Current cyber threat implications of COVID-19

April 3, 2020

Cyber threat actors and organized criminals are attempting to exploit and cash in on our need for information related COVID-19. This coupled with the exponential shift to a remote workforce has exposed new attack vector(s) for exploitation by these nefarious groups. COVID-19 themed spear-phishing campaigns were launched immediately in concert with the World Health Organization's declaration.

These phishing campaigns fall into three main categories that are utilizing social engineering lures that request:

Personal information: In exchange for information related to government economic stimulus checks, loan or mortgage abatement, airline refunds, or other types of economic relief.

Fraud: These take the form of brokerage or retirement emails that result in an account takeover (e.g., "In light of COVID, we're asking you to move your money to a different account."), fake charitable contributions, fake cures, counterfeit testing kits and vaccines, or counterfeit personal protective equipment.

eCommerce: With more people at home and ordering online, the order volumes have increased exponentially. Fraudsters are using this to hide in the volume through the following types of phishing schemes: ATO (account takeover) of dormant accounts and return/refund/replacement fraud.

The more sophisticated phishing campaigns will utilize the above lures to entice individuals to click malicious links that download remote administration tools (RATs) on their devices.

Virtual private network (VPN) targeting of remote workers has also increased, and most recently ransomware threat actors have adopted new tactics by searching for unpatched vulnerabilities in VPN servers to facilitate deployment of malware.

Overall, cyber threat actors will continue to take advantage of the current global uncertainty and disruption.

KPMG Cyber Services recommends the following steps to keep information and employees safe:

- Ensure staff are aware of reputable sources of COVID-19 information (e.g., federal and local government sites)
- Remind remote workers to:
  - Avoid clicking on information propagated via social media
  - Not click on emails and attachments from unknown sources
  - Not forward emails from external or nonreputable sources
  - Beware of transactional or information requests from perceived "trusted" sources (which would normally be validated via phone or face to face)
- Review your remote access, including:
  - Updating security settings/configurations
  - Ensuring approved access methods are used by staff
  - Confirming remote user lists are up to date and access privileges are appropriate
- Verify that the level of security and operational monitoring and defined exception events are appropriate (e.g., baselines for peak usage times may differ)
- Remind staff of approved cloud-based services and expectations around appropriate use.

In addition, we recently published a new paper around what information security professionals can do to keep their business going during this challenging time. To access that paper, click here.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Contact us

Tony Buffomante
Principal
Cyber Security Services
E: abuffomante@kpmg.com

Ed Goings
Principal
Cyber Security Services
E: egoings@kpmg.com

Ron Plesco
Principal
Cyber Security Services
T: 717-260-4602
E: rplesco@kpmg.com