Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:24:55 UTC

Tool: IRONSQUIRREL

Names	IRONSQUIRREL
Category	Exploits
Type	0-day, Loader
Description	This project aims at delivering browser exploits to the victim browser in an encrypted fashion. Ellyptic-curve Diffie-Hellman (secp256k1) is used for key agreement and AES is used for encryption. By delivering the exploit code (and shellcode) to the victim in an encrypted way, the attack can not be replayed. Meanwhile the HTML/JS source is encrypted thus reverse engineering the exploit is significantly harder.
Information	<https://github.com/MRGEffitas/Ironsquirrel>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool IRONSQUIRREL

Changed	Name	Country	Observed	
APT groups				
	Poison Carp, Evil Eye		2018-Jun 2023	

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