D.L. Evans | BANK

What is Ransomware?

Ransomware is a type of malware that locks a victim's data or device and threatens to keep it locked unless the victim pays a ransom to the attacker.

The earliest ransomware attacks simply demanded a ransom in exchange for the encryption key needed to regain access to the affected data or use of the infected device. By making regular or continuous data backups, an organization could limit costs from these types of ransomware attacks and often avoid paying the ransom demand.

In recent years, ransomware attacks have evolved to include double-extortion and triple-extortion attacks that raise the stakes considerably—even for victims who rigorously maintain data backups or pay the initial ransom demand. Double-extortion attacks add the threat of stealing the victim's data and leaking it online, and triple-extortion attacks threaten to use the stolen data to attack the victim's customers or business partners.

Types of Ransomware

There are two general types of ransomware. The most common type, called *encrypting ransomware* or *crypto ransomware*, holds the victim's data hostage by encrypting it. The attacker then demands a ransom in exchange for providing the encryption key needed to decrypt the data.

The less common form of ransomware, called *non-encrypting ransomware* or *screen-locking ransomware,* locks the victim's entire device, usually by blocking access to the operating system. Instead of starting up as usual, the device displays a screen that makes the ransom demand.

Prominent Ransomware Infection Vectors Include:

- Phishing emails | social Engineering Attacks: Phishing emails manipulate users into downloading and running a malicious attachment (which contains the ransomware disguised as a harmless looking .pdf, Microsoft Word document, or another file), or into visiting a malicious website that passes the ransomware through the user's web browser.

- Operating system and software vulnerabilities: Cybercriminals often exploit existing vulnerabilities to inject malicious code into a device or

network. Zero-day vulnerabilities, which are vulnerabilities either unknown to the security community or identified but not yet patched, pose a particular threat. Some ransomware gangs buy information on zero-day flaws from other hackers to plan their attacks.

- Credential theft: Cybercriminals may steal authorized users' credentials, buy them on the dark web, or crack them through brute force. They may then use these credentials to log into a network or computer and deploy ransomware directly. Remote desktop protocol (RDP), a proprietary protocol developed by Microsoft to allow users to access a computer remotely, is a popular credential-theft target among ransomware attackers.
- Drive-by downloads: Hackers can use web sites to pass ransomware to devices without the users' knowledge. Exploit kits use compromised web sites to scan visitors' browsers for web application vulnerabilities they can use to inject ransomware onto the device. Malvertising – legitimate digital ads that have been compromised by hackers can pass ransomware to devices, even if the user doesn't click the ad.

Cybercriminals don't necessarily need to develop their own ransomware to exploit these vectors. Some ransomware developers share their malware code with cybercriminals via ransomware-as-a-service arrangements. The cybercriminal, or 'affiliate,' uses the code to carry out an attack, and then splits the ransom payment with the developer. It's a mutually beneficial relationship: Affiliates can profit from extortion without having to develop their own malware, and developers can increase their profits without launching additional cyberattacks.

Source: https://www.ibm.com/topics/ransomware

Important Information

D.L. Evans Bank will not request personal or sensitive information (full social security number, passwords, full debit/credit card number, or PINs) when contacting you. However, D.L. Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious

of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00am – 5:00 pm.