על ארנקים מבוססי חומרה ואמון

מאת עו"ד יהונתן קלינגר

הקדמה

עולם הקריפטו מלא נוכלים והונאות. את זה כולם יודעים. היקף הנוכלויות תלוי בצורה שבה מגדירים נוכלות, אבל הכלל הוא פשוט: ביטקוין* הומצא כדי להיות מטבע חופשי מכבלים מדינתיים וחסין צנזורה. הרעיון הוא שכל מי שהוא חלק מקהילת הביטקוין הוא בר-חירות לבחור את הדרך בה הוא משתמש בכספים שלו, למי להעביר, למי לקבל, והכל תוך הבנה שיש כללים סגורים לנושא. לכן, ההתקנה של ארנקי ביטקוין היא לא דבר פשוט: נכון. אנחנו לא ב-2010 שצריך להתקין תוכנה מיוחדת על המחשב, לסנכרן אותה במשך שבוע מול הרשת ורק אז לייצר ארנק, אבל הטכנולוגיה בכוונה קשה.

מדוע הטכנולוגיה בכוונה קשה? מלא נוכלים והונאות כיוון שמדובר בכסף. המטרה היא לסבך ולמנוע מצב שבו קל מאוד לגנוב את כל הכסף שלכם, ולכן גם התוכנות הידידותיות ביותר רוצות שלפני שכסף יוצא מהארנק שלכם יבוצעו פעולות לא פשוטות. בין היתר, הליך הגיבוי של הארנק הוא מסובך. ומה זה הליך גיבוי? אם התקנתם ארנק על הטלפון הסלולרי שלכם, אתם תקבלו במעמד יצירת הארנק קובץ סודי שכל מי שיש לו גישה לקובץ הזה יכול לקחת את כל הכספים שלכם. זה נחמד כשיש לכם יתרה של מאתיים שקלים, או אולי אפילו אלפיים, אבל כשאתם מחזיקים מיליון דולר? פחות. לכן, נוצרו ארנקי חומרה.

ארנקים מבוססי חומרה

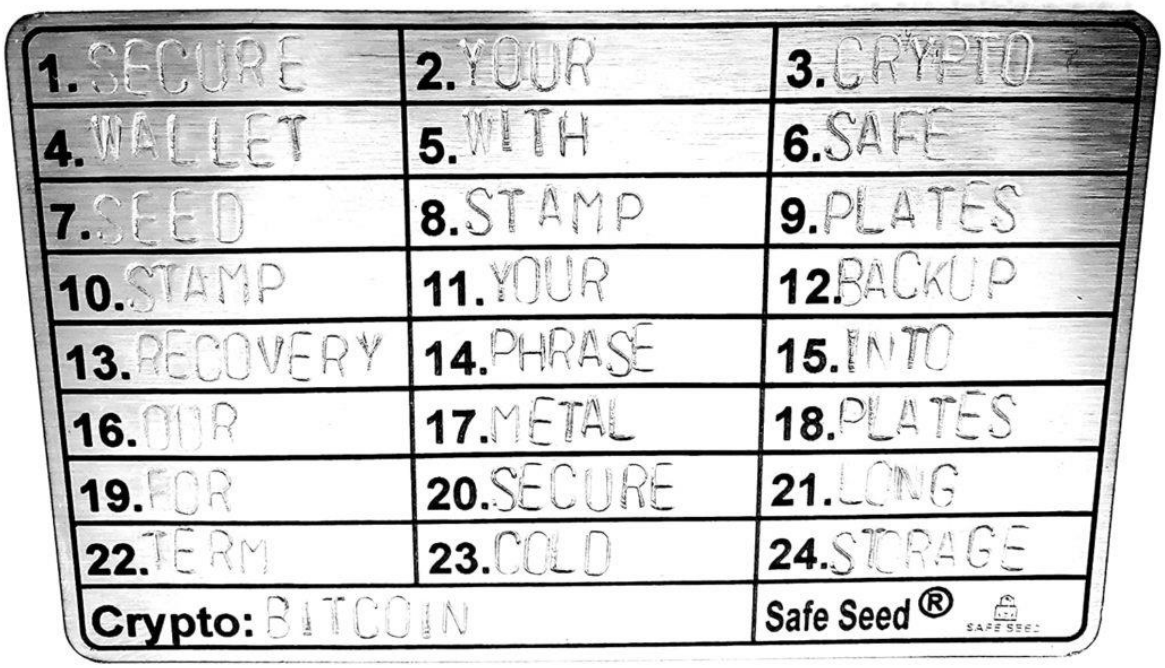
מה זה ארנק חומרה? ארנק חומרה הוא מכשיר שמחזיק את מפתחות הקריפטו שלכם בצורה מאובטחת על המכשיר, ושאי אפשר לחלץ או לפרוץ אותו גם אם המחשב נגוע. הנחת המוצא של ארנק חומרה היא שיש לכם וירוס או סוס טרויאני על המחשב או הטלפון. ומה זה אומר? אם יש לכם סוס טרויאני על הטלפון, וארנק הקריפטו שלכם על הטלפון, אז הסוס יכול לרוקן את הארנק כי יש לו שליטה על הטלפון. לעומת זאת, אם מפתחות הקריפטו שלכם לא נמצאות על הטלפון אלא ברכיב חומרה ייעודי שהטלפון לא יכול לגעת בו, אז גם אם יהיה סוס טרויאני על הטלפון לא יהיה אפשר לגנוב את הכסף. זה גם אומר שצריך לעשות עבודה

