Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:06:00 UTC

Tool: HTTPSnoop

Names	HTTPSnoop TOFULOAD
Category	Malware
Type	Backdoor
Description	(Talos) HTTPSnoop is a simple, yet effective, new backdoor that uses low-level Windows APIs to interact directly with the HTTP device on the system. It leverages this capability to bind to specific HTTP(S) URL patterns to the endpoint to listen for incoming requests. Any incoming requests for the specified URLs are picked up by the implant, which then proceeds to decode the data accompanying the HTTP request. The decoded HTTP data is, in fact, shellcode that is then executed on the infected endpoint. HTTPSnoop consists of the same code across all observed variants, with the key difference in samples being the URL patterns that it listens for.
Information	<https://blog.talosintelligence.com/introducing-shrouded-snooper/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.httpsnoop>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool HTTPSnoop

Changed	Name	Country	Observed	
APT groups				
	ShroudedSnooper	[Unknown]	2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=734dd7c9-ea82-4ee7-9850-65bbde4b198f