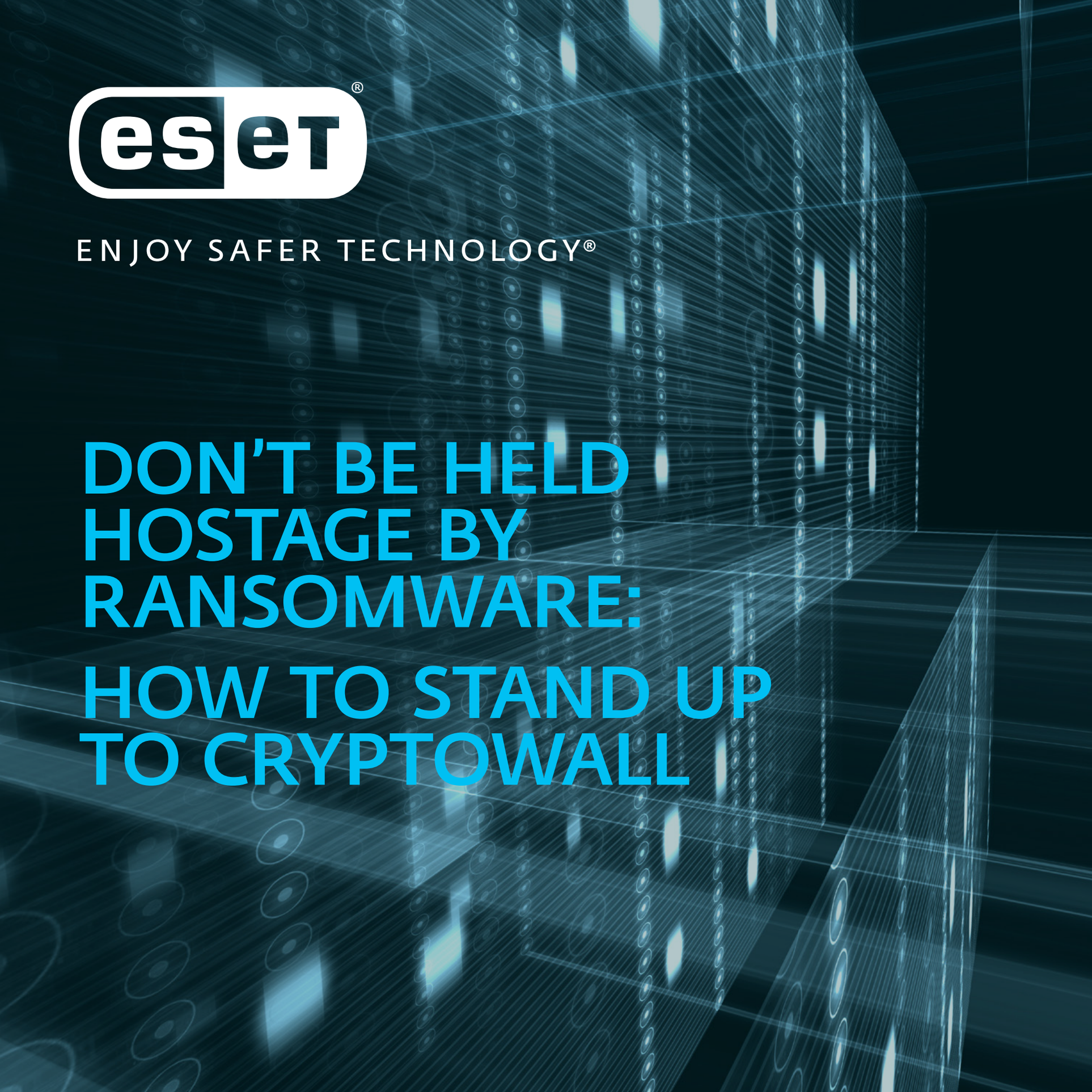

ENJOY SAFER TECHNOLOGY®
DON'T BE HELD HOSTAGE BY RANSOMWARE:
HOW TO STAND UP TO CRYPTOWALL

Don't be held hostage by ransomware: How to stand up to Cryptowall

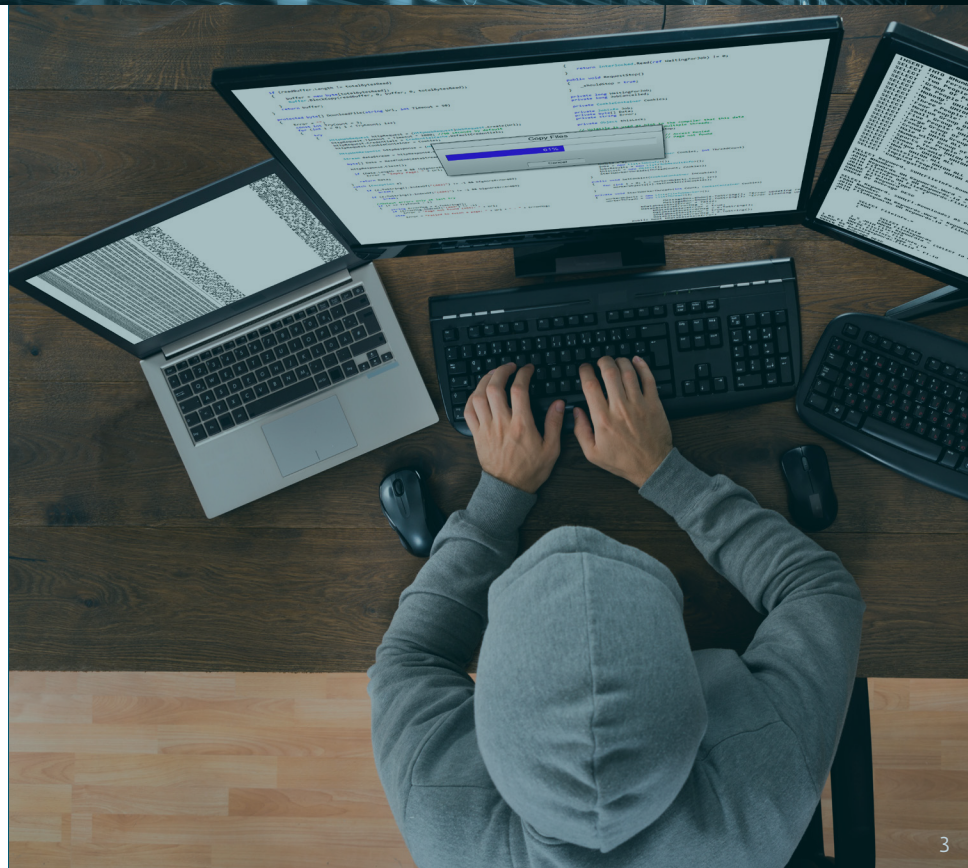
By Michael Aguilar

In the last few years, it is hard to talk about computer security without the word "Cryptowall" being brought up. In February, Hollywood Presbyterian Medical Center was hit by this strain of infection and forced to pay the ransom to get critical client data back from the attackers.

Many do not understand the nature of the infection, looking only to the result, which is heavily encrypted files. When you trace back the infection, the details you learn are almost as important as knowing that you have been hit by the infection. It reminds me of the saying "An ounce of prevention is worth a pound of cure." For IT managers, learning how to prevent these infractions will save you much time and provide a huge reduction in stress levels.

What *IS* Cryptowall?

Cryptowall is an infection that will encode your files with heavy encryption so they cannot be used until the ransom is paid to the attacker. The files affected are personal files, like Pictures, Documents, and PDFs. Normally, it does not encrypt Windows files, as they would like your machine to



be operational enough to pay the ransom. The infection uses Windows Encryption services to encrypt files with up to 2GB encryption, which is nearly unbreakable.

