DeerStealer malware spread via fake Google Authenticator websites

Archived: 2026-04-06 01:36:35 UTC

A new malicious campaign distributing infostealer variant dubbed DeerStealer has been identified in the wild. The malware is spread under the disguise of fake Google Authenticator app and the malicious binary is hosted on the Github repository. The malware is written in the Delphi programming language, collects confidential data from the compromised endpoint and exfiltrates the stolen data in form of PKZIP archives to the C2 servers controlled by the attackers.

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

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 malwares 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

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

Machine Learning-based

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

Web-based

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

---

Source: https://www.broadcom.com/support/security-center/protection-bulletin/deerstealer-malware-spread-via-fake-google-authenticator-websites