February 4, 2025

Coyote Malware Expands Reach: Now Targets 1,030 Sites and 73 Financial Institutions

Overview: The Coyote Banking Trojan is an advanced malware targeting Brazilian Windows users, now affecting 1,030 websites and 73 financial institutions. Initially documented by Kaspersky in early 2024, Coyote has evolved, using Windows Shortcut (LNK) files and PowerShell commands to deliver its payload. Once deployed, it enables keylogging, phishing overlays, and screenshot capture to steal sensitive credentials. It also establishes persistence through registry modifications and evades detection using sandbox bypass techniques. The malware's expansion increases the financial cybersecurity risk, emphasizing the need for enhanced defenses.

CTI Analysis: Coyote's infection chain starts with an LNK file executing a PowerShell script, retrieving a Base64-encoded payload from tbet.geontrigame[.]com. The malware then establishes persistence by modifying the Windows Registry and executes its MSIL-based final payload using the Donut framework. Key tactics observed include LNK file execution (T1204.002), PowerShell scripting (T1059.001), registry modification (T1547.001), keylogging (T1056.001), and data exfiltration via C2 servers (T1071). The malware also gathers system information and installed antivirus details while performing sandbox detection.

Impact Analysis: Coyote poses a significant financial and operational risk, enabling credential theft, unauthorized transactions, and account takeovers. Its ability to collect sensitive system and user data increases exposure to fraud and cybercrime. Financial institutions and businesses risk reputational damage, regulatory penalties, and operational disruption due to fraudulent activities linked to the malware. Its evasive techniques and persistent infection

methods make detection and removal difficult, further increasing the risk of long-term exposure.

Mitigation

- **Endpoint Security**: Disable PowerShell for non-admin users, monitor LNK file execution, use behavior-based detection.
- **Network Defense**: Block known malicious domains, use DNS filtering, implement network segmentation.
- **User Awareness**: Educate users about LNK file risks, encourage reporting of suspicious activity.
- **System Hardening**: Restrict registry modifications, disable LNK execution from untrusted sources, enforce application whitelisting.

Conclusion

The Coyote Banking Trojan is a growing financial cybersecurity threat, leveraging multi-stage infection techniques and evasive tactics to steal banking credentials. Its expansion to 1,030 websites and 73 financial institutions highlights its increasing sophistication. To prevent financial and reputational damage, organizations must implement proactive cybersecurity defenses, enhance user awareness, and continuously monitor for emerging threats linked to this malware.

Source:

- https://thehackernews.com/2025/02/coyote-malware-expands-reach-now.html