Chinese Scammers Launder Money via Fraud Payment Gateways: A New Threat to India's Digital Payment Ecosystem

Intelligence Type: Adversary Intelligence
Threat actor Motivation: Financial
Industry: Banking & Finance
Region: Global

White papers and reports can be downloaded from CloudSEK website by visiting https://cloudsek.com/whitepapers-reports or by mailing to info@cloudsek.com.
INTRODUCTION

In today's interconnected world, where technology and finance intersect, CloudSEK's dedicated research team delves deep into the layers of complexity to uncover a story of financial manipulation. In this comprehensive report, we explore a money laundering scheme that exploits India's Unified Payments Interface (UPI), revealing a web of deceit with real consequences for unsuspecting victims.

EXECUTIVE SUMMARY

On September 8, 2023, a group of cybercriminals set their sights on India's financial ecosystem, and started advertising a malicious app impersonating a Bank headquartered in Tamil Nadu with a revenue of $23 million USD (Source: Zoominfo), this bank became the unwitting pawn in a meticulously orchestrated attack. The impersonated domain name of the identified C2 server had pattern of [BANKNAME].online.

KEY OBSERVATIONS

As we delve deeper into this investigation, several key revelations emerge:

1. **Accumulating Illicit Gains**: Between July and September 2023, our research uncovered an accumulation of over INR 37 lakhs. This money flowed into the coffers of cybercriminals who used more than 55 malicious Android apps to deceive their victims.

2. **The Hidden Payment Gateways**: Our analysis revealed over 15 obscure payment gateways operated by Chinese individuals. These adaptations are a response to increased legal scrutiny as cybercriminals seek to evade detection.

3. **The Escalation of Tactics**: In their quest to outsmart law enforcement, these cyber scammers are employing more sophisticated methods. The need for vigilance on the part of organizations and regulators has never been more critical.

CloudSEK is committed to building a safer internet for individuals and organizations. Towards this, we publish white papers, threat intelligence reports and blogs uncovered by our Security Research team. You can check them out on [https://cloudsek.com/threatintelligence/](https://cloudsek.com/threatintelligence/)
THE MODUS OPERANDI
The scammers' playbook is deceptively simple:

1. **Creating False Promises:** The first step involves the creation of counterfeit instant loan apps that promise substantial loans with flexible repayment terms.

2. **Data Gathering:** Victims are tricked into sharing personal information, including their name, address, phone number, and bank account details, all under the pretense of securing a loan.

3. **Permissions Granted:** To further their scheme, the malicious app coerces users into granting access to their contacts and other sensitive data stored on their mobile devices.

4. **The Elusive Loan:** Once the victim has provided all requested information and paid the processing fee (typically 5% of the promised loan amount), the scammers disappear, and the promised loan remains elusive.
KEY STATISTICS

From Fraud Campaign *(Between 22nd July 2023 and 18th September 2023)*

- **Compromised Individuals**: [Graph showing a range from 0 to 40,000]
- **Compromised Aadhaar Cards**: [Graph showing a range from 0 to 40,000]
- **Compromised Devices**: [Graph showing a range from 0 to 40,000]
- **Accounts Breached**: [Graph showing a range from 0 to 40,000]

GLOBALLY SPREAD SCAM

The fraud payment gateways operate in multiple countries including Indonesia, Malaysia, South Africa, Mexico, Brazil, Turkey, Vietnam, the Philippines, Colombia etc.

- **Total Loan Value Promoted by Scammers**: INR 641 Crores
- **Total Money Lost by Victims**: INR 37 Lakhs
- **Total Malicious Apps Advertised**: 55 Apps advertised
- **Total Payment Gateways Weaponised**: 22 weaponised

Disclaimer: This threat intelligence report contains confidential and proprietary information solely intended for the designated recipient(s), and any unauthorized disclosure, distribution, or use of this report is strictly prohibited.
Chinese Payment Gateways: The Enabler:

Central to this operation are Chinese payment gateways, exploiting the QR code feature of UPI with precision:

1. **A Global Network:** These scammers operate across multiple countries, including Indonesia, Malaysia, South Africa, Mexico, Brazil, Turkey, Vietnam, the Philippines, and Colombia.

2. **Exploiting UPI Vulnerabilities:** UPI service providers currently operate without coverage under the Prevention of Money Laundering Act (PMLA). Scammers manipulate mobile numbers associated with victim accounts to initiate illegal transactions.
Sourcing Money Mules: Telegram's Role:
The rise of Telegram channels plays a pivotal role in recruiting money mules:

1. **The Money Mule Network**: These individuals agree to receive ill-gotten gains from scammers and transfer them to other accounts, often in exchange for a modest commission.

2. **Targeting Indian Banks**: Scammers are actively targeting customers of Indian banks, drawn by the large customer base and ease of opening accounts.

3. **Luring with Incentives**: Money mules are enticed with commissions ranging from 1% to 2% of the total transaction amount. For those handling a high volume of transactions, this seemingly small commission can quickly add up.

4. **Face-to-Face Temptations**: Scammers go to great lengths, offering face-to-face meetings and sponsoring travel for those willing to participate.
Cashing out the Stolen Money:

An in-depth analysis of these fraudulent payment gateways reveals a significant daily influx of illicit funds:

1. **Flexible Withdrawal Routes**: Money is funneled through online avenues, such as UPI, or offline methods, including debit cards. The funds are then distributed to various recipients, including hawala networks, scammers, or other actors within India.

