NDVR Endeavour Foundation

Edition 2

You've Got Mail and Malware: New QakBot Email Scam

You may have seen a suspicious email that appears to come from a trusted source, such as a friend or a popular brand. But have you ever seen a suspicious email that appears to come from you? In a new scam, cybercriminals use your own email address to send phishing links to other users.

The scam works by using the newest version of malware called QakBot. To begin the scam, cybercriminals send you an email that contains a phishing link. If you click on the link, QakBot will be installed on your computer. The newest version of QakBot can record your keystrokes, steal your login credentials, and even access your email accounts.

If QakBot is installed on your computer, cybercriminals can use your email account to send phishing emails to users in your email threads. Using the "Reply to All" functionality, QakBot will send the phishing emails to users you have already interacted with. Since the phishing emails will look like they came from your email address, they will appear more trustworthy and will be difficult to spot.

Follow the tips below to stay safe from these types of scams:

- Watch out for a sense of urgency in emails or messages that you receive. Phishing attacks rely on impulsive actions, so always think before you click.
- Never click on a link or download an attachment in an email that you were not expecting, even if the email seems to come from someone you know.
- Watch out for emails that contain only a short message and a link. If you're unsure if the link is safe, reach out to the sender by phone to confirm the email is legitimate.

Stop, Look, and Think. Don't be fooled.