SPRING 2021 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss mobile device trends for legal and security, including malware, authentication, and legislation around backdoors to end-to-end encryption.

Mobile Malware: Big Business from Big Danger

According to data aggregator Statista, as of January 2021, 55% of web pages were being accessed via mobile devices (https://www.statista.com/statistics/306528/share-of-mobile-internet-traffic-in-global-regions), a trend that has continued to grow for at least four years. All market segments have seen growth: internet shopping, entertainment, banking, and news sites are all seeing increased visitor numbers from cell phones, tablets, and other mobile devices. As a result, mobile malware is also seeing exponential growth. As larger volumes of data are being stored on mobile devices, black hat hackers have increased their attention on targeting sensitive data stored on mobile devices including banking credentials, contacts, and files. Gone are the days when mobile device users were discouraged from storing data on mobile devices by the limitations of storage or had their exposure fears assuaged with mobile devices running “hack-proof” operating systems. We’re solidly in the age of Mobile Malware.

Today’s Mobile Malware

The most common variety of mobile malware is a familiar foe with whom most security conscious people are acquainted: the Trojan Horse. Now identified more commonly as simply a Trojan, this type of malware wears the mask of a legitimate app, email, attachment, or file, but hides a dangerous secret. Emotet is the reigning champion of Trojan malware, known for seeking out banking data, brute force passwords attacks, spreading additional malware, and an ability to avoid malware detection. Emotet will celebrate its seventh birthday this year, and still sits on the Department of Homeland Security’s list of the most destructive and expensive malware products (https://us-cert.cisa.gov/ncas/alerts/TA18-201A). Most Emotet deployments are the result of spam emails that recipients allow to infect their devices, including mobile devices. One of Emotet’s newest tricks is spreading via WiFi from one infected device to other unprotected devices across open networks and replicating itself as many times as possible.

These WiFi attacks have also been known to attack IoT devices including smart home devices.

Phishing schemes have made their way into our mobile devices via messaging apps. Users receive a text or a message from what appears to be a legitimate financial organization asking for users to click on a link that will take them to a special offer or to some problem with their existing account that needs to be resolved. The link, once opened, then installs its dangerous payload or directs a user to a fake website that appears real, some including chatbots, designed to lure victims into sharing data, including credentials and files, that cyber criminals desire. Many of these phishing schemes rely on a contact scraping virus that searches devices for the email address and then sends phishing emails to those contacts from the user's email identity, or a close approximation thereof. File sharing services are also a new favorite of phishing attacks. By sending the user a link to view some new file shared by a contact scraped from a contact list, phishing hackers will attempt to get users to voluntarily enter their passwords or to open infected files and attachments.

Both Trojans and phishing attacks can be the carriers of ransomware – a problem that is just not going away. Ransomware malware works within devices and networks to deny access to stored data, often threatening to make the information public, sell it, or destroy it if a ransom is not paid within a short timeframe. The ransom demands are often made payable only in Bitcoin because of the anonymity of the cryptocurrency system. There's also no guarantee that once the ransom is paid that the data will be restored or all damage to the device and network undone. It's not unusual for malware to root itself into the firmware, to create a path for reentry, or to continue communicating with a Command and Control server.

Not Just Bad but Big Business

Malware is a big deal in many ways, not the least of which is business – both from the demand and the supply side. An investigation into the business of buying malware on the internet found that for as little as fifty dollars ($50.00), entrepreneurial black hat hackers could purchase "advanced" malware tools, some including tech support (https://cybernews.com/security/buying-your-own-malware-has-never-been-easier). Malware is also showing up in the software supply chain leading to mobile device infections. By infiltrating app developer's networks, a Trojan was slipped into an application preloaded on cellphones. Discovered in 2019, this malware app was capable of hijacking SMS messages without the user's knowledge (https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf). Fortunately, the malicious app was discovered prior to distribution of the phones. Finally, Magecart is a consortium of financial cyber criminals that placed credit card skimming malware onto various online shopping sites. When users would key in payment details, the information would be sent to Magecart simultaneously. With up to forty percent of online shopping conducted from mobile devices, a tremendous amount of data is at risk.

Recognizing Mobile Malware Threats

Identifying potential malware before devices are infected is the surest way to prevent damage, but it can also be the most difficult. The adage not to open emails and attachments that don't look quite right is all good and well until a scraped contact list turns into an email from the boss that looks completely on the level. When you're part of an organization that shares files through a trusted cloud service with a handy app, notifications alerting you to new shared documents are going to grab your attention. So, what do you need to look for?

1. File extensions: .zip, .rar, .ace, and other extensions that indicate a compressed file is going to open when allowed to. Malware often will be compressed into one of these file types and upon extraction, will begin an automatic installation.
2. Unusual file names: If your organization employs a standardized file naming convention, then any "internal" file you receive that doesn't meet that convention should raise a red flag. Additionally, malware files have often been known to incorporate false flags embedded in their file names to lure potential victims. If you see a file that resembles something familiar: prodsales.q1.2021.xll.exe, you should be wary of the extensions. The .xll might lead you to believe this is a spreadsheet produced in a popular software product, but the .exe at the end is an executable file that could spell trouble.
3. UFOs – Unidentified File Objects. While the UFO term is a little tongue in cheek, the danger is real that a file that will not open of its own accord and requests the user to "Enable Editing" or enter a password is potentially malware. In January 2020, Microsoft discontinued it's support of Windows 10 Mobile operating system, and not long after, Emotet malware harnessed the Windows 10 Mobile obsolescence as a mask to lure victims into enabling macros that installed the Trojan.

Mobile malware is the natural evolution of malware as we spend more time on mobile devices, thanks to their increased processing power and storage capabilities as well as the variety of work and entertainment apps available. Black hat hackers motivated by money are going to follow the opportunities as they present themselves. As users, we are the ones who need to take precautions, remain vigilant, and protect our data.

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

UPCOMING INDUSTRY EVENTS

DATA CONNECTORS CYBERSECURITY CONFERENCE
Seattle & Portland: March 31, 2021 - April 1, 2021

LEGALWEEK VIRTUAL SERIES 3
April 13, 2021

THE SEDONA CONFERENCE WORKING GROUP 11 ANNUAL MEETING 2021
April 14-15, 2021

IAPP GLOBAL PRIVACY SUMMIT 2021
April 27-28, 2021

THE SEDONA CONFERENCE WORKING GROUP 1 MIDYEAR MEETING 2021
April 28-29, 2021

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. 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: