Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:49:43 UTC

Tool: PipeSnoop

Names	PipeSnoop TOFUPIPE
Category	Malware
Type	Backdoor
Description	(Talos) The PipeSnoop implant, created in May 2023, is a simple implant that can run arbitrary shellcode payloads on the infected endpoint by reading from an IPC pipe. Although semantically similar, the PipeSnoop implant should not be considered an upgrade of HTTPSnoop. Both implants are likely designed to work under different environments. The HTTP URLs used by HTTPSnoop along with the binding to the built-in Windows web server indicate that it was likely designed to work on internet-exposed web and EWS servers. PipeSnoop, however, as the name may imply, reads and writes to and from a Windows IPC pipe for its input/output (I/O) capabilities This suggests the implant is likely designed to function further within a compromised enterprise--instead of public-facing servers like HTTPSnoop — and probably is intended for use against endpoints the malware operators deem more valuable or high-priority. PipeSnoop is likely used in conjunction with another component that is capable of feeding it the required shellcode.
Information	<https://blog.talosintelligence.com/introducing-shrouded-snooper/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pipesnoop>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool PipeSnoop

Changed	Name	Country	Observed
APT groups			

	ShroudedSnooper	[Unknown]	2023	

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