Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:02:10 UTC

Tool: TinyZBot

Names	TinyZBot
Category	Malware
Type	Backdoor, Keylogger, Info stealer, Credential stealer, Downloader, Exfiltration
Description	(Cylance) TinyZBot supports a wide array of features that continually evolved over time. The following is a list of supported features: • SMTP exfiltration • Log keystrokes • Monitor clipboard activity • Enable a SOAP-based command and control channel • Self-updating • Download and execute arbitrary code • Capture screenshots • Extract saved passwords for Internet Explorer • Install as a service • Establish persistence by shortcut in startup folder • Provide unique malware campaign identifiers for tracking and control purposes • Deceptive execution methods • Dynamic backdoor configuration • FTP exfiltration • Security software detection • Ability to disable Avira antivirus • Ability to modify PE resources • Dynamic plugin structure
Information	<https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0004/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tinyzbot> <https://malpedia.caad.fkie.fraunhofer.de/details/apk.tinyz>

Last change to this tool card: 22 May 2020

Download this tool card in JSON format

All groups using tool TinyZBot

Changed	Name	Country	Observed	
APT groups				
	Cutting Kitten, TG-2889		2012-Mar 2016	
Other groups				
	Cron		2015-Dec 2017	

2 groups listed (1 APT, 1 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=cf1c4408-2236-4656-bb9f-0773acbb26af