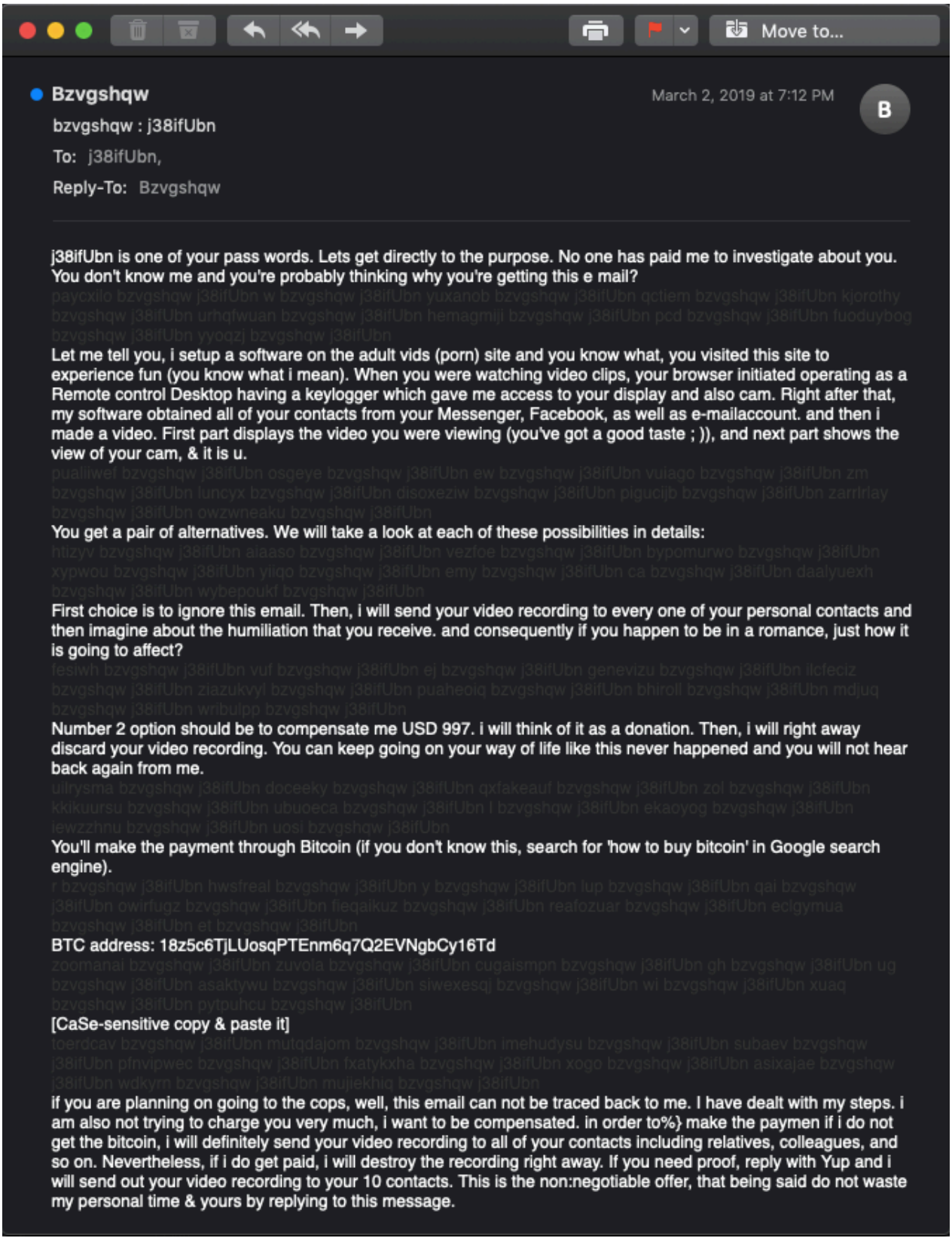
安全性

要錢還是要命：數位勒索詐騙

Ben Nahorney
2019 年 3 月 14 日 - 0 則留言

自 2018 中期開始，有種特別狡詐且只針對特定目標的網路釣魚詐騙逐漸風行起來。思科 Talos 研究人員一直以來都在監控這些詐騙，我們會在此處列出一些主要案例。就如同大多數網路釣魚詐騙的案例，這些人的目的都是您的金錢，但他們並不會利用愛情或財富來誘騙您上鉤。相反地，這些詐騙人士會利用您的信譽、關係，有時甚至是您的生命來威脅您。本質上就是從獎勵轉往懲罰的手法。

