SPRING 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of mobile device management and malware prevention. With the unprecedented increase of telecommuting resulting from the Coronavirus pandemic, secure data management by organizations is more critical than ever.

Stopping Mobile Malware from Halting Your Productivity

Mobile malware is especially insidious because we've come to rely so much on devices such as smartphones and tablets. Because these devices are meant to be easy to use and simultaneously powerful, they can also be difficult to secure and protect. Users are more likely to conduct regular security scans on their laptops and desktop computers, but smartphones and tablets don't appear to undergo the same regular virus scanning or have the same level of firewall protection as our larger, less portable devices. Whether we should attribute this lower level of caution to the less visible nature of mobile device operating systems, or to the persistent myth that certain mobile device operating systems are impervious to malware we may never know. What we do know is that mobile malware continues to be a threat to both companies and individual users.

Flexible and Adaptable

In so many circumstances, flexible and adaptable are positive attributes. If you have flexible and adaptable employees, they're a boon to your company. We want our consumer products, including our mobile devices, to fit into our work and personal lives seamlessly, which explains why smartphones and tablets are so popular. Unfortunately, mobile malware has evolved with the same qualities. As online banking has exploded in functionality and popularity, so has banking malware designed to steal login credentials, credit card numbers, and other financial details. For more than a decade Trojans from Zeus to Backswap have been disguising themselves as legitimate communications and apps, then stealing critical information.

Short Messaging Services, SMS, or "texting," is also prone to malware attacks. Text messaging is perhaps the most popular method of communication and with Multimedia Messaging Service,

which includes text and media such as videos, photos, and voice recordings, providing malware a new home. Worms are a type of mobile malware that is spread by SMS and MMS and often don't require the user to open a message in order to take up residence in the user's device and spreading itself via subsequent messaging transmissions. One of the biggest SMS/MMS malware threats of 2019 was the Backdoor Family, which used both an SMS notification of a voice message and an MMS attachment. To hear the voice message, users needed to follow a link to install a new voice messaging player app, which turned out to be a Trojan that even when "deleted" still retained its malicious functionality.

Mobile cryptocurrency mining malware also made the list of malware threats to watch in 2019, as the popularity of bitcoin continued to grow (https://www.coindesk.com/trendmicro-detects-crypto-mining-malware-affecting-android-devices). Transmitted via spam email and SMS links, mobile mining malware is easy to detect because of the resources they consume, however, many include code that prevents them from being removed easily. If you think you're involuntarily hosting a cryptocurrency mining operation, consult with a professional team such as Digital Mountain for help in shutting that operation down.

Security on the Go

Mobile device security continues to evolve right alongside mobile malware threats. There are steps you can take to protect your mobile devices that won't cost you an arm and a leg, but may prevent you from losing a fortune:

- Don't text with strangers: with the proliferation of mobile malware spread via text, the best way to deal with a message from an unknown source is not to open or respond to the message. Clear it off your phone immediately.
- Install device security software and keep it updated: Just as you would for your laptop or the desktops in the office, maintaining updated threat detection and elimination software on your devices is a best practice.
- Isolate your work and personal data with partitioning. Don't know how? We can help.
- Never hand your unlocked device to someone in whom you don't have full confidence and trust: It's easy when you're in a bind to hand your phone to someone who says, "Here, let me help." But if you're not sure who the person is and what they're going to do to your device – pass on that offer. Even if they don't do something overtly harmful, they could unintentionally make a change to your device that renders it more susceptible to malware.
- Vet apps before downloading: Remember, Trojans often come disguised as legitimate applications - games, messaging apps, even banking applications. Check your bank's website for a link to download their official banking app. Run a search for the name of the app before you download – cybersecurity forums are quick to post new threats.
- Change your passwords frequently: This is one of the most time-tested precautions for mobile device security. The more frequently you change your passwords, the harder you make it for someone who may have purchased a list of stolen usernames and passwords.
- Configure Multi-Factor Authentication on your accounts whenever the option is available for banking, email, medical records, etc.
- Don't click that link: If you harbor any doubt about a link or an attachment, don't click on it or open it.
- Watch for odd behavior: If your device starts making calls or taking pictures on its own,

draining battery levels at lightning speed, performing normal functions at reduced speed, or behaving in any other way which seems unusual – contact a professional like Digital Mountain immediately to have the device scanned and restored to health.

Mobile devices have become integral to our lives, and with the ability to use them in multiple ways to stay connected with our family and friends, its vitally important to protect them from malware threats. Cybercriminals know this and are ramping up attacks on mobile devices, especially as we face trying times. The most we can do at this juncture is to use best practices to protect our devices from harm, and in the event that we suspect a problem, reach out for help immediately – and at Digital Mountain, we're just a phone call away.

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

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. In the short term, she is available for webinars and remote e-conferences.

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: