Attacking Zcash Protocol For Fun And Profit
Whitepaper Version 0.1

Duke Leto[†]

May 4, 2020

Abstract.

This paper will outline, for the first time, exactly how the "ITM Attack" works against Zcash Protocol and how Hush is the first cryptocoin with a defensive mitigation against it, called "Sietch". Sietch is already running live in production and undergoing it's first improvement from a round a feedback. This is not an academic paper about pipedreams, it will describe production code and networks.

Beginning with a literature review of all known metadata attack methods that can be used against Zcash Protocol blockchains. This includes their estimated attack costs and threat model. This paper then describes the "ITM Attack" which is a specific instance of a new class of metadata attacks against blockchains which the author describes as "Metaverse Metadata" attacks.

A few other new privacy issues and metadata attacks against Zcash Protocol coins will be enumerated for the first time publicly in this treatise.

The paper then explains Sietch in detail, which was a response to these new attacks. We hope this knew knowledge and theory helps cryptocoins increase their defenses against very well-funded adversaries including nation states and chain analysis companies.

In privacy zdust we trust.

If dust can attack us, dust can protect us.

– Sietch Mottos

Keywords: anonymity, freedom of speech, cryptographic protocols, electronic commerce and payment, financial privacy, proof of work, zero knowledge zk-SNARKs .

Contents

[†] duke@leto.net , duke.leto.net, @dukeleto, 8DFC BF8E 5A4D 8019 , https://keybase.io/dukeleto

1 Introduction

2 Metadata Analysis of Zcash Protocol Blockchains: Basics

3 Metadata Analysis of Zcash Protocol Blockchains: Advanced

4 De-anonymization techniques literature review

5 ITM Attack

...

6 Metaverse Metadata Attacks

TODO: Explain how they can be used on all blockchains with transaction graphs, including CryptoNote Protocol and MimbleWimble Protocol

7 Sietch: Theory

8 Sietch: Code In Production

9 Advice To Zcash Protocol Coins

10 Special Thanks

Special thanks to jl777, ITM and denioD for their feedback.

11 References