ANALYZING ADVERSORY ATTACK ON MOVEIT FILE TRANSFER APPLIACTION

Course: CIS*6530 Cyber Threat Intelligence and Adversarial Risk Analysis

PRESENTED BY-

ADITI VENKATESH (1302387)

SHREYA BHOJE (1301655)

UNIVERSITY of GUELPH

CONTENTS

- Introduction
- Objective
- Terminologies
- The Attack Process
- Solutions
- Conclusion

INTRODUCTION

What is MOVEit Transfer?

- Secure file transfer application for businesses and enterprises
- Helps transfer sensitive files such as financial or medical records

UNIVERSITY of GUELPH

Who is TA505?

- Advanced Persistent Group, certainly speaking Russian, active since at least 2014
- Also known as Cl0p
- Financially driven
- Changing use of malware, malware distribution, ransomware campaigns

BIGGEST HACK OF THE YEAR

60M+

IMPACTED INDIVIDUALS

1000+

IMPACTED ORGANIZATIONS

$100M

EXPECTED REVENUE OF CL0P

TERMINOLOGIES

ZERO DAY VULNERABILITY

Newly found flaw for which there is no security patch and which is unknown to the impacted vendor

ZERO DAY VULNERABILITY ATTACK

Result of zero day vulnerability exploitation

SQL INJECTION

Manipulating the execution of predefined SQL commands by inserting SQL commands into input data allowing unauthorized access to database

WEBSHELL

Segments of code crafted in various scripting languages, and they are uploaded onto web servers following the exploitation of injection vulnerabilities

THE ATTACK PROCESS

CVE-2023-34362

- Zero day vulnerability
- SQL Injection vulnerability
- Potentially enable an unauthenticated attacker to access and manipulate a business's database

LEMURLOOT

- Custom web shell written in C#
- Execute commands to download files from the MOVEit Transfer system to gather information on database
- Access comprehensive record information, create insert, or delete a specific user,
- Authenticate incoming http requests using a hard-coded password

UNIVERSITY of GUELPH

- Scanning for Windows servers
- Utilized internet indexing services like Shodan or port scanning techniques
- Tactic: Reconnaissance — Techniques: Gathering victim network information [T1590]

- Lemurloot: Mimics human.aspx from MOVEit Transfer
- Tactic: Initial Access —Techniques: Exploit Public-Facing Application [T1190]

Tactic: Defense Evasion —Techniques: Masquerading [T1036]

- Installing the LEMURLOOT web shell on MOVEit Transfer web applications is vulnerable to the CVE-2023-34362 vulnerability
- Tactic: Command and Control— Technique: Ingress Tool Transfer [T1105]

- SQL injection vulnerability to execute commands
- Install the LEMURLOOT web shell on the targeted system, gaining unauthorized access and control
- Tactic: Execution —Techniques: Execution through API [T1202]
  Tactic: Collection — Technique: Data from Local System [T1005]
  Tactic: Discovery — Technique: System Information Discovery[T1082]

- The installation of the webshell served the purpose of maintaining persistance by evading being detected, data collection and perform data exfiltration.
- Tactic: Persistence — Technique: Scheduled Task [T1053]

  Tactic: Collection — Technique: Data from Local System [T1005]

  Tactic: Discovery — Technique: System Information Discovery [T1082]

  Tactic: Defense Evasion — Technique: Obfuscated Files
or   Information [T1027]

- The web shell established communication channels with the attackers, allowing them to control the compromised system and issue commands
- Tactic: Command and Control — Techniques: Multi-stage channels [T1104]

- The adversary executed a range of malicious activities, including obtaining Microsoft Azure system configurations, enumerating the SQL database, storing and retrieving files, generating administrator accounts, and deleting specific user accounts
- Tactic: Exfiltration — Technique: Exfiltration Over C2 Channel, [T1041]

Tactic: Collection — Technique: Data from Local System [T1005]

SOLUTIONS

To strengthen their organization’s security posture in reaction to threat actors' actions, the authoring agencies advise organizations to put the mitigations and prevention.

Mitigations

- Stop additional exfiltration is closing off Hyper Text Transfer protocol (HTTP)and HTTPs data traffic, both inbound and outbound, modify firewall rules to prevent receiving traffic from HTTP and HTTPs on port 80
- Administrators can still access MOVEit Transfer by connecting to the Windows device via remote desktop and going to https://localhost/

Prevention

- Using security software
- Implement application control
- Strictly limit the use of RDP and other remote desktop services
- Restrict use of PowerShell, etc.

CONCLUSION

On analyzing this attack we found:

- TA505 focused on targeting the service instead of targeting a industry for financial gain
- Using third party tools comes with security and the organizations should make sure to keep the software up to date and have an rapid incident response plan ready.

UNIVERSITY of GUELPH

Q&A