Are you a victim of the MOVEit breach?

So what is the MOVEit ransomware attack and how has it affected so many people? Are you one of the 62 million people affected by the MOVEit breach?

The MOVEit breach was one of the biggest hacks of 2023, with the Clop ransomware group ransoming thousands of organizations and taking tens of millions of dollars.

What is MOVEit?

MOVEit is secure file transfer software and service developed by Progress Software, designed to facilitate the secure transfer of sensitive data between organizations and individuals. MOVEit is used by businesses, government organizations, universities and basically any organization that stores and manages its data, allowing companies to securely transfer files and data. secure to protect them from unauthorized access or violation.

However, in May 2023, the Clop ransomware group attacked thousands of organizations that were using MOVEIt to obtain their data.

How did the MOVEit breach occur?

In May 2023, the notorious ransomware group Clop exploited multiple zero-day vulnerabilities in the MOVEIt application.

A zero-day vulnerability is a software security vulnerability that is unknown to the vendor or the public and is exploited by attackers before a fix or patch is available. Zero-day vulnerabilities are especially dangerous because they can be secretly exploited without the vendor's knowledge for a very long time.

Progress Software eventually patched these vulnerabilities, but it was too late. During the time the vulnerability was unknown to the public and vendors, attackers accessed and breached the data of thousands of organizations that used MOVEit to manage and transfer their data.

The Clop ransomware group discovered multiple SQL injection vulnerabilities in the MOVEit application, allowing them to access organizations' databases and download and view data. SQL injection is a vulnerability in which malicious SQL code is inserted into input fields, exploiting vulnerabilities in database-based applications. Unauthorized code can manipulate the database, potentially revealing or altering sensitive information.

The discovered SQL injection vulnerabilities are CVE-2023-34362, CVE-2023-35036, and CVE-2023-35708, patched on May 31, 2023, June 9, 2023, and June 15, respectively 2023. All versions of the MOVEit transfer application have this vulnerability. When exploited, it allows an unauthenticated attacker to gain access to the contents of an organization's MOVEIt transfer database. This means that an attacker can download, change or even delete the database without any restrictions.

Impact of the MOVEit breach

According to Emisoft's analysis and statistics related to the MOVeit data breach, as of November 9, 2023, 2,659 organizations were affected by the MOVeit breach and more than 67 million people became victims, which organizations are primarily based in the United States and Canada, Germany, and the United Kingdom.

Education was the sector hardest hit, with data from many universities stolen by these attackers. Educational institutions affected by this breach include the New York City public school system, John Hopkins University, University of Alaska, and Webster University, along with many other prominent universities. Other sectors greatly affected by this breach include the healthcare industry, banking, financial institutions, and businesses.

Some of the famous organizations affected by MOVEit ransomware include BBC, Shell, Siemens Energy, Ernst &Young and British Airways.

On September 25, 202, the leading prenatal, infant and child registry service, BORN Ontario, released a statement regarding the MOVEit breach, revealing that they were affected by the breach. MOVEit. According to their report, the MOVEit vulnerability allows malicious third-party actors to illegally access and copy personal health information files contained in BORN Ontario records, which were transferred using secure file transfer software. full.

In response, Born Ontario immediately isolated the system, shut down the affected server, and launched an investigation, collaborating with cybersecurity experts to determine the severity and specific data. has been stolen.

Many of these organizations were attacked not because they used the MOVEit app, but because they sponsored third-party vendors that used the MOVEit transfer app, leading to them being breached as well. The same situation happened to other organizations, costing billions of dollars in ransomware payments and other security fixes.

If you have been affected by the MOVEit breach, what to do next?

If you are still using MOVEit, update to the latest version immediately to prevent your files and data from being stolen by hackers.

Unfortunately, the Internet and the software that uses it are vulnerable to hacking and ransomware attacks, and you must keep yourself and your assets safe by changing your passwords regularly, using anti-virus software, and using anti-virus software. virus and enable multi-factor authentication.

But as the MOVEit breach shows, even though you can do all that, hackers will constantly find new exploits.