ebook

Ransomware

Learn about the steps hackers take to execute ransomware attacks and how you can keep your network safe.

radius180
Managed IT Solutions

Ransomware

What is it?

Ransomware is a type of malware specifically designed to capture information by locking data and files via encryption. Once obtained, hackers will extort their target by refusing to release data until they are paid a predetermined amount of money.

With the largest payout in 2021 being $40 million, the ransom is rarely cheap. The US Government reported about 4,000 ransomware attacks daily, predicting that the frequency will continue to trend upward in 2023. Avoid becoming a target by educating yourself in the following pages.

The Process of Ransomware

Stage 1: Reconnaissance

Hackers will take inventory of your organization's IT infrastructure and security. They look for vulnerable accesses and entry points to your systems by scanning your organization's network and ports.

What you can do:

In order to recognize when a hacker is targeting your organization at this stage, it needs to have the ability to detect when scans are performed on your network. To install software that can do this, contact a local MSP or your IT department.

The Process of Ransomware

Stage 2: Weaponization

At this second stage, hackers will adjust the code of the ransomware so that it won't be able to be traced or detected by networks and/or file-based security measures. For example, hackers can adjust the payload to make it look like a simple, unassuming word document.

What you can do:

The best way to evade this step is to be proactive. Make sure to always update software when new security patches and updates become available. Also, install software that can identify high-risk devices and outdated operating systems. For this step, the best way to avoid being a victim is to be proactive.

Stage 3: Delivery

At this stage, the hacker loads the ransomware into your organization's system and there are a variety of ways they can do this. The most common way is via email. Phishing has long been a favorite for delivering viruses for hackers as infected attachments or directing the user to a malicious website. Other ways include plugging in a compromised USB or gaining access from employee credentials via social engineering

What you can do:

There are a variety of techniques to combat an attack at this stage. Micro-segmentation (quarantining the small section of a device that is compromised), change management, and application whitelisting are just a few. The appropriate action depends on the specific attack.

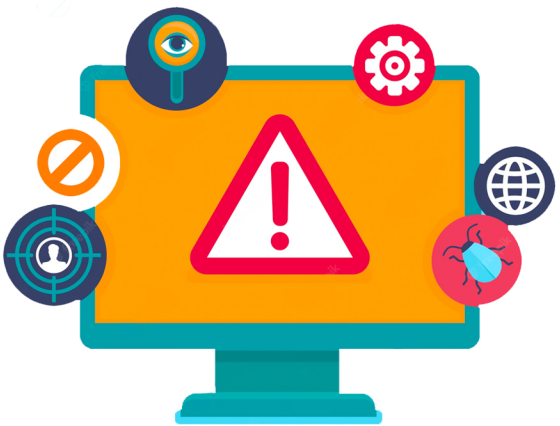
The Process of Ransomware

Stage 4: Exploitation

During this stage, the ransomware infects the victim's device. There are two ways this is done. If a specific vulnerability is known the hacker will launch a targeted exploitation. If it isn't know, they will launch an exploit kit. This is a sort of toolbox hackers use to attack common vulnerabilities in a system so they can distribute the ransomware.

What you can do:

Enable continuous network monitoring so your I.T. team will be notified in the event of suspicious or irregular activity. In addition, the best offense is a good defense. Be sure your network is as secure as possible by allowing security patching, multifactor authentication, and strong passwords.



radius180

The Process of Ransomware

Stage 5: Installation

If hackers reach this step without interference, the virus will begin to distribute itself amoung the network. It will target files as well as any backups. Sometimes, the virus will require external communication to begin this process, but some can opperate completely independent.

What you can do:

Ensure your IT team is monitoring for these external communications. It could alert your team that something questionble is going on.

Stage 6: Ransom

Once the ransomware is installed, encryption of your files and documents begins. At this point, they are in control of the situation and can demand payment in exchange for releasing your files. However, attackers are under no obligation to return

What you can do:

As soon as you have received a ransom. contact your local FBI office and IT team immediately.

radius180

The Next Steps

Contact your IT department to ensure you are prepared in the event of a ransomware attack. Be proactive in your preparation so you aren't caught off gaurd.

DO A 180

For more information:

David Roberts CEO, Co-Founder

Phone: 856.282.1131 x101
Email: droberts@radius180.com

http://www.radius180.com

radius180