* אני הולך להשתמש בביטקוין וקריפטו בצורה תחליפית כאן, אבל ברור למה אני מתכוון

קשה כדי לשלוח כסף: בשלב הראשון מאשרים את העסקה על הטלפון, ורק אחר כך העסקה מופיעה גם על המסך של הארנק. אם שתי העסקאות זהות (כדי למנוע מצב שבו הסוס הטרויאני זייף את כתובת השליחה) אז מאשרים, והכסף יוצא.

הכלל הכי חשוב של ארנקי חומרה הוא שאין למי שייצר את הארנק שליטה בכסף שלכם. זה אומר שאף אחד, לא מי שבנה את הארנק, לא מי שעובד שם, ולא חבר שלהם, לא יכול לגשת לכסף שלכם. זה כל כך חשוב כי במקרים אחרים בעולם הקריפטו, כשהכסף נשלט על ידי גופים מסוימים הוא פשוט נעלם. בורסות שהחזיקו כספים נפרצו, שירותי מימון פשטו רגל, חוזים חכמים הופעלו על ידי פרצות אבטחה. כלומר: אם לכם אין שליטה בלעדית במפתחות שלכם, אז אתם לא מחזיקים באמת בכסף.

וזו החשיבות של ארנק חומרה: כשאתם קונים את הארנק הוא מחולל פעם אחת מחרוזת גיבוי. המחרוזת הזו, שמורכבת בדרך כלל מ-24 מילים, היא סוד שכל מי שיש לו גישה אליו יכול לקחת את כל הכסף שלכם. וזה לא תרחיש תיאורטי. זה וקטור התקיפה הכי פופולרי שיש: בגלל זה מזהירים אתכם שבכל מקרה אסור לכתוב את 24 המילים האלה אונליין, אסור להקליד אותן במחשב ואם אתם רוצים לשחזר את הארנק צריך להזין אותן רק בארנק ולא בכל מקום אחר. למה? כי הארנק הוא רכיב מאובטח שמנותק מהרשת.



[כך נראית לוחית גיבוי מאובטחת: ה-Seed חרוט על הלוחית ולא מאוחסן על מחשב]

חברות המייצרות ארנקי חומרה, אם כן, מוכרים אמון. זה המוצר שלהם. בלי אמון אין להם משמעות. בשוק של ארנקי החומרה בקריפטו היו עד החודש שני שחקנים מרכזיים: Trezor ו-Ledger.

Ledger, שהיא הנושא של המאמר הזה, חוו אירוע אבטחת מידע שבו פרצו לרשימת התפוצה שלהם.

בעיית אמון

זה קרה בשנת 2020 כשרשימת כתובות המייל של אנשים שרכשו בחנות של Ledger, ביחד עם כתובת המשלוח שלהם ושמם דלפו. זה לא היה טוב במיוחד כי זה ייצר בנק מטרות. מה זה אומר? זה אומר שעכשיו מסתובב ברשת מאגר מידע שלם של אנשים שקנו ארנק חומרה לקריפטו. כלומר יש רשימה של אנשים שיכול להיות שמחזיקים סכומים משמעותיים. אותם אנשים בשלוש השנים האחרונות היו קרבנות של שני סוגי תקיפה.

[ארנק מבוסס חומרה: Nano X של חברת Ledger]

הסוג הראשון הוא **פישינג**. פישינג זה לא קריטי, אבל זה הופך להיות קריטי כשההודעות מתחזות להודעות מ-Ledger. אנשים קיבלו הודעות מייל שצריך לעדכן את התוכנה, הורידו עדכון מאתר מזויף ואז התבקשו לכתוב את 24 המילים במחשב (וגם שיחות טלפון). רוב האנשים נעדרים בידע טכני כדי להבין כמה ולמה זה פסול ולכן עשו את זה, וכך איבדו את מיטב כספם. אבל זו הונאה שקל היה יחסית למנוע: פשוט לזהות את הפישינג וליישם פרקטיקה שאומרת "אל תקליד את המילים על מחשב".

