Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:42:52 UTC

Tool: WellMail

Names	WellMail
Category	Malware
Type	Backdoor
Description	(NCSC-UK) WellMail is a lightweight tool designed to run commands or scripts with the results being sent to a hardcoded Command and Control (C2) server. The NCSC has named this malware 'WellMail' due to file paths containing the word 'mail' and the use of server port 25 present in the sample analysed. Similar to WellMess, WellMail uses hard-coded client and certificate authority TLS certificates to communicate with C2 servers. The binary is an ELF utility written in Golang which receives a command or script to be run through the Linux shell. To our knowledge, WellMail has not been previously named in the public domain.
Information	<https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c> <https://www.intezer.com/blog/cloud-security/top-linux-cloud-threats-of-2020/> <https://www.pwc.co.uk/issues/cyber-security-services/insights/wellmail.html> <https://securelist.com/apt-trends-report-q3-2020/99204/> <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> <https://www.intezer.com/wp-content/uploads/2021/02/Intezer-2020-Go-Malware-Round-Up.pdf> <https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors> <https://blog.talosintelligence.com/2020/08/attribution-puzzle.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0515/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.wellmail>

AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:WellMail>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool WellMail

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=011052ce-7891-4761-88ca-b493dcf2f15d