Malware:
What You Need to Know About the Cybercriminal’s Tool of Choice

Cybercriminals capitalize on computer weaknesses. Their objective is to exploit and collect sensitive data that can be used for either profit or bragging rights...and their tool of choice is malware.

Malicious software, known as malware, is any software designed to:

- **disrupt** computer operations;
- **collect** confidential or sensitive information; or
- **gain** unauthorized access to computer systems.

Cyberattacks are an ongoing and ever-evolving threat to healthcare providers.

Knowing that malware is the tool of choice for most hackers, it’s crucial to understand how it works and the form it takes so that you can better prepare your defenses.

How Malware Works

Malware can be a virus, application, or any unwanted software that gets installed on a computer or mobile device without the user’s consent. It is typically installed when a user:

- **clicks** on a link in an email (rather than typing the URL directly into a browser);
- **opens** an email attachment; or
- **browses** to an infected website.

Hackers also bundle malware with popular free downloads.

BLUE ORANGE COMPLIANCE

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com

Malware: What You Need to Know About the Cybercriminal's Tool of Choice

8 Popular Forms of Malware You Need to Know

1. **Virus**

   A virus is a form of malware that infects programs and data files. Viruses can be transmitted as attachments to an email, in a downloaded file, or through external devices.

2. **Worm**

   A worm is a malicious payload that can infect operating systems. Worms are designed to replicate themselves through a network or organization without additional input or guidance from the hacker. While worms can infect a system when a user clicks on an attachment, they can also propagate as a result of network vulnerabilities, infected file shares, links to infected websites, and other creative methods.

3. **Spyware**

   Spyware is a type of malware that collects information or takes control of a computer without the user's consent or knowledge. Spyware can monitor a user's computer habits as well as detect and gather sensitive data. Cybercriminals may also piggyback spyware onto legitimate software. The presence of spyware is typically hidden and can be difficult to detect.

4. **Keylogger**

   A keylogger is an application that records keystroke on an affected computer. Hackers then use the information captured to gain access to passwords or other confidential information.

5. **Botnet**

   The term "botnet" is blend of the words "robot" and "network." A "bot" is a form of malware that infects a computer, remaining hidden until commanded by a hacker to complete a task. Hackers distribute bots across the internet in search of unprotected computers to infect. Once a series of computers has been infected, a "botnet" has been created. Hackers typically use botnets to transmit additional content, circulate spam, steal sensitive personal information, and generate denial of service attacks.

Malware:
What You Need to Know About the Cybercriminal's Tool of Choice

6. Ransomware

Ransomware is a type of malware that restricts access to the infected computer system, followed by demands that the user pay a ransom to the malware operators to remove the restriction. This is the only type of malware designed to notify a user that the infection has occurred. Once the ransomware has locked the files, it will announce what it has done, and communicate ransom demands.

7. Trojan

A Trojan is used to install malware, but typically does nothing else of ill intent. Trojans are often disguised as legitimate software and used by hackers to create a "backdoor" into a system that can later be used to gain access. Ransomware usually propagates with a Trojan.

8. Cryptojacking

In 2018, the practice of cryptojacking systems surpassed the use of ransomware. Unlike ransomware, the aim of the hacker running a cryptojacking campaign is to remain unnoticed for as long as possible. It begins when a user's computer is infected with malware designed to generate or mine cryptocurrencies such as bitcoin, litecoin, or monero. The longer the malware goes unnoticed, the longer the hacker can use the system to keep mining the cryptocurrency, creating a higher payoff.

A machine can become infected with cryptojacking malware from many of the same sources as traditional malware, including browser-based infections, phishing campaigns, or existing vulnerabilities on enterprise networks. Even when the source of the infection is determined or malware is detected, the path leading back to the hacker is virtually untraceable.

Cryptojacking malware can be a strain on system resources, causing slower performance, system overheating, and higher utility costs. In extreme scenarios, the malware can overwhelm system resources and disable the system altogether.

Cyberattacks are an ongoing and ever-evolving threat to healthcare providers. **The key is to be prepared.** Develop a system of protecting against cyberthreats, detecting them, responding to them, and recovering from them. With a solid system in place, a provider can prevent attacks and mitigate the effects if breaches should they occur.

BLUE ORANGE® COMPLIANCE

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com