Many times, in an enterprise environment, a Server is affected, however, the infection originates on a Client machine and affects the user's mapped drives. Determining the user that started the infection can be difficult, though many times the owner of the generated *Help_Decrypt* or *Restore_Files* documents is the user that started the infection. From that client machine, you would investigate the system and registry, trying to locate any dropped files and possibly an encryption key if the writer was careless or the power was unplugged from the machine while the infection was active.

There are many variants; here at ESET we detect the infection as *Filecoder*. There are many variants and infections that have the same end result of encrypted files, such as **Teslacrypt, Cryptowall 1.0-4.0**, and even some that are now popping up as a *SAAS* (Software as a Service) complete with customer service of some sort to facilitate payment and answer questions on hopes of getting you to pay. Last year, a younger hacker by the handle of *Tox* created an underground site that did just that, Ransomware as a Service. The site allowed the users to create a Crypto virus, package it, and distribute it in exchange for a portion of the ransom. Due to its publicity, *Tox* eventually sold the site to a buyer for $5,000, according to a report on *BusinessInsider.com*.

Why was I infected?

The first thing I am normally asked when viewing a site that has been infected is "How?" How did the infection get past my defenses and infect my servers? There are many ways, but normally, it is due to weak applications on the system. This is why, in many instances, the first place I will visit when investigating a system is the Add/Remove programs area. Here, I am normally greeted by an out-of-date Adobe or Java installation. Even with antivirus, these weak applications can be attacked using a buffer overflow or other means to make the application itself execute malicious code.

Even more frightening, some of the exploit kits leave no files on the system, such as with the Angler and Nuclear Exploit kits. They can deliver a payload of Cryptowall, Teslacrypt, or other variants by obfuscating javascript code on infected websites in a "Drive by download" attack or leverage the use of macros in Outlook or other email clients to infect the system, again, with leaving no files other than the *Help_Decrypt* or *Help_Your_Files* once the

encryption process has already started. Even worse, they are very easy to use and anyone can buy them. Patch management is key, and though it is a pain, it can end up saving you from dealing with an infection like this.

