Assignment #2
Social Engineering

Ramazpreet Dhothar
Ahmed Almass
Madusha Samarajeewa

Contents

Introduction

DeltaStream Energy is an exploration petroleum company; companies like this make plans for development - from new methods, to discovering land, to producing petroleum products. The objective of this paper will discuss methods of corporate espionage, focusing on potential exploration on the land. Hence, obtaining this information is sensitive because if an attacker were to gain this information about the land leased before DeltaStream makes the buy, the sensitive data could be sold to another company and the other company can lease the land to make the production. The first part of the paper will discuss information gathering. The second part will discuss methods used to get the information. Finally, the third part will be advantages and disadvantages of the research.

Information Gathering

In the petroleum industry, before they decide to lease the land that they are interested in (which may be owned by the provincial government or First Nations), they look at core samples first for the lithology. These core samples are obtained from third parties who do drilling with special drills into the rock. Companies are regulated to submit new core samples to Alberta Core Research Centre for public use. These samples can later be acquired for research by other companies like DeltaStream. Newer samples can be obtained through Canamera Coring. The target can be found using Accumap software which will contain core logs relating to previous wells that were drilled. These logs have the company and supervisor names addressed on the document. AER documents which is published for the public also hold this data. Another common place to look at core samples is Alberta Core Research Centre for older cores samples that have drilled. These are kept by the government for the public to access. DeltaStream primarily communicates to these third parties through email or phone.

The objective is to gather information from a third party; by targeting the third party there is a less of a risk of getting caught by DeltaStream - the main target. Information is gathered about the location that is used for the development of the petroleum product.The manager of Canamera Coring, Orren Johnson, is the target. This information is found on Accumap by looking at an older location that they've drilled. The phone number of Orren Johnson was found to be (780) 440-1942. Verna Yee is the Senior Geologist of Deltastream who communicates with the Canamera Coring for the arrangements. Another method that was used is phishing Alberta Core Research Centre, as they log and keep track of who accessed the cores (this is also arranged by Verna Yee). The email for Alberta Core Research Centre was found to be CRC.ServiceDesk@aer.ca.

Vishing

Vishing (voice phishing) is done towards Orren Johnson. He is told that the individual he is communicating with is an employee from DeltaStream Energy. A pretext is planned out for this scenario as well as potential responses that can be given by him. Orren Johnson is told that Verna Yee is not capable to work because she is hospitalized and is in critical condition, and through management this employee was chosen (the attacker) to fill in the position. Orren will leak the location that DeltaStream was looking at for drilling. Thus, the objective is complete. For this strategy, planning possible responses, using sympathy (emotion), having a casual demeanour but also expressing urgency, and having a strong pretext is the key to be successful.

Pretext Example:

Attacker: Hi, this is Sandy from DeltaStream Energy.

Orren Johnson: Hey how's it going, what can I do for you?

Attacker: I'm calling because Verna Yee is not able to work right now, as she is in the hospital. I was told by my VP to replace her for the time being.

Orren Johnson: I'm sorry to hear that, what happened to her?

Attacker: She got in to a car accident on the highway and she is in critical condition at the moment.

Orren Johnson: Oh my god.

Attacker: Sorry I'm in a bit of a rush right now. Since this incident occurred, she didn't tell us the plans for quotes and location of cores samples and I don't have access to her email password or I don't see anything she wrote on her desk. Can you provide that information? I have to report everything in like 10 to 15 minutes.

Orren Johnson: Definitely, the prices are ____ and locations are _____.

Attacker: Thanks a lot, I really appreciate it! Have a nice day.

Phishing

For this technique, Alberta Core Research Centre is selected as a target for the attack. This is another effective method because core samples are sent there after being observed or companies get core samples to look at from nearby locations where that core sample was obtained from. Alberta Core Research Centre is chosen as the target because they record which core samples have been taken and which company gave them the cores. Obtaining this information will let the attacker know the location that DeltaStream Energy was looking at and what time they were doing so. Phishing will use pretexting and spoofing of the email address to make it seem that it is being sent from DeltaStream Energy. The pretext will mention that Verna Yee has been laid off and a lot of data been lost, allowing us to ask for an update of what she was looking at, what cores has been borrowed and has been submitted.

Pretext Example

To: CRC.ServiceDesk@aer.ca
From: SteveBrownridge@deltastreame.com

Dear Service Desk,

Verma Lee, the geologist in charge of observing the core samples, has been laid off. We've lost the information regarding which core samples were borrowed from your organization and which samples have already been submitted.

Please update me on the borrowed and submitted samples with locations and the due dates.

Thanks,

Steve Brownridge
Executive Vice President
DeltaStream Energy Corporation.

Advantages & Disadvantages of Research

Advantages

Multiple published documents regarding the target were used for the following attack. These documents include information regarding companies that currently or previously worked with DeltaStream Energy as contractors. This information is publically available and can be obtained easily. Contact information can also be found easily as many individuals in the petroleum industry post this information on websites.

Disadvantages

It is not guaranteed that Orren Johnson still works with Canamera Coring as there isn't a daily timestamp of his current position available online. Another disadvantage is that there isn’t certainty that Canamera is still a client of DeltaStream because sometimes companies change clients based on price of the services (which may have occurred).

References:

https://www.zoominfo.com/p/Orren-Johnson/-1960989243 - Orren Johnson phone number
https://www.aer.ca - Alberta Core Research Centre email