DIGITAL MOUNTAIN®

WINTER 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss third-party keyboards on smartphones for emoji usage, keylogging and protecting your digital keystrokes. We also discuss the California Consumer Privacy Act of 2018 and its impact on our industry.

Keeping Your Digital Keystrokes Safe

In our associated article on keystroke logging, we begin with the story of what is arguably the first keylogging incident – the Soviet bugging of electric typewriters at US embassies during the early 1980s. One of the more interesting questions about the bugging incident is, how did the Soviets access the typewriters to install the bugs? If you watch spy movies, you're probably envisioning a double agent, or a mysterious Soviet cleaner, sneaking around the embassy late at night with a tool kit hidden in her uniform. In this case, the truth is rather mundane. According to The Crypto Museum, the most likely scenario is that the typewriters were bugged during a customs' inspection, before delivery to the US embassy (*https://www.cryptomuseum.com/covert/bugs/selectric/index.htm*). The Soviets simply took advantage of an opportunity when the Americans gave up control of the typewriters and put the security of the units in the Soviets' hands. As obvious an error as it is to turn over control of a device on which sensitive data is created and stored, we seem to have forgotten that lesson when it comes to our mobile devices. In fact, if we examine some of the latest plug-ins, we may be handing over control without ever letting our mobile devices out of our hands.

Subtracting Security by Adding Keyboards

Third-party app developers have designed add-ons, or plug-ins, that increase functionality of mobile devices and other apps that often include installing additional or replacement keyboards. Apps of all varieties have keyboard components, for example, Tenor, a GIF keyboard for inserting short clips and animations into other applications; Grammarly Keyboard, an app that checks your grammar as you type; and Gboard, Google's mobile device keyboard, all have the capacity to capture data input via the keyboard. Bitmoji, another app that includes a third-party keyboard, allows users to create their own personal avatars and incorporate those avatars into other applications. To date, more than one hundred million Bitmoji avatars are in use, and Apple included Bitmoji in the top ten of its most downloaded apps of 2018. Grammarly Keyboard has over fifteen million users, and Gboard installs eclipse one billion. By now, you're asking yourself, where's the digital double agent?

As the term third-party connotes, apps that include third-party keyboard plug-ins are developed by app companies, not the device manufacturers. Apple iPhones alert app users at installation that certain third-party keyboards permitted Full Access may collect data beyond that transmitted via the app. Apple's warning states, "[t]hese keyboards can access all of the data you type, including bank account and credit card numbers, street addresses as well as personal and other sensitive information…If you enable Full Access, developers are permitted to access, collect and transmit the data you type." These keyboards, with a few exceptions, replace the original operating system keyboard, becoming the keyboard which will be utilized by apps on the device until removed or supplanted by another keyboard. This warning, and the potential capability it implies does not mean that the app is definitely keystroke logging all input, but Full Access does mean Full Access. The bottom line is that a third-party keyboard with Full Access permission may become a keystroke logger for all input to all apps on that device, recording and sharing the keyboard input from a device with the developer's server. Additionally, according to the websites of most app developers, any information collected from users via keyboards or otherwise, may be shared with their partners, as well.

As if the idea of installing a universal keystroke logger weren't enough to cause concern, there have been at least two third-party keyboard-based apps that have had their servers hacked, exposing users' personal data. Swiftkey and ai.type, both apps that install third-party keyboards on mobile devices, collected and stored users' personal data. In ai.type's case, the data was stored on an unprotected database – there was no password required to access 577 gigabytes of user data. Ai.type's open database exposed the names, phone numbers, contacts, social media links, and other identifying information of more than thirty-one million iOS and Android device users. And yes, this alarming fact was brought to light after that information was lifted from the database (it's hard to say hacked in the absence of a password).

Swiftkey, an app owned by Microsoft, is a predictive text app which began suggesting random user emails stored on the app's server in response to keyboard strokes. Users reported receiving emails from unknown senders alerting them that the app was suggesting their email addresses despite no previously established connection between the users. While that function has been locked down by Microsoft, the data cannot be recalled once released.

Keystroke Logging: Is Anybody Looking Out for You?

Keystroke logging, also referred to as keylogging, is the process of recording the input from a keyboard as its transmitted to or through a device. Our associated article, "Keystroke Logging: Organizational Risk and Protection" discusses keylogging in detail. Suffice to say, keystroke logging is one way users can hand over sensitive data without giving up their device. There is more than a decade's worth of incidents where cybercrimes were committed via keystroke logging, including examples where corporate networks were accessed via phishing emails that contained keystroke logging and transmitting code.

Considering the clear and present danger that keystroke logging presents, and the fact that many of the third-party keyboards being downloaded to mobile devices are in fact keystroke loggers, the natural question arises: what are device manufacturers doing to reduce the incidence of malicious keyboard capture? The answer is to warn users and let them make the decision, and to caution app developers via operating system platform websites.

