Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:02:06 UTC

Tool: C0d0so0

Names	C0d0so0
Category	Malware
Type	Backdoor
Description	(Palo Alto) Two variants of the malware employed by C0d0so0 were discovered—one that used HTTP for command and control (C2) communications, and one that used a custom network protocol over port 22. In these newly discovered C0d0so0 attacks, several of the targeted hosts were identified as server systems, instead of user endpoints, suggesting the possibility that these specific targets will be used in future attacks as additional watering holes. Both of the malware variants encoded and compressed the underlying network traffic to bypass any network-based security controls that were implemented. The malware variants in question do not appear to belong to any known malware family, although the structure of the network communication does bear a resemblance to the Derusbi malware family, which has shown to be unique to Chinese cyber espionage operators. Past observations of Derusbi in various attack campaigns indicate the version used was compiled specifically for that campaign. Derusbi has had both the client and server variants deployed, using different combinations of configurations and modules. The newly discovered activity is consistent with this procedure, with compile times only a few days prior to the observed attacks.
Information	<https://unit42.paloaltonetworks.com/new-attacks-linked-to-c0d0s0-group/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.c0d0so0>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:C0d0so0>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool C0d0so0

Changed	Name	Country	Observed	
APT groups				
	APT 19, Deep Panda, C0d0so0		2013-Mar 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f01aa65c-7a53-43fa-a0f1-873061171574