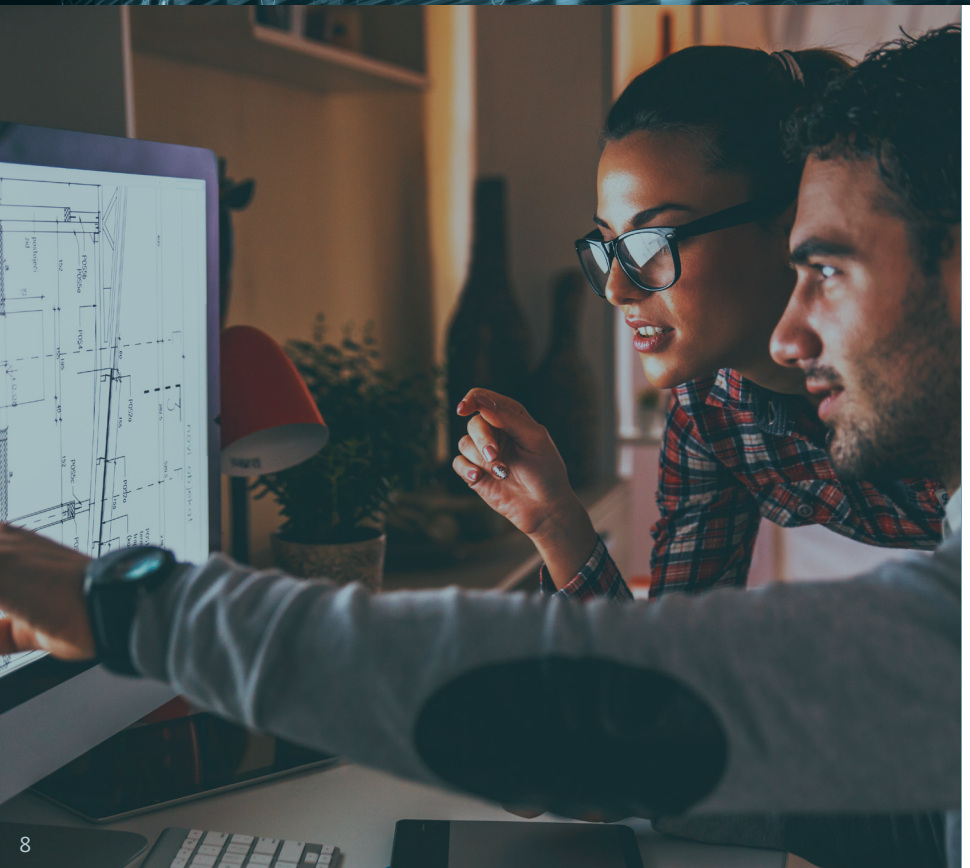
Recovery and prevention

If you have been affected by the virus, you'll need to clean your system, restore your files and get everything back in order. These tips will help you to prevent these types of infections and get back on your feet should you ever encounter another one.

- **Backup software**—A good backup solution should support versioning, so you can get a clean copy of the files back. If it does not, and you run another backup, you may end up restoring encrypted files OR your files may be overwritten with an encrypted copy. You can try to use something like Shadow Explorer to browse the Windows Shadow volumes on Windows Server 2008 and above builds, but many times this is erased to make the option of paying the ransom all the more enticing. If you do not have any backup software, take a look at ***StorageCraft*** as it will allow you to restore to a good state when your files were not encrypted.

- **Antivirus**—Hopefully you already have one deployed, but ensure that your Antivirus protection is solid, updated and working. Sometimes, the user that started the infection did not have an updated AV definition for months, leaving them vulnerable to attacks that otherwise would have been stopped. You will want to also make sure that the policies set for your AV have the appropriate settings to block these infections. **ESET's Live Grid** is one of those settings that you will want to enable. This system cloud sources multiple unknown detections, allowing them to be blocked even if there is not a definition written yet. ESET has had a very good ratio of stopping infections with this system in ***ESET Endpoint version 5.x (latest) and Endpoint Version 6.***

- **Employee training**—One of the largest attack vectors for a hacker is the end user base. I have seen a large amount of phishing emails with malicious attachments that could have been prevented with the proper education or policies in place. These attacks prey on the users to get them to click a file to infect the network or machine, depending on infection. Most of the time, they are blocked by the Anti-Spam systems on the network or in your email client. If an item is not blocked by Antivirus/Anti-Spam protection, then it is up to the end user to make an educated choice of whether to open an



attachment or not to. Many times, the emails seem legitimate and would warrant reading, however, it is not often that Bank of America will send a ZIP file attachment or any kind of attachment. As the end users make up the largest user base in any organization, training them on safe computing is a necessity. You cannot expect a new end-user to be 100% safe online without first training them on acceptable use and what should be accessed during work hours. The training for new users should be part of your security framework, and it should be revisited often.

- **Restriction of rights and software**—Many times, when a user changes positions, they take their rights with them. Instead of changing the rights to match the job, Administrators may just add rights to them, allowing them more privilege than they should have for their job. As an administrator, I tend to go for the least amount of rights the user needs to get the job done. If anything arises where they need more rights, it can be added. This way, the user would be restricted from possibly executing the file as they would not have permissions to do so; or the OS would restrict the infection from dropping the payload and becoming active. The same can be said for the Operating System, as the user should only have enough permissions on the system to do their job. There are many types of

restrictions, such as the restriction from accessing application data, and even some that are prebuilt as a GPO to prevent Cryptowall or its variants, but you will need to test and refine to get the ideal restrictions in place.

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via *Coursera.org*. He is currently responsible for working with large scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

Learn more about Filecoder, Cryptowall and Cryptolocker now.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®