SECURITY Smart™ NEWSLETTER

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

3 Ways Cybercriminals Are Exploiting the COVID-19 Crisis

Cybercriminals are taking advantage of the coronavirus crisis to spread malware, disrupt operations, sow doubt and, as always, make a quick buck, via virus-themed emails, apps, websites and social media. Here are some of the techniques you need to watch out for:

1 Phishing emails

Sending unsuspecting recipients emails related to current tragic events is a classic tactic cybercriminals use to snag victims, and this pandemic is no exception. Themes in these emails include analyst reports specific to certain industries, details of official government health advice, requests for donations, and offers of face-masks or other assistance regarding operations and logistics. These emails often contain malicious links or attachments, or requests for sensitive information. Delete them, and never click on the links or open the attachments.

“Our threat research team has observed numerous COVID-19 malicious email campaigns, with many using fear to try and convince potential victims to click,” says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint. She says around 70 percent of the emails the threat team has uncovered deliver malware, with most of the rest aiming to steal victims’ credentials through fake landing pages like Gmail or Office 365.

DID YOU KNOW?

- 94% of malware is delivered via email.
- Phishing attacks account for more than 80% of reported security incidents.
- Every minute, $17,700 is lost due to phishing attacks.
- Data breaches cost enterprises an average of $3.92 million.

2 Malicious apps

Although Apple has placed limits on COVID19-related apps in its App Store and Google has removed some apps from the Play store, malicious apps can still pose a threat to users. One site, for example, urged users to download an Android app that provides tracking and statistical information about COVID-19, including heat map visuals. However, the app was actually loaded with an Android-targeting ransomware now known as COVIDLock. The ransom note demanded $100 in bitcoin in 48 hours and threatened to erase contacts, pictures and videos, as well as the phone’s memory.

3 Bad domains

New websites are springing up that purport to disseminate information relating to the pandemic. In fact, many of them are traps for unsuspecting victims. Recorded Future, a company that analyzes threat data, has found that hundreds of COVID-19-related domains are being registered every day. The UK’s National Cyber Security Centre has reported fake sites that are impersonating the U.S. Centers for Disease Control (CDC) and creating domain names similar to the CDC’s web address to request passwords and bitcoin donations to fund a fake vaccine.

> “Hackers and cybercriminals think like marketers—they’re always looking for trends and how to market their scams. [Videoconferencing] is trending, work from home is trending, coronavirus is trending, so we’re seeing a lot of new types of threats because of that. It hits everyone because people are more dependent on technology today than ever.”
>
> – Gabriel Friedlander, founder of the security awareness training firm Wizer

CSO FROM IDG
Security Smart is published by CSO, the leader in news, analysis and research on security and risk management.
If you have questions or topic suggestions email **securitysmart@idg.com** or **marketing@idg.com** for more information.