Major cryptocurrency provider compromised in a supply chain attack

Reference: Memo [191126-1] – Version: 1.0
Keywords: cryptocurrency, finance, Monero, supply chain attack
Sources: Publicly available information

Key Points

- The official command line interface Monero wallet was compromised and used in a supply chain attack.
- At least one person has reported financial loss due to the compromise.
- Cryptocurrency platforms and software are a high-value target for cyber-thieves.

Summary

On November 19, the Monero cryptocurrency team announced[1] that for 35 minutes, the wallet tools available from the official download site getmonero[.]org, had been compromised and harboured additional code that was designed to steal cryptocurrency. According to reports, at least one user lost about $7000 from their cryptocurrency wallet as a result of using the modified binary. As of writing, it is not clear how the compromise was achieved.

The breach came to light when some users noticed that the command-line Monero cryptocurrency wallet components downloaded from the official site had hashes that differed from the officially published checksums. This indicates that either the files have been modified or an incorrect hash value has been published. Monero team confirmed the breach and recommends that everyone who downloaded the tool recently should replace it with a known good one. Also, Monero recommends that if a cryptocurrency wallet was accessed with the compromised tool, all funds should be transferred to a different wallet immediately to avoid theft of virtual money.

Comments

Cryptocurrency management platforms and software are a preferred target for cyber criminals, simply "because that's where the money is." The Monero platform compromise is an ideal supply chain attack. Perpetrators altered the tools that cryptocurrency owners would use to manage their virtual money. These tools were stored and available at a trusted location and unsuspecting users who did not check the unique hash values of the binaries and compare them to the officially published ones, are at risk of losing all their Monero cryptocurrency earnings.

Other techniques used to compromise cryptocurrency platforms include spear phishing, gaining access to a trusted partner's computer and pivoting from there, exploiting unsecured private keys stored online, exploiting vulnerabilities in virtual wallets, etc. These breaches have sometimes resulted in the bankruptcy of the victimised cryptocurrency exchanges. Others have survived and regained the trust of their users.

According to open sources, as of November 2019, the top 5 historical cases by money lost are:

- Coincheck (Jan 2018): $533 million
- Mt. Gox (Mar 2014): $350 million
- BitGrail (Feb 2018): $170 million
- NiceHash (Dec 2017): $62 million
- Bitfinex (Aug 2016): $73 million

A more complete list of historical hacks of cryptocurrency trading platforms is provided in Annex. As the cryptocurrency market is extremely volatile, there is a big difference in the exchange rates over time. Higher number of cryptocurrency units lost does not always translate to a higher loss figure in dollars.

[1] https://web.getmonero.org/2019/11/19/warning-compromised-binaries.html

Annex. Attacks on cryptocurrency platforms[2]

Date		Victim	Cryptocurrency	Actor	Impact	Amount in cryptocurrency	Amount $
2019	June	Bitrue	XRP, ADA		Loss of funds	9.3 million XRP 2.5 million ADA	$5 million
	May	GateHub	XRP		Loss of funds	23.200.000 XRP	$10 million
	May	Binance	BTC		Loss of funds	7.000 BTC	$40 million
	March	Bithumb	EOS, XRP		Loss of funds	3 million EOS 20 million XRP	
	March	CoinBene	Several		Unknown		
	February	Coinmama	Several		Compromised Emails & Passwords	450.000 users	
	January	Cryptopia	ETH		Loss of funds	19.390 ETH	
2018	September	Zaif	BTC		Loss of funds	5.966 BTC	$60 million
	June	Coinrail	ETH, NPXS, ATX, DENT		Loss of funds	1,927 ETH 2.6 billion NPXS 93 million ATX 831 million DENT	$40 million
	June	Bithumb	XRP	Lazarus	Loss of funds		$31 million
	May	Bitcoin Gold	BTG		Loss of funds		$18 million
	May	Taylor	ETH		Loss of funds	2.578 ETH	
	April	CoinSecure	BTC		Loss of funds	438 BTC	$3,5 million
	February	Bitgrail	NANO		Loss of funds	17.000.000 NANO	$170 million
	January	Coincheck	NEM		Loss of funds	17.000.000 NANO	$533 million
2017	December	NiceHash	BTC		Loss of funds	4.736 BTC	$62 million
	December	Youbit	Unknown		Bankruptcy	Unknown	Unknown
	July	Bithumb	BTC, ETH		Loss of funds		$7 million
	April	Yapizon	BTC		Loss of funds	3.800 BTC	$5 million
2016	August	Bitfinex	BTC		Price of Bitcoin plunged	120.000 BTC	$73 million
	May	GateCoin	BTC, ETH		Loss of funds	250 BTC 185.000 ETH	$2 million
	April	ShapeShift			Loss of funds		$230.000
2015	February	BTER	BTC		Loss of funds	7.170 BTC	$1,5 million
	February	KipCoin	BTC		Loss of funds	3.000 BTC	
	January	Bitstamp	BTC		Loss of funds	19.000 BTC	$5,1 million
	January	LocalBitcoins	BTC		Loss of funds	17 BTC	
	January	796	BTC		Loss of funds	1.000 BTC	$7 million
2014	October	MintPal	BTC		Loss of funds	3.700 BTC	
	July	Cryptsy	BTC, LTC		Loss of funds Exchange declared insolvency	13.000 BTC 300.000 LTC	$8,2 million
	July	MintPal	VRC		Loss of 30% of all Vericoin	8 million VRC	
	March	Mt. Gox	BTC		Loss of funds Bankruptcy	850.000 BTC	$350 million
	March	Poloniex	BTC		Loss of funds	97 BTC	
2013	November	BitCash	BTC		Loss of funds	484 BTC	$3,4 million
	May	Vicurex	BTC		Loss of funds	1.454 BTC	$10 million
2012	September	BitFloor	BTC		Loss of funds	24.000 BTC	$250.000
	May	Bitcoinica	BTC		Loss of funds Exchange closed	18.457 BTC	
	March	Linode	BTC		Loss of funds	46.000 BTC	
2011	June	Mt. Gox	BTC		Artificially lower price	2.643 BTC	
	October	Bitcoin7	BTC		Loss of funds	11.000 BTC	

[2] https://selfkey.org/list-of-cryptocurrency-exchange-hacks/