

Flexible Ferret malware distribution campaigns continue to target macOS users

 broadcom.com/support/security-center/protection-bulletin/flexible-ferret-malware-distribution-campaigns-continue-to-target-macos-users

November 28, 2025

A new run of the malicious campaign dubbed "Contagious Interview" has been reported on by the researchers from JAMF. The attackers target macOS users, lure them to fake job websites, and then trick into downloading malware via a bogus software updates. The attackers pose as recruiters and contact victims via LinkedIn, encouraging them to apply for a role. The final payload of this distribution campaign is the latest iteration of Flexible Ferret, a multi-stage Go-based malware. Flexible Ferret establishes persistence via a LaunchAgent to ensure it runs upon every login. Once established on the victim endpoint, it grants attackers full remote control, allowing them to execute shell commands, steal sensitive files, extract Chrome profile data, and harvest detailed system information.

Symantec protects you from this threat, identified by the following:

Adaptive-based

- ACM.lcacIs-Lnch!g1
- ACM.Ps-Wscr!g1

Carbon Black-based

Associated malicious indicators are blocked and detected by existing policies within Carbon Black products. The recommended policy at a minimum is to block all types of malware from executing (Known, Suspect, and PUP) as well as delay execution for cloud scan to get maximum benefit from Carbon Black Cloud reputation service.

File-based

- Downloader
- Phish.Gen
- OSX.Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.1

Web-based

Observed domains/IPs are covered under security categories in all WebPulse enabled products

[Back To Search Results](#)

Copyright © 2005-2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.