SECURITY INSIGHTS:

The Rising Threat of Identity Phishing via File Hosting Services

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

In the constantly changing world of cybersecurity, threat actors are always adjusting their methods to take advantage of new weaknesses. According to Microsoft Threat Intelligence, one of the recent trends involves using legitimate file-hosting services for identity phishing. Services like SharePoint, OneDrive, and Dropbox are important for businesses as they provide a platform for storing, sharing, and collaborating on files. However, because of their widespread use, they have become attractive targets for cybercriminals. These services are being misused to distribute malicious files and links, often getting around traditional security measures because users inherently trust these platforms. The phishing campaigns that use these file hosting services employ sophisticated tactics to avoid detection, such as using files with restricted access and view-only permissions, making it difficult for email security systems to recognize and block malicious activities.

Attackers often use social engineering to trick users into opening malicious files or links. These files can be delivered through various means, such as email attachments in formats like PDFs, OneNote, and Word documents. Once a user interacts with these files, their identities or devices can be compromised, leading to further attacks such as business email compromise (BEC), financial fraud, and data exfiltration.

Adopt a multi-layered security approach to thwart these types of attacks:

- Both Microsoft 365 and Office 365 support MFA and passwordless sign-in by default. Enabling these features can significantly reduce the risk of account compromise
- Verify sender. It's not uncommon for attackers to use legitimate email addresses from common platforms like Microsoft, Google, or Yahoo
- If you recognize the sender but are not expecting the email or want to validate context legitimacy, contact the sender out-of-band
- **Don't enter credentials on the website you landed from the email link**

As cyber threats continue to evolve, staying informed and proactive is essential.