Coinbase Feb 2023 Social Engineering Attack

Incident Name	Coinbase Social Engineering Attack
Date of Incident	February 5th, 2023
Summary	Coinbase is an American cryptocurrency exchange platform. On February 5th, 2023, the company came under a social engineering attack in which several employees were targeted with SMS messages urging them to log in to their accounts to read a message. One employee fell for this campaign and entered their credentials into a phishing site which the attacker then harvested. The attacker attempted to log in with these credentials but needed an MFA token. The attacker then called the employee and, impersonating an IT team member, asked the employee to log in on their workstation and follow further instructions. Coinbase's security team noticed this strange activity and asked the employee what was happening which led the employee to notice that they were speaking with an attacker and not another member of staff, so they terminated communications. Coinbase has stated that some employee details (names, email addresses, and numbers) were breached but no customer details or funds were taken. On February 17th, Coinbase officially announced that it had come under attack earlier in the month and released a comprehensive report on the Tactics, Techniques, and Procedures (TTPs) used by the attacker. Coinbase believes that the threat actor responsible is 0ktapus, who targeted many other organizations last year such as Twilio.
Key Social Engineering /OSINT Themes	• Recon - Coinbase employee and organizational information harvested. The hacker leveraged exposed employee information (phone numbers) to conduct a social engineering attack. • Smishing - The attacker sent a convincing SMS message to certain employees which prompted one of them to click on a link. Once the user clicked on this link, they were presented with a legitimate-looking phishing site that prompted them for credentials. The attacker then used these credentials attempting to gain unauthorized access. • Vishing - The attacker was able to harvest the employee's credentials but could not get past the MFA stage of authentication, so they called the employee claiming to be from IT to get them to log in and perform actions on their behalf.
Remediations	• Identify and block newly registered domains similar to your org's. This way if used in an attack (e.g., user clicking), the request to domain is blocked. • Monitor for expiring domains which could be leveraged for the above. • Monitor for suspicious activity and web traffic (TTPs identified in Coinbase's report). • Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts. • Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party. • Regularly audit employee access to one of least privilege (including offboarding). • Regularly audit 3rd party access to one of least privilege. • Monitor and remove sensitive information disclosure, including exposed employee phone numbers.
Industry	Crypto

Actor	0ktapus
Motivations	Financial
Related Hacks	Twilio
Breach Notice/Company Notice	https://www.coinbase.com/blog/social-engineering-a-coinbase-case-study
Other Sources	https://www.bleepingcomputer.com/news/security/coinbase-cyberattack-targeted-employees-with-fake-sms-alert/ https://securityaffairs.com/142507/cyber-crime/coinbase-smishing-attack.html https://www.group-ib.com/media-center/press-releases/0ktapus-campaign/