

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:49:18 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool BootWreck

## Tool: BootWreck

Names	BootWreck MBRkiller
Category	<a href="#">Malware</a>
Type	<a href="#">Wiper</a>
Description	<p>(<a href="#">Flashpoint</a>) Wiper malware that may have destroyed as many as 9,000 workstations and 500 servers inside the Banco de Chile in a late-May attack has similarities to the Buhtrap malware component known as MBR Killer, leaked to the underground in February 2016.</p> <p>Analysts at Flashpoint reverse-engineered the identified malware linked to the May 24 attack against the country's largest financial institution, and said the malware is a modified version of a MBR Killer module known as kill_os. MBR Killer infections render the local operating system and the Master Boot Record unreadable.</p>
Information	< <a href="https://www.flashpoint-intel.com/blog/banco-de-chile-mbr-killer-reveals-hidden-nexus-buhtrap/">https://www.flashpoint-intel.com/blog/banco-de-chile-mbr-killer-reveals-hidden-nexus-buhtrap/</a> >
Malpedia	< <a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.bootwreck">https://malpedia.caad.fkie.fraunhofer.de/details/win.bootwreck</a> >

Last change to this tool card: 24 April 2021

Download this tool card in [JSON](#) format

## All groups using tool BootWreck

Changed	Name	Country	Observed	
<b>APT groups</b>				
	<a href="#">Lazarus Group</a> , <a href="#">Hidden Cobra</a> , <a href="#">Labyrinth Chollima</a>		2007-May 2025	

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

---

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=ab8fab81-e119-4c00-94f6-15127b3f5db4>