SECURITY INSIGHTS:

A Sneaky New Phishing Attack: Corrupted Word Documents

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

There's a new phishing campaign that's using a clever trick - **corrupted Word documents**. This technique allows malicious content to pass through to the user without detection by any email security tools.

The attacker intentionally (slightly) corrupts the attached Word document so that antivirus and security scanners can't scan it. Because the file has a .docx extension, when the unsuspicious victim opens it, Microsoft Word detects the corruption and asks the user if they want to repair it. If the user confirms, Word will repair and open the file.

Inside the recovered file is a QR code that leads to a credential harvesting page that steals both the user's credential and the MFA.

The timing of this attack is impeccable. Security firm Any.Run, which discovered it, found that the email appeared to come from Human Resources and focused on end-of-the-year benefits and bonus payouts.

Takeaways:

- Hackers frequently time and theme their attacks to seasonal, disaster or business events - always stay alert during business seasonality (i.e., end-of-month, quarter, year activities, benefits, payouts, income-tax events)
- Attackers continuously attempt to find ways to stay under the radar of security technologies - always proceed with caution
    - Every attachment from an unknown source should be considered malicious until proven otherwise
    - Any new behavior (recovery of corrupted attachment) should be a red flag
- QR codes have alarmingly become mainstream for cybercrooks due to the inability to analyze the destination with the naked eye. Scrutinize all QR codes and avoid using them in emails and attachments if possible.
- Do not enter any credentials on the site you landed on from the email or attachments unless it came from a trusted and verified source