Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:15:04 UTC

Tool: RDFSNIFFER

Names	RDFSNIFFER
Category	Malware
Type	ATM malware, Backdoor
Description	(FireEye) RDFSNIFFER, a payload of Boostwrite, appears to have been developed to tamper with NCR Corporation's “Aloha Command Center” client. NCR Aloha Command Center is a remote administration toolset designed to manage and troubleshoot systems within payment card processing sectors running the Command Center Agent. The malware loads into the same process as the Command Center process by abusing the DLL load order of the legitimate Aloha utility. Mandiant provided this information to NCR.
Information	<https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0416/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool RDFSNIFFER

Changed	Name	Country	Observed	
APT groups				
	FIN7		2013-Jul 2024	

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