Final Report

On July 6, the Cloud services organization experienced a data breach, where the system was accessed by a hacker and data from the financial department was stolen from the system, this action puts the company in a vulnerable position that exposes us to financial, legal and reputational risks.

The cloud security department receive some alerts about unusual behavior on the routine server maintenance, meaning the server was acting different from the normal daily behavior. After investigating and getting evidence, we find that a hacker got access into a device that was connected to the organizations network, and from there, the hacker:

- Started to scan the system looking for users and passwords
- Steal credentials from all the users in the system
- Use the credentials to access sensitive data from different departments
- Copy the folder with sensitive data from the financial department
- Created a user to move the copy and original folders of the financial department
- Erased all files related to the user ‘admin’

The hacker got access to the whole system thanks to the credentials of each user, the evidence demonstrates that only the financial department files were manipulated by the hacker and that both the copy and original folder were moved to a new user created by the hacker, meaning the sensitive data was stolen by the hacker.

This incident affects essentially the financial department, right now all the information that this department would need to work, is all gone, there is no way to access it. Our customers got some

personally identifiable information like first and second names, SSN, phone numbers, emails, also payment card data like: bank account number, security code, and recent payments.

Next, we are going to present the essential recommendations the organization should take:

- Report to each customer that there was a data breach without giving any specific information, in order to avoid any phishing methods
- Reset all user credentials and enforce both multifactor authentication and biometric authentication (Touch ID or Face ID) across the organization
- Assign from zero the privileges and roles of every worker in the organization to enforce least privileged access
- Establish pentestings and vulnerability assessments to keep improving security and making sure to no allow a same attack twice

Incident Overview

The system administrator noticed the unusual alerts during routine server maintenance, what trigger the alerts was: High CPU usage on an administrative server (something that is not normal), unusual login patterns attempt in the authentication logs, alerts from the intrusion detection system, and the constant requests the CPU was receiving from an unusual IP.

After the team saw the patterns and determine the class of attack that it was without getting to analyze the depth of it, they were sure that sensitive data could have been erased or stolen, in these types of organizations, is easier and more threatening to get data from customers than from the company itself.

The first action the system administrator took, despite being the standard protocol, is the correct in any similar situation, escalating the problem to the security team, what they did immediately was collect the logs from three sources, logs are one of the most importance and useful weapons that never lies, never forgets and never gets its fact wrong.

For the investigation, logs from different defensive systems were analyzed in Linux command line. Suricata IDS gave the alerts.log file that shows network-based alerts, some authentication records that showed login attempts and user management activities and the file audit.log, this one was a system audit that records from auditd showing file/folder operations, system changes, and user activities. We used the tool of MITRE ATT&CK to identify the description of our conclusions and match them with the type of attack that better fits.

Before the main attack even happen, the system registers some actions made by john, erasing a user named ‘attacker’, this is an important point, because its prove that the hacker already has analyzed the Attack surface and identify the attack vectors to get into the system. Just a few hours after erasing that user, the hacker started a brute force attack with and after thirty minutes, the hacker got credentials on a user with access to the whole system, The hacker accessed the financial folder and stole the data in that folder by sending it to a new user that was created by the hacker, the admin account was completely erased by the hacker.

Technical Analysis

How can it be confirmed that the system was accessed by hacker and it was not just a common behavior by the system? Thanks to the evidence that was gather, it can be clearly shown that it was an outside hacker:

- The CPU usage is clear evidence that a brute force attack happened, the system was receiving constant traffic from the hacker, guessing different types of usernames and passwords, over 858 SSH connections were closed by the system in fourty six minutes, something humanly impossible, which leads us to the next point. The change of the CPU usage demonstrates that the system was trying to be accessed by some hacker.
- Malicious script was used to scan and capture weak credentials in the system. Malicious scripts are repetitive systems that via an interaction with a service that checks validity of credentials, try using a library of common users and passwords in an exaggerate amount of time. This demonstrate that the hacker broke into the system by just executing this tactic.
- Normally, an administrator has access to all the accounts and users in the system, maybe it has a folder where it stores all of them. In the system activity log was recorded the same IP that start all the brute force attack, surprisingly getting access to all the different accounts after compromising the ‘admin’ account. This is clear evidence of the hacker broking even more into the system and obtaining total control over all the system data.
- Creating a user, moving the original and a copy folder of the financial department to the new user folder, and then erasing the ‘admin’ user. The hacker with all the access it got into the system, steal data by creating a new user, and then deleting the ‘admin’ user to erase its tracks and movements into the system.

The attacker got access using different very known techniques like reconnaissance of the whole system to find any attack vector and start planning the attack, brute force attacks combinate with execution of malicious script into the service of validating credentials. Thanks to the technology of malware, the attacker just executed a malicious script and after thirty minutes, weak credentials from the ‘admin’ user were compromised, giving access to the hacker.

What was more concerning is that the IP that made all the attack, was a local IP, meaning that the hacker got access to the network first, and form there, it started to do everything. The network was affected since a long time, the system in general was also affected, inside the system, a total of 306 movements were made inside the financial folder, confirming that all the sensitive data that was stored was steal by the hacker, and the hacker leave the user that was created as a tunnel to come back into the system. The attacker movements, where accessing credentials of user’s folder (to obtain access into other users), creating and granting Sudo privileges to a new user, stealing data and saving it in the new user, erasing the ‘admin’ user.

The MITRE ATT&CK framework was used to identify these behaviors correctly, in order to look for security improvements and responses to the incident:

- TA0001 Initial Access, T1078.003 Local Accounts: A local IP (192.168.10.15) was used to gain initial access and start the attack.
- TA0043 Reconnaissance, T1596.003 wordlist scanning: This is related to what John finds before the attack occurred, a user named ‘attacker’ in the system used to gain information about the infrastructure.
- TA0010 Exfiltration, T1537 Transfer data to cloud account: The hacker make a copy of the financial folder and move both to the new user ‘stepahine’ created.

- TA0006 Credential access, T1110.001 password guessing: The malicious script uses different usernames and passwords to try and get into the system
- TA0004 Privilege escalation, T1098.001 Additional cloud credentials: The hacker used the compromised account ‘admin’ to create and assign sudo privileges to a new user
- TA0005 Defense evasion, T1222 File and directory permissions modification: The hacker used the ‘admin’ account to add the user he created into the group of users with privileges

The financial department was the most affected, because the folder that contain all the data that was needed it to work was stolen by the hacker.

Business Impact Assessment

The impact of the attack, target specifically the financial department, by stealing and erasing sensitive data from the folder, this would interrupt the service and worsen productivity. Talking a little more general, the CPU usage that the server suffers, interrupt some process and make the servers lower, making the experience for the customers worser. The attack impact affects the confidentiality, integrity, and availability of the data, the hacker got access to sensitive information (confidentiality), stole the data and copy it, being able to modify it (integrity), and the users would not be able to access the data stolen (availability). Losing the financial data could cost a high amount of money for the organization, because the customers can sue against us for not protecting their data, money would be needed to upgrade security. Customers would not trust in the company if we let the data, they entrust us leak, the organization needs to recover that trust by implementing more security improvements.

Security Recommendations

The security team analyze in deep what was the root problems of the attack in order to patch and improve those vulnerabilities with the following security recommendations, the roadmap is 1 being the first to be done:

1. First for the immediate containment and recovery actions, these are needed to stabilize the environment and prevent any attack while the system is vulnerable:

- Reset and change all user credentials in the company, to prevent the same hacker to access again
- Restart all active sessions and force to re-authenticate again to close any possible session that the hacker could have
- Block the malicious IP in the cloud firewall (192.168.10.15) to cut the connection the hacker had with the server
- Close any unnecessary ports that could be used again for malicious purpose

2. Then the medium-term focusing more in increasing the detection capabilities and identify important and critical vulnerabilities in the system:

- Execute different security patches that the systems could be missing, for the known vulnerabilities
- Restrict the incoming traffic, only for required IP's and ports
- Execute security actualizations patches in all the servers and machines, actualizations could patch different bugs in the systems
- Implement a momentary least privilege structure to prevent any escalate privileges attack

3- Long-term recommendations now, this are for enforcing the infrastructure of security in all the system:

- Implement for each user biometric authentication, both face ID and touch ID to enforce the security
- Implement a login attempts limitation service that block the IP that is trying to access
- Design a new infrastructure with semi-segmentation networks
- Implement a monthly pentesting analysis on the cloud infrastructure to keep finding and fixing any vulnerability

The requirements needed for most of these recommendations are money to implement different security systems, hire an external white hat hacker to make the pentestings into the system. The expected time needed for these implementations depends on immediate that the words already describe it, medium an expected time of 2 weeks and long term would be like 2 months, but everything depends on how the implementations progress.