比如說，您會收到一封電子郵件，主旨包含您的使用者名稱和密碼。令人驚訝的是，真正引起您注意的是電子郵件內文。



Move to...

Bzvgshqw

March 2, 2019 at 7:12 PM

B

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?

paycxiio 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.

pualiiwei bzvgshqw j38ifUbn osgeye bzvgshqw j38ifUbn ew bzvgshqw j38ifUbn vuiago bzvgshqw j38ifUbn zm bzvgshqw j38ifUbn luncyx bzvgshqw j38ifUbn disoxeziw bzvgshqw j38ifUbn pigucijb bzvgshqw j38ifUbn zarrirlay 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 vezfoe 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 ziazukvyl bzvgshqw j38ifUbn puaheoiq bzvgshqw j38ifUbn bhiroll bzvgshqw j38ifUbn mdjuq bzvgshqw j38ifUbn wribulpp 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 l 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 hwstreal bzvgshqw j38ifUbn y bzvgshqw j38ifUbn iup bzvgshqw j38ifUbn qai bzvgshqw j38ifUbn owirfugz bzvgshqw j38ifUbn fieqaikuz bzvgshqw j38ifUbn reafozuar bzvgshqw j38ifUbn eclgymua 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 pytouhcu 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 wdkyrn 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.

寄信的人是誰不重要，但此人會宣稱已經破解了某個您曾經造訪過的色情網站。這位詐騙人士說其已經控制了您的螢幕和網路攝影機、把您和色情影片都錄製了起來，並將兩個影片串流同步。

這樣做彷彿還不夠嚇人，詐騙人士更聲稱已經從 Messenger、Facebook 和電子郵件中收集了所有您的聯絡人資料。最後，詐騙人士會暗示說，若將這些影片寄給所有這些聯絡人，一定會讓人非常尷尬。

然後再宣稱他們也不是惡魔，這些資料都能輕鬆清除。他們其實很樂意為了價值數千美金的比特幣把這些資料清除掉。

這聽起來像是勒索，其實它就是勒索。但這也是虛張聲勢。就如同預付款詐騙 (Advance Fee Scam)，這些「性勒索」詐騙中不懷好意的演員們把一群容易上當的使用者當作獵物。他們利用大量郵寄的網路釣魚活動，預期會有部分收件者覺得自己可能在有相機的裝置前面做了一些郵件中提到的行為。他們倚賴的是某些收件者會因為感到強烈的困窘和羞恥感，而不辨真偽來付錢避免這種事情發生。

但首先且最重要的一點是，這些電子郵件都是假的。只不過是藉由大量傳送網路釣魚活動，希望騙到足夠的收件者，讓這些詐騙人士從中獲利。這些電子郵件大部分是由 Necurs 殭屍網路發送，透過大規模置入詐騙訊息、勒索軟體和其他該殭屍網路為人所知的惡意活動，讓它們看起來很合理。

這些電子郵件中也包含大量一般人難以理解的技術性語法。遠端檢視您的桌面或網路攝影機並非完全辦不到，但考量詐騙人士所述方式，這種做法其實非常不可行。但這些詐騙人士可能就是要讓這些電子郵件觸及不知情的使用者。正如容易受害的收件者可能會忽略預付款詐騙 (Advance Fee Scam) 中的拼字和文法錯誤，這種情況下的受害者也會因忽視或不夠瞭解技術性細節，而無法意識到這種不可能的駭客行為。

