DIGITAL MOUNTAIN®

SUMMER 2022 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 data exfiltration including prevention, digital forensics and case law.

Ten Warning Signs of Data Exfiltration

Whether you call it corporate espionage, Intellectual Property theft, data leakage, or internal data risk, data exfiltration is the unauthorized movement of organization-owned data outside the organization's permitted distribution and storage boundaries. Data exfiltration can be as simple as a leaked draft of a marketing memo or as complex as the chemical formulation of a pharmaceutical innovation or entire volumes of computer code, all of which can have disastrous consequences for an organization. Additionally, with more data stored on the cloud to conserve resources, facilitate remote work, and increase collaboration, the temptation to move that data outside the organization's control continues to grow. Knowing what to watch for when it comes to data exfiltration is the first step to preventing loss.

The Threat is Real and It's in the House

Blackhat hackers aren't the only ones motivated to lift organizational data. Legitimate employees and contractors may also look to exfiltrate data for both malicious and seemingly innocuous reasons. A workaholic partner's offline vacation in Bali may have them thinking that downloading sensitive organization data to their laptop is okay because it's temporary and done for a seemingly valid purpose. A departing salesperson may believe that the contacts they've made working for one organization are fair game for their next job. And a contractor who may need to see the specifications for a highly confidential product in development may never consider that downloading product plans to his or her personal device is an unauthorized data transfer and not a task needed to perform the job. What do they do with that data once the contract or employment comes to an end? For these and many other reasons, organizations are forced to watch carefully for signs, situations, and events that could indicate a problem. Here’s our watchlist of data exfiltration indicators:

1. **Sudden increases in file movement from cloud storage or a network drive.** Files being downloaded, sent, or shared in new or unusual patterns could signal data exfiltration. Large transfers of data within short periods of time should always trigger a response, even if it’s just to confirm legitimate file maintenance. When moving data, employees may try to reduce the volume of data by compressing files into .zip, .tar, .rar, or other compressed file formats to decrease volume size and transfer time.
2. **New email contacts or collaborative suite team members** to which an employee begins sending data may be a soon-to-resign employee sending data to themself. In contemplation of a resignation, an employee may begin shifting data well in advance of giving his or her employer notice. Data transfers may also happen via personal cloud-based drives (discussed more below), personal email accounts, chat applications, or from work email to a personal email account.
3. **File Sharing Sites.** Sudden or dramatic increases in file movement to a cloud storage site may signal an issue. Digital Mountain examiners are well aware of a number of mainstream file sharing sites such as Dropbox, Box, Google Drive, as well as less noteworthy sites such as Wormhole, Drop.lol and Pastebin. FTP site transfers should also be considered. A careful search of a former employee’s Internet history may reveal other exfiltration methods that should be evaluated.
4. **Portable storage device hookups.** Thumb drives and other external storage devices that connect through USB ports are so cheap and easy to use that many organizations routinely disable these ports for uploading from or downloading to external storage devices. However, when an employee can log in using their own laptop or desktop, saving data to an external device can be much easier. Digital Mountain examiners know when and where to look for the artifacts that these USB connections leave behind.
5. **Photos or videos with a second device.** With camera-equipped mobile devices, taking photographs or videos of data displayed on a monitor is another simple way to exfiltrate data. At Digital Mountain, our digital forensics examiners know the most effective approaches to search for evidence of exfiltration via photos or videos.
6. **Renaming.** With a modicum of knowledge, renaming a file with an extension that hides the true file type may help bypass certain automatic triggers that data exfiltration is likely. Once past the gatekeeping protections, the data can be transferred at will and then renamed properly. The MD5 hash or digital signature of these files still remains the same even if a file is renamed or the file extension changed.
7. **Opening Permissions.** Any employee with the ability to set access permissions to data has an opportunity to open the doors to a third party who can steal data for them. These permissions can be quickly revoked in hopes of hiding the evidence of wrongdoing.
8. **Wiping/Mass Deletions.** Exfiltration isn’t confined to just copying or moving data out of the network. Wiping data or mass deletions can be another sign that a bad actor is taking data and then removing the original data from the network in an attempt to hide their theft, attempt to collect a ransom later, to sell it, or just to damage the company by deleting crucial data from the network. Any installation of any application, especially applications capable of wiping away or deleting data, should be tightly controlled. Already happened? Bring in a trusted partner, such as Digital Mountain, before attempting to recover the data yourself. There’s a great deal involved in preserving the evidence that the data was wiped and then properly recovering as much as possible.
9. **Login Assistance Apps.** Remote login apps are fantastic for helping remote workers log into your network from anywhere they can access the internet. They’re also helpful for

organizations that want to conduct remote technical support on remote workers' devices. The very real downside to these apps is that they can create a vulnerability that allows for an employee to access the organization's network from anywhere at any time, potentially allowing for a window in which data exfiltration can be achieved. If you know the Trojan Horse scams, where a remote login program is downloaded without knowledge or permission and then used to access the target device to extort money, you can see how a remote login assistance app might pose a data exfiltration threat.

10. **Spiking print volumes.** Printing paper copies of confidential data is old school, for sure. Printing and carrying out a few pages at a time is still an effective way to sneak data out the door. However, printing a stack of papers may be detectable with proper system configurations.

Any or all of these red flags may occur during normal operating hours, but off-hours and long holiday weekends seem to be a popular option for data exfiltration attempts. Once someone makes the decision to steal data, they're going to try to do so when they are least likely to get caught – and if they realize that data security is lax at a particular time or on a specific day, that's when they'll make their data moves.

Smart data protection doesn't have to bring productivity to a screeching halt. By keeping an eye out for the ten warning signs above, your organization can take the first steps toward stopping exfiltration before data walks out of the door – whether it's going with a disgruntled employee, a careless contractor, or professional corporate interloper.

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

UPCOMING INDUSTRY EVENTS

BLACK HAT USA 2022
Las Vegas, NV: August 6-11, 2022

DEFCON
Las Vegas, NV: August 11-14, 2022

ILTACON 2022
National Harbor, MD: August 21-25, 2022

PFIC 2022
Nashville, TN: September 6-9, 2022

SEDONA CONFERENCE WG12 ANNUAL MEETING 2022
Reston, VA: September 7-8, 2022

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:

in f