CASE STUDY

PHISHING IN RED TEAM ENGAGEMENTS

March 1, 2024

Mark Puckett (mark@raxis.com)

PHISHING IN RED TEAM ENGAGEMENTS

ABSTRACT

In the ever-evolving landscape of cybersecurity, organizations face relentless threats from adversaries seeking to exploit vulnerabilities. Among these threats, phishing remains a potent weapon, capable of breaching even the most robust defenses. This white paper examines a real-world case study involving a large retailer, where a red team engagement orchestrated by Raxis demonstrated the power of social engineering techniques. By infiltrating an internal Zoom call and successfully phishing attendees, Raxis gained critical insights and domain administration privileges. This study underscores the importance of vigilance, security awareness, and proactive measures to combat phishing attacks.

1. INTRODUCTION

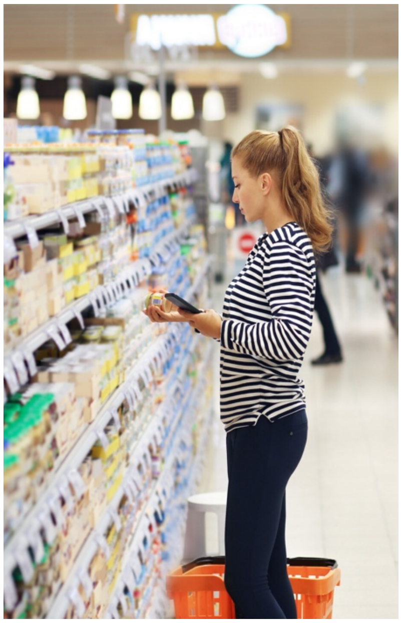
Phishing attacks continue to plague organizations worldwide, leveraging human psychology to bypass technical safeguards. In this case study, we explore how Raxis, a leading cybersecurity firm, executed a sophisticated phishing operation during a red team engagement. By exploiting trust and seizing opportunities, Raxis demonstrated the potential consequences of a successful phishing campaign.

2. BACKGROUND AND SCOPE

Customer Profile

The client, a large retailer, sought Raxis' expertise to assess its security posture. The engagement was part of a broader red team exercise aimed at identifying vulnerabilities and enhancing defenses.

Phishing remains a significant risk for retailers due to its ability to exploit human psychology and bypass technical defenses. Cybercriminals use deceptive emails, fake websites, and social engineering tactics to trick employees into revealing sensitive information or granting unauthorized access. Retailers, with their large customer databases and financial transactions, are prime targets. A successful phishing attack can lead to data breaches, financial losses, and damage to the retailer's reputation. Vigilance, employee training, and robust security measures are essential to mitigate this ongoing threat.



Objective

Raxis focused on social engineering techniques, specifically phishing, to evaluate the client's resilience against targeted attacks. The goal was to gain unauthorized access to critical business data while remaining undetected to evaluate our client's security posture and resilience.

3. THE INTRICATE PHISHING OPERATION

Initial Access

Raxis gained a foothold by compromising a user's machine. With access secured, they downloaded the user's entire mailbox contents for offline analysis. Specialized software helped identify critical information within the mailbox.

Zoom Call Infiltration

Our investigation revealed that the user of the machine was scheduled to participate in an internal Zoom call, during which confidential company information would be discussed. Seizing the opportunity, the Raxis team joined the Zoom meeting incognito, assuming the identity of an "Administrator."

Successful Phishing

Remarkably, our presence went unnoticed. After a few minutes, one of our Raxis engineers initiated private messaging with other Zoom meeting attendees. Leveraging the trust established during the internal call, we successfully phished three attendees for their passwords. To be successful in a phishing attack, it's important to establish trust with your targets.

Gaining Domain Administration Privileges

These compromised passwords were subsequently used to launch further attacks against the corporation. The culmination of these efforts allowed Raxis to gain full Domain Administration privileges, granting us undetected access to the network throughout the engagement.

4. RECOMMENDATIONS

If you have encountered a situation like this case study, here are some recommendations to enhance your security posture and mitigate the risks associated with phishing attacks:

Employee Training and Awareness:

- Conduct regular security awareness training for all employees. Educate them about phishing techniques, red flags, and safe practices.
- Emphasize the importance of verifying email, chat, phone calls or any source and avoiding suspicious links or attachments.
- Never provide your credentials to anyone. It is common for organizations to be able to reset authentication methods or conduct administrative duties without your password or other credentials.

Multi-Factor Authentication (MFA):

- Implement MFA for critical systems and accounts. This adds an extra layer of security by requiring additional verification beyond passwords.

Email Filtering and Anti-Phishing Solutions:

- Deploy robust email filtering solutions that can detect and block phishing emails.
- Utilize anti-phishing tools that analyze URLs and attachments to prevent malicious content from reaching users.

Regular Security Assessments:

- Conduct red team exercises periodically to simulate real-world attacks. Evaluate the organization's response to phishing attempts.
- Engage third-party cybersecurity firms, such as Raxis, to perform penetration testing and vulnerability assessments.

Incident Response Plan:

- Develop a comprehensive incident response plan specifically addressing phishing incidents.
- Define roles, responsibilities, and communication channels for handling security breaches.

Access Controls and Privilege Management:

- Limit user privileges based on the principle of least privilege. Users should only have access to what is necessary for their roles.
- Monitor and audit privileged accounts regularly.

Behavioral Analytics:

- Leverage user behavior analytics to detect anomalies. Identify unusual patterns in email communication or login behavior.

Secure Internal Communications:

- Encrypt internal communications, especially during sensitive meetings or discussions.
- Validate participants in virtual meetings to prevent unauthorized access.

Regular Security Updates and Patch Management:

- Keep software, operating systems, and applications up to date.
- Patch known vulnerabilities promptly to prevent exploitation.

Collaboration with Industry Peers:

- Share threat intelligence and best practices with other retailers and organizations.
- Learn from incidents experienced by peers to enhance security strategies.
- Remember that proactive measures are crucial in preventing successful phishing attacks. By staying informed, training employees, and implementing robust security controls, retailers can significantly reduce their vulnerability to such threats.

5. CONCLUSION

In the ever-evolving landscape of cybersecurity, phishing remains a potent threat. The real-world case study presented by Raxis underscores the critical importance of vigilance, security awareness, and proactive measures. By infiltrating an internal Zoom call and successfully phishing attendees, Raxis demonstrated the power of social engineering techniques. Organizations must fortify their defenses, educate employees, and stay informed to combat phishing attacks effectively.