Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:44:45 UTC

Tool: PNGLoad

Names	PNGLoad
Category	Malware
Type	Loader
Description	(ESET) PNGLoad is the second-stage payload deployed by Worok on compromised systems and, according to ESET telemetry, loaded either by CLRLoad or PowHeartBeat. While we don't see any code in PowHeartBeat that directly loads PNGLoad, the backdoor has the capabilities to download and execute additional payloads from the C&C server, which is likely how the attackers have deployed PNGLoad on systems compromised with PowHeartBeat. PNGLoad is a loader that uses bytes from PNG files to create a payload to execute. It is a 64-bit .NET executable – obfuscated with .NET Reactor – that masquerades as legitimate software. For example, Figure 11 shows the CLR headers of a sample masquerading as a WinRAR DLL.
Information	<https://www.welivesecurity.com/2022/09/06/worok-big-picture/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.png_load>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool PNGLoad

Changed	Name	Country	Observed	
APT groups				
	Worok		2020	

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