ransomware.org
understand · prevent · recover

BY ActualTech Media

Ransomware

Being Prepared Leads to Successful Recovery

Ransomware attacks are on the rise! Enterprise data has become a very lucrative target for cybercriminals. Even with robust defense mechanisms in place, ransomware attacks continue to increase. In the first half of 2020, there were approximately 2.5 million new ransomware attacks, according to the November 2020 *McAfee Labs Threat Report*.

According to the U.S. Department of Health and Human Services Fall 2019 OCR Cybersecurity Newsletter, the FBI estimates that cybercriminals will earn over **$1 billion in ransom**.

The U.S. Cybersecurity and Infrastructure Security Agency's (CISA) ransomware site defines ransomware as: *a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.*

TYPES OF RANSOMWARE ATTACKS

Encryption ransomware: Encrypts files, folders, and shared network storage.

Network-attached storage (NAS) ransomware: Encrypts and/or deletes files on home directories, virtual machine (VM) hypervisor backups, shadow volumes, and backup files.

Lock screen ransomware: Locks the user's computer screen and demands payment, but no personal files are encrypted.

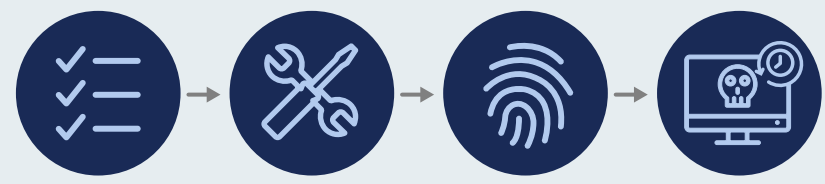
Hardware locker: Changes the computer's master boot record (MBR), preventing the operating system from properly starting.

Application/web server encryption: Encrypts files and web servers through application vulnerabilities.

Ransomware as a Service (RaaS): Widely available on the Dark Web, RaaS enables practically anyone to attack an organization.

Data exfiltration: Reads critical data from the attacked systems and copies it to the attacker.

Taking the time to prepare for a ransomware attack is key to successfully recovering from one.



RANSOMWARE PLAN BEST PRACTICES FOR A SUCCESSFUL RECOVERY

- **Response and recovery plan with playbook:** These should be reviewed and updated periodically and stored in a secure, post-attack accessible manner (such as a printed copy).
- **Employee response team:** Include stakeholders across departments and specify who will be responsible for executing and managing the plan. Hold training sessions and perform drills.
- **Communication plan:** Give thought to what will be inaccessible, and then identify alternate means of communicating both internally and externally.
- **Prioritize system recovery:** Knowing which systems need attention first and how they interact with other systems will facilitate a smooth and orderly recovery.
- **Data backup:** There are so many choices now for backup solutions, so determine what is best for your business: locally, offsite, cloud – you choose.
- **System protection:** Ensure all critical systems and data are being protected in a manner that guarantees Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) can be met.
- **Tools to identify affected data:** Having this data during an attack will be invaluable in speeding up recovery and preserving uninfected data.
- **Practice your plan:** Without testing, there can be no assurance that the recovery plan will work when an attack happens. Testing also provides the experience and confidence to response team members.

Want more ransomware information? Go to ransomware.org >