

access-c3 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:44:42 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool remote-access-c3

Tool: remote-access-c3

Names	remote-access-c3
Category	Malware
Type	Backdoor , Info stealer
Description	(Trend Micro) The remote-access-c3 backdoor seems to be inspired by Patchwork's NDiskMonitor because they share some behaviors, strings, and commands. remote-access-c3 is written in C++ using the Standard Template Library (STL) library. When remote-backdoor-c3 is executed, it waits for a certain time, because of its long initial time delay. It later loads and executes all modules saved in the system registry, establishes persistence via Task Scheduler, and starts a beaconing thread.
Information	< https://documents.trendmicro.com/assets/research-deciphering-confucius-cyberespionage-operations.pdf >

Last change to this tool card: 20 April 2020

Download this tool card in [JSON](#) format

All groups using tool remote-access-c3

Changed	Name	Country	Observed
APT groups			
	Confucius		2013-Aug 2021

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ee3e6bbf-bb27-4e85-a430-a09a76acab17>