Paul Garewal
V00803658

Title:

The World Cup of Cyber Security Attacks:

How a Subordinate Relationship in the Workplace causes a Social Engineering Threat

Summary:

This social engineering attack focuses on Jamie, a software engineer that works for the Qatari government in its World Cup reservation planning. Taking on the job for the money, Jamie becomes angry and vengeful when his subordinate Bob is chosen to build the reservation system for World Cup matches (and thus will earn the majority of the money). Looking to undermine Bob, make an extra few million dollars and pay off his debts, Jamie sabotages Bob's software and sells the personal data of high ranking Qatari officials/celebrities attending the World Cup to Israeli Government officials (enemies of Qatar). In order to mitigate this attack, the Qatari government should implement sensitivity training to Bob and all other co workers so they may be aware of such a threat and be able to respond with counter measures to secure their information.

Persona:

Jamie, a software engineer and cyber security expert working for the Qatari government, developed a prototype booking system for fans of the World Cup in 2022 to reserve and purchase their tickets to soccer matches. Recently, Jamie is struggling to pay his mortgage back in Canada due to increased interest rates and this Qatari job is his last chance to save his house.

The Qatari government reviews the prototype, although very secure from a cyber security standpoint, is not as user friendly as Jamie's co-worker Bob's booking system. The government selects Bob's design to move forward and gives him a large raise.

Jamie feels very angry, bitter and vengeful, since Bob is subordinate to Jamie. Additionally, Bob had received a lot of help from Jamie to develop his prototype, although a lot of the security features were left out, Jamie understands the inner workings of Bob's prototype well and can exploit it.

Jamie is now plotting to make Bob look like a fool by sabotaging his booking system and while he's at it, stealing the private data of Qatari officials and fans attending the World Cup to sell the information to Israel; Qatar's sworn enemy. Jamie's plan will make him a millionaire, as Israel is willing to offer top dollar on this type of information.

Jamie's Misuse Cases that Threatens the Operation of the Qatar World Cup

1. Enter Bob's software system, save a copy of the information of fans and officials attending matches.
2. After information is successfully extracted, introduce bugs such as double bookings, free tickets and relocations for fans to undermine Bob.
3. During the confusion of the software system, quickly meet with Israeli officials to strike a deal for the information, sending using Asymmetric Encryption.
4. Fly back home to Canada before being caught and safely deposit cash earned.

Goals:

1. Undermine co-worker Bob, show who the most talented software engineer is on the team.
2. Earn enough money to pay the mortgage and keep his family/investments together.
3. Exploit national governments in order to cause chaos and distractions from nefarious activity.

Skills:

1. Strong coding/hacking skills

2. Ability to influence officials and coworkers(social manipulation skills)

Information Gathering:

Jamie needs to gather the information of the inner workings of Bob’s system. Thankfully, Jamie helped build the system, recording data by the “Shoulder Surfing” method initially. Since Jamie is already the boss of Bob, it became easy to look over Bob’s shoulder as he was building the software for his reservation system. Jamie recorded passwords, usernames and encryption keys of Bob’s system to access its database. Therefore, Jamie will have the ability to get into Bob’s reservation system, acting as a supervisor he will go unnoticed and be able to extract as much data as he wishes.

Furthermore, Jamie will use “Intrusion/Roleplay" to contact Israeli officials, using a pseudo name as not to be tracked by the Qatari government. Moreover, the Israeli government will receive the extracted information from Jamie’s pseudo character and receive monetary value in Bitcoin as not to be tracked.

Psychological Principles:

The psychological principles used by Jamie in this attack will be in the category of “instant rapport”. Mainly, the sub principles will be establishing artificial time constraints, ego suspension and validation of others.

In this case, Jamie will coerce Bob by helping with the development of his software by stating it will take less time if they tackle the task together. From there, Jamie will suspend his ego when interacting with Bob, especially when talking about plans for the reservation system. Jamie may know more efficient algorithms to implement, but wants Bob to feel as if he is the smartest man in the room.

Additionally, Jamie will ask to validate Bob at every opportunity. Stating to the Qatari government how well Bob is performing on this software development, that they will be on time in implementing the software before the World Cup registration is open.

With all these psychological principles placed on Bob, Bob will have a low chance of suspecting Jamie of malevolent intent, freely giving important information to his software system and taking any advice on board, fully trusting Jamie.

Attack Script:

1. Observe Bob's software development, offering help and shoulder surfing at every given opportunity to record passwords and usernames.
2. As Bob increasingly asks for assistance, offer to help build the reservation software system in order to reduce time in development.
3. As a team, validate Bob at every opportunity, suspending ego and presenting Bob as a star performer to Qatari officials.
4. As fans start to sign up for World Cup tickets, create a copy of all their personal information, recording prominent individuals who are attending.
5. Begin contact with Israeli government with pseudo character name, establishing connection with their officials and offering the personal information acquired.
6. Start to commit nefarious acts on Bob's system, double booking expensive tickets and sending free trips to random individuals.
7. After Israeli government pays for the personal information of Qatari officials and important individuals attending matches, begin to plan travel back to Canada.

Mitigations:

One method to mitigate these situations is to track the people who have access to usernames, passwords and high-priority information, no matter their seniority level.

Additionally, the main method of mitigation will be sensitivity training for all employees, such as Bob, so they are aware of the risks of dealing with important information and how it may be exploited. This may have Bob being more aware of Jamie's attack methods and not leaving him alone with the software and its inner workings. Since many attacks can come from within, sensitivity training may be the best method so all team members can monitor themselves from social engineering attacks that come from within.

Lastly, screening of individuals in-depth before hiring for confidentiality information positions should be required. If the Qatari government questioned Jamie's motives for wanting to work with them, the hiring team may have noticed a flaw in Jamie's rationale for wanting to collaborate.

References:

[1]"General discussion," *Security Through Education*, 07-Jun-2021. [Online]. Available: https://www.social-engineer.org/framework/general-discussion/. [Accessed: 17-Oct-2022].

[2] Mead. Nancy, Shull. Forrest, Vemuru. Krishnamurthy, and Villadsen. Ole, "A Hybrid Threat Modeling Method," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Note CMU/SEI-2018-TN-002, 2018. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617