MODULE ONE – DIGITAL FORENSICS

1 Plan of action – Scope of the Incident

It has been identified by the client that there has been a suspected social engineering attack that has compromised their O365 environment. Early indications have the point of entry stemming from a phishing attack targeting a member of staff within the risk and compliance team. From this initial point of entry, it was advised that multiple executive level users were then targeted in a second wave attack in which another phishing email was sent from the compromised account to these users. For the purpose of this analysis, we will be examining the initial compromised account and network device, as well as examination and analysis of subsequent account device compromises that have arisen from the second wave phishing emails targeting executive level users.

2 Plan of Action – Identification and Approach

i. Logging – We will be requesting the following logs from the resident IT personnel.

- Microsoft Office 365 Security Audit Logs;
- Relevant Office 365 Exchange Audit Logs
- Azure Sign in Logs;
- Azure Audit Logs;
- Firewall Logs;

Explanation to requesting logs - *Logs are an integral part of an incident response collection. Through examination and analysis, forensic personnel can identify events such as initial point of entry and any mailbox change activity (Rule creation, mail deletion). Further to event analysis, logging provides examiners the ability trace the events back using information such as Source IP address and Geolocation attributes.*

NB – *Endpoint and Server logs are considered under physical device collection covered in the next point.*

ii. Network and Endpoint Devices – We will request to forensically image a number of relevant devices that will allow thorough examination of endpoint activity including host logging, malware analysis and internet activity.

- Forensic image of workstation of staff member in which credentials were entered.
- Forensic images of workstations of all 6 executive level staff members as it is unclear if any credentials were entered or malicious websites visited.
- Forensic images of on-prem servers

Explanation for Network and Endpoint Devices – *Although the compromise was said to have resolved from a phishing email, the importance of endpoint collection is critical as it contains key information such as windows event manager which collects all relevant event artefacts from actions on the system. This will allow examination and analysis to determine if any malicious software was installed along with the credential harvesting.*

iii. Other informational assets and staff interviews – We will request the following information from the client IT and extended team.

- Office 365 PST export of the account in which credentials were entered
- Office 365 PST export of the accounts of 6 executive level staff members.
- Interview with initial victim to determine what and how was entered and any other relevant information relating to the incident
- Interviews with all 6 executive level staff members to determine whether malicious links or credentials were entered from the second wave phishing attack.
- Interviews with relevant IT staff who were first notified about the compromise to determine what was initially done.

Explanation for informational assets and staff interviews – *Mailbox extractions are key in phishing email analysis as email chains can be rebuilt if required to recreate the conversation that took place between the threat actor and the victim. It allows the identification of the phishing email in a controlled environment to examine key information such as the sender and source IP from the email header.*

Interview are also key as information provided can assist in the analysis and allow examiners to get an understanding of the current network infrastructure to determine the severity and extent of the databreach.