雖然成人網站有時候也會無意間提供含有惡意廣告的內容，但這類攻擊卻著重在詐騙廣告的營收，而非刺探個人資料。當然，若有足夠資源和驚人的毅力，這類攻擊 (指刺探個人資料) 是有可能成功的。但這也衍生出另一個完全不同的問題：攻擊者為何要大費周章地入侵某個人呢？和大部分的網路威脅相比，這實在是個冗長又相當複雜的攻擊行為。

還有，如果只要用網路釣魚電子郵件就能嚇唬他們的目標，那何必花費那麼多心血呢？

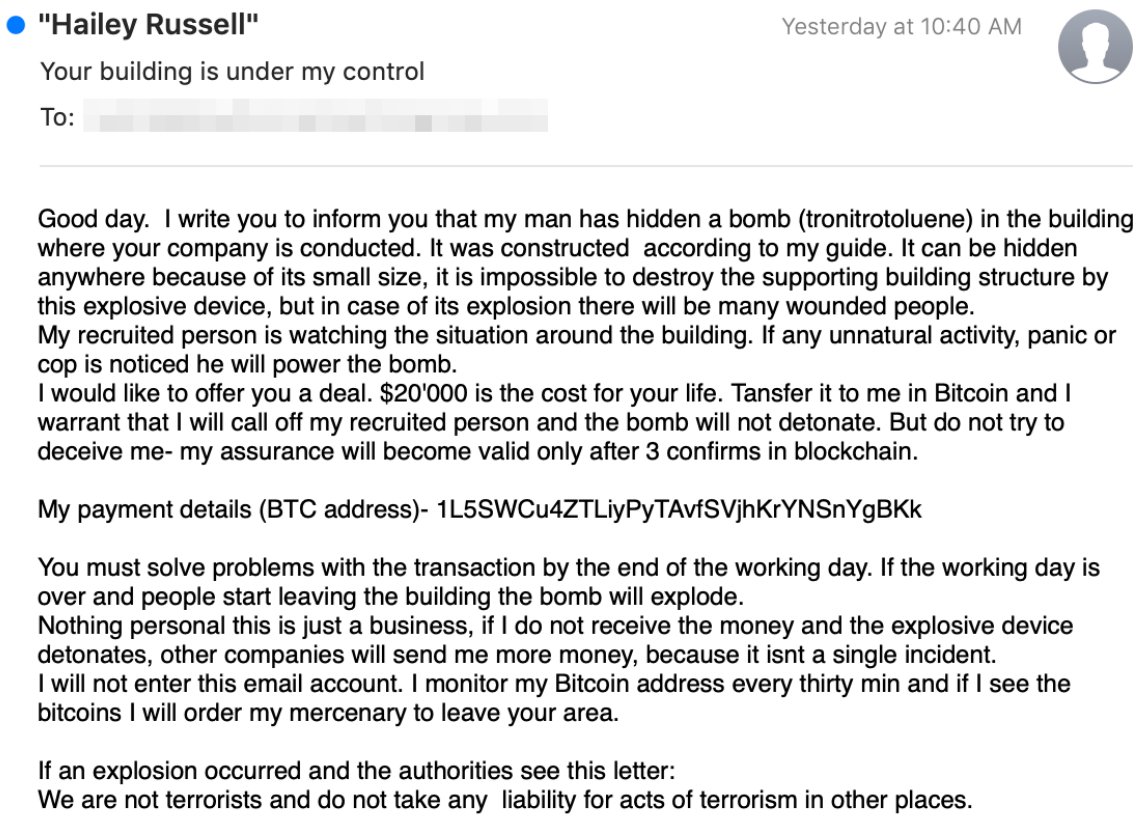
所以這類活動仍在持續中。Talos 在 10 月中第一次所調查的詐騙人士仍不斷散播數位勒索詐騙。根據 Talos 的新研究，Talos 調查中提及的「Aaron Smith」性勒索活動於 3 月初某天在所有垃圾郵件中佔具高達 5%。

