Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:47:55 UTC

Tool: SymonLoader

Names	SymonLoader
Category	Malware
Type	Loader
Description	(Palo Alto) When executed, the loader starts monitoring storage device changes on a compromised machine. If SymonLoader detects the targeted type of secure USB drive, it attempts to access the storage through the device driver corresponding to the secure USB and checks for strings specific to one type of secure USB in the drive information fields. Then, it accesses a predefined location of the storage on the USB and extracts an unknown PE file.
Information	<https://unit42.paloaltonetworks.com/unit42-tick-group-weaponized-secure-usb-drives-target-air-gapped-critical-systems/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:SymonLoader>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool SymonLoader

Changed	Name	Country	Observed	
APT groups				
	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	

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