BTCX kommenterar problemen med bitcoin-stölder från ColdCard - Bitcoin-protokollet i sig har inte blivit hackat

"Det här är ingen trevlig händelse för Bitcoin-communityt, men det är viktigt att veta att inget är fel med bitcoinnätverket som sådant, det är en enskild aktör som inte hållit måttet. Som ett av de äldsta bolagen i Europa och hela världen vill BTCX gärna komma ut med information om det som hänt och vad man bör göra om man använder den tjänst som har de här problemen. Hos BTCX kan man höra av sig till supporten om man har frågor, och för våra OTC-kunder lanserar vi en särskild tjänst om bara ett par veckor med fokus på både verklig och digital säkerhet." säger Christian Ander, VD för Goobit Group AB.

I korthet: Om du har genererat en seed phrase på en Coldcard-enhet, agera nu och flytta dina bitcoin. "Seed" är i praktiken dina 12 ord och i det här fallet är problemet att de har varit mer förutsägbara än vanligt, trots att allt ser normalt ut på ytan — läs vidare för tekniska detaljer.

Ett kritiskt entropifel i Coldcards hårdvaruplånböcker har offentliggjorts. Till skillnad från kollapserna hos Mt. Gox, Quadriga eller FTX handlade det här inte om en börs/handelsplats. Det drabbade användare som följde bästa praxis genom att generera sina egna nycklar på en hårdvaruenhet som många i branschen länge rekommenderat som ett säkert alternativ för self-custody. Hittills har cirka 594 BTC stulits från omkring 500 drabbade plånböcker.
Bitcoins underliggande kryptografi förblir intakt. Problemet låg i seed-genereringsprocessen på vissa Coldcard-firmwares, som i vissa fall skapade seeds med betydligt lägre entropi än avsett — i vissa fall så lågt som 40–72 bitar istället för avsedda 128. Seeds med låg entropi går inte att visuellt skilja från säkra seeds förrän de utnyttjas.

Vår ståndpunkt
BTCX har aldrig rekommenderat eller marknadsfört Coldcard-enheter. Vi har uteslutande hänvisat kunder till Trezor hårdvaruplånböcker. Säkerhet är ett ständigt rörligt mål. För alla meningsfulla belopp i bitcoin fortsätter vi att rekommendera diversifierade uppsättningar — olika hårdvarutillverkare, multisignatur-konfigurationer och stark extern entropi eller lösenfraser där det är lämpligt. Observera att en multisignatur-uppsättning som uteslutande består av drabbade Coldcard-enheter inte ger något skydd; minst en nyckel måste komma från en icke-drabbad källa.

Omedelbar åtgärd krävs
Enligt tillverkarens aktuella säkerhetsvarning påverkar problemet seeds som genererats under följande förhållanden:
- Coldcard Mk2 eller Mk3 med firmware-versionerna 4.0.1 till och med 4.1.9
- Coldcard Mk4 eller Mk5 före standardfirmware version 5.6.0
- Coldcard Mk4 eller Mk5 före Edge-firmware version 6.6.0X
- Coldcard Q före standardfirmware version 1.5.0Q
- Coldcard Q före Edge-firmware version 6.6.0QX

— **Vänta inte**.

Flytta dina bitcoin nu.
Använd en hög avgift så att din transaktion inte riskerar att trängas undan av ett replace-by-fee-försök från en angripare som eventuellt redan bevakar eller kapplöper om samma UTXO:s. Ta dig tid att noggrant kontrollera mottagaradressen innan du skickar — i en tidskritisk situation är en förhastad eller feltippad överföring i sig en vanlig orsak till förlorade medel.
Att uppdatera enhetens firmware reparerar inte en redan kompromitterad seed. Medel måste aktivt flyttas till en ny, säkert genererad plånbok.
När medlen väl har flyttats till en säker ny uppsättning kan du ta dig tid att bygga en mer robust långsiktig förvaringslösning. Lämna inte betydande värden kvar på en enkelsignatur-seed som genererades under de sårbara förhållandena.

Vägen framåt
Den här händelsen är en påminnelse om att ingen enskild enhet eller tillverkare utgör en permanent garanti. Se över din egen uppsättning. Föredra multisignatur med nycklar genererade på oberoende enheter från olika tillverkare. Verifiera entropikällor. Håll dina återställningsprocesser testade och privata.
Vi följer situationen noga och kommer att gå ut med ytterligare uppdateringar om ny information blir tillgänglig. Har du frågor om att migrera från en drabbad enhet, om hur du kontrollerar om din uppsättning är i riskzonen, eller om hur du stärker din nuvarande lösning — kontakta support genom de vanliga kanalerna. Vi finns här för att hjälpa till, och det är alltid bättre att fråga än att gissa.

För ytterligare information, vänligen kontakta:
Christian Ander, VD, Goobit Group AB

E-post: ir@goobit.se

Om Goobit Group | BTCX
Goobit Group AB (publ) är verksamt inom finanssektorn. Bolaget lanserade BTCX 2011 – världens första fortfarande aktiva bitcoin-only-börs. Goobit är Sveriges ledande bitcoinföretag inom finansiella tjänster och utbildning. Bolaget erbjuder växlingstjänster från fiatvalutor till bitcoin. De mest välkända varumärkena är BTCX Express Exchange, Standard Exchange (BTCX), OTC Exchange och Bitcoin Treasury. Goobit Group AB (publ) registrerades 2013 och är en koncern bestående av de helägda dotterbolagen Goobit AB och Goobit Blocktech AB. Koncernen har sitt huvudkontor i Stockholm, Sverige.

Bifogade filer

BTCX kommenterar problemen med bitcoin-stölder från ColdCard - Bitcoin-protokollet i sig har inte blivit hackat