

# en\_arkei\_stealer\_technical\_analysis\_report.pdf

Archived: 2026-04-05 22:32:29 UTC

## Sida 2 av 43

i

### Contents

WHAT IS ARKEI .....	1
ANALYSIS OF DTPDZGZ1HO.EXE .....	2
OVERVIEW .....	2
DETAILED ANALYSIS.....	4
ANALYSIS OF STAGE-2.....	7
OVERVIEW .....	7
DETAILED ANALYSIS.....	7
ANALYSIS OF STAGE-3.....	11
OVERVIEW .....	11
DETAILED ANALYSIS.....	11
TELEGRAM ADDRESSES .....	15
ANALYSIS OF 4KSOA92JSAL.EXE .....	20
OVERVIEW .....	20
DETAILED ANALYSIS.....	20
ANALYSIS OF STAGE-5.....	23
OVERVIEW .....	23
DETAILED ANALYSIS.....	23

ANALYSIS OF  
PUNPUN.EXE.....  
26

OVERVIEW ..... 26

DETAILED ANALYSIS..... 26

ANALYSIS OF  
INFODEBUG.EXE.....  
28

OVERVIEW ..... 28

ANALYSIS OF STAGE-  
8..... 29

OVERVIEW ..... 29

STAGE-9 (DONUTLOADER  
VARIANT)..... 30

OVERVIEW ..... 30

STAGE-10  
(REDLINE).....  
31

OVERVIEW ..... 31

YARA  
RULES.....  
32

MITRE ATTACK TABLE  
..... 40

SOLUTION OFFERS  
..... 40

PREPARED  
BY.....  
41

---

Source: <https://drive.google.com/file/d/1wTH-BZrjxEBZwCnXJ3pQWGB7ou0IoBEr/view>