

Application Breaches Are a Harbinger of Attacks to Come

by Robert (Bob) L. Kardell

The MOVEit, LastPass, and Microsoft breaches affected hundreds, if not thousands, of organizations across the United States. The breaches affected organizations of all sizes. These types of attacks were thoughtful, methodical, efficient, and effective and may just be a sign of future attacks.

MOVEit

For those unfamiliar with the service or the breach, the MOVEit software platform is a software-as-a-service offering by Progress Software.¹ The service allows users to move or transfer information securely using encryption. MOVEit is used by organizations as a means for customers, clients, or

vendors to share information securely. MOVEit may appear as a platform or service offered by the organization rather than Progress Software. Thus, companies may be unfamiliar with the name of the service or the developer and may not be aware they are using the service.

If reports are to be believed, the CL0P ransomware group identified a flaw in the MOVEit services in 2022.² The group then perfected their hacking techniques and tools for over a year before initiating the full attack. CL0P then used the identified flaw to attack the service and acquire as much information as possible in a short amount of time. The flaw itself was a type of SQL injection which would allow the perpetrator to view any of the documents stored in an identified MOVEit repository.

The CL0P group took as much information as they could in a very short period of time—sort of like a smash-and-grab. The group then began to review the information and extorting the affected companies. The affected companies are only now becoming aware that their information was stolen in a hack which occurred in May.

This type of breach was highly effective and extremely efficient because the group was able to acquire data from many different companies at once—one flaw, one hack, but many victims—as opposed to the traditional attack on one company at a time.

LastPass

The LastPass application allows users to save long, complex passwords in the application and access the information with the use of a “master” password. Users enter their master passwords, which then allows access all of their saved passwords. The advantages of such an application are that users can create complex passwords without having to remember all of them;

Robert (Bob) L. Kardell



Bob Kardell is an attorney whose practice focuses on cyber-breach incident response, legal and technology-based risk management solutions, technology and cyber-defense policy and protections, intrusion remediation, and fraud prevention and investigation. Bob has more than 22 years of experience working for the Federal Bureau of Investigation as a Special Agent. In his career,

Bob has also worked on cyber-crime investigations as well as public corruption, white collar, and financial criminal and civil investigations. Bob has been both a certified computer forensics examiner and an accounting forensics investigator. He has testified numerous times as a fact witness in criminal trials and before grand juries and drafted expert reports for both accounting and computer investigations.

TECH CORNER

the disadvantage is that losing control to the one master password means losing control of all of the passwords.

The LastPass breach was the result of a series of attacks³ late last year. The attackers were able to gain access to a trove of individual password vaults stored in the cloud. The company disclosed:

*unauthorized party gained access to a third-party cloud-based storage service, which LastPass uses to store archived backups of our production data.*⁴

The individual vaults were encrypted and protected by master passwords, but, in some cases, the master passwords were either not complex enough or the users' accounts had not been updated. The latest iteration of the software protects vaults with a more complex hash algorithm. Thus, had LastPass updated all of the accounts the master passwords may have protected the vaults.

Once the hackers gained access to LastPass's cloud storage, they downloaded the vaults. The downloading of the vaults to an off-line computer meant the attackers can attempt to brute-force the master passwords, or target the customers with phishing attacks. The attack has been attributed to a state actor, who has the time and resources to brute force the passwords of many of the vaults taken.

To make matters worse for LastPass, they admitted that the attack was carried out by targeting a developer's computer:

*This was accomplished by targeting the DevOps engineer's home computer and exploiting a vulnerable third-party media software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware. The threat actor was able to capture the employee's master password as it was entered, after the employee authenticated with MFA, and gain access to the DevOps engineer's LastPass corporate vault.*⁵

The attackers have been targeting users who kept cryptocurrency information in their LastPass account. Many users have alleged that LastPass was the only place they maintained their crypto-currency and therefore when their crypto wallets were found to be empty, LastPass is to blame. There has been a class action suit filed by LastPass crypto currency users in Massachusetts regarding stolen crypto currency.⁶

Microsoft

Microsoft most recently has been the target of two separate cyber incidents. The attack resulted in Microsoft losing control of a credential server.⁷ The loss of control means that the attack group can access any account protected by credentials issued by that server, which included some government organizations. The attack group is believed to be a government

sponsored organization who used the credentials to access government email accounts.

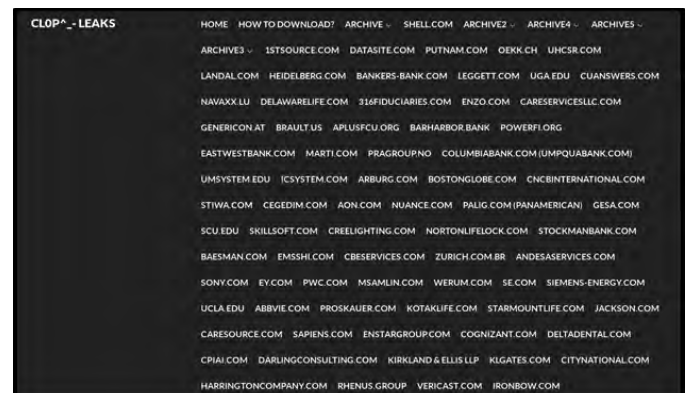
The second cyber incident involves a sharable, clickable link to view data stored on a Microsoft server. Microsoft apparently shared a link which exposed 38 TBs of information⁸ to anyone who had the link. The leak occurred in 2020 but was only recently reported. The information exposed includes Teams information and usernames and passwords. The full scope of the data lost is not yet known.

