

Intelligence Report

Fabricated Microsoft Crypto Wallet Phishing Site Spreads Infostealer

N/A info@netmanageit.com
N/A <https://www.netmanageit.com>
N/A
N/A

Table of contents

Overview

● Description	3
● Confidence	3

Entities

● Indicator	4
-------------	---

Observables

● Domain-Name	5
● StixFile	6

External References

● External References	7
-----------------------	---

Overview

Description

Cyble Research and Intelligence Labs analyzes Threat Actors spreading Luca Stealer disguised as a beta version of Microsoft Crypto Wallet.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name

480cea45f9c10159ef76555a0b86c25b232952b5cbc6da2862ff4b8cbb2943c1

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'480cea45f9c10159ef76555a0b86c25b232952b5cbc6da2862ff4b8cbb2943c1']

Name

microsoft-en.com

Pattern Type

stix

Pattern

[domain-name:value = 'microsoft-en.com']

Domain-Name

Value

microsoft-en.com

StixFile

Value

480cea45f9c10159ef76555a0b86c25b232952b5cbc6da2862ff4b8cbb2943c1

External References

-
- <https://otx.alienvault.com/pulse/64be9d4cf3011753893ad398>
-
- <https://blog.cyble.com/2023/07/21/fabricated-microsoft-crypto-wallet-phishing-site-spreads-infostealer/>