Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:51:26 UTC

Tool: Chinoxy

Names	Chinoxy
Category	Malware
Type	Backdoor, Info stealer
Description	(Bitdefender) In the context of the current attack, the Chinoxy backdoor was mainly used to execute ccf32.exe for data collection.
Information	<https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf> <https://medium.com/@Sebdraven/how-to-unpack-chinoxy-backdoor-and-decipher-the-configuration-of-the-backdoor-4ffd98ca2a02> <https://nao-sec.org/2021/01/royal-road-redive.html> <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf> <https://community.riskiq.com/article/56fa1b2f> <https://medium.com/@Sebdraven/new-version-of-chinoxy-backdoor-using-covid19-document-lure-83fa294c0746> <https://documents.trendmicro.com/assets/white_papers/wp-finding-APTX-attributing-attacks-via-MITRE-TTPs.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S1041/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chinoxy>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Chinoxy

Changed	Name	Country	Observed

APT groups

	FunnyDream		2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=29d70c9e-995a-43f8-8ac6-c9c5c446fd6f