A QUICK GUIDE TO STOPPING RANSOMWARE

Webroot does not believe that businesses should have to choose between extortion and losing precious data. This quick guide is an abbreviated version of our technical white paper, "A Guide to Avoid Being a Crypto Ransomware Victim," and outlines a few proactive steps you can take to reduce the likelihood that you'll fall victim to a crypto ransomware attack.

Deploy Reputable, Multi-Vector, Endpoint Security

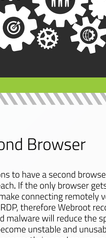
Having endpoint security that prevents malware infections in the first place is vital. Look for security that protects web browsing, controls outbound traffic, protects system settings, proactively stops phishing attacks, and continuously monitors individual endpoints.

Deploy Backup and Business Continuity Recovery

If there is a crypto ransomware infection, then the only recourse is to recover data and minimize business downtime. There are now many automated on-premise and cloud-based backup and continuity solutions that will back up data and create an air gap to stop ransomware from infecting networked drives. Business continuity also means minimal downtime so businesses can quickly return to normal.

Disable Macros and Autorun

Many types of crypto ransomware infect systems using macros. Macros can easily be disabled in the Trust Center of every version of Microsoft® Office. It is also possible to enable individual macros, should they be used for a particular task. While autorun is a useful feature, it is often used by malware to propagate. For instance, USB sticks will use autorun to proliferate, as do commonly used by Visual Basic Script (VBS) malware and worms. It is best to Policy disable autorun.

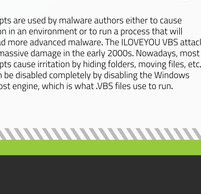


Create Strong Windows Policies

When it comes to crypto ransomware, consider using Windows Policies to block certain paths and file extensions from running. Policies can be set up in groups, which is useful if varying levels of access are required. (Note: Test any policies on a test PC.) Examples of useful policies include: blocking executables in temp or temp+appdata and the creation of startup entries. The following file types shouldn't be run in the following directories: .SCR, .PIF, and .CPL in users' temp, program data, or desktop.

Control Plugins

Java generally gets the most coverage when it comes to exploited software, but this rule applies to nearly all common plugins. Generally speaking, if certain plugins are not used, it is better not to have them installed. If plugins are being used, make sure they are up to date, i.e. do not disable the run keys for the Java updaters, etc.



Have a Second Browser

There are good reasons to have a second browser at the ready in case of a breach. If the only browser gets compromised, it will make connecting remotely very difficult. (Not everybody uses RDP, therefore Webroot recommends disabling it.) PUAs and malware will reduce the speed of browsers until they become unstable and unusable. Some sites might not render correctly in one browser, and having a second is an easy way to see if problems are browser-related. Different browsers offer different plugins that can be useful in protecting users like ad blockers, script blockers, and web filters.

Use Policies to Block Volume Shadow Copy Service

Windows creates local copies of files using the VSS copy service. Ransomware like CryptoLocker will encrypt this area because it holds VSS copies for the local drive (normally the C:\ drive). Using Windows Policies to block access to the service helps stop ransomware like CryptoLocker from erasing local drive file backups. Policies should point to the VSSAdmin executable. Any attempt to access or stop the service will result in a block.

Disable Windows Script Hosting

VBS scripts are used by malware authors either to cause disruption in an environment or to run a process that will download more advanced malware. The ILOVEYOU VBS attack caused massive damage in the early 2000s. Nowadays, most VBS scripts cause irritation by hiding folders, moving files, etc. They can be disabled completely by disabling the Windows Script Host engine, which is what .VBS files use to run.

Educate Users

As always with security, users are often the weakest link. Malware will continue to thrive and threaten businesses as long as staff are unaware and uneducated on the risks of the Internet. Providing the basics will protect users at home and in the office.

FIVE GENERAL TIPS

1. Make sure endpoint security is installed and updated
2. Check regularly that backups and business continuity is functioning
3. Ensure Windows is patched and up to date, as well as any plugins used
4. Use a modern browser with at least an ad blocker installed
5. Show file extensions for known file types

WEBROOT®
Smarter Cybersecurity®