Threat Group Cards: A Threat Actor Encyclopedia

Tool: BHUNT

Names	BHUNT
Category	Malware
Type	Banking trojan, Info stealer, Credential stealer
Description	(Bitdefender) Bitdefender researchers are constantly monitoring crypto wallet stealers. This is how we spotted a dropper with a hidden file that ran from the \Windows\System32\ folder. The dropper always wrote the same file, mscrlib.exet to the disk. Our analysis determined t a new cryptocurrency stealer, but its execution flow seems different from what we're used to seeing in the wild. We named the stealer BHUNT after the main assembly's name. BHUNT is a modular stealer written in .NET, capable of exfiltrating wallet (Exodus, Electrum, Atomic, Jaxx, Ethereum, Bitcoin, Litecoin wallets) contents, passwords stored in the browser, and passphrases captured from the clipboard.
Information	<https://www.bitdefender.com/files/News/CaseStudies/study/411/Bitdefender-PR-Whitepaper-CyberWallet-creat5874-en-EN.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bhunt>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool BHUNT

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

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