Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:07:12 UTC

Tool: Snugy

Names	Snugy
Category	Malware
Type	Backdoor, Tunneling
Description	(Palo Alto) The OfficeIntegrator.ps1 file seen in the ResolutionHosts task is a PowerShell-based backdoor we call Snugy, which allows an actor to obtain the system's hostname and to run commands. Snugy is a variant of the CASHY200 backdoor used by actors in previous attacks in the xHunt campaign. In July 2019, Trend Micro created a detection signature for this backdoor called Backdoor.PS1.NETERO.A, which suggests that this particular variant of CASHY200 has been around for over a year. We are calling this variant of the backdoor Snugy, as Netero is already a name of a variant of the Hisoka tool used by the xHunt actors.
Information	<https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.snugy>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Snugy

Changed	Name	Country	Observed	
APT groups				
	xHunt		2018-Aug 2019	

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