MALWARE SECURITY ALERT SCAM

Malware security alert scams aim to trick users into believing that malware has compromised their devices, data or applications. Victims may receive fake alerts as pop-ups on browsers or be targeted by email. These alerts claim that the user's applications or data have been compromised, and that immediate action is required, such as clicking a link to reactivate a subscription for antivirus software. The criminal creates a sense of urgency using language such as "Your device has been infected" or "Immediate action is required to avoid further data leaks." The message may appear to come from a legitimate security software company, potentially using its name, logo and/or branding to gain victims' trust. After victims click on the link to reactive their subscriptions, the criminals ask the victims to provide personal information or payment details, which they can then leverage for financial gain.

In some instances, the scam message may include a tech support number to call for assistance, which connects the victim to a call center. Speaking directly to the victim, the call center agent persuades the victim to download remote access software, allowing criminals to take control of the victims' computers to install malware, steal login credentials or change passwords. Additionally, the agent may attempt to convince victims to make unnecessary payments for fake software or customer support services.

These call centers are set up and operated by international organized criminal rings where people may have been trafficked and forced to scam victims. In many instances, the agents on the other end of this scam are victims themselves.

Refer to page 2 for a malware security alert scam example.

MALWARE SECURITY ALERT SCAM

1

Kevin is checking his email when he notices a message from a recognized software company with the subject line, "Warning: data compromise." Concerned, he opens it to learn more.

2

The message says his device has been compromised by malware and prompts him to click a link to reactivate his expired antivirus software. He calls a customer support number in the message.

3

An agent warns Kevin that if he does not act soon, he risks further compromises to his device and personal data. She says the quickest way to address the issue is for her to remote into his computer to help him download the required software.

4

Panicked, Kevin agrees. He downloads the remote access software as requested so the agent can take control of his device. After the download, she tells Kevin he does not need to take further action to protect his device or data.

5

The download was malware. The criminal uses the malware to steal Kevin's checking account credentials. She logs into Kevin's account, changes his password and phone number, then transfers $3,000 from his account to a money mule account.

6

The next day, Kevin tries to log into his checking account but receives a message that his credentials are invalid. He contacts his bank to ask why he has been locked out of his account.

7

The bank's representative tells him his account credentials were changed the previous day, and that a transfer was made to a new receiver account soon after.

8

Kevin explains that he never made that transfer. The bank freezes his account and begins to investigate the incident.