The 5Ws and 1H of Ransomware

Whom does it affect?

You! Do you use any mobile devices, PC, laptop, or the internet for surfing, emailing, working, or shopping online? If yes, then you are a potential ransomware victim. Ensure that precautionary measures are taken, see the Prevention section for details.

What is ransomware?

Ransomware is a malware that stealthily gets installed in your PC or mobile device and holds your files or operating system functions for ransom. It restricts you from using your PC or mobile device, and from accessing your files (files are sometimes locked or encrypted), unless you pay the ransom (in exchange for file decryption).

Paying the ransom (either through credit card or Bitcoins) however, does not guarantee that you'll get your files back. Prevention is still way better than allowing yourself to be infected and then trying to find a cure.

What does a ransomware attack look like?

Ransomware targets your pictures, documents, files, and data that are personally invaluable.

You can tell that you are under attack when you see any of the following:

- Ransomware note
- Encrypted files
- Renamed files
- Locked browser
- Locked screen

However, the ransomware attack symptom varies from one ransomware type to another:

What!?! There are several ransomware types?

Yes. From the time that it first surfaced in 1989, ransomware morphed into different forms as it assimilates to people's computing habits, leverage recent technologies, and monetization strategies available.

There are two types of ransomware – lockscreen ransomware and encryption ransomware.

- **Lockscreen ransomware** shows a full-screen message that prevents you from accessing your PC or files. It says you have to pay money (a "ransom") to get access to your PC again.
- **Encryption ransomware** changes your files so you can't use them. It does this by encrypting the files – see the Details for enterprises section if you're interested in the technologies and techniques we've seen.

Older versions of ransom usually claim you have done something illegal with your PC, and that you are being fined by a police force or government agency.

These claims are false. It is a scare tactic designed to make you pay the money without telling anyone who might be able to restore your PC.

Where can a ransomware attack happen?

Computers and mobile devices.

Ransomware employs its encryption and monetization strategies across PC and mobile devices.

When can a ransomware attack start?

Potential victims can fall into the ransomware trap if they are:

- Browsing untrusted websites
- Not careful about downloading or opening file attachments which are known to contain malicious code from spam emails. That also includes compressed files or files inside archives. Some possible attachments can be:
    - Executables (*.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .hlp, .ht, .hta, .inf, .ins, .isp, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .pcd, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .exe, .pif, etc*.)
    - Office files that support macros (*.doc, .xls, .docm, .xlsm, .pptm*, etc.)
- Installing pirated software, outdated software programs or operating systems
- Using a PC that is connected to an already infected network.

Why do malware perpetrators victimize people with ransomware?

Because they have malicious or criminal intentions, and see it as an easy way to make money. They take advantage of people's ignorance, unpatched software vulnerability, or zero-day vulnerability.

On the other hand, it mars an enterprise company's security and reputation as some ransomware incidents halt crucial services such as hospitals – thus forcing infected users to pay up if they haven't backed up their data.

Why must you educate yourself about ransomware?

Because it can take your hard-earned money in exchange of the stuff you already own – your data or files!! Exxroute ransomware, for example, demands $500 and doubles the ransom as you delay the payment. It also starts deleting your files if you delay the payment.

It can also violate your privacy, disrupt your work or personal life, and possibly harm your reputation.

If the ransomware perpetrators are cashing in on people's ignorance, then educating yourself about it can help disrupt their business.

How can you avoid and bounce from a ransomware attack?

Prevention

- Keep your Windows Operating System and antivirus up-to-date. Upgrade to Windows 10.
- Regularly back-up your files in an external hard-drive.
- Enable file history or system protection. In your Windows 10 or Windows 8.1 devices, you must have your file history enabled and you have to setup a drive for file history.
- Use OneDrive for Consumer or for Business.
- Beware of phishing emails, spams, and clicking malicious attachment.
- Use Microsoft Edge to get SmartScreen protection. It will prevent you from browsing sites that are known to be hosting exploits, and protect you from socially-engineered attacks such as phishing and malware downloads.
- Disable the loading of macros in your Office programs.
- Disable your Remote Desktop feature whenever possible.
- Use two factor authentication.
- Use a safe and password-protected internet connection.
- Avoid browsing web sites that are known for being malware breeding grounds (illegal download sites, porn sites, etc.).

Detection

- Install, use, and regularly update an antivirus solution like Windows Defender to detect ransomware.
- Enable Microsoft Active Protection Service (MAPS) to get the latest cloud-based ransomware detection and blocking.

Recovery

In Office 365's How to deal with ransomware blog, there are several options on how one can remediate or recover from a ransomware attack. Here are some of the few that are applicable for a home user or those in the information industry like you:

1. Make sure you have backed-up your files.
2. Recover the files in your device. If you have previously turned **File History** on in Windows 10 and Windows 8.1 devices or System Protection in Windows 7 and Windows Vista devices, you can (in some cases) recover your local files and folders.

To restore your files or folders in Windows 10 and Windows 8.1:

- Swipe in from the right edge of the screen, tap **Search** (or if you're using a mouse, point to the upper-right corner of the screen, move the mouse pointer down, and then click Search). Enter "*restore your files*" in the search box, and then tap or click **Restore your files with File History**.
- Enter the name of file you're looking for in the search box, or use the left and right arrows to browse through different versions of your folders and files.
- Select what you want to restore to its original location, and then tap or click the **Restore** button. If you want to restore your files onto a different location than the original, press and hold, or right-click the **Restore** button, tap or click **Restore To**, and then choose a new location.

Source: Restore files or folders using File History

To restore your files in Windows 7 and Windows Vista

- Right-click the file or folder, and then click **Restore** previous versions. You'll see a list of available previous versions of the file or folder. The list will include files saved on a backup (if you're using Windows Backup to back up your files) as well as restore points. Note: To restore a previous version of a file or folder that's included in a library, right-click the file or

folder in the location where it's saved, rather than in the library. For example, to restore a previous version of a picture that's included in the Pictures library but is stored in the **My Pictures** folder, right-click the **My Pictures** folder, and then click **Restore previous versions**. For more information about libraries, see Include folders in a library.

- Before restoring a previous version of a file or folder, select the previous version, and then click **Open** to view it to make sure it's the version you want. Note: You can't open or copy previous versions of files that were created by Windows Backup, but you can restore them.
- To restore a previous version, select the previous version, and then click **Restore**.

Warning: The file or folder will replace the current version on your computer, and the replacement cannot be undone. Note: If the **Restore** button isn't available, you can't restore a previous version of the file or folder to its original location. However, you might be able to open it or save it to a different location.

Source: Previous versions of files: frequently asked questions

Important: Some ransomware will also encrypt or delete the backup versions and will not allow you to do the actions described before. If this is the case, you need to rely on backups in external drives (not affected by the ransomware) or OneDrive (Next step).

***Warning**: If the folder is synced to OneDrive and you are not using the latest version of Windows, there might be some limitations using File History.*

3. Recover your files in your OneDrive for Consumer.

- Find lost or missing files in OneDrive
- Delete or restore files and folders

4. Recover your files in your OneDrive for Business.

If you use OneDrive for Business, it will allow you to recover any files you have stored in it. You can use either of the following options:

Restoring the files using the Portal

Users can restore previous version of the file through the user interface. To do this you can:

1. Go to **OneDrive for Business** in the office.com portal.

2. Right click the file you want to recover, and select **Version History.**

3. Click the dropdown list of the version you want to recover and select restore.

If you want to learn more about this feature, take a look at the Restore a previous version of a document in OneDrive for Business support article.

Site Collection Restore service request

If a large number of files were impacted, using the user interface in the portal will not be a viable option. In this case, create a support request for a 'Site Collection Restore'. This request can restore up to 14 days in the past.