Red Team Table Top Exercise: Banco do Brasil

Foreword

For this Red Team Table Top Exercise, I will be mainly using information from two sources. For the Introduction and the TTX Walkthrough Example, I will use the previous case study for this subject, with the title “Cybersecurity Threats to Banco do Brasil: A Risk Analysis”. I considered using this as a source due to the review of the case study and extensive knowledge gained on the topic, while writing the document. For the Intelligence Report Summary and Risk Register Entries, I will be using the Trend Micro blog article about cracking down on the Grandoreiro banking trojan, which affected multiple banks in multiple countries, with extensive cases especially in Brasil.

Introduction

Banco do Brasil, founded in 1808 in Rio de Janeiro, stands as Brazil’s first and oldest bank and is one of the largest financial institutions in Latin America. As a state-controlled entity with over 80,000 employees and branches in more than 20 countries, Banco do Brasil holds a critical position in the region’s finances, contributing significantly to the Brazilian economy [1]. This role makes it not only a bedrock of the national economy but also an attractive target for cybercrime. Over 90% of the bank’s transactions are now conducted digitally, which also increases Banco do Brasil and its customers to exposure to cyber threats, including financial fraud, extortion, data breaches, and insider threats [1]. As part of its commitment to bolstering cybersecurity defenses, the institution regularly assesses and updates its risk profile to anticipate and address emerging cyber risks.

Given its extensive digital reach and the valuable financial data it processes, Banco do Brasil faces both conventional and sophisticated cyber threats. To evaluate its resilience to these threats, this Table Top Exercise leverages insights from the Trend Micro articles. The exercise simulates possible attack scenarios and responses.

Intelligence Report Summary

For the exercise, I used the intelligence report from Trend Micro on the Grandoreiro banking trojan, available at https://www.trendmicro.com/en_us/research/24/d/trend-micro-collaborated-with-interpol-in-cracking-down-grandore.html. In this article researchers describe how Grandoreiro, a sophisticated banking trojan, has been targeting users in Latin America and Europe since 2018. The malware mostly spreads through phishing emails that impersonate financial institutions, aiming to steal sensitive financial information from victims [2]. Trend Micro, in collaboration with Interpol, supported law enforcement agencies in Brazil and Spain to analyze Grandoreiro's command and control infrastructure, resulting in the arrest of five administrators. The threat objective in this case is Financial Fraud, as Grandoreiro specifically targets banking credentials and personal financial data through malicious campaigns [2]. The seriousness of this threat objective is also highlighted in the previous case study [1].

Risk Register Entries

Phishing Emails Containing Banking Trojan Malware

Description:
The Grandoreiro trojan primarily spreads through phishing emails that impersonate legitimate financial institutions, leading users to download malicious attachments or visit fake websites [2]. In the TTX, this puts emphasis on the susceptibility to phishing attacks, especially those that bypass standard detection if they closely mimic trusted financial entities.

Likelihood: 9
Given that phishing is a very common initial attack vector for spreading the Grandoreiro trojan, and that phishing defenses often rely on user vigilance, when distributed, there's a high likelihood that similar tactics could succeed in our environment [2].

Impact: 8
If a user inadvertently downloads and installs Grandoreiro, sensitive financial data can be stolen, leading to potential financial losses and reputational damage, that comes with the misuse of the data [2].

Risk Score: 9 x 8 = 72 or HIGH

Remediation Task:
Develop a browser security add-on, that would help identify and block phishing sites attempting to impersonate the bank, reducing the likelihood of successful phishing attacks. This solution, combined with domain blacklisting, can significantly enhance client protection from this form of fraud. Assigned to the Software Development and Security teams, this add-on should be deployed within 90 days and updated regularly.

Command-and-Control Infrastructure Exploitation

Description:
The report indicates that Grandoreiro uses domain generation algorithms to establish

communication with C&C servers, evading traditional detection techniques. The TTX identified that the systems lack monitoring for unusual DNS queries, which could leave the bank vulnerable to similar DGA techniques.

Likelihood: 7
The use of DGAs for C&C is a common evasion technique among trojans [3]. Without proactive monitoring, it's feasible that an attack could exploit this gap.

Impact: 9
If the malware connects to its C&C servers, threat actors could maintain control over infected machines, leading to further data exfiltration or remote access, creating a severe threat to the bank's security [3].

