אבטחת ארנקי Bitcoin

מאת עו"ד יהונתן קלינגר

הקדמה

בחודש שעבר פרסמתי ספר בשם "Bitcoin Safety" שזמין למכירה כאן. המאמר הזה הוא תרגום של חלקים מהספר, בתוספת שינויים. הספר עוזר לכל מי שרוצה להכנס לעולם המטבעות הקריפטוגרפיים להבין את סוגי ההונאות הקיימות בתחום ואת הדרך בה הוא יכול להגן על המטבעות שלו מגניבה, אבדן או הונאות אחרות.

אם תעברו ברשת על מדריכים תמצאו עשרות, אם לא מאות, מדריכים על איך לקנות מטבעות קריפטוגרפיים, מה הארנקים המועדפים, איך (לא) להשקיע, איך לדווח לרשויות המס, ושלל נושאים אחרים. מה שלא תמצאו זה מדריך שיסביר לכם איך לשמור על הכסף שלכם בהנחה שאתם רוצים אותו זמין, מאובטח, ושלם.

את המדריך שלי התחלתי בשאלה הברורה: אם יש לך מיליון דולר במזומן, או בזהב, איך אתה צריך לאבטח אותו? ומשם עברתי להסביר מה ההבדלים בין כסף מזומן וזהב לביטקוין, ומה היתרונות והחסרונות. פרק שלם הקדשתי לנושא של "איך להוריש את הביטקוין שלך" כדי לדאוג שמי שקורא את המדריך ידע לשמור על המטבעות לדורות הבאים.

אבל כאן אני רוצה להתמקד בנושא אחר, והן ההונאות הנפוצות. בספר אני מפרט שש-עשרה הונאות קלאסיות, שמתחלקות להונאות כלכליות (כלומר לגרום לך לשלם ולא לספק לך משהו, פירמידה וכדומה) וחלקן הן הונאות סייבר. הונאות הסייבר הן החלק המעניין יותר.

איך עובד ארנק ביטקויין?

כדי להבין את ההונאות האלו צריך להבין איך עובד ארנק ביטקוין. כל ארנק ביטקוין מבוסס על הצפנה, ויש לו מפתח פרטי ומפתח ציבורי. המפתח הציבורי הוא כתובת הארנק שלך ואליה תקבל כסף. לדוגמא:

1E21dSRaRED2xnxdvaB2pqaWmVrLLUvhL9

הוא מפתח ציבורי, ש:

5KhsEkKzNPhn3jTejcdkcbubWQYToLPCF8skZuCS12VMi1KmjN8

הוא המפתח הפרטי שלו.

אבל, כיוון שברור לכולנו שאם הארנק שלנו מוחזק על ידי המפתח הפרטי, וכל מי שיש לו גישה למפתח הפרטי יכול לבצע עסקאות בארנק הביטקוין שלנו, אז צריכה להיות דרך יותר טובה לאבטח את הארנק ולגבות אותו.

רוב הארנקים היום לא מאפשרים לך גישה למפתח הפרטי שלך, אלא משתמשים במה שנקרא **BIP-39**. ביפ זה "**Bitcoin Improvement Protocol**" והוא בעצם הצעת שיפור. כיוון שביטקוין מבוסס קוד פתוח, אז כל אחד יכול להציע שיפורים, ואם רוב המפתחים והכורים מסכימים, ההצעה מתקבלת.

הצעה 39 אומרת שבמקום לבסס את המפתח הפרטי על מחרוזת ארוכה, אפשר להשתמש במחסן של 2048 מילים כבסיס, וכל רצף של 24 מילים ישמש לחולל את המפתח הפרטי.

בצורה כזו, אפשר לקבל מחרוזת של 24 מילים, לדוגמא:

topic solution bench hungry prize month day segment off shoulder duty help scatter twist rhythm marriage rocket crawl today fuel butter parent obscure sight

ולשמור אותה. לכן, כל מי שישתמש במחרוזת הזו, יקבל מספר רב של כתובות פומביות שמבוססות על המחרוזת כולל **NayPRBjwKyKTyiTRX7womuv1fpwG2GUih1**, לדוגמא.

