STAYING AHEAD OF RANSOMWARE, PART 3: SENSITIVE DATASET ACCESS AND DECEPTION

When monitoring sensitive datasets, our customers commonly ask, “What else should I be monitoring on my mainframe?”

Some of the “usual suspects” to monitor are:

- Enterprise service management (ESM) datasets
- ROC/PARMLIBS
- Encryption keys
- Authorized program facility (APF)-authorized libraries

Users often have a general idea of what to monitor. However, a fundamental question is **who** should be allowed to read this data. The default access to datasets should **not** be READ—it should be NONE, unless there is a business requirement for it.

ALLOW and BLOCK Lists

A practical and effective security strategy is to use ALLOW lists instead of BLOCK lists. The latter is often hard to maintain manually, and if someone is not on the BLOCK list, they are immediately allowed. What if a nefarious user elevates their privileges and attempts to access the above datasets? With a BLOCK list, there would be no mechanism to stop them. With an ALLOW list, only specified users will be able to access the dataset and any unauthorized attempts should generate

an alert.

Canaries and Honeypots

Another effective defensive tactic is canaries and honeypots. Canaries (inspired by the "canary in a coal mine") are datasets that, under normal circumstances, should never be touched or altered and serve as a warning mechanism for suspicious behavior. One example is a canary partitioned data set (PDS) such as "SYS1.USERDATA" placed as a decoy for any potential intruder because, to an attacker not familiar with the native environment, it looks like it might be a sensitive dataset. What's more, the value of canaries isn't just limited to intruders. Canaries can help detect threats from insiders looking for data in places they should not be.

Honeypots are also deception techniques aimed at tricking adversaries into exploring data or regions of your system they otherwise shouldn't be. So, then, what exactly is the difference between a honeypot and a canary?

Honeypots and canaries are often conflated terms, though they should be distinguished. Historically, the primary purpose of a honeypot was to observe adversary behavior in a decoy environment over time versus serving as an immediate alerting or warning mechanism like a canary. Therefore, a more appropriate comparison might be a "honeypot LPAR"—where attacker tactics, techniques, and procedures (TTPs) and behavior can be observed over time in a mock environment—with "canary datasets" that serve as warning mechanisms when triggered.

While there are many other ways to monitor sensitive data, the above are some quick wins BMC AMI Security can help implement in your environment today. Sometimes, the most effective detection and response tools aren't the fanciest and shiniest new things available, but are the ones immediately available to use within the environment.

In the next part of our series, we'll discuss how **Privileged User Monitoring** can help you stay ahead of the ransomware threat!

Check out part 1 of this blog: Initial Access and part 2: Privileged Access Management and Zero Trust.