10.0

New and Repackaged Fraud Types

Securing mobile infrastructure, devices, services and customers is an evolving activity, as threat actors constantly re-invent previous attack techniques, as well as inventing new attack types. Repackaged and re-imagined attacks seek to build on previous attacks but are disguised in new ways. This section explores a few of these repackaged attack types, which can be categorised as fraud, as they either fraudulently use mobile services or defraud mobile customers directly. Extensive measures are employed to limit the customer impact of fraud and avoid a negative impact on mobile operators' reputations.

Artificial Inflation of Traffic[81] is a type of SMS fraud seeking to generate high volumes of fake traffic via mobile applications or websites and then profit from higher revenue from the artificially-generated SMS traffic. For example, the fraudster exploits application-to-person (A2P) SMS verification, where a one-time password is sent to verify users' phone numbers during the registration process, then takes a share of the profits from the traffic, while the enterprise incurs inflated A2P SMS costs without added value.

An SMS text blast sends a message to a large group of people simultaneously. However, relatively low-cost, portable and easy-to-use fake mobile base transceiver stations (SMS blasters) can be used for fraudulent use[82]. These have been more traditionally used as IMSI-catchers[83] to spam mobile phones located within the transceiver's radio coverage area with fraudulent SMS messages. The relatively low level of technical skill involved in the use of these SMS Blaster devices has resulted in increased deployment of this attack type.

A 'flash SMS' is a special type of text message that displays immediately on the mobile phone screen without the user having to take any action to read it, even if the screen is locked. A Flash SMS also does not leave a record on the customer's phone i.e., it is not visible in the SMS inbox. Whilst there are legitimate uses for flash[84] SMS messages, they can also be used as part of a fraud attack as a 'convincer' aimed at fooling the mobile user into undertaking an action to further an ongoing scam.

Quishing, a combination of quick response (QR) code and phishing, is an attack technique that leverages QR codes to mislead users into interacting with malicious digital content. When a user scans a malicious QR code, it typically redirects them to an attack website[85], which may deploy malware or solicit log-in or personal information. When contained within an email, Quishing can be effective, as QR codes may not be scanned by traditional email security controls.

The GSMA has previously reported[86] on flubot attacks, often observed as blended attacks

[81] https://mobileecosystemforum.com/2023/01/12/artificially-inflated-traffic-the-latest-menace-in-sms/
[82] https://commsrisk.com/criminal-gangs-drive-imsi-catcher-sms-blasters-around-vietnam/
[83] https://commsrisk.com/oslo-imsi-catcher-arrest-suspected-malaysian-spy-now-investigated-for-fraud-with-international-ramifications/
[84] https://thesmsworks.co.uk/blog/flash-sms/
[85] https://www.linkedin.com/pulse/quishing-how-qr-code-phishing-form-social-engineering-ebenezer
[86] GSMA | T-ISAC Insight Report: Flubot - Security

combining smishing and voicemail lures, with banking malware injects. The 'lures' have been frequently framed in a message relating to a fake parcel or package delivery. Although some of the original flubot infrastructure has been taken down, the attack approach appears to have been re-invented on new infrastructure using new fraudulent messages. For example[87], these messages might impersonate family members asking for money or be framed as a Ramadan Competition[88] on WhatsApp.

The Qakbot banking trojan malware was primarily spread through phishing emails and malicious attachments. It was reported[89] that Qakbot has now started using OneNote .one documents in attacks.

Vendor email compromise (VEC) is a type of phishing attack where an attacker gains access to a vendor's business service account, and then, uses that account to spread malicious emails to the vendor's customers[90]. VEC can target entire supply chains by:

- Hijacking email accounts belonging to vendor employees.
- Setting forwarding rules or monitoring the inbox.
- Creating a spoofed domain to resemble the vendor's.
- Sending well timed messages to customers of the vendor, requesting changes to payment details.
- Using Office 365 tools to enhance the look and feel.

Reportedly[91], attackers have used VEC to spread phishing sites and to appear as legitimate as possible. Malicious emails were sent to multiple recipients, who appear to be customers or prospects of the company, and thus they are more likely to trust compromised emails from the vendor.

Analysis

The re-invention and repackaging of previously observed attack types means constant vigilance is required to respond to these new indicators of compromise (IoCs). The GSMA's Telecommunications Information Sharing and Analysis Center (T-ISAC)[92] community delivers a safe and secure platform on which to share new IoCs in real-time. In this way, a defensive force-multiplier can be delivered by sharing new knowledge that can benefit the wider range of stakeholders.

The GSMA's Fraud and Security Group has an intelligence sub-group that reviews and shares a range of reported security and fraud attack types. This regular sharing of attack techniques allows new modus operandi to be identified and evaluations made on the effectiveness of deployed security and fraud controls.

These agile operational security responses can involve tailoring and adapting existing control mechanisms, re-configuring existing security solutions or building the business case to install new capabilities.

[87] https://www.which.co.uk/news/article/notorious-hi-mum-and-dad-scam-spreads-from-whatsapp-to-text-message-an7N34c0gVbP
[88] https://theclearevidence.org/technical-resources/beware-of-ramadan-competition-fraud-messages-on-whatsapp-english/
[89] https://news.sophos.com/en-us/2023/02/06/qakbot-onenote-attacks/
[90] Closely related to Business Email Compromise (BEC). In a BEC attack, the scammer poses as a trusted figure and uses email to trick someone into sending money or divulging confidential company info. A VEC attack, the attacker gains access to a vendor's email account and uses it to send fraudulent emails to the organization.
[91] https://www.paloaltonetworks.com/blog/security-operations/behind-the-curtains-of-a-vendor-email-compromise-vec-attack/
[92] GSMA | - Security