Digital Fraud Wiki

Device Emulators

What is a Device Emulator?

A device emulator is software that creates a virtual simulation of a computer environment, hardware, operating system, or CPU. Fraudsters use device emulators to create many synthetic devices (usually smartphones) that run on and are controlled from a single computer en masse.

What Should Companies Know about Device Emulators?

Device emulators are one of a myriad of cheap, powerful tools that fraudsters are increasingly using to camouflage and diversify their attacks. Device emulators are especially powerful tools for fraudsters because emulators are virtual. This allows the creation, management, and deletion of synthetic devices to be completely automated using bots. In addition, fraudsters often combine device emulators with virtual private networks (VPNs) and GPS spoofing apps to change the IP address and the inferred location of each synthetic device to further obfuscate malicious activities.

Emulators allow fraudsters to circumvent device ID scoring services and rules-based fraud prevention systems. Device ID scoring services determine the fraud probability of a device mainly through device fingerprinting. When the device ID of a synthetic device is flagged as risky by a device ID scoring service or a rules-based fraud

Loan Stacking

Synthetic Identity Theft

detection platform, the fraudster can quickly create a new synthetic device with a new ID. Or the fraudster can program a bot to create a new synthetic device automatically.

Fraudsters commit many types of fraud using device emulators, stealing billions from organizations. For example, fraudsters use device emulators to commit mobile app install fraud. App install fraud entails a scammer receiving credit when a user installs an app. With a device emulator, a fraudster can make it appear that each new app install is from a new mobile phone. Device emulators also enable fraudsters to simulate realistic-looking engagement within each installed app. Recent estimates suggest that marketers lost nearly $2B in 2017 due to app install fraud.

Biometrics holds some promise as a more effective means of detecting emulators than traditional device fingerprinting techniques. Biometrics is a new technique that leverages phone sensors or code on websites to collect hundreds, sometimes thousands, of data points for each user. These data points are used to capture how users use their devices, and that behavioral definition is then used to identify and authenticate each user.

While biometrics is an improvement over traditional device fingerprinting techniques, biometrics is not foolproof. Today, tools are available that enable fraudsters to “record” real user activity—from keystrokes and mouse movements to motion data—and simulate this activity in emulation. Also, stolen device IDs can be found on dark web marketplaces. With a stolen device ID and activity information previously recorded from the real device, fraudsters can simulate the same identifying information and characteristics as the original device. Another drawback to biometrics is that the technology is prone to false positives. For example, if a user loses their voice due to a cold, a voice biometrics solution would flag that user as risky (a false positive). Or, a smartphone app that leverages biometrics for identification could mistakenly return a false positive if the user is wearing gloves while using the app.

A Holistic and Contextual Approach to Fraud Prevention

While biometrics and traditional device fingerprinting can be helpful when it comes to identifying users and the potential risk of each user at login, these security measures are not enough because they only look at accounts in isolation. Contextual detection is increasingly the only effective way to detect fraudsters using sophisticated tools such as device emulators, GPS spoofing apps, and VPNs. Organizations must analyze users and transactions holistically and assess data with the benefit of context to truly understand what is and isn’t fraudulent. DataVisor products such as dCube and dVector

leverage proprietary unsupervised machine learning algorithms to reveal suggestive patterns and surface connections between seemingly separate incidents, accounts, and actions. Using advanced tools like these, organizations can successfully expose fraudsters who engage in advanced camouflaging techniques such as device emulation.

Additional References

Blog Post: Dealing with the Complexity of Fraud Attacks in Mobile Application Fraud

Blog Post: Are Mobile Devices the Leading Target for Fraudsters?

Source: Is App-Install Fraud on the Rise?, eMarketer

Source: Banks and Retailers Are Tracking How You Type, Swipe and Tap, The New York Times