SVCStealer malware

Archived: 2026-04-05 21:32:54 UTC

SVCStealer is a new C++based infostealing malware identified in the wild. The infostealer collects various sensitive information from the infected endpoints such as system information, credentials, cryptocurrency wallets, data stored in browsers, screenshots, data from messaging applications (Discord, Tox, Telegram) or VPN apps, and others. The collected information is compressed into a .zip archive and extracted to the C2 servers controlled by the attackers.

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

Adaptive-based

- ACM.Untrst-RLsass!g1

Behavior-based

- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1
- 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.

File-based

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

Machine Learning-based

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

Network-based

- Audit: Bad Reputation Application Activity
- System Infected: Bad Reputation Process Request 4
- Web Attack: Webpulse Bad Reputation Domain Request

Web-based

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

---