有趣的是，考量到這些活動的一致性，就算收件者選擇付錢，他們似乎也不會支付全額。根據 Talos 對於比特幣錢包在這類活動中使用狀況的分析，受分析的錢包中只有很小部分還有比特幣餘額。其中許多錢包的餘額遠遠低於詐騙人士所要求的數千美元。即便如此，Talos 所調查的兩個活動最終仍收到了六位數的款項。

既然這些性勒索詐騙能夠取得一定的成功，數位勒索詐騙人士更擴展出其他更暴力的招數，往往會威脅收件者的生命。透過這種花招，詐騙人士會聲稱自己是職業殺手，簽了合約要來殺害您。不過這個人想要「改邪歸正」，所以他們改變了心意。如果您能夠以比特幣支付約定費用，他們便願意撕毀整個合約。

自 2018 中期出現這類詐騙後，它們便持續層出不窮，從硫酸攻擊的威脅到「我知道你在劈腿」之類的電子郵件等等。然而，數位勒索詐騙在 12 月轉變地更加黑暗：在過程中製造國家級新聞。這一波電子郵件包含炸彈威脅，讓遍布美國和加拿大的學校、報紙、交通系統和各種企業都在進行疏散。在這次案

例中，勒索的金額變得更高，大約為 20,000 美金，但至上次檢查為止，與此活動相關的比特幣錢包都沒有餘額。



好消息是，防垃圾郵件解決方案能夠透過封鎖名單和其他過濾器來攔截大部分數位勒索郵件。在您的郵件伺服器中啟用 DMARC 通訊協定，也有助於過濾掉非法電子郵件。然而，詐騙人士似乎也發現了這點，並已經採取措施來試圖躲過垃圾郵件過濾器。舉例來說，Talos 最近發現使用 base64 編碼和回收 HTML 文字的電子郵件會於訊息內文中呈現白色，因此使用白色背景的人便無法讀取信件內容。(請參閱第一個電子郵件範例。)

在其他案例中，詐騙人士會撰寫他們的電子郵件然後將文字螢幕截圖，再直接將該影像貼到訊息內文中。當然，這會給受害者造成更多麻煩，因為他們無法複製貼上相當複雜的比特幣錢包地址。詐騙人士顯然也考量到了這點，已經開始嵌入 QR 碼，來幫忙增加付款的便利性。

那麼，如果這只是徹頭徹尾的詐騙，那詐騙人士是怎麼取得您的密碼來開始這場騙局的呢？最有可能的是，他們會想辦法取得資料外洩記錄的清單，其中包含您的電子郵件和密碼。您可能是從數量龐大的電子郵件地址和密碼組合清單中被選出來的其中一人。如果這確實是您目前使用的密碼，請立即更改，也不要在其他地方使用這組密碼。如果您有興趣瞭解您的電子郵件地址是否暴露在外洩的風險中，請試試「Have I Been Pwned」之類的服務，它能夠列出可能遭洩漏的資料清單。

另外，請考慮使用以下產品：

- Cisco Email Security 包含進階的威脅防禦功能，能夠更快地偵測、封鎖及修復傳入電子郵件的威脅。同時能保護組織品牌、防止資料遺失，並保護端對端加密傳輸中的重要資訊。
- Cisco 進階釣魚防護進一步加強寄件者驗證和可於 Cisco Email Security 取得的 BEC 偵測功能。它整合了機器學習，而其會將本地身分、關係模型與行為分析結合起來，藉此抵禦身分詐騙的威脅。

畢竟，教育是最好的武器。訓練使用者識別此類詐騙手法，能夠有效降低它們的影響。最重要的是，如果某件事聽起來好 (或壞) 得難以置信，那應該就真的不可輕信。

深入閱讀：

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

喜歡這篇文章嗎？訂閱「本月威脅」系列部落格文章，以便在下一篇部落格文章發行時收到通知。

標籤：

- #安全性
- 進階惡意軟體防護
- Cisco Email Security
- 電子郵件
- 電子郵件安全性
- 精選
- 資安思維領導
- 威脅情報
- 本月威脅
- totm