Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:32:16 UTC

Tool: NachoCheese

Names	NachoCheese NACHOCHEESE Cyruslish TWOPENCE VIVACIOUSGIFT
Category	Malware
Type	Backdoor, Tunneling
Description	According to FireEye, NACHOCHEESE is a command-line tunneler that accepts delimited C&C IPs or domains via command-line and gives actors shell access to a victim's system.
Information	<https://blog.lexfo.fr/ressources/Lexfo-WhitePaper-The_Lazarus_Constellation.pdf> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239b> <https://baesystemsai.blogspot.com/2017/02/lazarus-false-flag-malware.html> <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/apt/rpt-apt38-2018.pdf> <https://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nachocheese>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool NachoCheese

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

	↳ Subgroup: BeagleBoyz		2014-Feb 2016	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5be3507d-33e7-4c7b-bf47-de35732f280a