Mainframe Hacks

Why it’s rarely reported in the news—and how you can keep it from happening to you
Table of Contents

04  Introduction

04  Is No News really Good News?

05  Real-world Mainframe Attacks

06  What You Can Do to Keep Cybercriminals Out of Your Mainframe

07  Don’t Let the Untold Story Happen to You
Mainframe Hack Leads to Massive Data Breach at US Financial Services Company

Ami Custodio, January 2021

In a stunning attack, a cybercriminal recently compromised the mainframe of a large U.S.-based financial services firm and downloaded all of the sensitive data on its mainframe. While the full scope of the attack is not yet known, the stolen data may have included personally identifiable information (PII) of customers such as names, account numbers, PIN numbers, and credit card information.

“This incident has been a wake-up call for our organization, as it should be for every business with a mainframe.”

The method used in the hack was clever, if not especially sophisticated. Rather than attacking the mainframe directly, the hacker targeted the firm’s Active Directory server. Once administrative credentials had been obtained, they were used to gain access to other enterprise platforms, including the mainframe, via secure shell protocol (SSH). Having logged onto the mainframe, the hacker used standard UNIX commands to look for unprotected properties files, and found a file that was world-readable. This contained a username and password for data on the firm’s mainframe. At this point, it was a simple matter to use these credentials to connect with the mainframe via a Windows ODBC/JDBC client and offload a significant amount of the firm’s mainframe data.

The firm now faces potential fines for non-compliance with data privacy regulations such as PCI DSS, GDPR, and CCPA, while its customers are now vulnerable to financial fraud, identity theft, and other related crimes. The reputational damage to the firm is expected to be severe.

“The attack appears to have gone undetected for approximately 3 – 4 months,” said the company’s Chief Information Security Officer. “Customers have been notified and a full investigation is underway to uncover the full scope of the attack. We will also undertake a comprehensive review of our mainframe security measures to better understand how and why the attack succeeded. This incident has been a wake-up call for our organization, as it should be for every business with a mainframe.”

At the time of this story, it is unclear what countermeasures or defenses were in place that could have prevented the attack or why the attack was unable to remain undetected. The Chief Information Security Officer stated that “A member of our operations team noticed some unusual activity and thankfully took the initiative to investigate. If they hadn’t been looking who knows how long access would have remained.”

We will continue to follow this story and share updates as more details emerge.
Introduction

If this story doesn’t sound familiar to you, there’s a good reason for that: you may rarely read an account like this in the press. But make no mistake: these events do happen. We know, because BMC Software has been involved in their remediation after the fact. In fact, the method described above is taken directly from an actual real-world incident.

To protect the company involved we have kept names and details anonymous. But we do want to help more companies avoid finding themselves in this situation. In this white paper we’ll talk about the often silent nature of mainframe hacks, a few of the forms they can take—and how you can keep it from happening to you.

Is No News really Good News?

Make no mistake, the mainframe is a prime target for cybercriminals. A workhorse of modern business due to its efficient, reliable data access and transaction processing at massive scale, mainframes play a central role in the daily operations of most of the world’s largest corporations, including banking, finance, healthcare, insurance, and many other types of enterprises. As a result, the platform holds a vast amount of critical—and valuable—data.

In many cases, the mainframe is underprotected, due in part to the longstanding misperception that the platform is inherently secure. In a recent Forrester Consulting study commissioned by BMC Software, 82 percent of security decision-makers said that the mainframe is very or extremely secure. But the same study found that only 41 percent are taking the steps needed to actively secure the mainframe—and over 80 percent said they have the right tools but still experience major security events.

While it is indeed highly securable, at the end of the day the mainframe is just another device connected to a network with privileged users and remote connections, and it can be attacked just like any other device. Organizations still need to take an active approach to protection including measures such as vulnerability scanning, penetration testing, and security audits. But many don’t, resulting in a target that’s both rich and all too vulnerable.

So why don’t we hear about more mainframe hacks in the news? To be fair, some do appear. Like the time South Africa’s Postbank lost more than $3.2 million USD from fraudulent transactions after employees printed out and then stole its 36-digit encryption master key. Or when an Australian 13-year-old hacked into Apple’s mainframe and downloaded internal documents and data. But many, many more incidents go unreported. For one thing, there’s no requirement to disclose the systems involved in an attack. And many security teams may be reluctant to admit that their complacency about mainframe security had left it underdefended compared with other enterprise systems. In some cases, such as the one described above, the attack itself might not have been mainframe-centric—even if its data ended up being stolen.
Real-world Mainframe Attacks

The fact is mainframe attacks do occur. Although not as public as others in the media, they do occur and confidence in the network perimeter or the mainframe's perception as invulnerable are misplaced. The victims in the incidents below have been anonymized but the following are real-world cases of attacks involving mainframes.

