Most Popular Malware Threats and How to Avoid Them

0

BY GUEST ON MARCH 23, 2015 ARTICLES FROM OUR CONTRIBUTORS, TECH TALK

Tech talk

Impersonating police, holding computers for ransom, and creating fake software. These are just a few of the new tactics cybercrooks are using to get into your personal computers and your wallets. They do this by way of viruses and malware installed on desktop computers and laptop computers. Some estimates say the illegal malware industry stole more than $4.5 billion from Americans last year.

It used to be that malware infections simply made your computer run slowly. Now, they can quite literally take over your computer, and in some cases, demand a ransom for returning it to its normal operating state.

A few of the most insidious examples of infections that the malware experts at EnigmaSoftware.com have identified to fit into this category of malware are listed below.

—Ransomware. This malware creates bogus pop-up messages on your computer saying all of your files have been encrypted and the only way to "release" them is by paying a steep fee – or ransom. One of the most prevalent versions of this infection today is called CTB Locker. Look at the frightening message that appears when computers are infected with it.

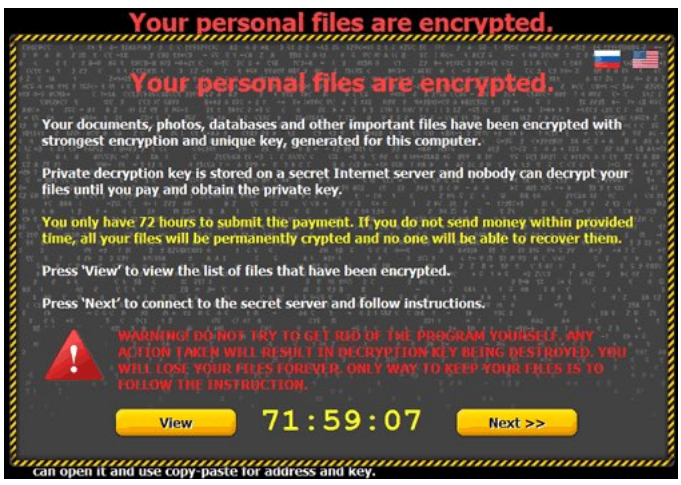

Figure 1. CTB Locker ransomware message screenshot

It tells users their personal files are encrypted and "you only have 72 hours to submit the payment. If you do not send money with in provided time, all your files will be permanently crypted and no one will be able to recover them."

Now, most people might realize this threat is bogus. But when tens of thousands of computers have this infection, it only takes a few scared victims to grant the hackers behind these schemes a handsome payday.

–Police Ransomware. This version is similar to the ransomware mentioned above, except it also adds the twist of impersonating a law enforcement agency. In these infections, pop-up messages purporting to be from law enforcement agencies claim they've detected illegal activity on your computer and the only way to avoid prosecution is by immediately paying a fine. Look at the logo in the upper left-hand corner the pop-up message below. It claims to be from the University of California-Irvine Police Department

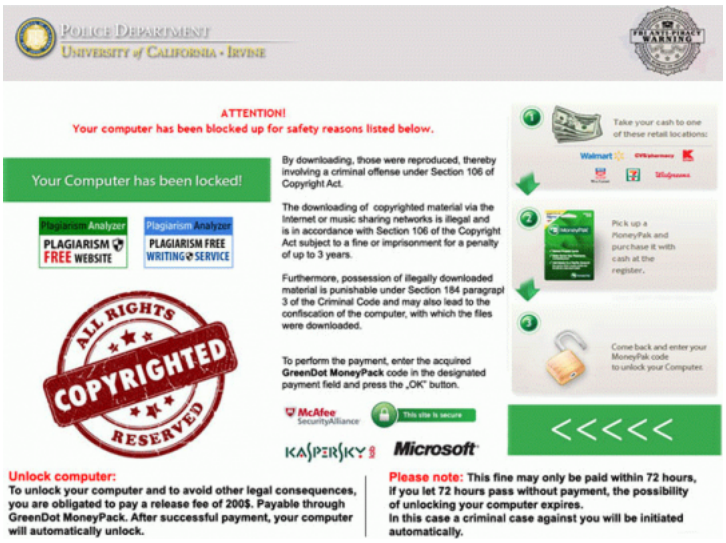

Figure 2. FBI ransomware example screenshot

The bottom of the message says "to unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200." The researchers at EnigmaSoftware.com have even found numerous examples of malware infections purporting to be from the FBI.

–Rogue Anti-Spyware programs

A third very tricky type of infection is an application that pretends to be a legitimate anti-spyware program. In this case, users will see a pop-up message that says a scan of your computer has revealed an infection. And that if you pay now, you can register for a program that will wipe the infection away. The only problem is the infection and the system scan are all fake. Once you purchase such a program, the bogus infection will appear to go away for a period of time. But a few weeks later the software may "find" another infection and demand more money to remove it. Here's an example of one of the bogus messages from a rogue anti-spyware infection called Home Malware Cleaner.

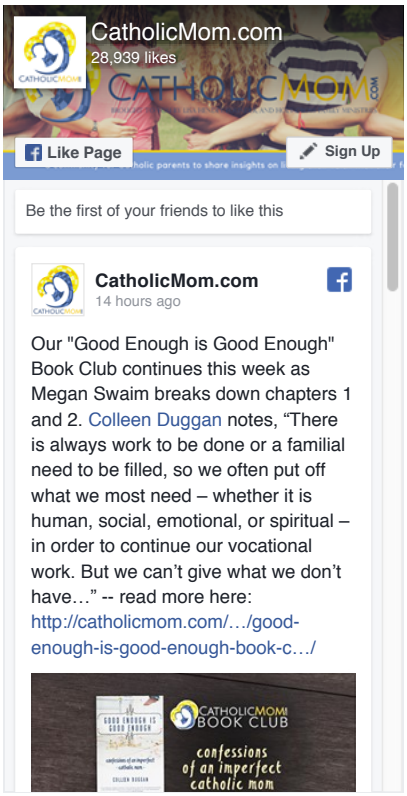

Figure 3. Home Malware Cleaner rogue anti-spyware program warning notification screenshot

It's easy to see how a message like this can trick someone into thinking their computer has a virus and that they need to pay to have it removed.

How do these infections end up on millions of computers nationwide? A lot of people incorrectly think that the only way these infections can get on computers is if someone is spending time in seedier places online: adult web sites, gambling web sites, illegal movie download sites. And while those sites do often contain viruses, there are plenty of ways that even the most mindful people can fall victim.

In most cases, malware infections are installed on computers because someone has been tricked into clicking on a link that opens up an application or a website containing the malware.

Below are a couple of the most effective ways crooks trick people into clicking on links.

–Compromised social media accounts

Cybercrooks know that if they can gain access to your Facebook, Pinterest or Twitter account, they can send fake messages to your friends and followers that look like they are coming from you. Those messages have links to potentially malicious sites in most cases. Here's an example of what one of those messages look like.

Figure 4. Potentially malicious social media message screenshot

The message above in Figure 4 has enticing language that naturally makes you want to click on the link, especially since it's coming from one of your trusted friends or followers.

–Fake emails from trusted companies/organizations

Cybercrooks and hackers can create authentic-looking emails that seem like they are coming from either businesses or government organizations you interact with. One of the most common fake emails this time of year comes in the form of IRS notices about taxes. Sometimes the emails will claim there is a problem with your tax filing and that you need to click on a link in order to resolve it. Usually, with a malicious email claiming to be from the IRS,

the link leads to a malicious site or one that downloads malware onto your computer. In the case of the fake IRS email below in Figure 5, cybercrooks have attached what they claim is a form that needs to be filled out for a tax exemption. In reality, when that attachment is opened, a malicious infection is installed.

Figure 5. Example of a malicious and fake IRS email with a malware attachment

Other tricks include fake emails from major online retailers telling you there is a problem with your recent order. The link to fix the problem actually contains malware. Those emails are particularly effective during the holiday shopping season when more people are buying more products online.

So with all of these threats online, how can someone safely surf and be confident they wont be exposed to infections?

Here are a few simple tips for staying safe online and evading popular malware threats.

–Think about that link. If you get a message via one of your social media accounts with a link in it, be very wary. Same with emails. Understand that the IRS will never communicate with you via email. And if you get a message about a problem with an online order, instead of clicking on the link in the message, open up your web browser and go to the main page of the online retailer's web site yourself.

–Install a trusted anti-spyware/anti-virus program on your computer, and make sure you set it to scan and update automatically. That way you don't have to remember to do it.

—**Keep an eye out for your senior friends and relatives.** Senior citizens are online a lot and may not be as proactive about applying the latest information or warnings related to internet safety. Some of our research indicates that seniors might actually be more susceptible to malware infections than younger computer users. That's due in part to the fact that seniors may not be as technologically savvy, and tend to have older computers and operating systems that are more susceptible to malware infections.

The crooks know there are billions of dollars to be made by lying, cheating, and stealing from any of the millions of people who are online every day. As more people do more things online, the opportunity for fraud will only grow. But by being vigilant, cautious, and proactive, you can dramatically reduce your chances of getting swindled.

SHARE.

ABOUT AUTHOR

GUEST

We welcome guest contributors who graciously volunteer their writing for our readers. Please support our guest writers by visiting their sites, purchasing their work, and leaving comments to thank them for sharing their gifts here on CatholicMom.com. To inquire about serving as a guest contributor, contact Lisa@CatholicMom.com.

RELATED POSTS

MAY 25, 2018 0

Quinoa Stuffed Bell Peppers

MAY 25, 2018 0

Daily Gospel Reflection for May 25, 2018

MAY 24, 2018 0

Enthronement to the Sacred Heart: A Devotion Designed for the Family

LEAVE A REPLY

Your Comment

Your Name

Your Email

Your Website

Notify me of followup comments via e-mail. You can also subscribe without commenting.

POST COMMENT

WHAT'S NEW AT CATHOLICMOM.COM

Quinoa Stuffed Bell Peppers

Daily Gospel Reflection for May 25, 2018

Enthronement to the Sacred Heart: A Devotion Designed for the Family

Riding a bike has become a faith-filled experience

We CAN Suffer With Joy

CATHOLICMOM.COM BOOKS

Visit our CatholicMom.com Book Series at Ave Maria Press