DIGITAL MOUNTAIN®

WINTER 2021 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, cybersecurity and data analytics needs. For this E-Newsletter, we focus on data leakage and organizational risk, as well as cybersecurity trends for 2021.

Get Out of My Data

Applications are not always “staying in their lane” with regard to what users expect and this can create unanticipated data leakage for organizations that may have serious unintended consequences. All organizations are rightly concerned about data security and protection. To keep information safe there are firewalls, intrusion detection, intrusion protection, antivirus software, spam blocking software, mobile device management software, and the menu of products that need to be implemented for an organization’s protection continues to evolve. However, in this dizzying mix, there are factors caused by application data leakage, often overlooked by traditional security approaches and security audits, that all organizations should be aware of. Below outlines the top seven applications of concern and factors to consider:

1. **<u>Off-Facebook Activity – Following You Almost Everywhere.</u>** In January 2020, Facebook released information whereby Facebook’s over 2.7 billion users could view their own off Facebook activity and see data being tracked on them. Facebook markets they released this information so users could configure what apps and websites should be removed from Facebook account activity to be able to provide a more optimal advertising experience. The problem is that even when you deselect this “personal” experience, you are still tracked; the information is now just disassociated from your profile. Websites that use Facebook components for ads and analytics, Facebook Social Plugins (for example the Like and Share buttons) and Facebook Login plug-ins, etc., are tools usually implemented by the web administrator and not typically reviewed by the data security group of an organization. Website owners, which include law firms, financial institutions, and medical institutions, may be transmitting information via their websites back to Facebook even if a page visitor is

not logged into Facebook or part of the Facebook community. This transmission occurs when an attorney or investigator is performing research on websites using these components or with general Web site surfing by employees when web sites are browsed containing these Facebook tools.

Builtwith.com, a site that reports what building blocks websites are constructed with, allows us to evaluate some common website Facebook components:

- *Facebook Signal*, which journalists use to uncover relevant trends, photos, videos, and posts from Facebook and Instagram for use in their storytelling and reporting, was utilized on 6,048,486 websites,
- *Facebook Pixel*, which is a conversion tracking system for ads on Facebook to websites, was utilized by 4,528,076 websites, and
- *Facebook Conversion Tracking*, which allows tracking of user advertisement clicks, was used by 3,923,043 websites.

Websites outside of Facebook are tracking information and reporting potentially sensitive information back to Facebook based on your profile. Whenever you visit an external site employing Facebook technology and you accept the cookies, the Facebook tracking cookie downloads whether you have a Facebook account or not. When you visit one of these sites, regardless of your Facebook user status, Facebook receives an IP address, location, browser details, and more. Facebook tracking cookies never expire.

What can you do? As a user, you can clear your history to prevent off-Facebook activity matching the data to your profile, but external sites will still transmit the data to Facebook in an anonymized method at that juncture. As an organization using Facebook tools, realizing you are transmitting visitor data back to Facebook from your website is a first step.

2. **Google History and Analytics Tracking.** Google tracks history across its various technologies on its users for YouTube, mapping programs, searches, and application activity. Similar to Facebook and other social media sites, you can download your data and take a peek at what they're storing. Google has a technology called Google Analytics that according to Builtwith.com is used by over 28 million sites. Google Analytics tracks time of visit, pages visited, and time spent on each webpage. It also tracks referring site details (such as the URL a user came through to arrive at this site), type of web browser, type of operating system (OS), Flash version, JavaScript support, screen resolution, and screen color processing ability. Network location and IP address are also tracked. In reviewing personal profiles, it was not obvious if that information was being transmitted and directly correlated to a user profile for Google's own marketing. Rather, it was being utilized for corporations to better analyze its own web traffic. What can you do to protect your data? They make it easy to pause and turn off tracking if you log-in and configure the settings properly. You can also do a Privacy checkup easily within Google.

3. **ZoomInfo Monitoring an Organization's Email Activity.** ZoomInfo, not related to the video conferencing company Zoom, is a content aggregator through which hackers can purchase information in order to conduct potential phishing hacks of company employees, accounting departments, and executives. The technology is used

legitimately by marketing departments to research prospects and their information for sales and advertising. However, the dark side to the legitimate use of the technology is that if an employee, through a click-through agreement that they rarely read, downloads the technology, an application is installed that monitors emails in Outlook and scrapes corporate contacts to further build up ZoomInfo’s repository from communications. Individual employees can request ZoomInfo to remove their own information, but it is very difficult for exfiltrated scraped contacts to be removed in a take-down process with ZoomInfo, even those that were never endorsed by the organization for distribution.

