TOP 8 WAYS HACKERS WILL EXFILTRATE DATA FROM YOUR MAINFRAME

In previous blogs I have already illustrated the various ways hackers will gain initial access to your mainframe and how they will execute a privilege escalation attack to gain full control over the system. Once a threat actor completely owns the mainframe, they will have complete access to the sensitive data that resides on it. While ransomware has created a scenario where hackers no longer need to exfiltrate data to profit off their cybercrime, theft of sensitive data is still a catastrophic risk to companies who face increasingly punitive fines and loss of customer trust.

This blog will focus on the top ways hackers will exfiltrate the sensitive data from your mainframe. This knowledge is critical in order to understand how to initially protect your system and effectively detect anomalous and malicious activity in time to respond to the breach. My goal is to help you have an answer to the following questions:

1. Is this possible on my mainframe?
2. Do I have alerts built for Indicators of Compromise (IOC) for each of these activities?

Mainframe Data Exfiltration Techniques

1. Hackers are going to use native tools available on the system before getting to more complex methods – especially if those tools are also ubiquitous on Windows/Linux where most will be more familiar. Since the primary method of initial access to most machines is compromised account credentials, hackers could simply use those credentials with Secure Copy (SCP) to

copy the files over the Secure Shell (SSH) protocol.
2. If SSH isn't available, hackers could also use the File Transfer Protocol (FTP) to easily download any files they are authorized to access on the system. FTP also makes it easy to upload/download files in bulk and can even be used in Job Entry System (JES) mode to execute commands on the mainframe.
3. The next tool designed to transfer files is the Network File Share (NFS) which is a distributed file system found in Linux that enables a hacker to "mount" the filesystem and download any files off the mainframe.
4. Another file transfer protocol that is built directly into the mainframe is IND$File which only requires a typical TN3270 connection and compromised credentials to simply download any file they are able to access. This one is harder to monitor as IND$FILE does not write a default SMF record.
5. The last native tool that hacker could weaponize to exfiltrate data is the Network Job Entry (NJE) protocol which is designed to transfer commands, messages, and jobs to the multiple systems in a network. Since the systems are already communicating, a hacker can use NJE to send any of the data it wants to exfiltrate to a separate system under their control.
6. Before getting too creative, hackers have one last capability available to them that is often overlooked. They could easily browse the datasets they are interested in and copy/paste the data onto their personal system. This is obviously limited to smaller quantities of data, or a tremendous amount of patience, but can be extremely useful if stealing small valuable components like usernames and hashed passwords for new accounts or encryption keys.
7. If hackers are looking to avoid standard file transfer mechanisms, they may look to build their Command and Control (C2) channel. This could be done quickly using socket tools like Netcat or more advanced by bringing over C code and compiling its own communication protocol. While this bypasses most typical tracking mechanisms on the mainframe, IOCs that are designed to search for anomalous port activity should quickly spot rogue C2 channels to the mainframe.
8. The last popular method for hackers is to upload the files to a cloud storage container they control. Using java, a hacker could quickly connect the mainframe to an S3 bucket on Amazon and upload all of the sensitive data outside the organization.

Shutting down all of these methods on the mainframe is a somewhat impossible task when you consider how important many of these protocols are to basic operations. This necessitates the ability to filter and monitor user behavior in real-time in order to detect anomalous user activity and ultimately catch the exfiltration of data before it is catastrophic. Hackers will continue to make this harder on the Security Operations Center (SOC) by hiding their exfiltration activity in normal scheduled activity, breaking a large heist into smaller chunks, or deliberately using methods which don't leave normal logs. These methods are not unique to the mainframe and are all detailed in the MITRE ATTCK Framework to guide your User Entity Behavior Analytics (UEBA) program.

Ultimately, visibility and automation are key factors to help ensure these forms of attack don't impact your mainframe systems. That's why BMC is committed to helping our clients build a modern mainframe security program with BMC AMI Security. AMI Security automates detection and response on mainframes while integrating the platform into the SOC's tools and processes. If you'd like to know more or have questions about the steps to effectively secure your mainframe environment, please contact Christopher_perry@bmc.com or visit BMC Software for more information.

https://www.bmc.com/blogs/top-6-ways-a-hacker-will-gain-access-to-your-mainframe/
https://www.bmc.com/blogs/top-10-privilege-escalation-hacks-for-the-mainframe/
https://enterprise.verizon.com/resources/reports/dbir/
https://kellgon.com/netcat-the-hackers-swiss-army-knife/
https://attack.mitre.org/