Lodestone

JUNE 2022

STATE OF CYBER

monthly newsletter

ACCOUNT AUDITING

This month's main topic may seem basic, but it is incredibly impactful. In the past few months, Lodestone has observed several instances of threat actors taking advantage of poor account hygiene to cause damage to businesses.

Threat actors can use poor account security to their advantage in several ways. Accounts with default or weak passwords, for example, can serve as an initial foothold into a network. Once that initial foothold is obtained, threat actors have a prime opportunity to attempt to compromise additional accounts and systems within the victim's environment.

Weak account passwords can also enable threat actors to escalate privileges – that is, to give a newly created or compromised account additional permissions to perform more impactful malicious activities. Over-privileged accounts, or accounts with special privileges that do not require them for day-to-day operations, are also a concern. If a threat actor is able to gain access to an administrator account, they may be able to obtain unlimited access across a network.

It is crucial to consider exactly what any administrator accounts, including service accounts, need access to. This falls in line with the principle of least privilege or providing no more and no less access than what is needed to perform the necessary work. Can administrator permissions be added for certain areas and not others? Are administrator permissions only needed for a limited period of time?

Group policy and appropriate network segmentation, along with strong passwords and the principle of least privilege, are vital components of proper user account management. Make sure that your company is reviewing its accounts regularly with, at a minimum, the following considerations in mind:

- Stale accounts (e.g., accounts that have not been active in the past 30 days)
- Accounts using default or weak passwords
- Appropriate group policy assignment, even for administrators
- Strong passwords and group policy assignments for service accounts

EMERGENCY DIRECTIVE 22-03 MITIGATE VMWARE VULNERABILITIES

Cybersecurity and Infrastructure Security Agency (CISA) is warning VMware customers that use Workspace ONE Access, Identity Manager, or vRealize Automation of a critical vulnerability. Customers with Internet-facing versions are at the highest risk.

ZERO-DAY EXPLOIT USE EXPLODED IN 2021

DarkReading highlights that financially motivated attackers have been increasing the speed at which they take advantage of zero-day vulnerabilities after they are announced. Lodestone recommends a review of security controls specific to after an attacker gains access to your network.

WEAK SECURITY CONTROLS AND PRACTICES ROUTINELY EXPLOITED FOR INITIAL ACCESS

The CISA has released an advisory that highlights the most frequently targeted vulnerabilities and mitigations that can be used to address them. Lodestone recommends considering these vulnerabilities in your own network.

QNAP ALERTS NAS CUSTOMERS OF NEW DEADBOLT RANSOMWARE ATTACKS

QNAP, a network-attached storage provider, has announced to its customers that the DeadBolt ransomware group is once again targeting customers that use QNAP devices within their environments. Ensure that QNAP devices are patched frequently.