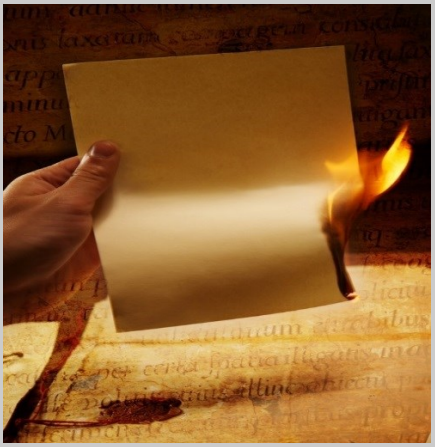
SPRING 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With the proliferation of data breaches, we chose to focus this E-Newsletter on the topic of encrypted email and transient messaging technologies and the impact on organizations.

"BURN AFTER READING" – DISCOVERY PROFESSIONALS CHALLENGED BY COMMUNICATION SECURITY TECHNOLOGIES



In light of publicity over government agencies (e.g. NSA) monitoring messages in-transit and pervasive corporate security breaches, computer users are increasingly aware that their private emails and messages are not secure. In response, users are turning to encrypted email and messaging to ensure their emails and messages stay private. For example, a number of free and paid services, such as Wickr and ProtonMail, allow users to send encrypted messages and files. All communications are end-to-end encrypted, meaning messages cannot be read while in-transit and only the recipient has the key to decrypt the message. Both services store messages encrypted and allow senders to specify an expiration period for messages. Additionally, these types of services do not keep track of user information (e.g. unique device identifiers such as computer or phone IDs). This approach is both a blessing and a curse in that it allows users to be anonymous, but if account information is lost there is no way to retrieve it; users must be vigilant in keeping track of their account information. The following table demonstrates the ways Wickr and ProtonMail differ greatly in usage and benefits:

ProtonMail	Wickr
Access: Occurs through a web browser, much like Gmail or Yahoo! Mail.	**Access:** Occurs via a smart device (e.g. iOS, Android) or computer (e.g. Windows, OSX, Linux) and operates in a way that both sender and recipient are in a closed network that requires both parties be able to access Wickr through an account.

Format: ProtonMail users can send encrypted emails to non-ProtonMail users by sending the recipients a passphrase and a link to the actual message on ProtonMail servers. Once the recipient clicks on the link in their email and enters the passphrase, they are then able to read the message. Email is stored encrypted on ProtonMail's servers and deleted after reading or if the message remains unread after an amount of time specified by the sender. ProtonMail users are able to attach files onto emails, much like Gmail or Yahoo! Mail. The attached files are encrypted automatically and if the receipient is not a current ProtonMail user, then the attachment can only be opened with the correct password protected link from the original encrypted message. There is a size limit of less than 25MB per email.	**Format:** Wickr more closely resembles a messaging service than an email service. Communications are similar to instant messages whereby a user can message individuals or set up groups in real-time and all messages to that group continue on a single thread. Wickr users can upload different types of files (e.g. Office type files) onto Wickr's secure cloud servers and Wickr automatically strips the metadata from the files. Wickr users can upload media such as photos and videos and have them automatically expire after a certain amount of time.
Server Location/Legal Process: Servers are located in Switzerland, which has more stringent privacy regulations; governments (most notably the US Government) cannot shut down the service or order ProtonMail to produce information.	**Server Location/ Legal Process:** Wickr's servers are located in the United States and as such must comply with law enforcement via valid requests such as emergency disclosure requests, warrants, or valid subpoenas. With that said, no content can be viewed since Wickr does not store the decryption keys.

Encryption Add-ons

Businesses can employ numerous solutions for email encryption. The encryption methodology is similar to that used by ProtonMail; however, the biggest difference is that enterprise providers such as Cisco, HPE Security (Voltage Security), Trend Micro, and ZixCorp provide greater control to businesses via various options for end-to-end encryption. For example, Cisco's email hardware appliance includes built-in functionality (e.g. anti-spam capabilities, malware protection) and still allows a business to choose either Cisco's hosted encryption key manager (Cisco Registered Envelope Service) or another product, such as ZixCorp's own hardware key manager appliance gateway (ZixGateway with Cisco Technology).

In contrast, Trend Micro approaches email encryption differently, by offering businesses a hosted solution for key management and policy-based encryption. Trend Micro, with its purely cloud-based approach, maintains its own hardware in their secure data centers, thus freeing businesses from worry about hardware maintenance costs. All the above solutions are compatible with Microsoft Outlook for workstations and have proprietary applications for mobile devices. From a corporate user perspective, they will also offer the same encrypted email functions such as message expiration.

Self-Destruction for Messaging

Lastly, free messaging services exist that allow users the security of ephemeral or self-destructing messages. Snapchat, a well-known service that lets users send ephemeral messages, is primarily used to send pictures and videos to be shown only once. However, one issue with Snapchat is that a screenshot of the picture or video sent could be created and render the message shareable by uploading the screenshot onto an image hosting service (e.g. Imgur). In addition, remnants of Snapchat may be found on smartphones by companies such as Digital Mountain. Another service, Confide, has addressed the issue by circumventing the screenshot capability. For example, if a user has an iPhone, pushing the power button and home button simultaneously takes a screenshot; however, if the Confide application is open, that screenshot will be just a blank gray screen.

As for text-based messages, Confide uses a unique method of revealing messages within the application. Only one line of characters is displayed at a time, and to reveal the entire message, the user must swipe downward until the end of the message before it can be erased from existence. Confide also offers a retract upgrade, which allows the user to take back a message after it was sent.

The explosion of new messaging applications and ephemeral data creates interesting quandaries for organizations faced with discovery, as the architecture of these products was not designed for litigation holds. Emails stored in an encrypted state or linked to a hosted third party application make discovery more challenging and potentially costlier than traditional centrally controlled and managed email. If the encrypted email has not expired, making the email viewable to a third party may involve printing to PDF manually or other creative measures. These types of barriers may not have been considered by organizations when a secure communications solution was implemented. Current case law is still grappling with proportionality between duty to preserve and produce versus potentially burdensome costs. Organizations should consider if the dictum "*burn after reading*" could have ramifications down the road for its operations.

UPCOMING INDUSTRY EVENTS

June 2016
LegalTech West Coast, San Francisco: June 13-14

July 2016
The Masters Conference, Managing the E-Discovery and Social Media Minefield,
New York: July 19

August 2016
HTCIA 2016 International Conference & Training Expo,
Las Vegas: August 28-31

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: