Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:46:52 UTC

Tool: HUI Loader

Names	HUI Loader
Category	Malware
Type	Loader
Description	(SecureWorks) HUI Loader is a custom DLL loader whose name is derived from a string in the loader (see Figure 1). The malware is loaded by legitimate programs that are vulnerable to DLL search order hijacking. HUI Loader decrypts and loads a third file containing an encrypted payload that is also deployed to the compromised host. CTU researchers have observed HUI Loader loading RATs such as SodaMaster, PlugX, Cobalt Strike, and QuasarRAT.
Information	<https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader>
MITRE ATT&CK	<https://attack.mitre.org/software/S1097>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hui_loader>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool HUI Loader

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	
	Bronze Starlight		2021-Mar 2023	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=afe97e74-7cbf-4bc0-8425-4520ad9f325d