Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:38:44 UTC

Tool: ModPipe

Names	ModPipe
Category	Malware
Type	POS malware, Backdoor, Info stealer, Credential stealer, Exfiltration
Description	(ESET) ESET researchers have discovered ModPipe, a modular backdoor that gives its operators access to 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. What makes the backdoor distinctive are its downloadable modules and their capabilities. One of them – named GetMicInfo – contains an algorithm designed to gather database passwords by decrypting them from Windows registry values. This shows that the backdoor's authors have deep knowledge of the targeted software and opted for this sophisticated method instead of collecting the data via a simpler yet "louder" approach, such as keylogging. Exfiltrated credentials allow ModPipe's operators access to database contents, including various definitions and configuration, status tables and information about POS transactions.
Information	<https://www.welivesecurity.com/2020/11/12/hungry-data-modpipe-backdoor-hits-pos-software-hospitality-sector/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.modpipe>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool ModPipe

Changed	Name	Country	Observed
Unknown groups			

	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)
