Waterstons
we're with you

+44 345 094 0945
www.waterstons.com

News article

Mar 2024

iOS Banking Trojan: Cyber Incident Review

iOS banking trojan can defeat biometric authentication. Security researchers have released a report on an ongoing campaign using what is believed to be the first mobile banking trojan targeting users' face ID scans, allowing them to bypass biometric authentication.





What Happened

The trojan malware, named 'GoldPickaxe', has been identified as targeting both Android and iOS users in Southeast Asia, primarily Thailand and Vietnam. The malware is disguised as a government service app, requiring users to upload a photo of their ID and create a face scan as part of the registration process. The threat actors can then use the face scan to create an AI-generated deepfake of the victim's face, before using it to login remotely to services protected by biometric authentication - such as banking apps. Notably this malware was first identified only three months after the Bank of Thailand announced a new policy that required facial recognition for all significant actions – such as opening an account, transferring large amounts of money, or changing account limits.

Infecting iOS Devices

While Android malware is not uncommon, since users can be tricked into downloading apps from outside the major app stores, it is uncommon for malware strains to be cross platform. This is primarily due to the difficulty in getting malicious apps onto Apple devices, which only allow installations from the official app store.

- In this recent 'GoldPickaxe' campaign, threat actors used two methods to install malware on user devices:
- Using Apple's application developer testing platform TestFlight, which allows developers to invite users to install beta version of apps that - crucially - have not yet gone through the app store review process.
- A sophisticated social engineering attack to convince users to install a Mobile Device Management (MDM) profile on their iOS device, effectively providing threat actors with full control of the device. The MDM profile allows the installation of malicious apps without any input from the user, replacing the legitimate version on the device.
- While this malware only has a limited scope in Southeast Asia, the success it has had will likely lead to an expansion of these techniques, and increased adoption from other threat actors into existing campaigns.

Wider Implications

This incident reflects a wider trend of targeting mobile devices, with the 2023 Verizon Mobile Security Index finding that mobile app threats increased by more than 30% between 2022 and 2023. This is primarily due to the widespread use of Bring Your Own Device (BYOD) policies for mobile phones accessing corporate information. Not only are users twice as likely to click a phishing link on a personal device than a company-issued one according to the Verizon report, but these devices often lack enterprise security controls that MDM enables, such as app download restrictions and mobile Endpoint Security and Response (EDR) solutions.

This incident also highlights the risks that AI advancements can pose to biometric authentication, and the importance of a defence in depth approach to security. While new advancements may allow threat actors to defeat individual security controls by implementing multiple levels of conditional access controls, and adopting a zero-trust approach to security, organisations can reduce the risk of a threat actor compromising an account and, if the account is compromised, reduce the impact of the breach.

Organisations Should

- Review their BYOD policies to determine if they pose a security risk. BYOD should be avoided wherever possible and, where there is a real business justification, compensating controls such as network mobile device management (MDM) software should be implemented and used to deny access to insecure devices.
- Ensure all devices are managed by the organisation via a Mobile Device Management (MDM) tool, to restrict the installation of software and ensure applications are regularly patched to the latest version, reducing the risk that malware can be delivered directly via the installation of a malicious app. Restricting the installation of mobile apps should be supported by the creation of an approved list of apps that employees can install on company devices.
- Consider implementing mobile endpoint security software on mobile devices, providing advanced threat protection against malicious apps. Note, Microsoft's E5 license includes Microsoft Defender for Endpoint, which allows EDR capabilities to be installed on mobile phones and tablets.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430