Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:06:12 UTC

Tool: CheeseTray

Names	CheeseTray CROWDEDFLOUNDER
Category	Malware
Type	Backdoor
Description	(US-CERT) This report analyzes a Themida packed 32-bit Windows executable, which is designed to unpack and execute a Remote Access Trojan (RAT) binary in memory. This application is designed to accept arguments during execution or can be installed as a service with command line arguments. It is designed to listen as a proxy for incoming connections containing commands or can connect to a remote server to receive commands.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar20-045c>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cheesetray>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool CheeseTray

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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