Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:31:34 UTC

Tool: IMAPLoader

Names	IMAPLoader
Category	Malware
Type	Reconnaissance, Backdoor, Downloader
Description	(PWC) IMAPLoader is a .NET malware that has the ability to fingerprint victim systems using native Windows utilities and acts as a downloader for further payloads. It uses email as a C2 channel and is able to execute payloads extracted from email attachments and is executed via new service deployments.
Information	<https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S1152>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.imap_loader>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool IMAPLoader

Changed	Name	Country	Observed	
APT groups				
	Tortoiseshell, Imperial Kitten		2018-Oct 2023	

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