February 2015

TechTidbit.com

brought to you by Tech Experts

CryptoWall 2.0: Ransomware Is Alive And Well

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

CryptoWall is the latest strain of ransomware to rise to prominence, extorting more than $1 million from victims and wreaking havoc on thousands of police departments, businesses, and individuals across the globe.

On the surface, CryptoWall is similar to its better-known predecessor Cryptolocker, another strain of crypto-ransomware. But there are many differences.

Victims are typically infected with CryptoWall by opening a malicious email attachment, though drive-by-downloads on websites are also possible. The email attachments are often zip files that contain executables disguised as PDFs.

Once infected, CryptoWall scans all mapped drives and encrypts important files. That's an important distinction: CryptoWall will scan your local drives, but also any server mapped drives, such as an S: or N: drive.

A text file then opens to explain the situation: The victim's files are encrypted and a ransom must be paid to unlock them. The ransom is typically $500 in Bitcoins, which will double if not paid within seven days.

Threat of a different color

A few features of CryptoWall 2.0 highlight the growing sophistication of ransomware.

CryptoWall infection begins with a "dropper" that enters the user's system. The dropper first checks whether it is operating in a virtual environment before downloading and installing the core malware files. If a virtual environment is detected, the download and installation do not occur.

Critical parts of CryptoWall arrive with multiple layers of encryption. This is to avoid detection by security products.

CryptoWall uses an anonymous network for its command-and-control communication. This makes it harder to find and shut down the ransomware's servers.

How to remove CryptoWall

CryptoWall removal is typically not a challenge. A simple scan with an up-to-date antivirus program can handle it in minutes.

The real challenge is how to decrypt files once they are locked. Even after the malware is removed, the files will remain encrypted. Unlocking them without a key is practically impossible.

Once files are locked, the only hope of unlocking them is to pay the ransom.

This is likely to work but it is far from guaranteed and we do not recommend it (feeding criminals just makes them worse).

A better idea is to remove the malware, delete the encrypted files, and restore them from backup if possible.

Preventing an infection

Explain to users the dangers and warning signs of phishing emails and suspicious attachments.

While it may be unpopular, ban through policy (and firewall changes) any personal use of the Internet on your business network.

Maintain backups of all important files both onsite and offsite. Test your backups regularly. Ensure they are configured to prevent backup of infected files.

Risks When Employees Use Their Own Mobile Devices

Michael Menor is Vice President of Support Services for Tech Experts.

BYOD (Bring Your Own Device) is an exciting development for increasingly mobile and interconnected employees, but also a new challenge for IT security teams.

Gone are the days where security professionals can lock down a finite set of machines and facilities; instead, they must manage an ever-growing, ever-changing landscape of employees, devices and applications, many of which have access to information that needs to be protected.

According to an article on eWeek, a survey was done on organizations with mobile devices connecting to their networks: only 33 percent have any official BYOD policy governing the use of personal portable devices, 67 percent do not.

The security risks are inherent in BYOD between viruses, hacking, improper security, and more. Flat-out thefts of smartphones, laptops, and tablets are also an issue.

In New York City alone, police data show that Apple products were stolen in a total of 11,447 incidents in the first nine months of 2012. That is an increase of 40 percent compared to the previous year.

Of course, employee education and awareness are important as informed users are more likely to act responsibly and take fewer risks with company data. Unfortunately, employees can be careless and criminals crafty, which is why network security defenses and policies are so critical.

Although implementing a restrictive device policy may feel like the most secure approach for your company, it can easily backfire.

Your craftiest employees are going to find a way to connect their devices to your network no matter what. And employees who do obey your “no iPhones” message will probably resent the policy and experience lower productivity.

Today’s workers expect to have 24/7 access to their information. They want to be able to catch up on emails on the evening train ride home or access information while away from the office.

BYOD lets IT staffs eliminate the hassle and expense of provisioning, distributing, and maintaining hundreds of corporate-owned mobile devices.

But setting up a BYOD program isn’t without its challenges. For starters, when you give employees free rein to bring in their own devices, you put your corporate documents and data at the mercy of the native security on these devices.

When you consider that many of your employees probably have “1234” as the PIN on their iPhones, that’s a pretty sobering thought.

Another major concern is your network. When you allow today’s increasingly powerful smartphones and tablets to request resources from your network, you really put your infrastructure to the test.

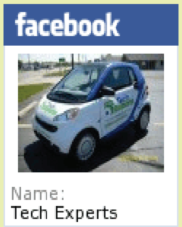
Are you ready to serve data instantly to hundreds of increasingly powerful hand-held mobile devices?

What if your mobile employees want to watch training videos, play back webinars, or listen to conference call recordings on their devices – can you deliver this kind of bandwidth?

Like most things, there are upsides and downsides, but a decision should be made on what best suits you, your employees, and your business.

