Threat Group Cards: A Threat Actor Encyclopedia

Tool: Infostealer

Names	Infostealer stereoversioncontrol
Category	Malware
Type	Reconnaissance, Info stealer
Description	(FireEye) Infostealer/stereoversioncontrol.exe downloads a RAR file, as well as the get-logon-history.ps1 tool. It runs several commands on the infected machine to gather information about it and also the Firefox data of all users of the machine. It then compresses this information before transferring it to a remote directory. Infostealer/Sha.exe/Sha432.exe operates in a similar manner, gathering information about the infected machine.
Information	<https://symantec-blogs.broadcom.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Infostealer

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

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