Report | The Mystery of Metador | An Unattributed Threat Hiding in Telcos, ISPs, and Universities

By Author:

Published: 2022-09-22 · Archived: 2026-11-20 02:10:56 UTC

Color

Size

of 27

1THE MYSTERY OF M E TA D O R | A N U N AT T R I B U T E D T H R E AT H I D I N G I N T E LCOS , I S P S , A N D U N I V E R S I T I E S
THE MYSTERY OF METADOR |
AN UNATTRIBUTED THREAT
HIDING IN TELCOS, ISPS,
AND UNIVERSITIES
Author: Amitai Ben Shushan Ehrlich,
Aleksandar Milenkoski, Juan Andres Guerrero-Saade
September 2022
SentinelLABS Research Team

2THE MYSTERY OF M E TA D O R | A N U N AT T R I B U T E D T H R E AT H I D I N G I N T E LCOS , I S P S , A N D U N I V E R S I T I E S
TABLE OF
CONTENTS
3 EXECUTIVE SUMMMARY
4 OVERVIEW
6 TECHNICAL OVERVIEW
7 THE MANY SUPPORTED
EXECUTION FLOWS
OF METAMAIN
11 MAFALDA
17 ADDITIONAL IMPLANTS
20 INFRASTRUCTURE
22 ATTRIBUTION AND TIMELINE
25 CONCLUSION
26 APPENDIX:
INDICATORS OF COMPROMISE
27 ABOUT SENTINELLABS

Source: https://assets.sentinelone.com/sentinellabs22/metador#page=1