הסוג השני הוא יותר קריטי. שוב, יש רשימה של אנשים שיש להם בבית מלא קריפטו. זה אומר שאפשר לדפוק להם על הדלת, להראות להם לום ולהגיד שאם הם לא משלמים אז הם יאבדו יד, רגל, איש אהוב. קרבנות סחיטה. זה אומר שלא משנה כמה טובה ההצפנה של Ledger, בסוף, **אם יש למישהו לום הוא יהלום בך עד שהאבטחה תשבר**.

אז אמון הוא עניין זמני. Ledger אולי הצליחו, עד החודש, לשחזר חלק מהאמון עם מוצרים טובים, ידידותיים למשתמש, וממשק טוב. הבעיה התחילה עם דחיפת עדכון התוכנה האחרון. העדכון הנ"ל הינו פרי שיתוף פעולה של Ledger עם חברת Coincover בשם Ledger Recover. Ledger אמרו בבסיס דבר חשוב: רוב הכספים שנעלמים נעלמים כי המשתמשים שלנו לא מבצעים גיבוי כמו שצריך. אם זו הבעיה, בואו נייצר להם דרך לגבות בצורה מאובטחת את המידע שלהם ולמנוע מצב שבו הם מאבדים גישה לכספים. אלא, שעם כוונות טובות לא מצליחים תמיד לעמוד בבעיות אמון.

הבעיה התחילה כך: Ledger דחפו עדכון קושחה לארנקים שלהם שביחד עם עדכוני האבטחה הרגילים הוסיפה את האופציה להרשם לשירות שבו רכיב האבטחה המוגן (תמורת עשרה דולר לחודש ובצירוף ביטוח עד 50,000 דולר), אותו רכיב שאף פעם לא אמור להיות מחובר לרשת, יכין שלוש חבילות מוצפנות שכל אחת מהן כולל חלק מהמפתח וישלח אותן לשלוש חברות שונות. השליחה תבטיח שאם אותו אדם יאבד את הגישה לארנק, הוא יוכל לשחזר את הכספים. אלא, שכדי להפעיל את זה, צריכה היתה Ledger

לייצר פגיעות: הפגיעות היא האפשרות לשלוח החוצה את הסוד הכי גדול: המפתחות. ברגע שזה הובן על ידי המשתמשים, התחילה סערה בקרב קהילת הקריפטו. הרי, שילמנו בסך הכל על מוצר כדי לקבל מוצר שאי אפשר לפרוץ, ופתאום אתם מוסיפים לנו חור אבטחה.

Ledger ערכו סמינר מלא והסבירו שלא מדובר בחור אבטחה אלא בעוד דרך לגבות את המידע (שווה לשמוע את השעה השלמה כדי להבין איך מחלקת יחסי ציבור עובדת). לדבריהם אין דלת אחורית. אלא שיש בכך מספר בעיות:

- הראשונה היא שברגע שהמוצר כבר לא מאובטח באותה צורה, ברור שאי אפשר לסמוך על כך שלא הוכנסו דברים נוספים כאלה.
- השניה היא שברגע שאת המפתח מחזיקים שלושה גופים חיצוניים (שמספיק שניים מתוכם כדי לגעת בכספים) ואותם גופים מחזיקים גם את הזהות של בעל החשבון, הרי שבתי משפט יכולים להתערב כאן: פתאום יכול לבוא שופט בארצות הברית ולבקש להעביר כספים מ-X ל-Y, או לתפוס אותם לטובת עצירת מה שהוא תופס כפעילות עבריינית

זה אומר שבעל החשבון איבד שליטה מלאה בכספים שלו והעביר אותם. לא משנה כמה זה מוצפן: אם אפשר לשחזר, זה אומר שאפשר גם לגנוב או להחרים.

לסיכום

גם לאחר ש-Ledger ערכו סמינר שבו ניסו להציג את הכל ולהסביר כמה הכל מאובטח ולא השתנה. זה לא ממש עבד מול הקהילה. הם איבדו את האמון של הקהילה וגם אם ימשכו את העדכון, כרגע ברור שהקוד שהם דחפו, שאמור היה להיות סודי ומאובטח, וחזק מאוד, כבר לא יתפס ככזה. בסופו של דבר, הם לקחו מוצר אבטחה ושנמכו אותו כדי להגיע להמונים. הפתרון לא היה צריך להיות שם אלא במקום שבו הם יכולים לתת להמונים מוצר אחר, פחות מאובטח, תחת מיתוג אחר.

אמון הוא משהו שקשה לרכוש, ועוד יותר קשה לתחזק.

על המחבר

יהונתן קלינגר הוא עורך דין בעל תואר שני במשפט עסקי מהמרכז הבינתחומי הרצליה (אוניברסיטת רייכמן) ובעל תארים ראשונים במשפטים ובממשל, דיפלומטיה ואסטרטגיה.

מאמר זה פורסם במקור כפוסט בבלוג "Intellect or Insanity" של עו"ד יהונתן קלינגר.