Brute force succeeds against a large U.S. financial services firm
Unlike the indirect method described at the beginning of this paper, in this case a large U.S. financial services firm's mainframe was targeted directly using a combination of user ID brute-forcing and simple password stuffing. The firm had failed to turn on TSOPREPROMPT, which would have allowed for enumeration of valid TSO IDs. As a result, the hacker was able to assemble a list of roughly 10,000 TSO IDs, and then use a password spraying script to try one or two common passwords across each ID. Multiple privileged IDs were found to have one of the passwords attempted, and these were then used to log onto the system with elevated privileges.

Default passwords sink a major global financial services firm
In an all-too-common type of incident, this firm fell into the dreaded default credentials trap. The victim was running multiple instances of Apache Tomcat open-source software that had been installed as part of an overall software package from a Z software vendor. Neither the vendor nor the firm changed the default credentials which had been enabled on Tomcat, making it simple for the attacker to log on and upload malicious JAR/WAR files. These files then provided the attacker with a shell running at the privileges of the Tomcat tasks, which were privileged.

Unsecured NJE leaves a large insurance firm vulnerable
The Network Job Entry (NJE) application was running on the firm's mainframe without line passwords or encryption. As a result, the attacker was able to sit in a privileged network position on the firm's internal network and sniff mainframe-to-mainframe NJE traffic and gain the node IDs for each of the endpoints. Next, the attacker used TCP RST/FIN to reset the NJE connection and impersonate one of the endpoints, connecting from their Windows machine to the target mainframe. From this trusted node, the attacker was able to run JCL as any user on the target system and enact a full-system compromise.

A shady developer dupes a major European bank
A mainframe developer working for a major European bank discovered a bug in his client's banking application—for which he also provided out-of-hours support. It was a simple matter to set up fake transactions creating accounts with an overdraft facility. The developer then transferred money from these fake accounts into a real account belonging to an accomplice, who ultimately reaped roughly £1M GBP in ill-gotten gains.

This is just a handful of the many cases that occur. The real number will likely never be known—what does matter is whether it can happen to you. If it did, would you have a way of detecting an attack in progress? How long would it take to alert the right people and take effective countermeasures?
What You Can Do to Keep Cybercriminals Out of Your Mainframe

There’s no silver bullet to stop cyberattacks. Rather, effective defense depends on comprehensive measures to prevent, detect, and respond to attacks before they put sensitive data at risk. As part of your strategy, BMC Software recommends the following best practices.

Bring mainframe data into your Security Operations Center (SOC)
A siloed approach to mainframe and distributed security can make it more difficult to detect a cross-platform attack like the one described at the beginning of this paper. Instead, your SOC should provide a complete, unified view across all your systems, including SIEM data generated by the mainframe, so your team can catch suspicious activity before an attack can spread.

Report on mainframe security events in real time
Nightly or weekly mainframe reporting leaves far too much time for data exfiltration to proceed. Your SIEM should automatically alert security admins and support staff in real time if anomalous behavior is detected.

Enable automated detection and response to threat events
A shortage of mainframe skills and resources can leave the mainframe highly vulnerable to zero-day threats, configuration weaknesses, and attacks like ransomware. Automation can help you detect and respond to threats, aid compliance, and reduce risk quickly without the need for specialized mainframe expertise. Automatic responses based on real-time behavioral analytics can halt suspicious and known malicious actions before they can disrupt your mainframe environment or put sensitive data at risk.

Zero in on indicators of compromise (IOC)
To catch potential cyberattacks in progress, your security event management system should look for breach markers such as:

- Port scanning
- Repeated failed password attempts
- Anomalous activity of privileged users
- Escalation of user privilege
- Incidence of probing

Implement real-time file integrity monitoring (FIM)
By automatically monitoring the state of your operating system for changes to an established baseline, you can detect signs of a possible intrusion. Even something as simple as a timestamp change to a file or folder can help you stop a zero-day threat as it emerges.

Monitor privileged users
Privileged users have unrestricted access across your most valuable IT asset. Make sure they’re actively monitored and set up alerts based on correlation rules to identify anomalous activity.

Test response readiness
All too few organizations have an effective cybersecurity incident response plan—and even fewer test them regularly. As you implement your mainframe defense strategy, make sure to implement regular testing to make sure that in the event of a breach, employees will know their roles and be able to perform them under pressure.
Educate employees
From poor password hygiene to careless email downloads and phishing gullibility, human error is a common thread across many successful attacks. Train employees regularly on cybersecurity best practices and reinforce the message with ongoing communications, signage, and refresher sessions. Nobody wants to be the one who allows their company to be a victim.

Don’t Let the Untold Story Happen to You

More organizations have suffered mainframe hacks than we’ll ever know about. Don’t let yours be one of them. By taking an active approach to mainframe security, you can keep the sensitive data on your mainframe out of the hands of cybercriminals—so you’ll have nothing to keep quiet about.

For more information
Want to know if you’re vulnerable to one of the attack methods above? Connect with a Mainframe Security Expert

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent www.bmc.com