Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:47:36 UTC

Tool: BlackLotus

Names	BlackLotus
Category	Malware
Type	Rootkit
Description	(ESET) The number of UEFI vulnerabilities discovered in recent years and the failures in patching them or revoking vulnerable binaries within a reasonable time window hasn't gone unnoticed by threat actors. As a result, the first publicly known UEFI bootkit bypassing the essential platform security feature – UEFI Secure Boot – is now a reality. In this blogpost we present the first public analysis of this UEFI bootkit, which is capable of running on even fully-up-to-date Windows 11 systems with UEFI Secure Boot enabled. Functionality of the bootkit and its individual features leads us to believe that we are dealing with a bootkit known as BlackLotus, the UEFI bootkit being sold on hacking forums for $5,000 since at least October 2022.
Information	<https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/> <https://www.bleepingcomputer.com/news/security/source-code-for-blacklotus-windows-uefi-malware-leaked-on-github/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.blacklotus>
Playbook	<https://media.defense.gov/2023/Jun/22/2003245723/-1/-1/0/CSI_BlackLotus_Mitigation_Guide.PDF>

Last change to this tool card: 05 September 2023

Download this tool card in JSON format

All groups using tool BlackLotus

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=df277b10-a9da-4574-abe2-a2ef0753eaca