



SOLUTION BRIEF

**MOVEit Vulnerability**

# MOVEIT VULNERABILITY

## DNS Attacks and How to Detect Them

Every day, threat actors attempt to exploit vulnerabilities present in your IT environment. In recent weeks, a vulnerability in the MOVEit file transfer system has been a top news story. Government agencies and large enterprises have seen zero-day attacks and found that their networks have been compromised by threat actors.

Throughout this white paper, we will delve into the specifics of the MOVEit zero-day vulnerabilities, exploring the potential consequences, and showcasing how Plixer's solutions can mitigate the risks of a cyberattack. By empowering your team with this understanding, you will become more adept at protecting sensitive data and fortifying your customers' security posture.

## WHAT IS THE MOVEIT VULNERABILITY

MOVEit is a file transfer system developed by Progress Software Corporation that provides a secure and automated way to transfer sensitive data. It's primarily used for sharing files within a team, department, or even across a company's supply chain. Its functionality relies on a web-based front end, which makes it easy to share and manage files using a web browser, a process generally considered less prone to misdirected or "lost" files than sharing them via email.

However, the recent zero-day exploits have shown that MOVEit's web-based front end has an SQL injection vulnerability. SQL injection is a code injection technique that attackers use to exploit vulnerabilities in a web application's database query software. When an attacker successfully performs a SQL injection, they can manipulate the application's SQL queries to execute arbitrary SQL code and potentially gain full access to the application's database.

In the case of the MOVEit exploit, attackers were able to inject rogue commands into the SQL back end

databases of the MOVEit system. This allowed them to perform a range of harmful actions, such as:

**Deletion of existing data:** The attackers could delete important data from the system, potentially causing significant disruption and damage.

**Exfiltration of existing data:** Instead of deleting data, attackers could also extract and steal data from the system.

**Modification of existing data:** Attackers could alter existing data in the system, causing further disruption and confusion.

**Implantation of new files, including malware:** The attackers could inject malicious code into the system that could further compromise the network or spread the attack to other systems.

It's worth noting that one group of attackers linked to the infamous CIOp ransomware gang were found to be using this vulnerability to implant what are known as webshells on affected servers. Webshells are malicious scripts that attackers use to maintain access and control over compromised servers. Once an attacker has successfully implanted a webshell on a server, they can execute a wide range of commands



remotely, effectively giving them control over the server.

For the most part, these actions happen in the background, invisible to users unless they are specifically looking for signs of a breach or have detection systems in place to identify these types of attacks.

## TECHNICAL POINT OF THE MOVEIT VULNERABILITY

The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. The activities related to the MOVEit exploit and the subsequent use of webshells can be mapped to several techniques within this framework.

**1. [Exploit Public-Facing Application \(T1190\)](#):** This is the initial attack vector, where the attackers exploited a zero-day vulnerability in the MOVEit file transfer software.

**2. [Command and Scripting Interpreter: SQL \(T1059.005\)](#):** The SQL injection vulnerability in MOVEit's system aligns with this technique. Attackers could inject rogue SQL commands to manipulate the system.

**3. [Server Software Component: Web Shell \(T1505.003\)](#):** The attackers installed webshells on compromised servers to maintain access and control, which corresponds to this technique.

**4. [Data Destruction \(T1485\)](#), [Data Encrypted for Impact \(T1486\)](#), [Data Manipulation \(T1565\)](#):** These techniques could potentially be used by attackers once they have access to the system via the webshell.

**5. [Exfiltration Over C2 Channel \(T1041\)](#):** If the attackers use the webshell to exfiltrate data, it would fall under this technique.

It's important to note that the specific techniques used can vary with each attack, even when the same vulnerability is being exploited, as it depends on the goals and methods of the individual attacker or group.

One group of attackers, linked to the infamous Clop ransomware gang, were found to be using this vulnerability to implant webshells on affected servers. This would give the attackers ongoing access to the compromised servers, even after the initial breach had been discovered and addressed. From these compromised servers, the attackers could then execute a wide range of commands remotely, giving them control over the server and potentially the wider network it is a part of.

So, while webshells are not a feature or aspect of MOVEit itself, they are a tool that was used by attackers exploiting a vulnerability in MOVEit's software to maintain access to compromised systems and carry out further malicious activities.

A webshell is a malicious script used by attackers that enables remote administration of a machine over a network. Essentially, it provides a back door that allows attackers to maintain access to and control over a compromised server.

Webshells are usually injected into a server through vulnerabilities in web applications, and they can be written in any language that the target web server supports. This includes, but is not limited to, PHP, ASP, Java, and Perl.

Once a webshell is installed, an attacker can execute a wide range of commands remotely. These can include actions such as viewing, editing, deleting, or downloading files; executing shell commands or scripts; sending emails; or even launching distributed denial of service (DDoS) attacks from the



compromised server. In some cases, webshells are used to further compromise the network by deploying additional malware or exploits.