אתם לא צריכים להאמין לי, אתם יכולים להכנס לאתר בקישור ולהזין את 24 המילים ולראות זאת.

כעת, כאשר אתם מתקינים ארנק ביטקוין (או כמעט כל מטבע קריפטוגרפי אחר) במקום לתת לכם מפתח פרטי לגיבוי, יתנו לכם את המחרוזת הזו (שמה: **סיד**). אם בעת חילול הארנק אין לכם מפתח פרטי או סיד, זה אומר שהארנק שלכם הוא ארנק משמורת; כלומר, הכסף שלכם נשמר על ידי שירות חיצוני. לזה יש בעיות. מדוע? כי הרבה פעמים שירותי משמורת נפרצים. בשנת 2014 נפרצה הבורסה הגדולה ביותר בזמנו שאפשרה מסחר בביטקוין, Mt. Gox. הפריצה גרמה לכך שכל מי שהחזיק את המטבעות שלו באותה הבורסה איבד אותן, הבורסה פשטה רגל, ולמדנו: **לא המפתחות שלך, לא הביטקוין שלך**.

לכן, יש שלושה סוגים של ארנקים: ארנקי משמורת, בהן שירות חיצוני מחזיק את הכסף, ארנקי תוכנה, בהן המפתח הפרטי ניתן לך, אך הוא מחולל על המכשיר שלך, וארנקי חומרה. אליהם נגיע עוד מעט.

איך ארנק תוכנה עובד? המחשב שלך מחולל את המפתח הפרטי, והוא נשמר על המחשב. זה נהדר לארנק סלולרי שמחזיק כמה מאות שקלים, אבל מתחיל להיות בעייתי כאשר הסכומים עולים. מדוע? מספיק Keylogger על המחשב (או הטלפון) כדי לגנוב את הכספים מהארנק. מספיק שהגיבוי (המפתח הפרטי) שמור ב-Google Drive או Dropbox כדי להביא לכך שהכסף יגנב.

כלומר, כאשר אתה משתמש בארנק תוכנה, יש מגבלה משמעותית: המטבעות שלך מאובטחים בדיוק כמו הציוד החלש ביותר שלך. גם שימוש ב-Factor Authentication-2 והצפנה לא ממש יעזרו, כי הרבה פעמים פריצות לשירותים נובעות מתקלה בשירותים עצמם.

יותר מזה, אי אפשר לבטח את הכספים האלה נכון להיום, כך שהסיכון לאבדן וגניבה גדל.

כאן נכנסו ארנקי החומרה לפעולה. ארנק החומרה הוא מחשב כיס קטן, בגודל של דיסק-און-קי, שמכיל רכיב הצפנה. ארנק החומרה מאחסן את המפתח הפרטי על שבב מאובטח בתוכו ולא מוציא אותו החוצה. היתרון? גם אם המחשב נגוע בוירוס, אין גישה למפתח הפרטי ואי אפשר לגנוב את המטבעות. כאשר צריך לאשר עסקה, הארנק חותם עם המפתח הפרטי על העסקה בתוך הרכיב המאובטח ושולח אותו למחשב.

גם כאשר עושים עסקה, מקבלים חיווי על מסך ארנק החומרה לגבי העסקה. במצב כזה, אם השתלטו על מחשב מסוים והתיקנו וירוס שמשנה את הכתובת לשליחה של מטבעות, אז המשתמש החכם יראה הבדל בין הכתובת שמופיעה על המסך והכתובת בארנק.

יותר מזה: כאשר מאתחילם את ארנק החומרה הוא מספק לך 24 מילות גיבוי, אותו "סיד". הוא מציג אותן על הארנק ומסביר שאסור, באמת אסור, לכתוב אותן על מחשב. מדוע? מכל הסיבות שאראה כאן. כי ברגע שהמילים נשמרות במחשב, הן מאובטחות בדיוק כמו ארנק תוכנה. כלומר, לא מאובטחות.