Third-Party Vulnerabilities

These breaches should cause everyone to assess the state of cybersecurity on their systems. If international tech companies in the business of protecting data can suffer data breaches, then can a small law firm be expected to secure its data against a nation-state actor?

These three breaches are also emblematic of how effective hackers have become at targeting high-value, commonly used applications. By targeting large repositories of information from many different companies, hackers have become very efficient at gathering data from a large variety of sources with one exposure or one vulnerability.

Below is a screen shot of the CLOP site:



The site contained over 250 individual organizations whose sensitive data was available for download. (Please take note that the CLOP organization provides a link to show “How to Download?”)

The breaches of MOVEit, LastPass, and Microsoft affect organizations of all types and sizes, and the effects have rippled through thousands of businesses and millions of affected individuals.

Steps to Security

Individual organizations may have painstakingly secured their data with firewalls, virtual private networks, multifactor authentication, risk assessments, and security plans, only to find out that their data is in the hands of international organiza-

TECH CORNER

tions is now at risk. How is a small or medium-sized company then to protect their data in the hands of vendors?

There are several steps companies can take to secure such information:

1. Regularly review where sensitive data is stored and move any unnecessary data offline.

The continuous accumulation of data in a cloud environment can quickly add up to gigabytes of information. This accumulation of information can create a greater risk of exposure if it is being maintained in online cloud platforms. If the data is no longer being accessed on a regular basis, consider moving the data to a physical drive, such as an external USB drive which can be stored in a bank safety deposit box or a fire-proof safe in the office. Removing the data from online access protects the data from hackers and nation-state hackers against whom an organization would have little to no recourse.

2. Regularly inventory online accounts.

Access to online accounts has become extremely common, especially in the legal environment. Law firms are required to share information using such services such as Box, Dropbox, OneDrive, iCloud, and online services such as Everlaw, Legal Zoom, UpCounsel, Relativity, Logikcull, Epiq Discovery, etc. A firm may be using one of these services to conduct e-discovery but may also have access to additional sensitive data because of services shared by another firm.

Take time on an annual basis to review and document access to each of these online portals. As cases settle, consider requesting deletion of access to the service or deletion of the account completely. Do not leave access to such services unattended. Such access is likely to become the target of hackers trying usernames and passwords exposed in other breaches.

3. Regularly review vendor agreements.


Vendor agreements for online services have become ubiquitous and are rarely, if ever, reviewed in detail. And, just when the review may be complete the vendor may update or change their terms of services with an email and another click-through agreement. Reviewing such agreements is necessary to determine who is responsible for the costs of a breach, security for the information, and notifying authorities and individuals in the case of a breach. If you are unsure who has that responsibility, then it is probably you. Consider LastPass' statement

regarding responsibility:

Because of the hashing and encryption methods we use to protect our customers, it would be extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices. (emphasis added)⁹

LastPass implies that users who do not follow their best practices are responsible for their data being accessed even though LastPass did not force older accounts to upgrade to the latest security techniques.

Conclusions

Organization's data can be at risk directly on a local server or workstation, but hackers are increasingly targeting common software platforms such as cloud storage. Law firms should take care to identify and secure any data, wherever it may reside. Do not wait for tech companies to secure data or to provide notification services in the case of a breach. Ultimately, security of the data and notification of individuals will be the responsibility of the user even if the tech company is at fault and the user has been diligently tracking, securing, and deleting data. While large international tech companies may be able to withstand the onslaught of hackers or the costs of providing breach notifications, such costs to a smaller organization can be devastating. 

Endnotes

- ¹ <https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability>.
- ² The flaws were assigned the Common Vulnerabilities and Exposure (CVE) numbers of: CVE-2023-35708 (June 15, 2023), CVE-2023-35036 (June 9, 2023), and CVE-2023-34362 (May 31, 2023). The reports of these flaws can be reviewed at the NIST or the MITRE organization's websites.
- ³ <https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/>.
- ⁴ *Id.*
- ⁵ *Id.*
- ⁶ <https://assets.law360news.com/1562000/1562534/https-ecf-mad-uscourts-gov-doc1-095111497456.pdf>.
- ⁷ <https://www.forbes.com/sites/betsyatkins/2023/07/18/microsoft-security-breach-a-wake-up-call-for-board-of-directors/?sh=26142b661c95>.
- ⁸ <https://techmonitor.ai/technology/cybersecurity/microsoft-leak-teams-azure-data>.
- ⁹ <https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/>.