

# Sanctions Be Damned | From Dridex To Macaw, The Evolution of Evil Corp

By Author:

Archived: 2026-04-05 12:59:18 UTC

1 SANCTIONS BE DAMNED | FROM DRIDEX TO MACAW, THE EVOLUTION OF EVIL CORP

SANCTIONS BE DAMNED |  
FROM DRIDEX TO MACAW,  
THE EVOLUTION OF EVIL CORP

Author: Antonio Pirozzi, Antonis Terefos and Idan Weizman February 2022 SentinelLABS Research Team

2 SANCTIONS BE DAMNED | FROM DRIDEX TO MACAW, THE EVOLUTION OF EVIL CORP

TABLE OF  
CONTENTS

3 EXECUTIVE SUMMARY

4 BACKGROUND

6 THE EVIL CORP

MALWARE LINEAGE

28 OTHER TOOLSET EXPANSION

29 MACAW LOCKER

RANSOMWARE

34 CRYPTONE: THE PACKER

44 INFRASTRUCTURE OVERLAPS

46 CONCLUSIONS

48 MITRE ATT&CK

TTPS OBSERVED

52 YARA RULES

53 INDICATORS OF  
COMPROMISE [IOCS]

60 APPENDIX

63 ABOUT SENTINELLABS

---

Source: [https://assets.sentinelone.com/sentinelabs/sentinelabs\\_EvilCorp](https://assets.sentinelone.com/sentinelabs/sentinelabs_EvilCorp)