HALFBAKED (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:29:32 UTC

HALFBAKED

Actor(s): Anunak

The HALFBAKED malware family consists of multiple components designed to establish and maintain a foothold in victim networks, with the ultimate goal of gaining access to sensitive financial information. HALFBAKED listens for the following commands from the C2 server:

info: Sends victim machine information (OS, Processor, BIOS and running processes) using WMI queries
processList: Send list of process running
screenshot: Takes screen shot of victim machine (using 58d2a83f777688.78384945.ps1)
runvbs: Executes a VB script
runexe: Executes EXE file
runps1: Executes PowerShell script
delete: Delete the specified file
update: Update the specified file

References

There is no Yara-Signature yet.
