STAYING AHEAD OF RANSOMWARE, PART I: NORMALCY BIAS AND INITIAL ACCESS

What one word gets any IT professional's attention in 2021? Ransomware**.** In this blog series, we will explore best practices for stopping ransomware **before** it happens and before an organization needs to activate its backup and recovery plan.

For good reasons, backup and recovery capabilities headline the ransomware security discussion, with many IT teams asking how they can check their backups for integrity, better secure them, and test recovery plans. While these are important questions, ransomware discussions must also include the topics of prevention and detection. What can we do to stop ransomware from happening in the first place, and how can we stay ahead of adversaries targeting the mainframe?

Before we dive into prevention and detection, let's address some "elephants in the room."

Normalcy Bias

Some readers who are more experienced with the mainframe might be saying, "But ransomware has *never* happened on the mainframe!" or "But ransomware *would never happen* on the mainframe!"

First of all, ransomware *has* happened on the mainframe.

Secondly, when I thought about this a concept came to mind - **normalcy bias.** Normalcy bias (or normality bias) is the assumption that since a disaster never has occurred, it never will occur. **This can result in the inability of people to cope with a disaster once it occurs.** Normalcy bias leads to

difficulties reacting to something never experienced before, whether it's ransomware or some other intrusion. It can cause people to interpret warnings in the most optimistic way possible, seizing on ambiguities to infer a less-serious situation.

Wikipedia adds that normalcy bias is:

"...a cognitive bias which leads people to disbelieve or minimize threat warnings. Consequently, individuals underestimate the likelihood of a disaster, when it might affect them, and its potential adverse effects. Normalcy bias causes many people **to not adequately prepare** for natural disasters, market crashes, and calamities caused by human error."

Examples of normalcy bias throughout history include:

- Experts connected with the Fukushima nuclear power plant were strongly convinced that a multiple reactor meltdown could never occur.
- Officials at the White Star Line made insufficient preparations to evacuate passengers on the Titanic and passengers refused evacuation orders, because they underestimated the odds of a worst-case scenario and minimized its potential impact.
- When the volcano Vesuvius erupted, the residents of Pompeii watched for hours without evacuating.

In the context of normalcy bias, is a security "disaster" like a ransomware attack on the mainframe any different from the examples above? Mainframe operators and systems programmers are often strongly convinced that unauthorized intrusions, let alone ransomware, aren't possible on the mainframe and "could never occur." Mainframes often have been insufficiently prepared to prevent or detect threats as serious as ransomware because administrators have underestimated the odds of a worst-case scenario occurring.

The threat of ransomware does not discriminate by platform, and security by obscurity is only one layer of security.

With that, let's dive into our first ransomware enabler on the mainframe: **initial access**. In the coming weeks, we'll discuss additional prevention and detection mechanisms like privileged access management, dataset monitoring, and others.

Preventing and Detecting Initial Access

MITRE defines initial access as "techniques that use various entry vectors to gain their initial foothold within a network." Simply put, adversaries cannot execute code or run ill-intended jobs on the mainframe unless they gain internal access. This sounds self-evident, but if the solution was as simple as, "just stopping them from getting in," there wouldn't be so many intrusions today. Something is clearly missing.

Many people would suggest that brute force tools won't work on the mainframe, but a quick search for "TSO brute force" returns "TSO Brute – The z/OS TSO/E logon panel brute forcer." According to the script's author, "Because the logon panel for TSO/E tells you if you have a valid user account vs a valid/invalid password, you can enumerate users. Since you can enumerate users adding a brute forcer was trivial."

So, why are so many mainframes still relying on password-based authentication?

Credential Re-use and Multifactor Authentication (MFA)

One of the most vulnerable initial access vectors on the mainframe is credential re-use. However, attackers cannot re-use credentials when there is an effective MFA implementation. If you want to stop ransomware before it starts, the best thing you can do is implement and enforce MFA to ensure attackers are not exploiting the "low hanging fruit" in your environment, such as weak passwords or compromised credentials. Simply put, MFA is the most effective way to stop an initial attack on the mainframe.

Initial Access Monitoring

An attacker cannot ransom a mainframe if they cannot get in – full stop. It bears repeating that MFA stops the initial attack and attackers cannot re-use credentials when there is an effective MFA implementation!

Lastly, implement security software which detects and alerts on anomalous logon activity such as password spraying attacks and brute force attempts. A potential brute force attack is an Indicator of Compromise (IOC) indicative of a compromised system on the network attempting to pivot into the mainframe. The same goes for a password spraying attack. If a host on your network is attempting to legitimately access your mainframe and you can detect this in real-time, this provides your security operations team with ample time to investigate and/or remediate the host in question.

The bottom line is initial access attempts should be closely monitored and audited. However, it is nearly impossible to do this in real time without automated detection. BMC AMI Security can monitor and alert you to anomalous logon activity in real time, so you know precisely when someone is attempting to access your mainframe or has done so.

For the next part of our series, we will discuss how privileged access management (PAM) is essential in stopping ransomware before it happens.