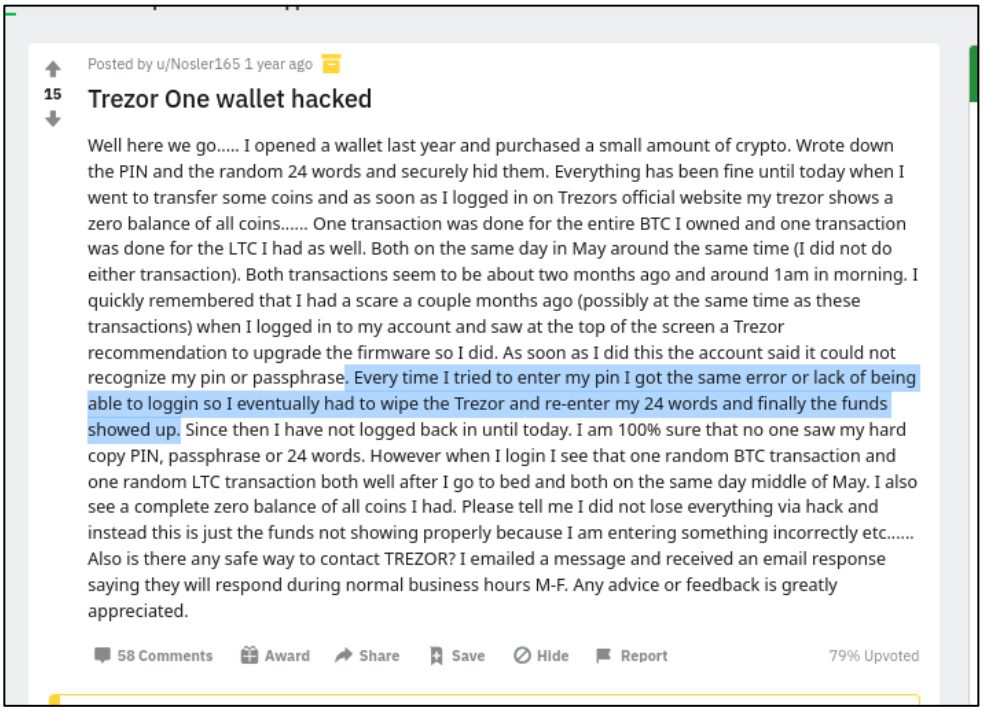
גם כאשר משחזרים את ה-Seed הדבר מבוצע באותו ארנק חומרה, ולא על מחשב. חשוב לזכור את זה.

הבעיה היא שהרבה אנשים קוראים את האזהרה הזו וחושבים שהם יותר חכמים. עוד בעיה היא שהרבה האקרים מפעילים שירותים שמנסים לגרום לאנשים לטעות ולתת להם את אותן 24 מילים. איך הם עושים את זה? כאן היופי. אני אביא מספר דוגמאות מהחיים האמיתיים שמדגימים כיצד האקרים ניסו להטעות אנשים.

כמובן, ההאקרים חכמים וכל יום מעדכנים את ההונאות שלהם, אז חשוב לקחת את זה בחשבון וללמוד.

הונאת העדכון המזויף

איך זה עובד? הקרבן מקבל אימייל שאומר שארנק החומרה שלו חשוף לפגיעה, או מנסה לגלוש לאתר של החברה שמייצרת את הארנק ומגיע ללינק מזויף. ברגע שהקרבן מתקין את "העדכון" הוא מקבל חיווי שהוא לא יכול להתחבר לארנק ונדרש להקליד את ה-Seed על המחשב. ראינו אזהרות לגבי זה מחברת Trezor, אחת מהיצרניות, על כך שאנשים רוכשים מודעות גוגל כדי להטעות אנשים. כפי שניתן לראות בדוגמא הזאת, משתמש התקין עדכון מזויף והתבקש להקליד את ה-Seed שלו:


Posted by u/Nosler165 1 year ago

15

Trezor One wallet hacked

Well here we go..... I opened a wallet last year and purchased a small amount of crypto. Wrote down the PIN and the random 24 words and securely hid them. Everything has been fine until today when I went to transfer some coins and as soon as I logged in on Trezors official website my trezor shows a zero balance of all coins..... One transaction was done for the entire BTC I owned and one transaction was done for the LTC I had as well. Both on the same day in May around the same time (I did not do either transaction). Both transactions seem to be about two months ago and around 1am in morning. I quickly remembered that I had a scare a couple months ago (possibly at the same time as these transactions) when I logged in to my account and saw at the top of the screen a Trezor recommendation to upgrade the firmware so I did. As soon as I did this the account said it could not recognize my pin or passphrase. Every time I tried to enter my pin I got the same error or lack of being able to loggin so I eventually had to wipe the Trezor and re-enter my 24 words and finally the funds showed up. Since then I have not logged back in until today. I am 100% sure that no one saw my hard copy PIN, passphrase or 24 words. However when I login I see that one random BTC transaction and one random LTC transaction both well after I go to bed and both on the same day middle of May. I also see a complete zero balance of all coins I had. Please tell me I did not lose everything via hack and instead this is just the funds not showing properly because I am entering something incorrectly etc..... Also is there any safe way to contact TREZOR? I emailed a message and received an email response saying they will respond during normal business hours M-F. Any advice or feedback is greatly appreciated.

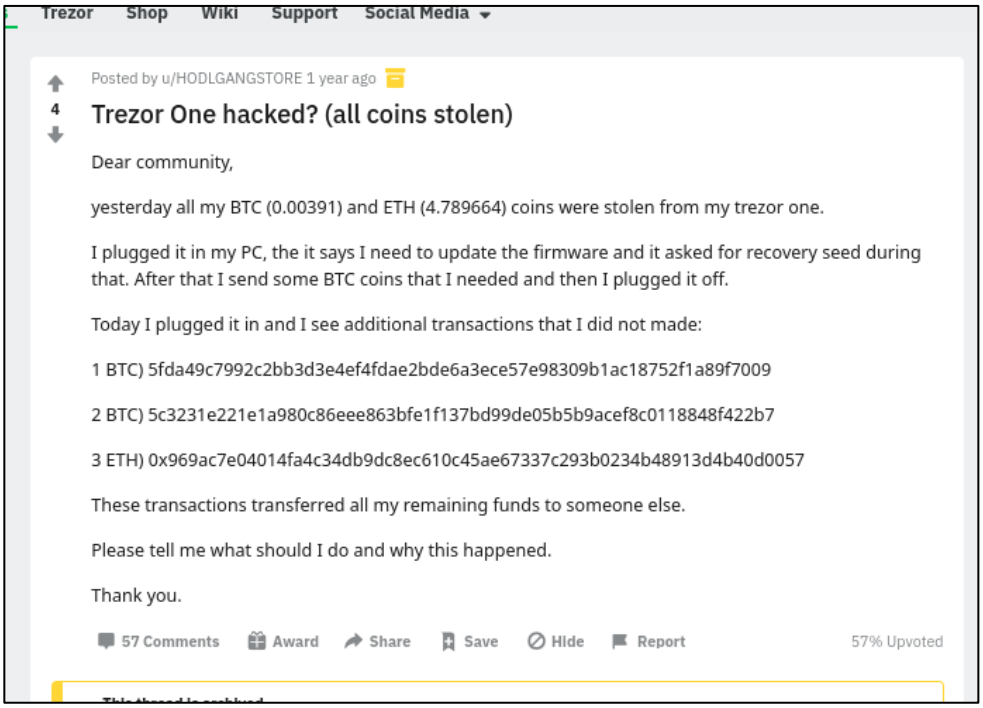
58 Comments Award Share Save Hide Report 79% Upvoted