Detecting webshells can be challenging because they often use obfuscation techniques to hide their presence, and they can be embedded within legitimate files or mimic the names of system files. Network monitoring, file integrity checks, and regular security audits are key strategies for detecting and removing webshells.

## WAYS TO LESSEN THE IMPACT OF MOVEIT VULNERABILITY EXPLOITS

In light of the recent MOVEit zero-day exploit, companies can take several steps to safeguard their systems:

**1. Patch Management:** Ensuring that all software, including MOVEit, is up-to-date with the latest patches is a crucial first step. As soon as a patch is available, it should be applied immediately to reduce the window of opportunity for attackers.

**2. Network Traffic Monitoring:** Given that some companies may already be infected internally without knowing it, it's essential to monitor network traffic for abnormal behavior. Unusual network activity can be a sign of an active breach or an indication of a compromised system within the network.

**3. Implementing a Security Awareness Program:** Employees should be educated about the risks of cyber threats and how to recognize them. This includes being cautious about clicking on links, opening attachments, and understanding how data breaches can occur.

**4. Using Firewalls and Antivirus Software:** Firewalls can help protect your network by controlling internet traffic coming into and flowing out of your business. Antivirus software can often detect and remove malware before it causes damage.

**5. Regular Backups:** Regularly backing up important data ensures that, in the event of a data breach or loss, your business can restore the data from a point prior to the incident.

Taking these steps can significantly reduce a company's risk of falling victim to cyberattacks like the recent MOVEit exploit.

## HOW TO MONITOR FOR MOVEIT VULNERABILITY EXPLOITS

NetFlow and IPFIX are network protocols used for collecting IP traffic information. These protocols provide a way of understanding what traffic is passing through an interface on a network device, such as a router or a switch. The collected data can then be analyzed for network planning, security, and operational purposes.

In the context of detecting an exploitation of a vulnerability like the one found in MOVEit, NetFlow or IPFIX could be useful in the following ways:

**1. Detecting Unusual Traffic Patterns:** NetFlow and IPFIX data can be used to establish a baseline of normal network behavior. Any significant deviation from this baseline, such as a sudden increase in data being transferred or connections being made to unfamiliar IP addresses, could be an indication of malicious activity.

**2. Identifying Data Exfiltration:** One of the potential outcomes of the MOVEit exploit is data exfiltration.



NetFlow and IPFIX data can help detect this by identifying large amounts of data being transferred to an external IP address, particularly if the data is being sent to an IP address or a geographical location that is not normally associated with the organization's network traffic.

### **3. Detecting Unusual Source And/Or Destination Relationships:**

In a SQL injection attack, the attacker might make connections to unusual destinations, such as unfamiliar databases. If the NetFlow or IPFIX data shows connections being made to unfamiliar or suspicious IP addresses, it could be an indication of such an attack.

### **4. Observing Network Behavior Over Time:**

NetFlow and IPFIX data can be collected and analyzed over time, which can help identify trends and patterns in network behavior. This long-term analysis can be useful for identifying slow, low-and-slow, or otherwise stealthy attacks that might not be immediately obvious.

### **5. Leveraging Threat Intelligence:**

NetFlow and IPFIX data can be correlated with threat intelligence information to identify connections to known malicious IP addresses or domains. If the data shows connections being made to an IP address or domain that is known to be associated with malicious activity, it could be an indication of a compromise.

It's important to note that while NetFlow and IPFIX can provide valuable data for detecting potential compromises, they are just one part of a comprehensive security strategy. They should be used in conjunction with other security measures, such as intrusion detection systems, firewalls, and antivirus software.



## SUMMARY

While the MOVEit vulnerability is a new vulnerability that attackers are exploiting, the tactics and techniques used are common to many other attacks. By using a network security solution that does not use signature but does use ML to process traffic and detect anomalies, you can detect threats like the MOVEit vulnerability as well as other DNS exploits.

Don't leave yourself exposed to threats hiding in your network. Plixer helps you rapidly detect and neutralize critical threats in real-time. With advanced AI and machine learning, you can identify, prioritize, and respond with laser precision and accuracy. With Plixer you get 90% less noise from false positives, an 80% reduction in investigation time, a 47% increase in threat neutralization accuracy, and a 40% cost-efficiency compared to other NDR solutions.


Join the new network defense revolution today and [book a demo](#).

## ABOUT PLIXER

Plixer gives you visibility and context of every network transaction so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. Supercharge your business defense with AI-powered visibility and insight that goes beyond traditional NDR.

 [sales@plixer.com](mailto:sales@plixer.com)

 [plixer.com](https://plixer.com)

 68 Main St Ste 4  
Kennebunk, ME 04043



©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.