堅牢なウォレットも使い手次第で脆弱に

仮想通貨取引所での不正送金事件等でホットウォレットへの攻撃が注目を集める一方で、コールドウォレットであり安全性が高いとされるハードウェアウォレットに対する攻撃も確認されている。今後仮想通貨が普及する中で、ウォレットを狙った攻撃は加速すると考えられる。ユーザのセキュリティ意識を啓発していくことがさらに重要になるだろう。

ウォレットのセキュリティ事情

仮想通貨におけるウォレットとは、仮想通貨を扱う上で必要となる秘密鍵[1)]を保管するためのものである。仮想通貨における秘密鍵とは、仮想通貨の所有権を証明するものであり、仮想通貨の送金は、秘密鍵を用いて所有権を移動することによって実現される。

オンライン環境下で秘密鍵を管理するものをホットウォレット、オフライン環境下で秘密鍵を管理するものをコールドウォレットと呼ぶ。昨今、仮想通貨取引所における不正送金事件が世間を賑わせているが、この多くはホットウォレットへの攻撃によるものである。外部犯行視点で見た場合、オンライン上にあるウォレットの方が攻撃の標的にしやすいという点が理由として挙げられるだろう。これに対してコールドウォレットは、その特性上、外部犯行に対する耐性は高いとされている。現在、仮想通貨に対するセキュリティ意識が高まっている中で、ウォレットを選ぶ際、コールドウォレットを採用するユーザも増えてきているのではないだろうか。

注目されるハードウェアウォレット

現在利用されている代表的なコールドウォレットとしては、ペーパーウォレット[2)]やハードウェアウォレット（以下H/W）がある。中でもH/Wは、携帯可能なデバイス型であり、PC等の端末にUSB接続するだけで利用可能であったり、万一紛失等をしてもリカバリ可能な機能が提供されていたりと、利便性に優れていることから、コールドウォレットを採用する際の有力な選択肢であろう。

H/Wは秘密鍵を専用デバイス内に保管しており、秘密鍵を用いた署名を専用デバイス内で行う。例えば、秘密鍵をPC内に保存している場合、PCがマルウェアに感染した際に、秘密鍵を窃取されるというシナリオが考えられる。しかしH/Wの場合、PC等の接続端末が感染していたとしても、その仕組み上、秘密鍵を窃取されるリスクは低い。

現在、H/Wはセキュリティと利便性の両面で注目されており、H/Wを使えば安全であるという論調を見かけることも少なくない。また、実際にそのような認識でH/Wを利用しているユーザもいるのではないかと推測する。

「使えば安全」は危険

使えば安全とも思われるH/Wだが、その認識は誤りである。2018年6月末、多種の仮想通貨を扱うことができ人気があるH/W、TREZORを狙った攻撃が観測された。内容としては、TREZORを操作するためのWebサイトが何らかの理由でハイジャックされ、TREZORの公式サイトにアクセスすると、攻撃者が用意したサイトへアクセスさせられるというものであった。

一見H/Wには影響がなさそうなWebサイトのハイジャックだが、攻撃に繋がった理由には、H/Wで送金等を行う際の仕組みが関係している。TREZORは端末にUSB接続した場合、ブラウザ拡張[3)]等の専用のアプリケーションにより送金等の操作が可能となる。例えば、ブラウザ拡張を利用して送金を行おうとした場合、送金に必要となる情報を取得するためにTREZORのサ

NOTE

1) 仮想通貨の所有権を証明するもの。送金の際は、送金用のトランザクションを生成して、秘密鍵で署名を行い、ネットワークに伝搬する。
2) 秘密鍵を紙に印刷したもの。
3) Webブラウザの機能を拡張するためのプログラム。
4) H/Wのシードを生成するための英単語を羅列したもの。控えておくことによって、必要なときにH/Wを再構築できる。

イトへアクセスを行うが、攻撃発生時にはTREZORの正規サイトではなく、攻撃者が用意したサイトへアクセスさせられる状態にあった。攻撃者が誘導したサイトでは、ブラウザ上にH/Wのデバイスが破損した旨のメッセージが表示されると共に、復旧するためのニモニックコード[4]の送信が要求された。この要求に応じ、攻撃者が用意したサイトへニモニックコードを送信すると、攻撃者による秘密鍵の復元、不正送金を許してしまうという仕掛けである。

今回のTREZORの事件から、H/Wを利用していたとしても、その機能を利用する上でオンライン端末に接続する必要がある場合、ニモニックコードの窃取や不正送金の被害にあうリスクが存在することがわかる。

ユーザのセキュリティ意識が重要

H/Wは秘密鍵窃取の観点では安全といえるが、必ずしも秘密鍵の直接的な窃取だけが不正送金につながるというわけではない点に注意が必要である。つまり、H/Wを利用していたとしても、ユーザはニモニックコードの窃取や不正送金のリスクに警戒する必要がある。

一般的にH/Wでは、アプリケーション上で指示される重要なオペレーションについては、専用デバイスのディスプレイ上にも同様のメッセージが表示されるようになっており、この情報に攻撃者が直接干渉することは基本的にできない。前述したTREZORの事件を例にとると、ブラウザ上でニモニックコードを要求されていたとしても、デバイスのディスプレイ上に関連するメッセージが表示されていなければ、ユーザはその異変に気づくことができる。

今回紹介した例だけでなく、送金先アドレスや受金アドレス等をアプリケーション上で改竄されるということも有り得る。そのため、H/Wを用いて重要なオペレーションを行う際は、デバイスのディスプレイ上の表示を「真」と認識することが、基本的な対策として有効である。

また、H/Wで提供されているセキュリティ機能を利用することもよいだろう。例えば、TREZORでは任意でパスフレーズを追加設定できる。パスフレーズを設定した場合、万一ニモニックコードが漏洩してしまっても、パスフレーズまで漏洩しなければ、秘密鍵の復元はできない。今回の例に限らず、何らかの理由でH/Wやニモニックコードが窃取されたとしても、パスフレーズまで窃取されていなければ被害を防止できる。

仮想通貨取引所の事件を代表としたホットウォレットに対する攻撃が注目を集めているが、本稿で紹介したように、安全性が高いとされるH/Wのようなコールドウォレットを狙った攻撃が発生していることにも注意すべきである。

ユーザはウォレットを利用する以上、発生し得るセキュリティ上のリスクを理解し、適切な対策を講じる必要がある。今後仮想通貨が普及していくようになると、ユーザのウォレットを狙った攻撃はますます加速していくことが予想される。ユーザのセキュリティ意識に対する啓発をさらに進めていくことが重要である。

Writer's Profile

田中 悠一郎 Yuichiro Tanaka
NRIセキュアテクノロジーズ
セキュリティエンジニア
専門はブロックチェーンセキュリティ
focus@nri.co.jp