Risk Score: 7 x 9 = 63 or HIGH

Remediation Task:
Deploy DGA-based anomaly detection on DNS traffic to flag suspicious patterns, assigning it to the Network Operations and Security teams. To be deployed within 60 days.

Exploitation of VBScript for Malware Execution

Description:
Grandoreiro's use of VBScript, as part of its infection chain, allows it to evade detection and execute malware efficiently [2]. This vulnerability emerged in the TTX, where it was observed that VBScript execution is currently not restricted on user machines, potentially allowing malicious scripts to run unchecked.

Likelihood: 8
VBScript remains a common scripting language that many organizations do not adequately restrict, making this a rather easy entry point for attacks like Grandoreiro.

Impact: 7
If a VBScript-based attack succeeds, it could initiate a broader malware campaign on the bank's systems, leading to loss of sensitive data and impacting operational continuity.

Risk Score: 8 x 7 = 56 or HIGH

Remediation Task:
Implement VBScript execution restrictions on all internal systems and apply endpoint security measures on the bank's own infrastructure. This would be assigned to the Endpoint Security team with a completion target of 45 days.

TTX at Banco do Brasil Walkthrough Example

The following scenario illustrates Banco do Brasil's potential response in this TTX and Encourages an honest evaluation of current cybersecurity defenses.

Scenario: A phishing email disguised as a legitimate bank notification is sent to several Banco do Brasil employees. An employee opens the email, believing it is genuine, and clicks a link that

downloads malware onto their system. This grants the attacker access to internal systems and paves the way for a ransomware attack.

- **Discussion Points**:
    - **Email Security and Phishing Detection**: How effectively do current email security restrictions detect and block phishing attempts? Would this email bypass existing set of filters?
    - **Employee Awareness and Training**: Are all employees equipped to recognize and report phishing attempts? How frequently is training conducted, and are there refresher courses to keep security top of mind?
    - **Incident Response Plan**: Once the malware infection is detected, what immediate actions are taken by the incident response team? Are response protocols effective in containing the infection and preventing escalation? Is the IRP, perhaps, outdated?
    - **Backup and Recovery**: In the event of a ransomware attack, are there tested, reliable backups to restore critical systems without data loss? Is there a team designated to those special occasions?
- **Post-Incident Actions**:
    - **Enhanced Phishing Simulations**: Conduct quarterly phishing simulation exercises to reinforce employee awareness and ensure quick identification and reporting. Keep track of the data for each simulation.
    - **Incident Response Plan Review**: Update incident response protocols for handling ransomware and insider threats, with special focus on early detection and containment.
    - **Audit and Monitoring Improvements**: Increase monitoring of user access logs to detect potential insider threats, conduct regular audits, and investigate unusual activity.

Conclusion

Banco do Brasil's increasing reliance on digital operations makes it more vulnerable to cyber threats, including phishing, ransomware, and insider attacks. This Red Team Table Top Exercise (TTX) identified critical weaknesses in the bank's defenses, especially in phishing detection and malware containment. The Grandoreiro banking trojan, a key example, exploits common vulnerabilities like phishing emails and domain generation algorithms (DGAs), presenting significant risks to the bank's operations and reputation.

Moving forward, Banco do Brasil must prioritize certain cybersecurity measures, including advanced email filtering, DGA anomaly detection, and enhanced endpoint security. Implementing VBScript execution restrictions and bolstering employee training on phishing threats are essential next steps. The bank should also strengthen its incident response protocols and ensure that its backup and recovery systems are fully prepared to handle ransomware attacks. Regularly reviewing and updating its cybersecurity framework, and conducting tests of how does it work out in practice, will be crucial to maintaining resilience against the threats.

References

[1] N. Baborova, "Cybersecurity Threats to Banco do Brasil: A Risk Analysis," Oct. 2024.

[2] "Trend Micro Collaborated with Interpol in Cracking Down Grandoreiro Banking Trojan," *Trend Micro*, Apr. 24, 2024. https://www.trendmicro.com/en_us/research/24/d/trend-micro-collaborated-with-interpol-in-cracking-down-grandore.html

[3] "What is DGA Attack? - zenarmor.com," *www.zenarmor.com*, Nov. 21, 2023. https://www.zenarmor.com/docs/network-security-tutorials/what-is-dga-attack