Severity

High

Analysis Summary

Panda stealer is a malicious program, a new variant of CollectorStealer, designed to collect and exfiltrate sensitive and personal data from infected computers. It primarily targets cryptocurrency to steal Bytecoin, Dash, Litecoin, and other crypto wallets.

Panda can steal log-in credentials from VPN software (NordVPN), messaging platforms, and digital distribution services for video games. It can also take screenshots of the infected machine and steal information from browsers such as cookies, passwords, and credit cards. It places files in the %Temp% folder, which keeps stolen data under randomized file names before sending it to a command-and-control (C&C) server. Spam campaigns have been used to propagate Panda stealer. It is also known to propagate through malicious Microsoft Office Excel files.

Impact

- Credential Theft
- Unauthorized Access

Indicators of Compromise

MD5

- 98b87b6c0b7917c16a79ad38efa12f75
- 21703b52fb6ba89fd261ce76dab5ef32
- 840d99c89f366505d06259a89273f8b1
- 7414bb0aea775bacdfd25ad94ec8e567
- 6f504e4d2887038775a8636d246f38a1
- 83a82cacf8a42eb833b95c0985095457

SHA-256

- 934a224d90cc0e59ae26855b5318e684d918b6dc4ecee920bdac061e62267e36
- 6413be289cf38c2462bd8c6b8bad47f8d953f399e1ccba30126a1fb70d13a733
- 4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e
- 0a9f466fb5526fd512dd48c3ba9551dbd342bdb314a87d5c6f730d3c80041da6
- 05d38ac5460418b0aa813fc8c582ee5be42be192de10d188332901157c54287c
- 1efa74e72060865ff07bda90c4f5d0c470dd20198de7144960c88cef248c4457

SHA-1

- dc4f6db58f7cdb53324cba1250340b86866b50b9
- 68cf06862be9183607e21d3170b644aab64e5887
- 68b4e58f7af755fa82d36cfa8198b099104e8665
- 22fde5fe9e7dc275922834c2383e80b85c722489
- 0546178c38a3abb7837156bd6ff5fe890fa07e41
- d07493ef698766e82d5f5dff6b95c2dcd3537fb0

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.