New Poco RAT distribution campaign

Archived: 2026-04-05 23:50:36 UTC

A new campaign distributing Poco RAT to Spanish-speaking users in Latin America has been reported in the wild. The campaign has been attributed to the Darkling APT (aka Dark Caracal). The group is known to leverage Bandook-based backdoors in their attacks. The Poco RAT malware is spread via phish email messages containing malicious PDF attachments. The attached files redirect the victims to the download of .rev files from often legitimate file-sharing services. The downloaded .rev files lead in turn to execution of malware droppers that infect the targeted endpoints with the Poco RAT payload. The dropped payloads provide the attackers with remote control of the compromised machine, command execution and system information collection, among others.

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

Adaptive-based

- ACM.Untrst-RunSys!g1

Behavior-based

- AGR.Terminate!g5
- SONAR.SuspOpen!gen11
- SONAR.TCP!gen1

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.

Email-based

- Coverage is in place for Symantec's email security products and Email Threat Isolation (ETI) technology provides an extra layer of protection for our customers.

File-based

- Infostealer.Bancos
- Phish.Pdf
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.2

- WS.SecurityRisk.3

Machine Learning-based

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

Web-based

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

---