RANSOMWARE TARGETS BUSINESS COMMUNITY

Learn more about this cybercrime and precautions to help protect your company or organization.

Initially, ransomware criminals targeted personal computers. Now, they are focusing on government entities, nonprofit organizations and businesses of all sizes. For example, ransomware attacks have forced gas pipelines to shut down and hospitals to turn away patients, leaked confidential information at law firms and police departments, and left multinational manufacturers with no other option than to shut down manufacturing production.

Although schools, hospitals and government entities have been recent victims, no business is immune to these attacks. During the COVID-19 pandemic, ransomware criminals who focus on remote services and their vulnerabilities discovered a wealth of new opportunities thanks to work-from-home policies. That's why it's important to know how to identify ransomware attacks and to discover how you can 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

Ransomware is openly marketed on the dark web. To best position their attack, crime groups penetrate networks to perform reconnaissance, which can intensify the impact on the victim and potentially maximize the ransom.

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.

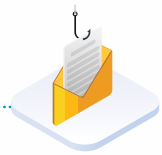
REMINDER: If you receive a suspicious email or text that claims to be from PNC, forward it to PNC Cyber Defense at abuse@pnc.com, and include background information in your email.

PNC BANK

TAKE PRECAUTIONS

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

- Maintain offline, encrypted backups of data, including system images and configurations. Test your backup data and files regularly — after all, there's no need to pay ransom for data that's accessible via backup.
- Install software updates and patches as soon as possible.
- Ensure that antivirus and anti-malware software is set to automatically scan and update.
- Establish basic security practices and policies for employees, including strong passwords and multifactor authentication.
- Educate employees on social engineering and phishing, including how to spot red flags and report suspicious activity.
- Restrict internet access. Use a proxy server for internet access, and implement ad-blocking software. Restrict access to common ransomware entry points, such as social networking websites.
- Use a secure email gateway/system to detect and block malicious emails, flagging external emails to alert employees of potential spoofing.
- Block all unauthorized software from executing on all devices and servers.
- Conduct regular vulnerability scanning and perform penetration testing to find and patch vulnerabilities.
- Apply a policy of "least privilege" to all systems and services; users can only access required platforms.
- Monitor your server, network and backup systems to detect unusual file access activities and network activity.
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification to lower risk of spoofed or modified emails from valid domains.



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 which they purchased on the dark web.

RESPONDING TO AN ATTACK

If you ever experience a ransomware attack, don't panic. Take these steps:

- Disconnect the infected system from the network to contain the spread.
- Determine if a decryption key may be available; other organizations may have investigated similar malware.
- Restore files from regularly maintained backups.
- Notify your financial institution, customers and third parties that might have been affected by the attack.
- **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.

A post-event investigation is also recommended. This will help to determine the mode of infection, strengthen your preventive controls and improve your incident response plan.

For more information, visit the Cybersecurity & Infrastructure Security Agency's (CISA) Multi-State Information Sharing & Analysis 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

CON PDF 0520-057

PNC BANK