A major security incident unfolded on July 6, 2024, when a possible brute force attack was detected. This report provides an incident analysis, including attempts to exploit vulnerabilities, usernames targeted, potential access gained, and most importantly, how this intelligence aligns with the MITRE ATT&CK framework. Cloud Services management was compromised, and user data was endangered. But what really happened?

According to the logs, there were 744 failed login attempts, strongly suggesting a possible brute force attack. A brute force attack is a method used by adversaries to gain unauthorized access to a system by trying all possible combinations of passwords until the right one is found. Indications of a brute force attack include a high number of failed login attempts in a concentrated amount of time. In this case, attempts were made using the IP address 192.168.10.15 against a spread of usernames, concentrated in a way that significantly suggests the use of a "script" to issue the numerous login requests. Usually, when logging in, a user will not have to make too many tries for their correct credentials to be registered. In the event that a user has forgotten their password, the process of remembering it can be mistaken for a number of attempts with the wrong password. It is easy to see how logging in or resetting a password could look like a stay-and-try situation. Between the normal and resetting phases, a user is not really a hacker in the sense of hacking into a system. A hacker who uses a better system of intelligence might not even be physically present at the system they're hacking into. They might be using the internet for a high number of failed login attempts that look like they're coming from the inside.

Out of the eleven successful logins, only one came from an IP address that wasn't 192.168.10.15, which is the address of the attacking machine. The would-be intruder appears to have attempted to guess passwords, as the usernames associated with the failed attempts indicate a range of potential valid user accounts. The successful attempts, on the other hand, seem to indicate that the intruder may have had some success with the password portion of the login process.

From 3:18 p.m. to 3:19 p.m., five login attempts were made. The users attempting to log in were kathy (two attempts total), bill (three attempts), and kathy (once more). Invalid login attempts came from 62 different port numbers, with the invalid port number 52238 being used twice. There are an unusually large number of entries associated with SSH (1559) for the IP address 10.0.0.12:22. This suggests that there is some sort of attack—likely a brute force attack, given the volume—that is trying to gain access to the SSH service on that particular IP address. Although this is an internal IP address associated with a private network, these attacks are not very discriminating and will try to brute-force any password that is weak enough to allow access.

The logs show that users were both added and removed. The user stephanie was added, but users attacker and admin were deleted. Two users, John and Admin, used sudo to give themselves elevated privileges. John used sudo with great frequency, employing it in commands for system updates, installation of audit tools, setup of audit rules, user deletion, and opening of root shells. Admin also used sudo, but for different purposes (mainly concerning the

search for and generation of audit reports), and he too opened a root shell. As for who "needed" to use sudo, well, if we had it all to do over again... John's frequent command usage could be concerning, given his generally elevated level of access. The attacker managed to get into several accounts and was doing some very questionable things—like trying to wipe out the financial records of the organization and manipulating the list of authorized users. The actions of the attacker can be aligned with the tactics and techniques of the MITRE ATT&CK framework. Initial access was gained through a brute force attack on SSH. Once inside, the attacker established persistence by adding new users and placing them in the sudo group. When root access was needed, sudo was used to escalate privileges. The attacker evaded detection by deleting users and removing the audit logs that would have contained incriminating evidence. While attempting to gain full access to the system, the attacker also made moves that would qualify under the "Impact" category. Financial files were deleted in an attempt to destroy any evidence of what had been done.

The analysis reveals that a brute force assault was launched against numerous usernames from the IP address 192.168.10.15. This assault succeeded in compromising multiple accounts, and the attacker used those accounts to carry out several different kinds of "suspicious" activities. Among other things, the attacker deleted a number of files related to the organization's finances. The activities of the attacker match up with several techniques from the MITRE ATT&CK framework. To boost security and avoid more attacks like this one, we recommend the following: block the source IP address, 192.168.10.15; make authentication mechanisms even more robust by employing multi-factor authentication and mandating strong passwords; watch for and alert on failed login attempts; and, finally, review security configurations and make necessary changes to "harden" them. Auditing these changes on a regular basis helps find and fix potential vulnerabilities before anyone can exploit them.

This incident underscores the critical need for having secure systems in place and for constant observation to catch and respond to any threats that might arise. It shows that an organization can't be too careful when it comes to cybersecurity; it must maintain a posture of vigilance and proactivity. The systems that the organization uses—especially when they are used by the organization's many employees—must be secure against evolving threats. If not, the organization risks sowing the seeds of a disaster that can (and, in this case, did) affect many of its users.Alongside technical strategies, organizations must create clear protocols for incident response to allow for rapid and effective reactions to security problems when they occur. They need to have a dedicated incident response team in real time and perform regular drills and simulations of potential incidents. They should also maintain up-to-date documentation of procedures to ensure a knowledgeable response team.

Working together with industry colleagues and organizations devoted to cybersecurity can sharpen an individual organization's threat detection and response capabilities. This is because the collective knowledge, experience, and expertise of even a few industry partners can significantly bolster an organization’s cybersecurity program. When these organizations collaborate in the realm of cybersecurity, the benefits can be felt across the private sector, and the public sector can also be better served as a result. In the end, the secret to a successful cybersecurity program is a multi-layered model that combines not just technology, but also

procedures and humans. By reducing the technical risk, cutting the procedural risk, and lowering the human risk as close to zero as possible without becoming counterproductive, organizations can better prevent unfriendly entities from gaining entry. An increasingly proactive approach to cybersecurity allows organizations to do much more than just safeguard their assets and data. Such an approach also enables them to foster an atmosphere of trust with customers and stakeholders. In a world whose lifeblood seems to be flowing mostly through digital veins, the strength of your cybersecurity posture largely determines your reputation.

Additionally, the event underscores the necessity for companies to have solid backup and recovery plans in place. They should regularly back up all of their important data and ensure that the backups are stored securely. If organizations do these things, then they can recover almost instantaneously after being hit by a cyberattack. Testing the backup and recovery plan seems like a no-brainer, but it is often neglected. Hearing "it worked fine the last time we tried it" is an inadequate substitute for actually seeing the plan work when you need it to work. Regular penetration testing is something every organization should consider. It serves two purposes, it identifies vulnerabilities that your internal people might miss, and it addresses those vulnerabilities before actual bad actors can exploit them. Don't think of penetration testing as something you only do when you suspect you've been compromised.

The July 6, 2024 security incident provides valuable lessons for organizations to learn from. Not only was it a high-visibility attack, but it also exposed numerous low-hanging fruit that many organizations hadn't patched despite them being known vulnerabilities. The incident serves as a useful reminder that the bad actors are not only trying to get through the walls of your house; they are also swimming across the moat and scaling the walls. A strong cybersecurity posture must consider and defend against every possible avenue of attack.