4. **Microsoft’s Cortana is Watching My Email.** Microsoft's Cortana is designed to be a digital assistant and workplace productivity tool. However, it's now built into Windows 10, available as an app for Android and Apple, and Microsoft is trying to bring it to your car. While Cortana recordings are now transcribed in “secure facilities,” according to Microsoft, the transcription program is still in place, which means someone, somewhere still might be listening to everything you say to your voice assistant. Starting in late August 2020, Microsoft introduced a new tool called the Cortana Daily Briefing Email. This Daily Briefing is a personalized email that Office constructs for you, based upon what Microsoft 365 (or Office) knows about you and your day. The tool automatically opts you into the technology which is creepy (or cool, depending on your perspective) as it summarizes action items you need to take from within potentially sensitive communications. A user has to Unsubscribe to stop the emails, like a nosey neighbor that you have to tell to “butt out.” If you’re an organization using Windows 10 Professional or Enterprise, the easiest way to disable Cortana is by using the Local Group Policy Editor. For individual users, you used to be able to turn off Cortana in Windows 10, but Microsoft removed that easy toggle switch, so now you have to do a registry hack. If you don’t apply the hack correctly, it could render your system unstable.

5. **Custom Emojis are Cool, but Could Translate into Keystrokes Being Monitored.** Although most custom emoji providers will put in their terms of services the specifics of how they will be using data when you download a special fun new app like Bitmoji, these applications typically need Full Access to the keyboard on the smartphone. Apple warns, “When using one of these keyboards, the keyboard can access all the data you type. Third Party Keyboards provide an alternative way to input keyboard data. These keyboards can access all of the data you type, including bank account and credit card numbers, street addresses, as well as other personal and sensitive information. These keyboards may also access nearby text or data, which is useful for improving autocorrect functionality.” It’s important to understand what that cool new application is doing and the organizational risk that may be exposed through your smartphone activity.

6. **Grammarly is Not Only Correcting Your Punctuation, They are Also Tracking You.** Grammarly offers a digital writing assistance tool based on artificial intelligence and natural language processing. When you install the plug-in, you’re letting a 3rd party unknown server somewhere in the Ukraine access (for "proof reading") every single thing you type. Grammarly also tracks the IP addresses you’ve logged in from. In 2018, Grammarly's flawed Chrome extension exposed users' private documents. Grammarly has fixed this security bug, but this demonstrates how a free tool can lead

to unintended data leakage within an organization.

7. **Virtual Assistant Listening Devices.** Whether it's Cortana, Amazon's Alexa, Google Voice or Apple's Siri, these technologies transmit data back to servers to improve their speech recognition algorithms. Digital assistants can be found in the workplace, home, car, hotel, phone and many other places. In order to hear a command, these devices require an always-on microphone. If a malicious actor hacks into any of these systems, confidential and private data may be exposed. Have we entered an era where we have to assume every word is being recorded?

With free, cool apps and productivity technologies, there are trade-offs. As we enter 2021, we need to put more thought into what a technology is doing behind the scenes and whether the data leakage is worth what we get in return. Organizations need to look beyond traditional security risks as these technologies report back "home" to third party providers not controlled by you or your organization. Digital Mountain's cybersecurity and data forensics professionals can provide a unique perspective in strengthening your organization's security posture for internal risk mitigation, compliance and security audits.

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

UPCOMING INDUSTRY EVENTS

ALA MIDWINTER MEETING & EXHIBITS, VIRTUAL
January 22-26, 2021

PLI GOVERNMENT INVESTIGATIONS 2021: INVESTIGATIONS ARISING FROM DATA BREACH AND PRIVACY CONCERNS AND PARALLEL PROCEEDINGS, VIRTUAL
January 27, 2021

EDRM EXPOCOM 2021
February 1-3, 2021

LEGALWEEK VIRTUAL SERIES 1
February 2-4, 2021

TECHSHOW 2020, VIRTUAL
March 8-13, 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: