Bofamet Stealer malware

Archived: 2026-04-06 00:44:48 UTC

Bofamet is a new Python-based infostealer found in the wild. The malware collects miscellaneous information from the compromised endpoints including: credentials, system information, browser cookies, Telegram session data, Discord tokens, screenshots, Steam configuration files, etc. The collected data is exfiltrated back to the attackers with help of a Telegram bot.

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

Adaptive-based

- ACM.Untrst-RunSys!g1

Behavior-based

- SONAR.Stealer!gen1
- SONAR.TCP!gen6

Carbon Black-based

- Associated malicious indicators are blocked and detected by existing policies within VMware 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 VMware Carbon Black Cloud reputation service.

File-based

- Infostealer
- Trojan.Gen.MBT
- WS.Malware.1

Source: https://www.broadcom.com/support/security-center/protection-bulletin/bofamet-stealer-malware