When it comes down to it, BYOD isn’t a completely ridiculous idea. In fact, the benefits of BYOD may be worth the extra security precautions required to implement it.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we’re doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

Remote Employees And Network Connections

Scott Blake is a Senior Network Engineer with Tech Experts.

As businesses begin to downsize their ecological footprint, the need for remote or satellite employees grows. Business leaders and owners are now faced with the daunting question on how to allow remote employees access to their existing network without compromising network security.

One of the best ways to accomplish this is through the use of VPN.

VPNs allow secure access to business resources by creating encrypted pass-throughs via the Internet. The Internet, combined with present-day VPN technology, allows businesses a low cost and secure means to extend their networks to their remote employees.

The two most common methods in which to set up remote access are IPsec (IP Security) or SSL (Secure Sockets Layer). Both methods work well and both have their advantages depending on the needs and size of your business.

VPNs created using SSL technology provide remote-access connection from almost any Internet-enabled location or device using a web browser interface.

No special client software needs to be preinstalled on either device. This makes SSL VPNs a true “anytime, anywhere” connection to company-managed desktops.

There are two different SSL VPN connections to choose from: clientless and full network access.

Clientless requires no special software. All traffic is transmitted and delivered through a web browser.

There is no need to install or download any unique software to establish the connection. With clientless access, only web-enabled programs and apps are able to be accessed, such as email, network file servers and local intranet sites.

Even with such limited access to network resources, this style of connection is well-suited for most businesses.

Additionally, because there is no need for special software to be supported by the IT department, businesses can cut down on managed overhead.

A full network access VPN allows access to almost any program, application, network server, and resource connected to your business network. Unlike clientless access, full network access connection is made through the use of VPN client software. Because the client access software is dynamically downloaded and updated, it requires little or no desktop support.

As with clientless access, you have the ability to customize each connection based on employee access privileges. If your remote employees require the full functionality of installed programs and applications as if they were sitting inside the office building, utilizing a full network VPN connection is the obvious choice.

IPsec based VPNs are the staple of remote-access connection technology. IPsec VPN connections are created by using installed VPN client software on the user’s workstation and connecting device.

Client software allows for greater customizability by modifying the VPN client software. Businesses are able to configure and maintain the appearance and function of the VPN client, which allows for easier implementation for connections with other desktops, kiosks, and other special need cases.

Many businesses find that IPsec connections meet their requirements for the users, but the advantages of self-updating desktop software, accessibility from non-company managed devices, and customizable user access make SSL VPNs a front runner for remote-access connections to your office.

If you have any questions or would like more information about how a VPN can help your company, you can reach Tech Experts at (734) 457-5000.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Tips For Your Next Tablet Purchase

Now that tablets have become ingrained in the techie lifestyle, it's hard to believe the first Apple iPad arrived on the scene just four years ago. In the time that has passed since then, tablet sales and development have skyrocketed.

Consequently, there is a much larger variety to choose from today than just a single brand and its incarnations.

For those looking to upgrade their tablet or try one out for the first time, navigating the sea of tablet possibilities can be a daunting prospect. Here are a few tips to demystify your purchase choices:

Choose the right operating system for you: Apple's iOS gets the most attention by far, likely due to its length of time on the market, general ease of use, and plethora of applications available for download.

Android's OS is also competitive in the availability of apps, and it merges seamlessly with all of Google's applications.

Finally, the Windows OS is growing in popularity with users looking for a PC-like experience and aren't as concerned about installing various applications.

Get enough storage and a screen size you can work with: Just as if you were PC shopping, a huge concern is having enough space to store your files and a screen that is easy to read.

After all, it's no fun squinting to decypher text or choosing which applications to keep or ditch due to insufficient storage space.

Also, consider the screen resolution when choosing between models – it can be equivalent to the difference between a regular television screen and HD.

Decide if a WiFi only or cellular version fits your needs: There are two ways you can get online with a tablet – connecting via WiFi networks around you or using cellular service to gain entry.

WiFi only versions are typically cheaper, and you always have to option of turning your smartphone into a hotspot for on-the-fly connections. A cellular version is a tad pricier and requires additional service fees, but the advantaage is you will always be able to get online wherever you go.

New Security Risk For Android Phones

Just when you thought you had safeguarded your mobile device from any misuse, a new threat emerges.

For Android users, it's a big one. Rapid7 has recently discovered a security bug that allows cyber criminals to access a smartphone user's data.

Although this security problem is widespread, Google has responded that it will take no action to fix it. The bug exists in phones operating on Android 4.3 and below, and allows hackers to control your smartphone.

Although Android 4.4 and 5.0 users are not vulnerable to this risk, this issue affects approximately 60 percent of Android users – almost a billion people worldwide.

Google's official response is that their policy is not to develop fixes for older software versions, but it can notify people of the risk and others are welcome to create their own fixes.

To date, there are no known patches to address this issue. There is; however, one way to ensure your safety if you possess an affected smartphone. Simply download and install a newer version of the operating software.