Auto Casualty

5 COVID-19 Security Threats to Know About

June 25, 2020
4 MIN READ
Author profile image

Mike Cwynar

Senior Vice President, Product Delivery

Some studies estimate that more than half of the workforce is working from home amidst the COVID-19 crisis, and many companies have already announced plans to allow employees to work remotely even after the threat of the virus has subsided. While working from home has helped social distancing efforts across the country, it has also opened up companies to an onslaught of new security threats.

Emerging COVID-19 Security Threats

The COVID-19 pandemic has brought about a variety of security challenges for companies and individuals around the world. For example, the U.S. saw cyberattacks peak this year on April 7, 2020 with a total of 1,417,827 attacks, according to an Atlas VPN report. This was a 330% increase during the period March 10–April 10, 2020, compared to the average attack volume between February 9 and March 9, 2020. As cyber-attacks increase and the pandemic continues, there are a few key emerging COVID-19 security threats that companies should be aware of and prepare to address.

Coronavirus-Related Domain Names

From March 9 through April 26, there were 1.2 million newly registered domain names containing keywords related to the COVID-19 pandemic, according to TechRepublic. Out of those 1.2 million new domains, 86,600, or about 7%, are classified as “risky” or “malicious”—heightening cyber risk. There has been an increase in email scams that impersonate organizations like the Center for Disease Control (CDC) and the World Health Organization (WHO). Companies should be aware of these fake domain names as many are focused on phishing or spreading malware.

Direct Calls and Text Messages to Consumers

The Federal Trade Commission and Federal Communications Commission have reported an increase in robocalls and direct text messages "to profit from COVID-19 fears." Many of these calls are phishing exercises disguised as insurance or health organizations and are intended to collect personal information or attempt to sell fake testing kits.

Personal Computers Used for Work Related Tasks

One risk to working from home is that some positions and departments allow employees to use personal computers and mobile devices for work related tasks. According to DataProt 11% of personal desktops, 20% of personal laptops and 50% of mobile phones and tablets do not have antivirus installed. Working remotely also boosts the likelihood of employees connecting to public Wi-Fi connections. Without properly implementing security measures for a remote workforce, such as requiring antivirus and VPN access, it's possible that an employee's personal computer could be easily hacked, resulting in an increase in exposure to data breaches.

Telemedicine Storage

Since the start of the pandemic, telemedicine usage has increased at an incredible rate, with some telehealth providers reporting the number of virtual visits have doubled compared to last year. As providers shift to telemedicine to deliver care, some smaller medical practices are using personal mobile devices and the public cloud to store sensitive documents, which creates a security risk for medical records. Companies need to be aware of the difference between public cloud storage and more secure alternative (i.e. HIPAA compliant) cloud storage solutions that provide a higher level of data security.

Hardware Shortages

The COVID-19 pandemic has also resulted in computer hardware shortages, which has led to increased use of used devices. Companies should practice diligence as they reinitialize used hardware to make sure that malware isn't installed on the devices.

Steps to Take to Address Emerging COVID-19 Security Threats

There are a few steps that companies can take to help address these emerging security threats and any unknown concerns that may arise as the pandemic continues.

Company Issued Computers

Provide appropriate hardware to remote workers as much as possible to ensure that basic security requirements are being met. Company provided hardware can also be monitored for security threats vs a personal computer.

Multi-Factor Authentication

Make sure that all remote staff are using multi-factor authentication over VPN for secure connectivity.

Training

Continuously update security training programs to include COVID-specific phishing scenarios and educate employees so that they are aware of new security threats.

Partner Management

Increase the frequency of security assessments and audits for all partners and make multi-factor authentication mandatory for everyone with remote access to data.

Secure Data Management

As new remotely-accessible data storage solutions are added, be sure they provide a sufficient level of security and data protection.

Pandemic Plans

Create and refresh your pandemic-specific business continuity plans to address emerging threats.

Monitoring

Continuously monitor federal security channels for emerging trends. Some recommended channels to follow include the Cyber Security and Infrastructure Security Agency Coronavirus page, the Department of Homeland Security Cybersecurity page and the Federal Communications Commission COVID-19 Scams page. By building a strong security foundation and continuously monitoring new threats, companies can be well positioned to protect their data from COVID-19 security threats as they exist today and as they grow and change as the pandemic continues.

mitchell | genex | coventry