Case Study: XRP-Node.com Crypto Phishing Campaign

Executive Summary

An independent investigation was conducted into a cryptocurrency phishing campaign promoted via YouTube advertisements. The domain xrp-node.com falsely claimed users could earn passive XRP income by connecting their wallet or running a “node.” Analysis determined the operation leveraged social engineering to induce victims into approving malicious transactions, resulting in automated wallet draining.

MITRE ATT&CK; Mapping

- TA0001 – Initial Access: Phishing (T1566)
- TA0001 – Initial Access: Drive-by Compromise (T1189)
- TA0006 – Credential Access: Input Capture / Credential Harvesting (T1056)
- TA0002 – Execution: User Execution (T1204)
- TA0040 – Impact: Data Manipulation / Financial Theft

Indicators of Compromise (IOCs)

- Domain: xrp-node.com
- YouTube ads promoting passive XRP node income
- Wallet connection prompts
- Copy-and-execute code instructions

Response Actions

- Conducted domain and behavioral analysis
- Documented phishing indicators
- Assessed financial risk and impact
- Reported malicious content
- Published public awareness documentation