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.

Keylogging: Organizational Risk and Protection

There's an amusing story about one method by which the Soviets spied on Americans in US embassies in the Soviet Union via IBM Selectric electric typewriters used by American Embassy personnel in the 1980s. IBM Selectric typewriters made use of a ball with raised letters rather than individual letters on arms attached to the keys. The ball would spin and pivot in response to keystrokes via a magnetic process that was also able to respond to fast typing speeds, a process called "typeahead." The Soviets surreptitiously installed bugging devices in the Selectric typewriters that recorded and transmitted the magnetic impulses to the typeball allowing them to reproduce what the Americans were typing, and thus, in 1983, keystroke logging was born. Keystroke logging wouldn't end with the replacement of the IBM Selectric; in fact, it's now a commonly used method of transmitting data, and in many cases, perfectly legal. In this article, we'll look at the technical side of keystroke logging, its uses, and how to prevent malicious keystroke logging from enabling cybercrime.

The Basics of Keystroke Logging

Keystroke logging, also identified as keylogging and keyboard capturing, is a method of recording the input from a keyboard, including wireless keyboards, and touchscreen keyboards or soft input keyboards, found on mobile devices. When the user presses or taps on a key, an encoder translates the signal input from the key to a unique code assigned to that key. That binary code is then displayed on the monitor as the corresponding graphic representation of the key, or other symbol assigned to the key such as an emoji or other character. Keylogging functions and apps intercept and copy the signals sent to/through the encoder simultaneously with the signals transmission to the monitor, generally with no delay detectable by the user. Once limited to keyed input, keylogging has expanded to include clipboard contents and screenshots. Keystroke logging can be limited to capturing signals within a specific app or can intercept all input keyed.

There are both hardware and software methods for keylogging and the components or software can be purchased for less than fifty dollars online. Wireless keyboards are especially susceptible to keyboard capturing, although those with AES encryption are less vulnerable. Hardware keystroke logging devices are available in a range of devices, many of which are WiFi compatible. Early models required that the keylogging device be plugged into the keyboard port of a PC tower, with the keyboard cable then plugged into the device. The keylogging interface collected the input from the keyboard and then allowed the signal to pass through to the computer. Early models had only small memory capacity and had to be accessed often or required the installation of additional software to store or transmit the captured data. With the advent of larger memory and WiFi-enabled transmission, keystroke logging devices can be attached to USB or serial ports, embedded inside keyboards, or connected via ethernet cabling, and accessed remotely via an app on a mobile device.

Keystroke logging software can be installed remotely provided the correct directories and user account settings of the target computer are accessible. For a corporation's network administrator, setting up keylogging software to monitor employee computer use, many of the popular keylogging software suites involve an administrator-agent setup, meaning that the IT staff will set one PC as the administrator with control of the software while the other PCs on the network will be setup as agents of the administrator, and will send captured data back to the server according to settings determined at the time of installation or modified thereafter. For stand-alone PCs, laptops, and mobile devices, keylogging software must be installed directly, or, some variety of remote access must be established first. Malicious keylogging software is often a rootkit, meaning that it can exploit a weakness and install itself in the core operating system software, often making it difficult to detect and hard to remove.

Too Legit to Quit

There are a number of legitimate purposes for which hardware designers and application programmers rely on keystroke logging as a method of collecting data. Research into human-computer interaction has benefited from keystroke logging as a means to enhance accessibility for users with disabilities, children, language learners, and writing instruction. Predictive text, which suggests text based upon common keystroke patterns, was developed and continues to be enhanced in part through keystroke logging. Parental controls, which many families rely on to safeguard children's online activity, law enforcement, and corporations also commonly employ keylogging functions to provide security and protect assets.

One of the most basic keystroke logging functions is that of a keyboard buffer. An invaluable tool for programmers, a keyboard buffer allows the coder to inspect and edit commands before they are processed. Everyday mobile device, PC, and laptop users benefit from keyboard buffering as well in the form of a smoother input to display experience. To experience the keyboard buffer in action, rapidly enter a random string of characters (easiest done with a PC or laptop), depressing as many keys simultaneously as possible. If the buffer limit is exceeded, there will be short pauses, then the display will populate with the keystroke results, often doing so in bursts or small groups. This delay-burst-display activity is the buffer at work translating the onslaught of signals from the keyboard grid to a graphic display.

Keyboard buffering isn't the only keylogging users might find inherently recording their keystroke activity. Microsoft's Windows 10 operating system installed a keystroke logging function that transmits user keystroke activity to Microsoft without the user's knowledge or consent. For users not comfortable sharing their keyboard activity with Microsoft, there is an opt-out in Windows 10 Settings, under Privacy, where in the General settings menu users can turn off keylogging by disabling “Send Microsoft info about how I write to help us improve typing and writing in the future.”

The Opposite Extreme

Despite the acknowledged benefits to technology advanced by keystroke logging, there is no question that intercepting user keyboard input can lead to cybercrime. The same technology that helps parents keeps their children safe online is the same technology that a jealous ex-partner can use in stalking, and the same law enforcement tool used to track hackers, in the wrong hands, can be used to capture passwords and confidential information, as well as, steal intellectual property or personally identifying information from organizations, often through the unauthorized access of an organization’s network. In addition, keyboard logging tools have also been used as the first step in remote installation of malware, including ransomware. As if we haven’t already raised enough concerns, spyware companies aren’t known for excellence in security practices of their stolen data. Information stolen via keystroke logging and sent to cybercriminals’ servers may in turn be easily hacked or stolen by another entity, hence multiplying the potential exposure.

Keystroke logging software employed in cybercrime isn’t used to steal a kid’s book report. Keylogging targets personally identifying and financial data:

- User Names
- Passwords
- Contacts
- Account numbers
- Credit card information
- Social Security and other identification numbers

If the information is valuable to you, it’s valuable to a cybercriminal, and whether you access your organization’s bank accounts, databases, or payroll information via mobile app or website, keylogging software can capture that data and share it without your knowledge.

Phishing emails are a popular method of distributing keylogging viruses, often via a Trojan virus which allows remote installation of secondary keylogging code. By clicking on attachments, and not just to emails, but also in texts, chats, and in social media apps, cybercriminals have been able to infect devices and entire networks with keylogging code. In 2017, a password protected Microsoft Word file was sent via email to a US-based financial services provider. Once opened, keylogging software was installed that sent back keystroke data, including sensitive customer data, to spammers. The Hawkeye Keylogger was a similar email-spread virus that popped up in 2018 and included access-removing functions that allowed the perpetrators to run a ransomware scheme.

Keeping the Keys Safe

Protecting yourself from the nefarious use of keystroke logging is another area in which organizations must implement best practices including:

- Install and maintain reputable anti-virus software.
- Use caution in opening attachments. Avoid opening attachments sent from unknown persons or organizations.
- Be judicious in installing apps, especially those which contain third-party keyboards. Be sure to read about the dangers of third-party apps in our associated article.
- If you use a computer or laptop in a cybercafé or other public venue, check for devices

attached to the ports. That strange dongle may not be someone's forgotten fitness tracker interface.

- Avoid using a public PC or laptop to access sensitive data.
- Save your wireless keyboard for closed, secure networks.
- If you suspect that there may be unauthorized keystroke logging capturing your activity, have your PCs, laptops, and mobile devices inspected and cleared by experienced professionals, such as Digital Mountain.

Technology, like most tools, can be used for advancing the good, like making computing power more accessible for those with physical challenges and increasing work efficiencies; but, it can also be used for the worst of all purposes, like spying, stalking, and stealing. Fortunately, there's enough good people in the technology industry that are committed to advancing the good not just for profit, but also, to keep those who would use technology in harmful ways from getting the best of us. The idea, of course, is keeping the keys in the right hands.

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: