RANSOMWARE: IT'S PERSONAL

If you've heard of ransomware attacks but are confident that you're not a target — think again. Your personal devices and network are at risk, and so are the businesses and organizations with whom you and your family interact. Consider that:

- Home sales in a major U.S. city were suspended when real estate records couldn't be accessed.
- A 911 response center was impacted when computers at the local fire and police departments were temporarily offline.
- A public school system unexpectedly suspended remote learning when they lost access to servers.
- Medical procedures were postponed when a healthcare system's access to medical records was restricted.

Ransomware attacks are a threat to everyone. That's why it's vital to know how to identify cybercrime and to protect yourself.

WHAT IS RANSOMWARE?

Ransomware is malware that attempts to prevent users from accessing data by encrypting it with a cryptographic key that is known only to the hacker.[1] The data — which is typically critical to business or system operations — is unusable until the victim pays a ransom. A pop-up message on the locked screen notifies the victim of the ransom's terms. In some cases, the hacker threatens to sell the encrypted data.

Verizon estimates that in 2020, ransomware attacks accounted for 27% of all malware activity. This is a 20% increase from 2019.[2] These attacks can result in:

- Temporary or permanent loss of sensitive information, personal files and data
- Financial losses related to the restoration of systems and files
- Disruption to business operations

WHO IS IMPACTED?

Initially, ransomware criminals attacked personal computers; however, these professionals are increasingly targeting government entities, nonprofit organizations and businesses of all sizes. According to PNC Enterprise Technology & Security experts, small to medium-sized businesses are primary targets because they often have a simple network infrastructure, lack dedicated information technology and security personnel, or have insufficient access to control policies.

Report the attack! Contact a local Federal Bureau of Investigation (FBI) Field Office and/or file a complaint with the FBI's Internet Crime Complaint Center.

RANSOMS AND REPORTING

The FBI doesn't recommend paying ransom to any criminals because:

- It doesn't guarantee you will regain access to your data and/or systems.
- Criminals don't always provide decryption keys.
- The same or other cybercriminals might repeatedly target you.
- This may encourage more ransomware crime.
- You might incur fines and civil penalties for violating the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) laws, which prohibit transactions with a sanctioned entity.

Ransomware attackers are professional, organized criminals. According to PNC Enterprise Technology & Security, they reinvest the ransoms to develop better attack tools and talent.

REMINDER: If you receive a suspicious email or text that claims to be from PNC, forward it to PNC Cyber Defense at abuse@pnc.com, and include background information in your email.

PNC BANK

METHODS OF ATTACK

Attackers have many methods of delivering malware, including:

- **Phishing emails:** An email recipient opens a malicious attachment or clicks on a compromised link.
- **Drive-by download:** A compromised website downloads malware onto your device without your knowledge.
- **Strategic attacks:** These attacks target software vulnerabilities.
- **Remote desktop protocol compromise:** A user logs on to a computer remotely, and hackers use brute force methods and credentials that they purchased on the dark web.

TAKE PRECAUTIONS

The best defense is prevention. The tips below, while not all-inclusive, can help protect your business and personal devices from attack:

- **Never click on links or open attachments in unsolicited emails or texts:** Verify that the email or text is legitimate with the sender and only use known contact information, not the information within the suspicious email/text.
- **Update software and operating systems with the latest patches:** Hackers target outdated applications and operating systems.
- **Regularly back up your data on a separate device:** Store the device offline.
- **Don't respond to requests for sensitive personal or financial information:** Verify requests first with the sender using known contact information. Don't use the contact information within the email or text.
- **Maintain up-to-date antivirus software:** Scan software you downloaded from the internet before you install it.

RESPONDING TO AN ATTACK

If you receive a ransomware message, stop it from spreading to shared network resources (such as file shares) by:

- Unplugging ethernet cables
- Turning off Wi-Fi and Bluetooth
- Putting the device on airplane mode
- Disconnecting external devices, such as USB drives, phones and cameras
- **Report the attack!** Contact a local Federal Bureau of Investigation (FBI) Field Office and/or file a complaint with the FBI's Internet Crime Complaint Center.

[1] National Institute of Standards and Technology (NIST), "Small Business Cybersecurity Corner Glossary," accessed May 17, 2021, https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

[2] 2020 Verizon, "2020 Data Breach Investigations Report," accessed May 17, 2021, https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf

These articles are for general information purposes only and are not intended to provide legal, tax, accounting or financial advice. PNC urges its customers to do independent research and to consult with financial and legal professionals before making any financial decisions. This site may provide reference to internet sites as a convenience to our readers. While PNC endeavors to provide resources that are reputable and safe, we cannot be held responsible for the information, products or services obtained on such sites and will not be liable for any damages arising from your access to such sites. The content, accuracy, opinions expressed and links provided by these resources are not investigated, verified, monitored or endorsed by PNC.