nLightenedThoughts

January 2017

William Blinn Communications
Worthington, Ohio 43085
www.blinn.com • 718.577.1054

Serious Threats Are Aimed at Your Data Right Now

Whether Russia's tampering had any effect on the election or not, it's clear that computers are at risk from Russia and China, but also from Israel, England, other allies, and criminals that are snooping.

It's the crooks that pose the greatest danger to most of us because they encrypt your data and then offer to sell you the key needed to decrypt the files. Unless you're a Fortune 500 company, you don't have much to fear from Russian, Chinese, Israeli, or Turkish hackers, but anyone with a trove of old family photos or other important documents on the computer should be concerned about crooks who want to extort money from you by holding your files for ransom.

Russian hackers are smart, possibly because theoretical subjects were safe havens in the old days of the Soviet Union. The best Russian hackers scorn western developers. You needn't fear them, though. Instead, fear the high school kid who's about to flunk out or the angry middle manager who's been downsized out of a job.

Crooks don't need to be elite (or even smart) to use malware. Instead, they pay for *ransomware as a service*. Just as large companies pay for legitimate software as a service, small-time crooks rent big-league malware even if they don't have the skill to write even a simple computer program.

The people who encrypt your files and then demand payment within 48 hours are likely to be a teenager, a drop-out, or an out-of-luck person who's unemployed.

McAfee Labs says that increasingly malware is served from sites that the dumb crooks rent from the smart crooks. But how dumb are you if you pay a few hundred dollars, plus a commission, to the people who make it possible for you to "earn" tens of thousands of dollars by hijacking important files at homes and small businesses?

Ransomware!

Your computer has been locked and all your files has been encrypted...

Big thefts are engineered by the elite. The attack that crippled Hollywood Presbyterian Medical Center in Los Angeles until the thieves were paid $17,000 to unlock the encrypted files was almost certainly one of these. But the grandmother who pays $500 to restore all of her family pictures is probably dealing with what was once derisively called a *script kiddie*.

Business records are valuable and crooks know that companies can afford to pay higher ransoms than consumers. A survey by IBM found that about half of the respondents had experienced a ransomware attack and 70% of them paid to get their data back. *Would your business survive if every file on every computer vanished?*

If your computer network is infected with ransomware, there's not much you can do but pay up and hope that you're dealing with "honest crooks" *unless you have a full, complete, and verified backup*. Having a full backup is the second best way to deal with ransomware. The best way to deal with ransomware is to avoid it entirely.

Avoidance Measures

Caution, intelligence, and wetware (the stuff between your ears) are the best defenses.

Victims of ransomware are often infected when they open an email attachment that contains malware or when they click a link that takes them to a corrupt website that installs malware.

In most cases, malicious email messages are easy to spot if you know what to look for. Is that message from UPS (or the USPS or FedEx) legitimate? You can be sure that the message is bogus if the *from* line indicates that it came from Albania, Ukraine, Brazil, or Hungary. The *from* line may appear to be legitimate, though, because it's easy to forge.

The critical step involves examining the message. A legitimate message UPS, the Post Office, or FedEx will have a tracking number, not an attachment. Any attachment should be presumed to be fraudulent until proven otherwise.

The same is true for messages that claim to be from banks, other financial institutions, or companies. Near the end of 2016, I noticed a spike in messages that claimed to be from either the accounts receivable or accounts payable departments of companies that I'd never heard of. They all contained zip files as attachments and the zip files all contained Javascript files.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, Worthington, Ohio.
Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com. All rights reserved.

Double-clicking the embedded Javascript file, which may be disguised as something else, will launch the Windows Script Host (WSH) and execute the script. Scripts run by WSH are not sandboxed as they would be in a browser.

But the Javascript file might be disguised to look like a Word file. By default, Windows hides the extensions of "known" file types. When extensions are hidden, "MyStuff.doc.js" will appear to be "MyStuff.doc".

Help from Our Friends

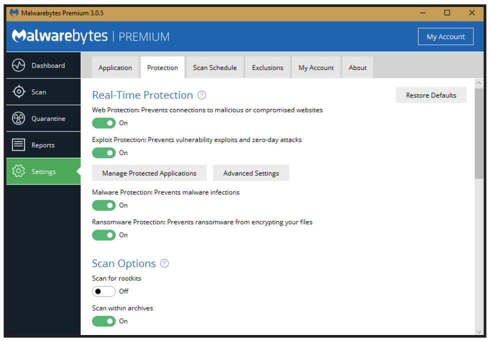
No matter how careful you are, it's prudent to have an application that watches for threats.

The problem is that most anti-virus, anti-malware applications aren't able to keep up with what are called *advanced persistent threats* (APT). An APT is a set of stealthy and continuous computer hacking processes that remain hidden until they are activated.