Device manufacturers have a predicament on their hands. On the one hand, every security weakness exposed in an operating system is damaging to brand reputation, and potentially, to sales. On the other hand, an effective method to build brand loyalty is to increase functionality and dependence on the device. A surefire way to accomplish this is to increase the number of apps available and downloaded to devices in a platform specific manner. Once users invest significant time, and potentially money, in downloading apps to their devices, the likelihood that users will switch platforms decreases. However, if device manufacturers make creating compatible third-party apps too difficult, a criticism of Apple in years past, they run the risk of losing market share to another platform with a larger variety of popular compatible apps.

As it stands now, third-party app developers are still subject to having their apps reviewed and tested by device manufacturers/platform developers. In this, there is a certain level of control and security offered. However, there are certain functions, like keystroke logging, which are not prohibited because there are acknowledged legitimate uses for what is also a potential security weakness. Android and Apple both address the app security issue with third-party app developers and device users.

In the developer guide for Android (*https://source.android.com/security/overview/app-security*), there's extensive information on permissions, and which functions of an app belong to which of three levels of permission: Normal, Signature, and Dangerous. Normal permissions do not require the user to grant a third-party app to seek permission to execute a function, such as setting a time zone. Signature permissions are those which the user must agree to at the time the app is installed and include things like allowing an app to use Autofill settings within the app. Once granted, a Signature permission will assume that the user continues to allow that function to operate unless and until the permission is revoked. Dangerous permissions, things like accessing a user's contacts, require the user to grant permission via actively selecting "Deny" or "Allow" in response to a specific warning. The user may elect to apply the permission to the app for this specific activity until revocation by checking the "Never ask again" box below the response options.

Apple addresses third-party keyboard app developers specifically in the following appeal for security framed by Apple as "trust":

> **Safety of keystroke data**. Users want their keystrokes to go to the document or text field they're typing into, and not to be archived on a server or used for purposes that are not obvious to them.
>
> **Appropriate and minimized use of other user data**. If your keyboard employs other user data, such as from Location Services or the Address Book database, the burden is on you to explain and demonstrate the benefit to your users.

Installation on an Apple device of a third-party keyboard requesting Full Access will trigger the warning detailed above. This serves as Apple's warning to the user that Full Access may open keylogging functions, which while Apple warns developers to avoid, still allows. However, when Full Access is denied, the app may still function, however some of the most attractive functions may not operate with limited access. Swiftkey requires Full Access to operate on iOS devices, and unfortunately, was the target of a hack which put six hundred million users at risk, albeit the devices hacked were Samsung devices. Irrespective of device platform, the risk that personal data will be exposed via a keylogging third-party keyboard exists and is something organizations should consider before allowing users to install.

Keep Control of the Keys with Best Practices

There's no better way to reduce the risk of data loss or exposure than to continue engaging in best practices for mobile device security. There are probably very few times that your mobile device is out of your control long enough for physical alteration, but the things you do to and with your phone can make all the difference:

- **Two-factor authentication**: if you're not already using two-factor authentication, you may wish to try it out. In addition to a password, two-factor authentication requires the input of a code received via text, email, automated call, or token system, which must be entered in a secondary field before the desired app or account is unlocked. The advantage of two-factor authentication is that the second code is valid for only one use and is generated upon request. Even if the code is keylogged, it cannot be reused.
- **Maintain anti-virus protection**: For most mobile devices, the security patches released with operating system updates are sufficient to thwart most viruses on mobile devices. However, if you enjoy using your Bitmoji avatar from your laptop or pc, you're going to want to make sure you're covered.
- **Know the sign**: You may already have a third-party keyboard installed on your phone and not know it. If you have an iPhone, you should see a small icon between the numerical keyboard icon and the microphone key that resembles a circle with intersecting lines. That key indicates that you have multiple keyboards available to you, some of which may be third-party installations.
- **Change your passwords**: Keystroke logging doesn't necessarily collect and transmit all keystrokes, and many third-party keyboard apps avoid collecting input from "secure text entry" fields, such as password fields. Still, things happen, and code bugs exist, but by changing passwords frequently, you may limit your exposure.

One of the reasons mobile devices are so popular is that in addition to the convenience of carrying your world around with you, mobile devices are fun. Whether we download games to play, videos to watch, music for grooving, or cartoon selfies to stand in for us while texting, mobile devices add digital amusement to our lives. Unfortunately, cybercriminals are just as amused by stealing valuable data from users and will do so any way they can. By staying alert to the risks, you can enjoy your mobile device, and hopefully, not discover that your keyboard is a double agent selling your secrets.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ABA TECHSHOW 2019
Chicago, IL: February 27, 2019 - March 2, 2019

MASTERS CONFERENCE
Dallas, TX: February 28, 2019

THE SEDONA CONFERENCE WORKING GROUP 11 ANNUAL MEETING 2019
Houston, TX: February 28, 2019 - March 1, 2018

RSA CONFERENCE 2019
San Francisco, CA: March 4-8, 2019

THE ASU-ARKFELD 8TH ANNUAL EDISCOVERY
Phoenix, AZ: March 6-8, 2019

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: