Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:53:32 UTC

Tool: WellMess

Names	WellMess elf.wellmess
Category	Malware
Type	Backdoor, Exfiltration
Description	(NCSC-UK) WellMess is malware written in either Golang or .NET and has been in use since at least 2018. WellMess was first reported on by JPCERT and LAC researchers in July 2018. It is named after one of the function names in the malware -‘wellmess’. WellMess is a lightweight malware designed to execute arbitrary shell commands, upload and download files. The malware supports HTTP, TLS and DNS communications methods.
Information	<https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> <https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html> <https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf> <https://www.botconf.eu/wp-content/uploads/2018/12/2018-Y-Ishikawa-S-Nagano-Lets-go-with-a-Go-RAT-_final.pdf> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b>
MITRE ATT&CK	<https://attack.mitre.org/software/S0514/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmess>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:WellMess>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool WellMess

Changed	Name	Country	Observed

APT groups

	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5619706d-69a0-45a6-9e40-f1c0e9ba2eed