"Advanced" signifies the use of sophisticated techniques that exploit vulnerabilities in systems. "Persistent" suggests that an external command and control system is continuously monitoring and extracting data from a specific target. "Threat" indicates human involvement in orchestrating the attack.

Several protective applications attempt to address these kinds of threats.

I no longer use any anti-virus, anti-malware application other than Microsoft's Windows Defender and the latest version of Malwarebytes. That may surprise you. *It surprised me and I'm the one who made the decision.*



Real-Time Protection

Web Protection: Prevents connections to malicious or compromised websites
On

Exploit Protection: Prevents vulnerability exploits and zero-day attacks
On

Malware Protection: Prevents malware infections
On

Ransomware Protection: Prevents ransomware from encrypting your files
On

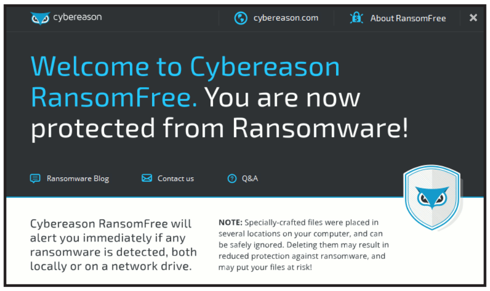
Scan Options

Scan for rootkits
Off

Scan within archives
On

Mainline anti-virus, anti-malware applications often create problems with essential applications. Windows Defender is part of the operating system. Protective applications should be part of the operating system. Although Microsoft's application is considered weak, I've found that it offers adequate baseline protection.

The latest version of Malwarebytes Professional includes website, malware, exploit, and ransomware protection. Although it continues to work well with any installed anti-virus, anti-malware application, it also functions well on its own. But there's one other option to consider, a newcomer called Cybereason RansomFree.



Welcome to Cybereason RansomFree. You are now protected from Ransomware!

Cybereason RansomFree will alert you immediately if any ransomware is detected, both locally or on a network drive.

NOTE: Specially-crafted files were placed in several locations on your computer, and can be safely ignored. Deleting them may result in reduced protection against ransomware, and may put your files at risk!

This new application that has virtually no user interface and yet claims to protect your computer from ransomware. The developers say that they are "former elite military cybersecurity experts" and that their mission is to eliminate cyber threats. They describe their product this way: "RansomFree is a free ransomware protection software … [that] detects and stops ransomware from encrypting files on computers and servers."

I've been running the application for a while now and it seems to be legitimate. When asked if this is a free trial and whether users will be asked to pay later, the developers say "No. RansomFree is a free tool. You will not be asked to pay a fee or subscription at any time."

Assuming that the developers are not independently wealthy, I asked how they will monetize this service. The response:

You're right that very little is free these days. I'll start by saying that we are an enterprise-focused company, and not really a consumer company.

Regardless of enterprise versus consumer, we have a mission at Cybereason to make life more difficult for the bad guys and to help defenders as much as possible. We all really come to work every day for that.

It takes time to build a consumer-oriented business, and if we slowed down to do that, we would be holding back technology that could make a difference. We decided to make this free and get it out there because it can make a difference, now.

Later, we might build an ability to sell and support more complex products to consumers; but for now, we'll be happy enough to see less victims and more frustrated attackers looking to take advantage of the internet and its users.

Pay or Not?

If, despite your best efforts, your computer is infected with ransomware, there's little choice if you don't have a full and complete backup.

The FBI doesn't recommend paying ransom because there is no guarantee that the criminals will actually unlock the files and paying the ransom can encourage criminals to attack others.

Many do pay because it's often the only way they can restore critical files. The criminals even provide tutorials on how to use digital currencies and some have help desks for their victims to aid them in paying the ransom.

The FBI asks that anyone who is hit with ransomware, whether or not they pay the ransom, to report the incident at the Internet Crime Complaint Center at *www.IC3.gov*.

Be Your Own Firewall

Regardless of how many protective measures you put in place, they won't catch everything.

The people who write protective applications can't write protections for dangers they haven't yet seen. That means somebody has to be victimized before the protective systems can be updated.

Microsoft has several simple suggestions that can be combined into a single overarching rule. "Often fake emails and web pages have bad spelling or just look unusual. Look out for strange spellings of company names (like 'PayePal' instead of 'PayPal') or unusual spaces, symbols, or punctuation (like 'iTunesCustomer Service' instead of 'iTunes Customer Service'). Don't click on a link on a web page, in an email, or in a chat message unless you absolutely trust the page or sender."

Microsoft's shortest advice says it all: "If you're ever unsure – don't click it!" Ω

RESOURCES

Here are links to the resources mentioned in this article.

Microsoft Security

Malwarebytes

Cybereason

Internet Crime Complaint Center