איך זה קרה? הקרבן עשה שתי טעויות. הראשונה היא שהוא לא ראה מה הוא הוריד ושהעדכון לא הגיע מהאתר הרשמי. הטעות השניה היא שהוא הקליד את ה-Seed על מחשב בניגוד לכל האזהרות שבאו עם הארנק. צריך לזכור: **אף פעם, אבל באמת אף פעם, לא נדרשים להקליד את ה-Seed על טלפון או מחשב.** אם הארנק שלך נפגם, תדרש להקליד את ה-Seed בארנק בעת השחזור, לא במחשב.

הלקח: להשתמש רק בתוכנה מהאתר הרשמי של החברה שמייצרת את הארנק ולעולם לא להקליד את ה-Seed או סיסמא במכשיר כמו מחשב או טלפון. תוקפים מנסים להטעות את הקרבנות על ידי שליחת מיילים מזויפים שאומרים שהארנק פגיע או הושחת, ושהכספים נעלמו, או אפילו שהגיעה העברה. זכור: כל עוד ה-Seed לא ניתן לאחרים, הוא שמור טוב.

השתלת Seed מזויף

איך זה עובד? בהונאה הזו, התוקף גורם לקרבן להאמין שהוא כבר היה תחת מתקפה ומבקש שתקליד מחדש את הסיד. התוקף מתחזה לחבר בצוות של הארנק אם כתבת פוסט במקום פומבי וביקשת עזרה, או משתמש בפישינג, כמו בעדכון הארנק המזויף. בדוגמא הזו, הקרבן התקין ארנק מזויף, כאשר יכול להיות שהיו לו רוגלות על המחשב שמחכות לחיבור של ארנק חומרה, או שפשוט גלש לאתר שנפרץ:

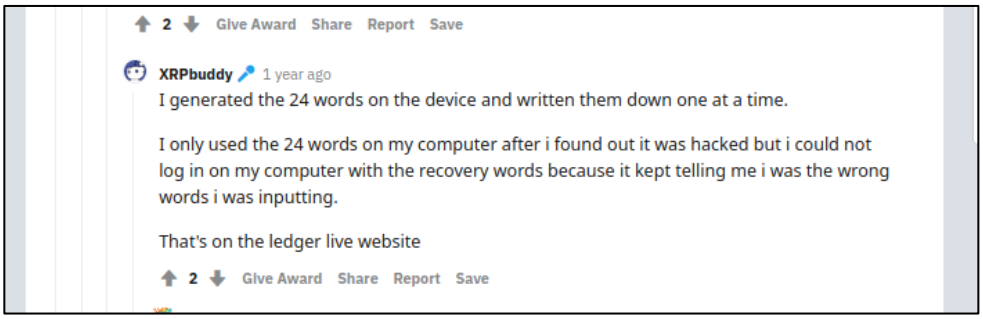


איך זה קרה? התוקף ניצל את הרצון של הקורבן לתקן תקלה במחשב או בארנק וקיבל אמון שלהם כאשר הם הקלידו את ה-Seed מחדש.

הלקח: אף פעם לא לתת לאחרים את ה-Seed שלכם או להקליד אותו במחשב.

תוסף לכרום או אפליקציה זדונית

איך זה עובד? בצורה דומה לאתרים וארנקים מזויפים, התוקפים מייצרים תוסף לכרום או אפליקציות סלולריות שמתחזות לאפליקציה הרשמית. בעת ההתקנה או העדכון, הם מבקשים מהקרבן "להקליד מחדש" את ה-Seed באפליקציה (ולא במכשיר). במצב כזה, הארנק מתרוקן. כפי שניתן לראות בדוגמא הזו, הקרבן התקין תוסף מזויף לכרום שביקש ממנו את ה-Seed:

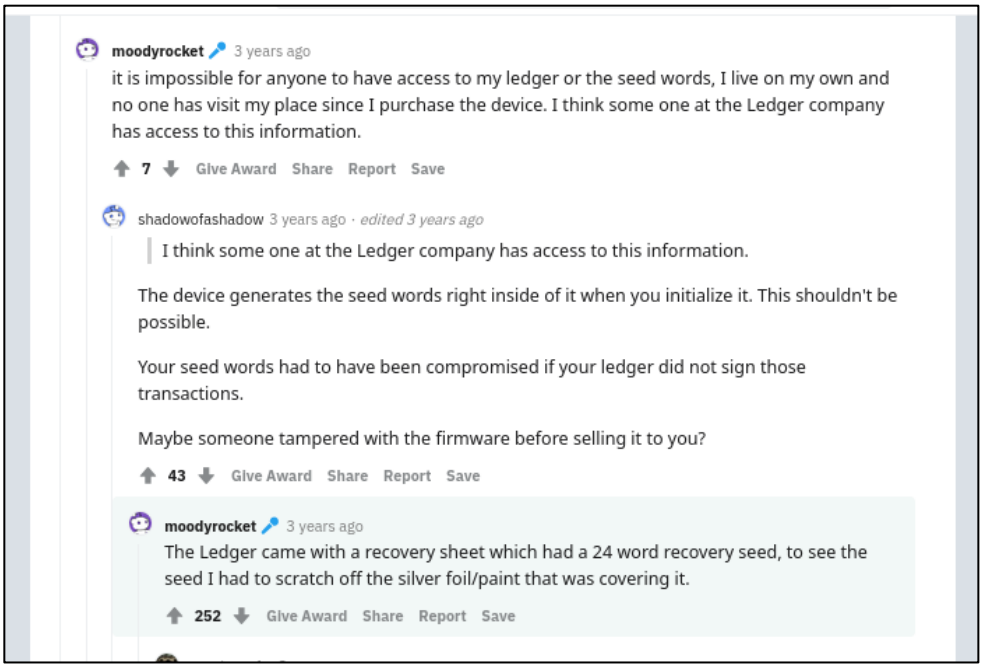


איך זה קרה? הקרבן לא הבין שהתוכנה שהוא התקין באה מתוקף. הוא הקליק על תוסף מזויף או חיפש לא נכון בתיבת החיפוש. יש לנקוט אמצעי זהירות כשמתקינים תוכנות שמתממשקות עם הארנק.

הלקח: לעולם לא להקליד את ה-Seed על מחשב. כך התוקפים מגיעים לקרבנות.

ה-Seed המוכן מראש

איך זה עובד? בהונאה הזו, הקרן רוכש ארנק חומרה באתר כמו eBay או Amazon ומקבל אותו. הוא חדש בתחום ולא ממש מבין איך זה עובד, אז הוא מקבל את ה-Seed כתוב כבר והארנק כבר מאותחל. במצב כזה, התוקף שומר אצלו גם העתק של הסיד. כדי לייצר תחושה של אבטחה, לפעמים ה-Seed מכוסה בסרט הגנה או משהו בסגנון. כפי שאפשר לראות בדוגמא הזו, הקרבן קיבל Seed מראש ולא הבין שהוא קרבן.



