# **Incident Report**

## **1. Executive Summary**

Insecure enterprise architecture of email server caused a successful phishing campaign by an attacker against SmartMeter Co in December 2023, which led to the compromise of several user credentials including that of a privileged user whose access level was not assigned based on role in the organization. The attacker was able to further exploit the network due to lack of continuous monitoring and incident handling process in place which led to compromise of sensitive and confidential information on SmartMeter Co servers.

## **2. Incident Details**

* **Short Description of Attack (include the attack vector and intrusion point)**:

SmartMeter Co experienced a phishing campaign attack which compromised several user credentials and was further exploited to compromise sensitive & confidential data stored on it’s critical server’s.

* **Date and Time**: December 2023
* **Incident Severity**: High

## **3. Root Cause Analysis**

**1. High Level Observations from Logs:**

**Observation 1**

From the Email Server Logs:

On Dec 14th at 08:00, a new SMTP client successfully negotiated a connection with SmartMeter Co’s email server with an email domain mail.mercifulredeemerchurch.com. At the same time five (5) SmartMeter Co employees, John, Vinod, Jack, Mary & Chillantra received a phishing email with the exploit payload from a spoofed Microsoft support email. The email address that sent this phishing email is micr0soft@microsoft.support.accounts.mercifulredeemerchurch.com.

**Observation 2**

From File Server Logs:

On Dec 14th 10:30am, John & Vinod accessed and modified IIOTProduct source code text file located in the Top-secret folder. The actions they performed were to read, copy and update the file. They would also carry out similar activities on Dec 19th at the same time. On Dec 16th at 10:35 - 10:36, Chillantra accessed and modified the MS word file XmasBonuses located in the HumanResources folder of /CriticalFileServer. She also read and copied the TopSecret folder in the Critical file server on Dec 16th at 00:35 - 00:36. Finally, on Dec 24th at 00:42:15, Jack performed read, copy and update actions to the IIOTProduct folder located in Top Secret folder, followed by attempts to delete 3 folders which failed an hour later. The folders that were attempted to be deleted were CompanyInfo, TopSecret and HumanResources.

**Observation 3**

From SQL Server Logs:

A user ‘db\_admin’ performed a deletion of the table SmartMeterCoDB.Readings at 10:45am everyday from Dec 14th to Dec 21st about 5mins after another user ‘admin’ makes update to this database table. On Dec 21st at 00:10:45, the user ‘Jack’ accessed and copied data from a csv file to SmartMeterCoDB.Readings table.

**2. High Level Interview Insights:**

**Insight 1 –**

Interview with CEO (Jack):

Jack received a phishing email which appeared to be from a trusted vendor asking him to verify his credentials via a provided url. He took the bait and entered his credentials in the link due to the urgency of the request & familiar look of the webpage which made him believe that it was legitimate. Jack received notification of the action taken on the SQL database server to copy an excel file into one of the tables, but he took no action from that even though he did not carry out this action himself. He also noticed weird emails sent from his account and assumed they were from his wife or kids using his blackberry device.

**Insight 2 –**

Interview with IIOT Engineer (John):

John reported that he was working with Vinod on production code at the time he received the first phishing email. He was overworked and multi-tasking a lot, so he clicked the link of the email and entered his credentials for verification like the email asked. John believed his work was very important to the organization and if he wasted any time, it would affect core operations, so he sacrificed being meticulous and security conscious to gain speed and efficiency. He also admitted to using the same password to log in to all systems.

**Insight 3 –**

Interview with HR Manager (Chillantra):

Chillantra reported that she received the phishing email from John and she opened the link in the email. She sensed that things weren’t right because the website had lots of spell errors and looked suspicious. However, she decided to put in her credentials anyway because she trusted that the source was from John who was probably testing a new technology proof of concept. She decided to change her password immediately after to prevent John from accessing and altering his data in the Xmas bonuses file.

**3. Root Cause Analysis Screenshots**

## **a) 5 Whys Analysis (for problem statement) screenshot**

A screenshot of a computer

Description automatically generated

**b) Fishbone Analysis Screenshot**

A diagram of fish with text

Description automatically generated

**4. Attack Vector**: Email. An attacker was able to launch a phishing campaign against employees of SmartMeter Co due to lack of anti-phishing technology on the email server which was poorly secured on the network.

**5.** **State the intrusion point:** The attacker was able to spread throughout the network because he was able to get the credentials of the CEO who was given access to sensitive infrastructure that he should not have.

## **4. Failed Controls**

**Security Training and Awareness (AT) Family:**

**Failed control 1 & 2 – AT-2 – Literacy Training & Awareness & AT-3 – Role based training**

Reason: The ease with which the attacker’s phishing campaign worked on some of the employees who gave up their credentials and based on the interview record of the employees that fell victim to the phish, there is a huge knowledge gap on general security awareness and social engineering.

On the other hand, the fact that a critical email server was left open to traffic from the internet rather than placed inside the DMZ where every packet to and from the server can be subject to inspection is an indication that the network security team require addition training to execute their role.

**Incident Response (IR) Family:**

**Failed control 3 – IR-4 – Incident Handling**

Reason: There was no live detection on the network to pick up on anomalous behavior like the CEO going into critical folders and the SQL database. This is not normal behavior and should have been detected and flagged for investigation. Automated incident handling processes are required to address such issues.

**Access Control (AC) Family:**

**Failed Control 4 & 5 – AC-5 – Separation of duties & AC-6 – Least Privileges**

Reason: Access privileges were not restricted based on roles as is evident with the CEO having access to the SQL database and access to critical file shares.

**Audit & Accountability (AU) Family:**

**Failed Control 6 – AU-6 – Audit Record Review, Analysis and Reporting**

Reason: There was a lack of real time correlation and analysis on event logs that was generated on key asset that would have led to early detection and mitigation of the attack.

**Assessment. Authorization & Monitoring Family (CA):**

**Failed Control 7 – CA-7 – Continuous Monitoring**

Reason: The network and Information security assets such as critical servers and file shares were not under continuous monitoring at the system level. A SIEM and SOAR solution would have satisfied this requirement and helped to mitigate the extent of damage due to this attack.

**Program Management Family**

**Failed Control 8 – PM-7 – Enterprise Architecture**

Reason: The email server was not placed in the DMZ where there was firewall inspection which is an indication of a lack of consideration for information security and privacy in the enterprise architecture.

**System & Communications Protection Family:**

**Failed Control 9 – SC-7 – Boundary Protection**

Reason: The attacker was able to successfully penetrate the network by using a phishing email. Boundary protection of telecommunication services such as email was lacking. Also the attacker using phished credentials was able to exfiltrate sensitive data from critical servers.

## **5. Prioritized Recommendations Based on Overall Risk**

**Prioritization template Screenshot**

## **A screenshot of a computer Description automatically generated**

## **6. Conclusion**

The most important recommendation to implement is the provision of security awareness training for all SmartMeter Co employees.

Any chain is as strong as its weakest link, and this applies in securing sensitive and critical information. The human elements that interact with technological assets are very crucial and it does not matter if we have all the technology set up to defend the systems if users would surrender their credentials easily to an attacker. Therefore, it is recommended that every employee of SmartMeter Co should take mandatory training in security awareness and social engineering techniques.