Threat Group Cards: A Threat Actor Encyclopedia

Tool: LATCHKEY

Names	LATCHKEY
Category	Malware
Type	Dropper
Description	(Mandiant) In one intrusion, FIN13 utilized certutil to decode a base64 encoded version of the custom dropper LATCHKEY. LATCHKEY is a PowerShell to EXE (PS2EXE) compiled dropper that base64 decodes and executes the PowerSploit function Out-Minidump which generates a minidump for the LSASS system process to disk.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico>

Last change to this tool card: 26 December 2021

Download this tool card in JSON format

All groups using tool LATCHKEY

Changed	Name	Country	Observed	
APT groups				
	FIN13	[Unknown]	2016	

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