SECURITY ALERT

Cyber Defense Intelligence

October 13, 2023

SECURITY ALERT: DropBox BEC (Business Email Compromise)

Researchers have discovered a new business email compromise (BEC) tactic involving the use of Dropbox messages to steal Microsoft user credentials. The tactic has been linked to over 5,000 attacks during the first two weeks of September 2023.

How does this new tactic work?

- The target receives a message that appears to come directly from Dropbox, advising the victim they have files to download
- The message contains a link to a page hosted on a legitimate Dropbox URL; however, the page resembles the Microsoft OneDrive login page
- The victim is prompted to enter their credentials, which is actually collected by a credential harvester

This tactic is effective in both its simplicity, and its ability to evade standard security countermeasures. The use of language pulled from legitimate services will not trigger Natural Language Processing (NLP) technology. Similarly, URL scanning is also ineffective due to the use of legitimate Dropbox addresses.

Mitigation Strategies:

- Security Awareness Training
- Email Verification
- Security solutions including document and file scanning

Conclusion:

BEC attacks continue to increase in popularity and threat actors continue to evolve in the "current BEC 3.0" environment of cloud services. Although threat actors have always imitated legitimate entities, the move to BEC 3.0 provides savvy threat actors

the ability to spoof real cloud based services. This evolution increases the difficulty of identifying and thwarting these types of attacks.

For more details: https://blog.checkpoint.com/harmony-email/phishing-via-dropbox/