مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Lucid PhaaS Campaign Targeting Global Entities via iMessage and RCS Smishing

Tracking #:432317030

Date:03-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a sophisticated phishing-as-a-service (PhaaS) platform named Lucid has been deployed to target 169 organizations across 88 countries.

TECHNICAL DETAILS:

A sophisticated phishing-as-a-service (PhaaS) platform named Lucid has been deployed by the XinXin group (aka Black Technology) to target 169 organizations across 88 countries. The campaign leverages Apple iMessage and Android's Rich Communication Services (RCS) to bypass traditional SMS spam filters, enabling threat actors to conduct large-scale smishing attacks aimed at stealing credit card details and personally identifiable information (PII).

Campaign Overview

- Targeted UAE Companies: UAE Pass, ICP, Noon, DU, Aramex, Emirates NBD,RAK Bank, HSBC
- Delivery: Smishing messages sent via iMessage (using temporary Apple IDs) and RCS (rotating sender domains/numbers to evade detection).
- Payload: Links to customizable phishing pages mimicking legitimate services, equipped with:
  - IP/user-agent filtering to block security researchers.
  - Time-limited URLs to hinder post-attack analysis.

Details of the Threat

1. Attack Mechanism

Lucid enables cybercriminals to distribute phishing links via:

- Apple iMessage (using temporary Apple IDs with impersonated display names)
- Google RCS (exploiting inconsistencies in carrier sender verification)

These methods allow threat actors to evade traditional SMS spam filters and increase their attack success rates.

2. Phishing Tactics

- Targeted Smishing Attacks: Victims receive phishing messages impersonating postal services, courier companies, tax refund agencies, and toll payment systems.
- Two-Way Communication Evasion: iMessage filtering restrictions are bypassed by using a "please reply with Y" technique to engage victims.
- Domain & Number Rotation: Attackers frequently change domains and sender numbers to avoid detection in Google RCS filtering systems.
- Advanced Anti-Detection Techniques: Phishing pages employ:
  - IP and user-agent filtering to evade security scans.
  - Single-use, time-limited URLs to prevent reuse.

3. Infrastructure & Automation

- Device Farms & Emulators: Large-scale phishing operations are conducted using iPhone device farms and Windows-based mobile device emulators to send hundreds of thousands of phishing messages.
- Data Collection & Real-Time Monitoring: Phishing panels allow cybercriminals to monitor victim activity in real-time, capturing credit card details and PII.

4. Overlapping PhaaS Platforms

Lucid is linked to Lighthouse and Darcula, two other PhaaS services developed by the XinXin group.

- Darcula can clone any brand's website for phishing.
- All three platforms share templates, target pools, and operational tactics, pointing to an organized cybercrime economy.

5. Industry-Wide Impact

- A 10,000-domain phishing campaign using "com-" domain names has been linked to similar phishing operations.
- Other PhaaS services like Tycoon 2FA, EvilProxy, and Sneaky 2FA have driven a spike in phishing attacks in early 2025.

RECOMMENDATIONS:

1. Enforce Multi-Layered Filtering for iMessage/RCS:
   - Deploy advanced threat detection tools capable of analyzing encrypted messaging content (e.g., behavioral AI for anomalous link patterns).
   - Block messages from unverified Apple IDs or sender domains with inconsistent naming conventions.
2. Disable iMessage and RCS if Not Used:
   - iMessage: Disable via Settings > Messages on iOS devices if not required for business operations.
   - RCS: Turn off in Android's Google Messages app (Settings > Chat features).
3. Educate Users on Smishing Tactics:
   - Test employee awareness of impersonation tactics & Emphasize scrutiny of shortened URLs in messages claiming to be from legitimate services.
4. Implement URL and Domain Monitoring:
   - Use threat intelligence feeds to block known malicious domains
   - Deploy DNS filtering to restrict access to newly registered or high-risk domains.
5. Strengthen Authentication for Financial Services:
   - Enforce multi-factor authentication (MFA) for online banking portals and educate customers to avoid sharing OTPs via smishing links.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://catalyst.prodaft.com/public/report/lucid/overview