**Deadbolt Ransomware**

A group known as deadbolt terrorized NAS (Network Attached Service) devices by the hardware maker QNAP, back in 2022. Ransomware is a type of malicious software that encrypts the victims’ files or entire computer system making the device essentially useless. Often, displaying a ransom letter demanding payment via crypto in exchange for the decryption key. In the case of Deadbolt, they were attacking NAS devices that were not properly set up and were exposed to the internet. Then the deadbolt team would exploit a security flaw in the software to gain access. Unlike computers, normally NAS devices are set up to run 24/7 so you can access your data from anywhere. You can see how this can become a problem if the right precautions were not taken. The devices affected by this attack were encrypted with an AES 256 encryption. This type of encryption is so secure that it would be impossible for any user to revert the damage that was done. Essentially bricking your device and files. QNAP was quick to respond and patched the security flaw but not before thousands of devices were affected. To this day you can still see devices that are affected by this ransomware by just searching by the HTML tag “LOCKED BY DEADBOLT”

<https://bit.ly/3PVOTc8>

Down below is an actually photo of the deadbolt in action.

A screenshot of a computer

Description automatically generated