Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:11:01 UTC

Tool: CASHY200

Names	CASHY200
Category	Malware
Type	Backdoor, Tunneling
Description	(Palo Alto) During our continued analysis of the xHunt campaign, we observed several domains with ties to the pasta58[.]com domain associated with known Sakabota command and control (C2) activity. In June 2019, we observed one of these overlapping domains, specifically, windows64x[.]com, being used as the C2 server for a new PowerShell based backdoor that we've named CASHY200. This PowerShell backdoor used DNS tunneling to communicate with its C2 server, specifically by issuing DNS A queries to the actor controlled name server at the aforementioned domain. CASHY200 parses data provided by the C2 server within DNS answers to run commands on the system and send the results back to the C2 via DNS queries. In several samples, CASHY200 used randomly generated identifiers that are stored in the registry at HKCU\Software\Microsoft\Cashe\index and used the command value 200 to communicate with the C2 server. These details are the basis for the name CASHY200.
Information	<https://unit42.paloaltonetworks.com/more-xhunt-new-powershell-backdoor-blocked-through-dns-tunnel-detection/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.cashy200>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool CASHY200

Changed	Name	Country	Observed	
APT groups				
	xHunt		2018-Aug 2019	

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