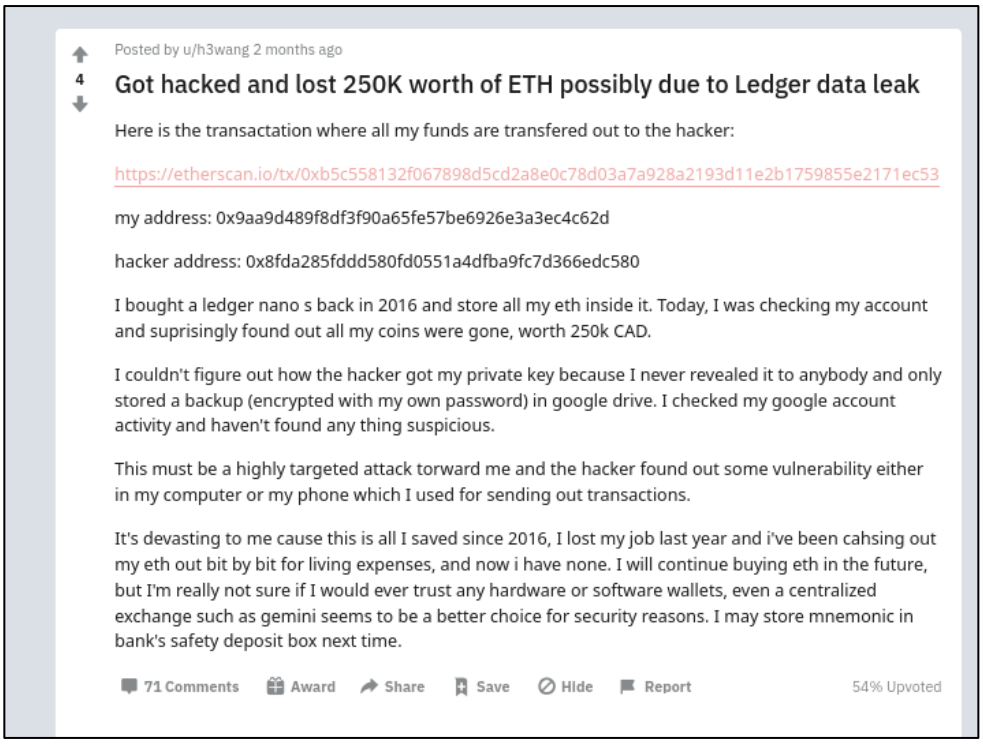
לפעמים, ה-Seed שהקרבן מקבל הוא אפילו לא ה-Seed האמיתי, ורק לתוקפים יש את הסיד.

איך זה קרה? הקרבן לא היה זהיר ורצה הנחה על ארנק החומרה שלו. המחיר שהוא שילם על ההנחה הזו היה כבד במיוחד. כאשר אתה קונה ארנק, תחשוב עליו כעל כספת: אין שלב ברכישת הכספת שצריך להיות חשוף, ולעולם לא לקבל את ה-Seed מוכן מראש.

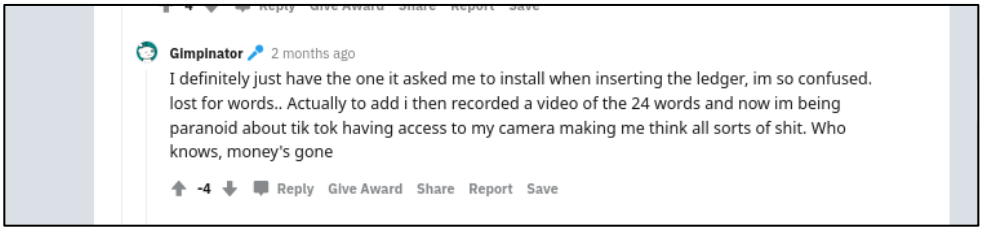
הלקח: לא להתקמצן על אמצעי אבטחה או לחפש הנחות. ככה התוקפים מגיעים אלייך.

