Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:20:29 UTC

Tool: IRONHALO

Names	IRONHALO
Category	Malware
Type	Downloader
Description	(FireEye) IRONHALO is a downloader that uses the HTTP protocol to retrieve a Base64 encoded payload from a hard-coded command-and-control (CnC) server and uniform resource locator (URL) path. The encoded payload is written to a temporary file, decoded and executed in a hidden window. The encoded and decoded payloads are written to files named igfxHK[%rand%].dat and igfxHK[%rand%].exe respectively, where [%rand%] is a 4-byte hexadecimal number based on the current timestamp. It persists by copying itself to the current user's Startup folder.
Information	<https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html> <https://www.fireeye.com/blog/threat-research/2015/12/the_eps_awakens.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ironhalo>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool IRONHALO

Changed	Name	Country	Observed	
APT groups				
	APT 16, SVCMONDR		2015	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ad6447b0-774f-48a1-a5da-d03c3e0b94e4