Severity

High

Analysis Summary

An emergent and effective data-harvesting tool dubbed Oski is proliferating in North America and China, stealing online account credentials, credit card numbers, crypto wallet accounts, and more. The malware is still in its developing phase but packs a punch with its capabilities. Oski C2's dashboard revealed that Oski's theft tactics involve extracting credentials using man-in-the-browser (MitB) attacks by hooking the browser processes using DLL injection, It also extracts credentials from the registry, passwords from the browser SQLite database, and stored session cookies of all stripes, including crypto-wallet cookies from Bitcoin Core, Ethereum, Monero, Litecoin, and others.

Impact

- Credential Theft
- Unauthorized Access

Indicators of Compromise

MD5

- 77819223ac9fc0d6577e56e7820b1df8

SHA-256

- 9ff70a733043441bef2128c621869e8139785059325ff105dafd91825069bc64

SHA-1

- c56c33b4d45ccaff25e9875e10632656ca794f17

Remediation

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