FALL 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss scary cyber trends, demystifying the new AI-enhanced legal applications, and courts' reactions to AI hallucinations. Of course, since it's almost Halloween, expect our annual dose of spooky fun, too.

Five Super-Scary Cybersecurity Trends

In celebration of all things spooky for Halloween, we've collected a list of five super-scary cybersecurity trends we hope don't trick you anytime soon.

AI Nightmares!

1. WormGPT/FraudGPT/and LLM clones for bad actors. Like any tool, ChatGPT, Bard, and the growing population of other AI-enhanced technologies are attracting their share of attention from cybercriminals. WormGPT and FraudGPT are both advertised on the Dark Web and in hacker forums as a means to create and perfect undetectable malware and other malicious code, as well as enhance the effectiveness of phishing emails. While correlation isn't causation, there are multiple reports that ransomware is on the rise for 2023, suggesting that threat actors are upleveling their attacks.

2. Indirect Prompt Injection Attacks. An Indirect Prompt Injection Attack is a way to force a Large-Language Model (ChatGPT, Bard, Claude, and others) to bypass standard controls and do something else. The simplest technical explanation we found is:

> A hacker slips a prompt in zero-point font—that is, invisible—into a web page that will likely be used by the chatbot to respond to a user's question. Once that "poisoned" page is retrieved in conversation with the user, the prompt is quietly activated without need of further input from the user (https://techxplore.com/news/2023-03-indirect-prompt-upend-chatbots.html, or https://arxiv.org/pdf/2302.12173).

What types of threats result from Indirect Prompt Injection Attacks? Fraudulent requests for Personally Identifiable Information (including banking and financial information), deliberately providing erroneous or misleading information, denial of service attacks, and malware propagation.

With an explosion of LLM applications for nearly every market and service sector, the potential nightmares caused by Indirect Prompt Injection Attacks are on our watchlist.

3. Deep Fakes Getting Deeper with AI Advances. Maybe seeing the Pope in a designer puffy parka is fun, but unfortunately, we can't count on threat actors not to fool us with important events that deserve accurate and authentic information. AI advancements in graphics and audio are propelling deep fakes into a new realm of realism, and researchers and regulators are sounding alarms. The Federal Election Commission recently concluded the comment period on the matter of deep fakes in election ads and what should be done about it. The next step will be to consider the merits of the issue and potentially begin rulemaking (https://sers.fec.gov/fosers/). And in what might be a new high for self-regulation, Meta recently announced the creation of Voicebox, a generative AI speech tool that is apparently so good at creating realistic speech, the company has decided not to release the product at this time due to concerns over misuse (https://ai.meta.com/blog/voicebox-generative-ai-model-speech/).

Gadget Goblins!

4. Flipper Zero and Other Annoying Tools with Cute Names. While these electronic multi-tools aren't new or hard to find (you can check out a Raspberry Pi from most public libraries), there's certainly concern over how quickly bad actors are making use of them. Cheap, easy to program, and legal, these devices can copy data from credit cards and hotel keys, clone automobile key fobs, remote controls, and electronic tracking tags, send disruptive pop-ups over Bluetooth, and spread malware or steal data through bad USB attacks. While the vast majority of these devices can't grab the CVV number from a credit or debit card (yet), there are still plenty of websites that will honor card numbers without the three-digit security code. Defending against these devices isn't all that difficult. To help protect your data, use a well-tested RFID blocking device for bank cards, turn off Bluetooth and WiFi in Settings when in public (enabling Airplane Mode is not sufficient), and never leave a mobile device unattended.

5. Tracker Stalking. This creepy, and potentially dangerous, trend has been on our radar. AirTags, Tiles, and even AirPods are being used to stalk celebrities and private citizens in messy breakups, as well as being used by auto theft rings for tracking target vehicles. Bluetooth-enabled trackers, such as those made by Apple, Tile, Chipolo, and others, use the same radio frequency technology that other Bluetooth devices use to connect to smartphones and tablets. Once paired, the two devices will communicate with each other on a regular basis provided both are functioning and in range. If the tracker's owner is out of range, Bluetooth crowdsourcing allows for enabled items to be tracked over increased distances provided that other compatible devices can "chain" the signal. For example, Person A pairs a tracker with their cellphone and then places the tracker in a vehicle. Person B then drives the vehicle home. Provided there are enough Bluetooth devices sending signals along the route and at the destination, Person A will be able to find the vehicle by locating the tracker with their cellphone or tablet (other devices serving as links in the chain remain anonymous). Both Apple and Android devices will issue alerts when an unknown tracker is traveling with you and moves away from the tracker owner's device. If you're concerned you're being tracked, Apple's support page offers ways to detect and disable unknown trackers (https://support.apple.com/en-us/HT212227). Android users should try Google's support page (https://support.google.com/android/answer/13658562?hl=en). If you discover one of these devices and suspect unwanted tracking, contact local law enforcement. Attorneys will want to let their clients know, especially those already in or contemplating litigation, that if their phone alerts of a mystery tracking device, this could be vital information to share. Fortunately, to locate the

tracker, it must be registered to a mobile number, an iCloud account, or an email, which is discoverable information, and often, can take authorities right to the person who placed the tracker.

While there are plenty of scary new cyber trends creeping up daily, Digital Mountain is constantly on guard for those that need expert attention. If you have questions or fear you may need some cyber ghost busting, don't hesitate to call.

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

UPCOMING INDUSTRY EVENTS

SEDONA CONFERENCE WG1 ANNUAL MEETING 2023
Indianapolis, IN: October 26-27, 2023

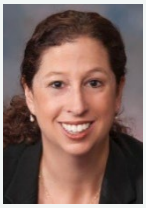
20TH ANNUAL GEORGETOWN E-DISCOVERY ADVANCED INSTITUTE
Washington, DC: November 9-10, 2023

MASTERS CONFERENCE NOVEMBER 2023
Atlanta, GA: November 9, 2023

ADC 64TH ANNUAL MEETING
San Francisco, CA: December 7-8, 2023

LAW.COM LEGALWEEK 2024
New York, NY: January 29, 2024 - February 1, 2024

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: