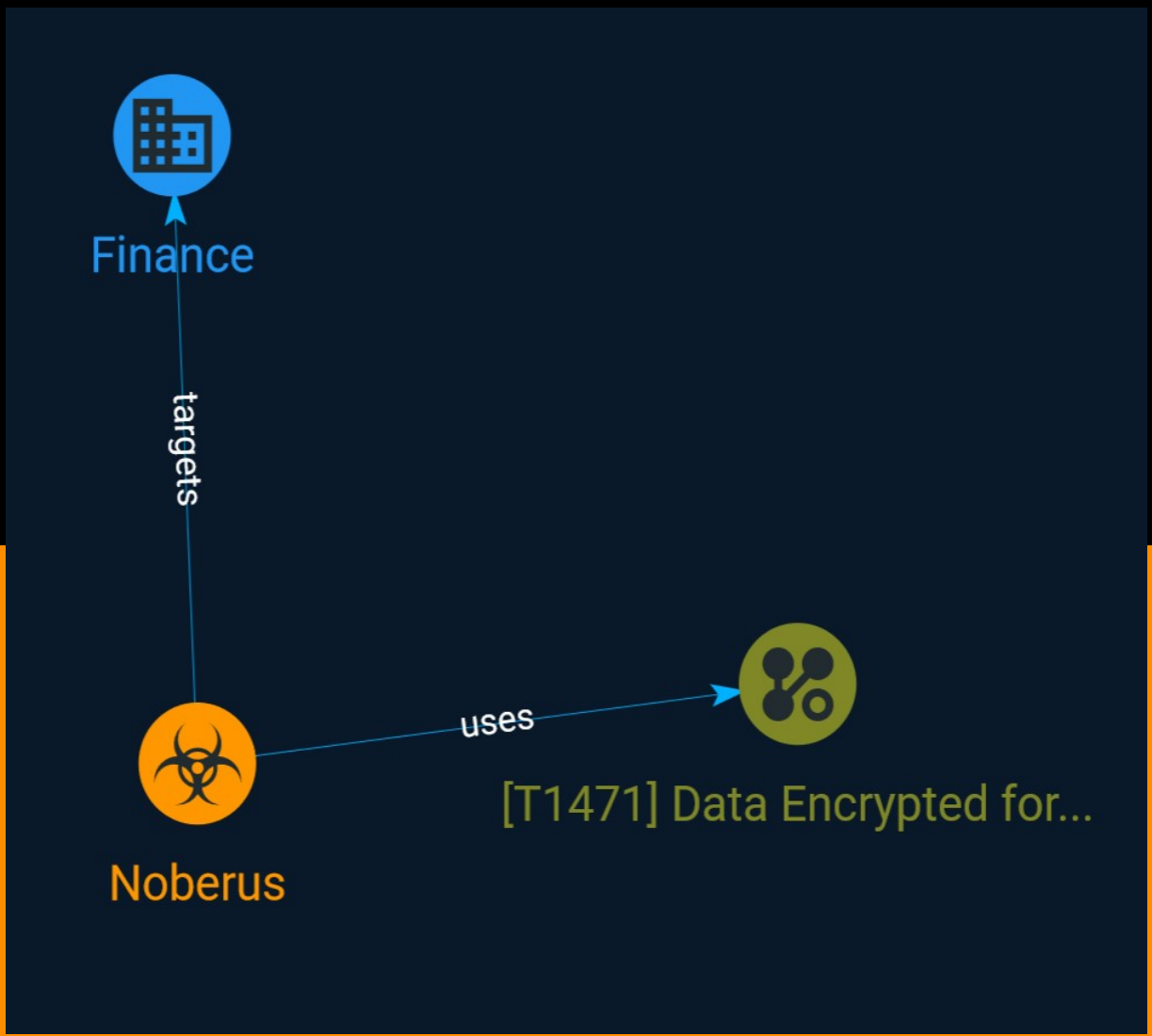
Jul 19 2023

NETMANAGEIT

# Intelligence Report

# FIN8 Uses Revamped Sardonic Backdoor to Deliver Noberus Ransomware



# Table of contents

## Overview



## Entities



## External References

# Overview

## Description

Financially motivated cyber-crime group continues to develop and improve tools and tactics.

## Confidence

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

15 / 100

# Malware

| Name |
| --- |
| Noberus |

# Attack-Pattern

| Name |
| --- |
| Data Encrypted for Impact |
| **ID** |
| T1471 |
| **Description** |
| An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. |

# Sector

| Name |
| --- |
| Finance |
| **Description** |
| Public and private entities involved in the allocation of assets and liabilities over space and time. |

# External References

- https://otx.alienvault.com/pulse/64b7a0336ca84d46de5d7f15
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sysssphinx-fin8-backdoor