2. **Operating on Indian Soil**: These fraudsters maintain a presence within India, primarily to facilitate the collection of SIM cards and bank accounts, essential components in the money-laundering process.
## STATISTICS FROM UNDERGROUND

*(Between 22nd July 2023 and 18th September 2023)*

### Money Mules Recruitment
- **Channels**: 20+

### No. of Money Mules (Estimate)
- **Mules**: 10,000+

<table>
<thead>
<tr>
<th>Bank Name</th>
<th>Account Type</th>
<th>Commission</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFC</td>
<td>Individual Account</td>
<td>1.30%</td>
</tr>
<tr>
<td>IDFC</td>
<td>Individual Account</td>
<td>1.30%</td>
</tr>
<tr>
<td>SBI</td>
<td>Corporate Account</td>
<td>1.70%</td>
</tr>
<tr>
<td>Equitas</td>
<td>Corporate Account</td>
<td>1.70%</td>
</tr>
<tr>
<td>ICICI (easypay UPI)</td>
<td>Corporate Account</td>
<td>1.70%</td>
</tr>
<tr>
<td>IDFC (CMS)</td>
<td>Corporate Account</td>
<td>2.00%</td>
</tr>
<tr>
<td>YES</td>
<td>Corporate Account</td>
<td>1.50%</td>
</tr>
<tr>
<td>IDFC</td>
<td>Corporate Account</td>
<td>1.50%</td>
</tr>
<tr>
<td>Kotak(CMS)</td>
<td>Corporate Account</td>
<td>1.50%</td>
</tr>
<tr>
<td>ICICI (Vanghee; Zoho)</td>
<td>Corporate Account</td>
<td>1.50%</td>
</tr>
<tr>
<td>IndusInd (in development)</td>
<td>Corporate Account</td>
<td>1.50%</td>
</tr>
<tr>
<td>PNB</td>
<td>Corporate Account</td>
<td>1%</td>
</tr>
<tr>
<td>ICICI</td>
<td>Corporate Account</td>
<td>1%</td>
</tr>
<tr>
<td>IDFC</td>
<td>Individual Account</td>
<td>1.80%</td>
</tr>
<tr>
<td>RBL</td>
<td>Corporate Account</td>
<td>1.80%</td>
</tr>
<tr>
<td>Canara</td>
<td>Corporate Account</td>
<td>1.80%</td>
</tr>
<tr>
<td>YES</td>
<td>Corporate Account</td>
<td>1.80%</td>
</tr>
<tr>
<td>ICICI</td>
<td>Corporate Account</td>
<td>1.80%</td>
</tr>
<tr>
<td>PNB</td>
<td>Corporate Account</td>
<td>2.30%</td>
</tr>
<tr>
<td>JANA</td>
<td>Corporate Account</td>
<td>2.30%</td>
</tr>
<tr>
<td>Indusind</td>
<td>Corporate Account</td>
<td>2.30%</td>
</tr>
<tr>
<td>YES</td>
<td>Corporate Account</td>
<td>2.60%</td>
</tr>
<tr>
<td>ICICI</td>
<td>Corporate Account</td>
<td>2.60%</td>
</tr>
</tbody>
</table>
LESSONS LEARNED AND MITIGATIONS

Learnings:

1. **Adaptive Scammers**: Cybercriminals are evolving, employing increasingly sophisticated tactics, challenging law enforcement efforts.
2. **Chinese Payment Gateways**: These entities play a central role in facilitating these fraudulent schemes, creating a global web of deception.
3. **UPI Service Vulnerabilities**: The absence of PMLA coverage for UPI service providers has enabled scammers to exploit these platforms with relative ease.

Mitigations:

1. **Enhancing Security Measures**: Banks and the National Payments Corporation of India (NPCI) must collaborate to implement additional security measures. One key initiative could involve verifying that any new mobile number added to an account matches the account holder's name, thwarting scammers from gaining control by altering phone numbers.
2. **Continuous Vigilance**: Organizations and regulatory bodies must remain vigilant, staying abreast of the ever-evolving tactics employed by cybercriminals. Implementing robust fraud detection and prevention measures is essential.
3. **Strengthening UPI Security**: UPI service providers should consider implementing additional security measures to safeguard their users from falling victim to fraud.
4. **Law Enforcement**: Legal authorities should maintain their vigilance and prosecution efforts, ensuring that these scams are met with the full force of the law.

Additional Mitigation Measures:

1. **Customer Education**: Banks and payment processors should take proactive steps to educate their customers about the risks associated with fraudulent payment gateways and hawala transactions.
2. **Exercising Caution**: Individuals should exercise extreme caution when sharing their bank account information with anyone, even if a commission is offered.
3. **Social Media Vigilance**: Individuals should be cautious of Telegram channels and other social media groups offering rewards in exchange for bank account information.
4. **Protecting Mobile Numbers**: Changing the mobile number associated with a bank account for someone else should be strictly avoided, given its potential for misuse.
To learn more about how the CloudSEK Initial Attack Vector Protection Platform can strengthen your external security posture and deliver value from Day 1, visit https://cloudsek.com/ or drop a note to info@cloudsek.com.