(YB)Backup

Ransomware: How it Works and What it Looks Like

You go to the office and log on to your computer. You start looking through your inbox. You open some emails, throw out others—procrastinate, sort, read, delete. You know the drill.

Then one particular email catches your eye. You didn't expect it, and maybe there is an urgency to it, something like, "Final Notice!" Wondering what critical notice you might have missed, you click on the attachment.

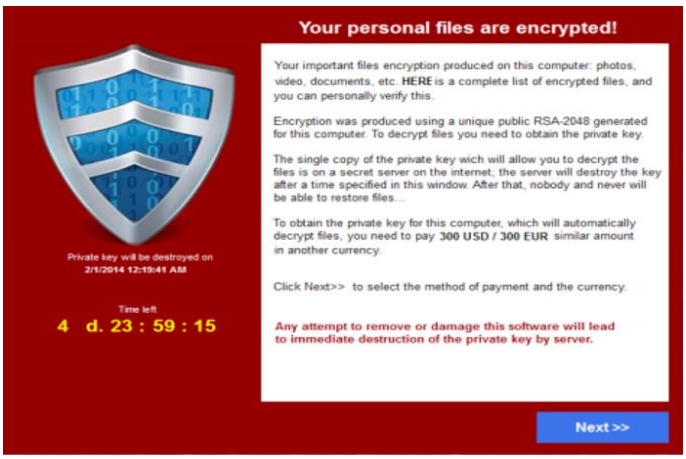
Bam.

You've been had and, at this point, you don't even know it. And you won't know it for a little while because encrypting all of your files is a fairly cumbersome computer process. For the record, it doesn't need to involve an attachment. Cybercrooks can sometimes simply send links to websites that are seeded with malicious code.

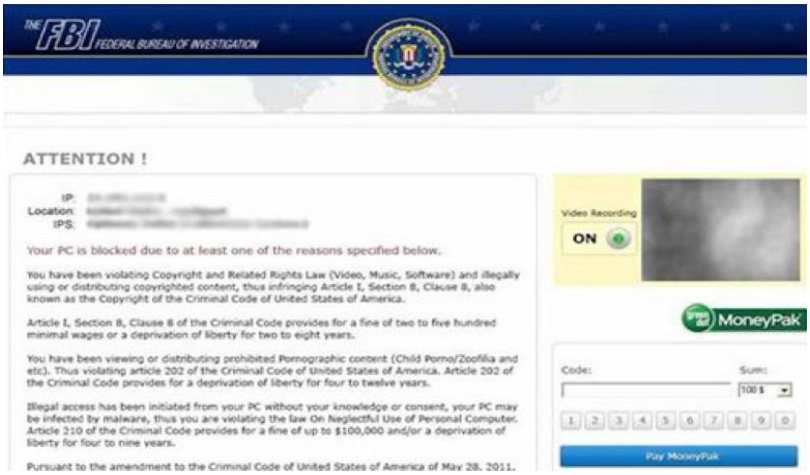
What happens next? The ransomware sends out a digital request to a remote server in another country, asking for encryption keys that it will install on your system. The overseas server generates two such keys—one that will sit on your computer, and one that will be housed on the system run by the cybercriminals who are getting ready to extort money from you.

Once the malware has received the key back, it begins the time-consuming and resource-intensive task of encrypting all the data on your computer—all documents, spreadsheets, files, pictures, videos, and so on—all of it.

When do you find out? Often the first outward sign is that your system begins to slow down. Your computer might get glitchy. You might see popups that say, "file corrupted" or "bad extension." (And then again, you might not.) But once the malware has completed its nefarious mission, your desktop will freeze and you might see an image like this:



Alternatively, the message might purport to be from the FBI, telling you that you have violated some law and, as a result, your computer is locked.



Either way, the message warns you that your files have been encrypted and that you no longer have access to them. It goes on to explain that you have a short period of time within which to pay a fee or your files will be deleted forever.

It used to be that the cybercriminals asked for ransoms in the thousands of dollars, but then they got smart. They realized that they had a much better chance of getting paid if the amount was in the hundreds, and sometimes even less. They figured, correctly, that people would be more willing to pay a small sum than deal with the time and money—and sometimes embarrassment—associated with cleaning up a ransomware attack.

The time frame to pay the ransom is typically only three days or so. At this point, you essentially have four options:

- Pay the ransom.
- Do nothing and lose your data.
- Hire an expert.
- Access your **cloud backup** and recover your lost data.

Industry analysts agree that the best way to protect yourself against ransomware is prevention—that is, guarantee you never fall for an online trap. After that, a secure backup copy of all your data is the best way to stay safe. Without that kind of security, many folks just pay the ransom. Once that happens, they are supposed to get a key from the crooks that will unlock and decrypt the files.

And then again, some people never get the decryption key. After all, these are very bad guys.