

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

By Author:

Archived: 2026-04-05 13:44:01 UTC

1THE MYSTERY OF METADOR | AN UNATTRIBUTED THREAT HIDING IN TELCOS, IS  
PS, AND UNIVERSITIES  
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 METADOR | AN UNATTRIBUTED THREAT HIDING IN TELCOS, IS  
PS, AND UNIVERSITIES  
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/sentinelabs22/metador#page=1>