A quick guide to

RANSOMWARE DEFENSE

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

See what your technology can do.

www.visualedgeit.com

A Brief History of Ransomware

Before understanding how to defend against ransomware, it's important to understand where exactly it came from. Though it may seem like a new concept, the reality is that ransomware is far from a new phenomenon.

In 1989, Joseph Popp distributed around 20,000 infected floppy disks via the postal system to recipients all around the world. These disks contained a hidden virus that activated after 90 startups of the computer. Once the infection took hold over the computer, the user was required to pay $189 to unlock the computer, and $378 for a software lease. Joseph Popp was eventually caught, and the virus was decrypted. Still, this set into motion the concept and eventual widespread usage of the virus known as ransomware.

"A study conducted by the FAU found that more than 50% of users click on links sent by unknown senders."

Since then, ransomware has come a very long way. Most notably, it made a big comeback in the new millenia, spawning countless different individual variants. One of the more famous ransomware viruses from the era was the Archiveus trojan, which encrypted all contents within an infected user's "My Documents" directory. It then required the user to purchase items from specific websites. Once purchased, the websites would deliver a string of letters and numbers to the user, who would use them to unlock their data.

What made the new ransomware variants special wasn't their ability to lock specified files. Rather, they began to use more advanced forms of encryption. The Archiveus trojan mentioned before utilized an RSA encryption, which was far harder to decrypt than its predecessors. This caused more people to take ransomware attacks more seriously, and truly expedited the rise of ransomware in more advanced global cyberattacks.

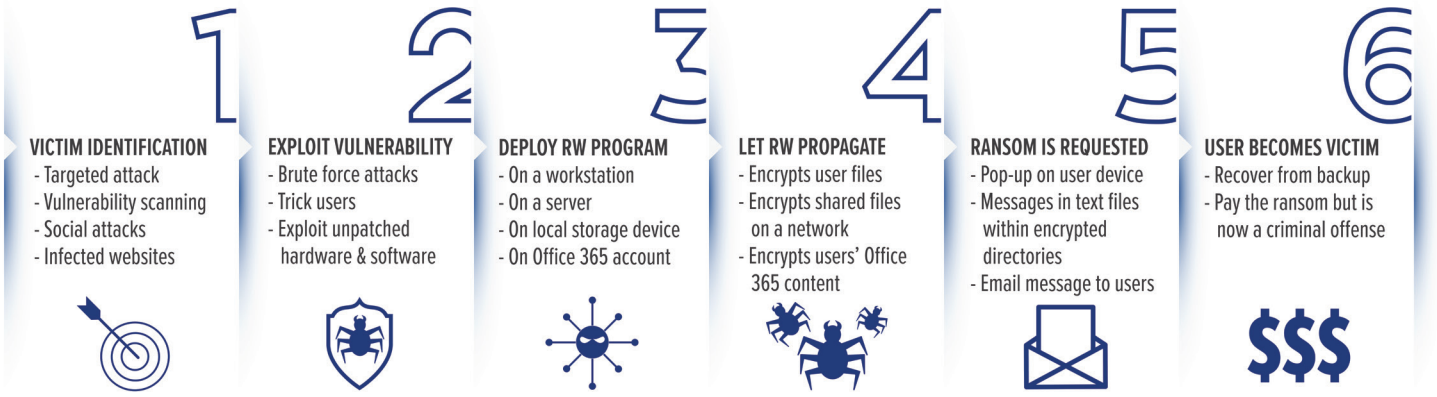
Ransomware has evolved considerably since the mid-2000s. It is now more dangerous than ever; it uses virtually uncrackable encryption patterns and requires ransom payments to be completed through bitcoin, which makes it totally untraceable.

As a dangerous threat to businesses, it's now more important than ever to develop a plan to fight ransomware. It can strike organizations any time, and the consequences from an attack can be dire.

That's why Visual Edge IT™ has developed a quick and useful guide for ransomware defense.

Anatomy of Ransomware

Ransomware is inherently sneaky; it can make its way into your computer and network from a variety of different ways. Most notably, it comes from end users downloading and executing an application that plants it within your file system. And it's not going anywhere, either – **THERE'S A RANSOMWARE ATTACK ON A BUSINESS ONCE EVERY 40 SECONDS.**



How to Fight Back

There are 3 highly effective ways to prevent ransomware from ever affecting you in the first place.

End User Security

The most effective way to handle ransomware is to circumvent it completely. For this to happen, company employees require ample amounts of cybersecurity training. In 2016, a study conducted by the FAU found that more than 50% of users click on links sent by unknown senders. The act of blind trusts particularly dangerous in companies with access to sensitive information.

By training employees to avoid possible infections and follow security best practices, you are cutting chances of ever being infected with a virus in the first place.

Security training doesn't have to be overly complex and tedious. Something as short as a 1-hour seminar on cybersecurity conducted once per quarter is enough to substantially lower the risk of being impacted by a ransomware attack.

Another way to minimize chances of a ransomware infection is to set proper administrative control on each machine. By setting the end user in their own group, you can prevent them from downloading any possibly harmful extraneous program.

Security Patches, Updates, and Programs

User training is only so effective. To stop ransomware from breaking into a network infrastructure, a company needs to be diligent in keeping its implemented software completely updated. Many times, viruses will sneak past security safeguards through gaps in unpatched application security protocols.

Depending on the sheer number of computers and programs within an organization, it can take a while to update everything. These updates should be automated and scheduled to occur at least once a month, during non-work hours to prevent any residual downtime that may come as a result of them.

Of course, having a dedicated antivirus system in place is also paramount to network security. A good antivirus program will scan and test each application that runs for potential virus activity. Performing regular scans of the computer systems is an effective method for catching dormant trojans and dealing with them before they activate. And to protect against known and unknown cyber threats, end point protection with AI ensures your business and data are safe.

Established and Tested Backups

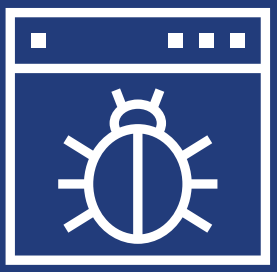
Even the most airtight contingency plan can fail. When this happens, it's vital to be prepared with a series of backup solutions. Ransomware can infect all of the files in your systems, which can leave you stuck with no way out. You'll be forced to choose between paying a hefty ransom, or losing all of your files.

Luckily, backups can save the day. You can fully restore your files from a backup, provided that the backup was isolated from the rest of the network and was encrypted properly. If the backup itself was infected, you must rely on an off-site backup.

Off-site backups are the most secure way to store your data. All of your files are kept within a datacenter that is physically and technologically secured. Your data is backed up and mirrored many times throughout the facility, to ensure maximum redundancy. It is also tested regularly, to ensure that it's fully functional when the need to restore it arises.

Having a backup solution can overcome any possible ransomware attacks. If a ransomware attack strikes and devastates your organization, restoring your data through a backup can get you back up and running in a matter of hours.

"Ransomware is inherently sneaky; it can make it's way into your computer and network from a variety of different ways... there's a ransomware attack on a business once every 40-seconds."



Where Do You Begin?

When used in tandem, each of the steps listed previously will significantly reduce the risk of ransomware affecting your organization. However, the truth is that they are not easy to implement alone. Each step will require meticulous planning and proper execution. That's why it's best to go about creating a ransomware defense plan with the help of experienced professionals.

That's where we come in. At Visual Edge IT, we have a team of skilled experts who have been combatting ransomware for many years. We'll work with you to create a defense plan that works on your terms. From there, we'll implement it and continue to monitor your company's security for any possible threats. You can focus on growing your business, while we focus on your cyberdefense.

Don't leave your ransomware protection up to chance. By partnering with us, you ensure that your data will be safe, sound, and ransom-free.

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

6050 Corporate Way
Indianapolis, IN 46278
(866) 863-2266

learnmore@visualedgeit.com
www.visualedgeit.com
@visualedgeit