ה-Seed נשמר על מחשב או בענן

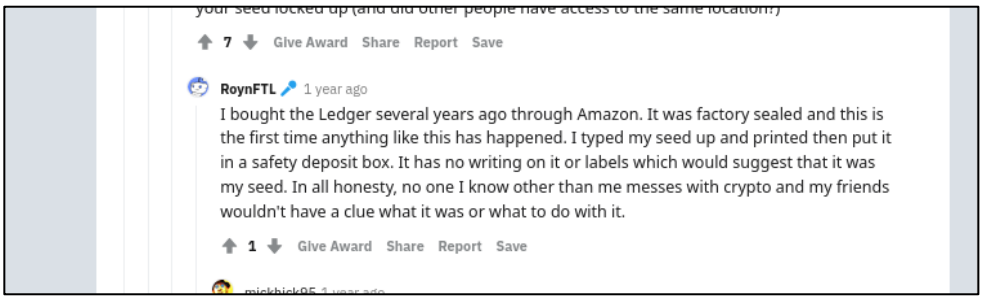
איך זה עובד? הקרבן חושב שהוא חכם יותר מכולם ושהידע שלו באבטחת מידע הוא ברמה גבוהה במיוחד. לכן, הוא כותב את ה-Seed שלו במחשב בקובץ טקסט, או מצלם את ה-Seed מהנייר ושומר צילום בחשבון ה-iCloud או Google Drive, מוצפן איפשהו בצורה כלשהיא. אחר כך, כאשר החשבון שלהם נפגע, התוקף גונב את הכספים. הקרבן הזה לדוגמא, שמר את הקבצים שלו בגוגל דרייב.



קרבן אחר הקליט וידאו עם מילות ה-Seed שלו רק כדי לגלות לאחר מכן שהוידאו נגנב.



איך זה קרה? המקרה הזה הוא של כמה אמצעי בטחון כושלים באותו זמן. לדברים אחרים על הדיסק הקשיח שלכם כנראה שהצפנה היא טובה מספיק. אבל תניחו לצורך העניין שלתוקפים יש תמריצים בגובה של מיליוני שקלים הם ינצלו ויעקבו אחרי כל מידע רלבנטי. במקרה הזה, התוקף חיכה שנים עד שלקרבן יהיה מספיק כסף בארנק. העובדה שהמידע היה שמור דיגיטלית היה מספיק כדי לקבל גישה:



הלקח: לעולם לא לשמור את ה-Seed על אמצעי דיגיטלי. תמיד להניח שכל מה שדיגיטלי נפרץ.

נכון, כל ההונאות האלו נראות בסיסיות במיוחד. בכולן אדם פותה לתת את ה-Seed שלו או שהוא נגנב. הבעיה היא שבעת שעולם אבטחת המידע רגיל לכך שכאשר יש מערכות שמחזיקות מידע בשווי של מיליוני דולרים התשתית היא ארגון מאוד מאובטח כמו בנק או חברת ביטוח, יש ביטוחים על ביטוחים, עשרות עובדי אבטחת מידע, הדרכות תקופתיות ואמצעים לשמור על המידע, בעולם הביטקוין נוצרו לא מעט מיליונרים שפתאום קובץ על הלפטופ שלהם מחזיק את המפתח למאות אלפי דולרים.

התמריץ של האקרים לפתוח את הארנקים האלו ולקבל גישה גדל בצורה אסטרונומית, וכך גם כמות הכספים שהושקעה ביחס לכך.

כאשר החומרה מאובטחת מאוד וכמעט בלתי אפשרית לפריצה, נוצר מצב שבו האדם, שהוא החוליה החלשה, נופל קורבן שוב ושוב לנסיונות הונאה והתחזות, וכך נאבדים עוד כספים.

סיכום

הונאות תמיד יתרחשו בעולם הביטקוין, ואין פתרון מבוסס חומרה אחד מושלם. זו בעיה כיוון שככל שנראה את הטכנולוגיה מתקדמת לא נצליח לעצור את התוקפים שעוברים דרך השיטות החברתיות, הלא טכנולוגיות. ההצפנה תמשיך להתפתח, האלגוריתמים ישתפרו, עוד אנטי וירוסים יגיעו, אבל בסופו של דבר אנחנו רואים שחלק משמעותי מהכספים נגנב בגלל הנדסה חברתית פשוטה שגורמת לאנשים לא להבין את הסיכון ולחשוב שהתוקף הוא אדם שמגיע לעזור להם.

בספר המלא תוכלו לראות אסטרטגיות מלאות להגנה על המטבעות, וגם ללמוד ממקרים נוספים, כולל הונאות פיננסיות והונאות טכנולוגיות אחרות. אפשר לרכוש אותו באתר: https://bitcoin-bookstore.com