ENTERPRISE INTEGRATION

& THE USE OF OPEN SOURCE INTELLIGENCE AND SOCIAL ENGINEERING BY SCAMMERS

ENTERPRISE INTEGRATION

This case study demonstrates how businesses are increasingly falling prey to a clever fraud based on publicly available information that does not use sophisticated hacking techniques. Enterprise Integration has recently investigated multiple attacks that relied on strong social engineering techniques and non-technical means to scam companies for goods, services or valuables.

In this particular instance, there seem to be two distinct phases in which the attack was executed.

1. RECONNAISSANCE PHASE

During the incident analysis, Enterprise Integration (EI) pieced together the information that was acquired and used by the scammers. The sequence may not be exact, but it appears the steps seen below were taken to obtain information prior to execution of the attack.

a. Reviewed European company HQ website and determined foreign locations including location in the US
b. Identified a Product Manager's name posted on the parent company's website including email and telephone number
c. Obtained company’s logistics email address (published on the parent company's website)
d. Identified the company's travel agency
e. Selected parent company's European HQ as the requestor
f. Selected a US location as the payer and determined the name and contact information of an Executive Administrator in the US location

2. BUILDING TRUST AND EXECUTION OF THE ATTACK

a. Perpetrators had conversations with US-based Exec Admin posing as the European Product Manager (later stating that the caller knew a lot of information and could not conceive that an outsider would know so much internal information).
b. Perpetrator called travel agent posing as the Product Manager and made flight reservations for 5 individuals for a meeting and requested that they bill the US office and email the tickets to the logistics email address on the parent company's website.
c. A few days later, the US Executive Admin emails the European Product manager requesting the name of the meeting to which they can back-bill the tickets. Receives a response from Product Manager saying they were not aware of any specific tickets and asks for a copy to track them down.
d. Product Manager inquires internally within the European HQ if anyone was aware of the reservation.
e. Reservation is determined to be a scam and reported to FBI and other security agencies within the US.

CONCLUSION

Whether in cases of a socially engineered attack or even an attack that takes advantage of a technical vulnerability, **humans remain the weakest link**.

Major security studies continue to say the same two things:
-Users are the weakest security link (whether on purpose or by mistake)
-Insider attacks pose the most serious threat to overall security

WHAT CAN YOU DO ABOUT IT?

1. Provide Security Awareness Training to employees
2. Review what you share publicly: website, newsletters, mass emails, etc.
3. Build (off the band) verification process within any process dealing with transfer of funds, intellectual property or any other valuable items
4. Develop an incident response process
5. Keep an updated list of government contacts in the incident response documentation
6. Conduct routine Physical and Technical Vulnerability Assessments
7. Ensure Social Engineering is included within Physical Assessments to test the 'system' and employee knowledge

If you need help with any of the above, contact Enterprise Integration Information Security at 904-928-8137.