ModPipe (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:59:18 UTC

ModPipe

ModPipe is point-of-sale (POS) malware capable of accessing sensitive information stored in devices running ORACLE MICROS Restaurant Enterprise Series (RES) 3700 POS – a management software suite used by hundreds of thousands of bars, restaurants, hotels and other hospitality establishments worldwide. ModPipe uses modular architecture consisting of basic components and downloadable modules. One of them – named GetMicInfo – contains an algorithm designed to gather database passwords by decrypting them from Windows registry values. Exfiltrated credentials allow ModPipe's operators access to database contents, including various definitions and configuration, status tables and information about POS transactions.

References

There is no Yara-Signature yet.
