Solutions are our Business

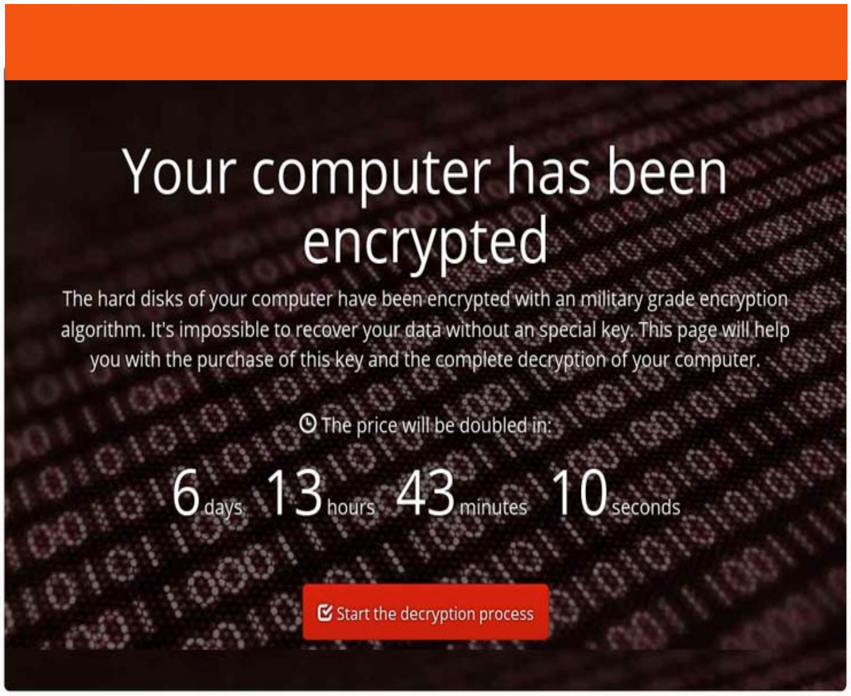
11301 N. US Hwy 301, Ste 106
Thonotosassa, FL 33592
(813) 246-4757 (phone)
(813) 246-4576 (fax)
www.aasysgroup.com

"SOLUTIONS ARE OUR BUSINESS"

MAY 2017

What You Need to Know About The Latest Malware Threats

(WannaCry and Adylkuzz)



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

By now, you have most likely read about the cyberattack that, last week, gripped the nation and the world with fear. A well-orchestrated ransomware by the name of WannaCry was launched, attacking many sectors and crippling more than 250,000 computers worldwide. Many hospitals in the UK fell victim to WannaCry, forcing them to divert patients to other hospitals while they scrambled for a solution.

Security researchers are deeming this the worst attack in 2017 thus far, and it has been reported that more than 57 million dollars has been paid out as of May 15th. That number is expected to rise as WannaCry continues to wreak havoc, even now.

Anyone running Windows XP, Windows 8 or Windows Server 2003 is the most vulnerable to the attack. This ransomware utilizes a vulnerability in Microsoft Operating Systems to quickly self-replicate and spread to other computers. In March 2017, Microsoft issued a patch to fix this vulnerability; however, many organizations were still running older versions of Windows and therefore were not able to update their software. This concern was so severe that it prompted Microsoft to release patches for software they no longer support in hopes of slowing down the rate at which computers were infected. That move was unprecedented and speaks to the magnitude of this attack.

INSIDE THIS ISSUE:

WannaCry is a ransomware that works by encrypting a user's computer, essentially locking out the user and inhibiting access to files or programs on the affected computer. Ransomware, as the name implies, most often comes with some sort of monetary demand, as was the case in this attack. WannaCry requested all affected users to pay $300.00 in bitcoins for the release of the attacker's hold on the encrypted data. The hackers also upped the ante and doubled the payout cost if the ransom was not paid within three days. If nothing was paid within seven days, the hacker threatened to delete all the files on the computer. With the amount of data that is stored on our computers nowadays, the possibility of losing all of that information is beyond horrifying.

Continued on page 2

As of this writing, the attack is still not over and there is still no apparent fix for those who have been affected. While a patch can assist with protecting your computer, it is not a fool-proof solution. Educating yourself and other end users about how to spot phishing and other types of malicious viruses can help protect your organization. Notify employees about the malware and make sure they are extra cautious about opening suspicious emails. Be extra vigilant about emails that contain attachments and links to URLs. Many of the strains of this virus are spread via .zip files attached to emails. It may sound redundant, but it cannot be stressed enough the importance of being aware of what you click on and what emails you open.

But just as users are struggling to make sense of WannaCry, there is yet another malware that has been behind the scenes for at least three weeks. Proofpoint has uncovered a malware attack that uses the same exploits which were used to spread WannaCry. It is called Adylkuzz. It's a cryptocurrency miner that installs itself on a computer and uses your computer's resources to mine Monero. It's being claimed that Adylkuzz has infected hundreds of thousands of PCs and servers worldwide. The worth of one Monero is about $28 and it's easier to mine as compared to Bitcoin.

Adylkuzz doesn't lock up the computer and demand a ransom, but instead causes servers and computers to significantly slow down. Because of this, it may potentially go unnoticed, which is why researchers believe it can be bigger than WannaCry. This attack shuts down SMB networking to prevent further infections with other malware like WannaCry. Ironically, it might have slowed down the growth of WannaCry.

Regardless if it is WannaCry or Adlykuzz, everyone needs to take precautions. It is imperative that organizations educate employees on best practices. Below are some tips to help protect against these malwares.

⇒ Always make sure you have the latest Windows updates.

⇒ Make sure your computer has the latest anti-virus updates.

⇒ Backups are crucial. Keep your files backed up regularly and periodically.

⇒ Do not open emails from unknown addresses.

⇒ Do not click on harmful links in your emails.

⇒ Be suspicious of visiting unsafe, unsecure or unreliable sites.

⇒ Take extra caution when on social media and do not click on skeptical ads.

⇒ If you receive a message from your family or friends with a link, before you click on it, verify that they did send it because infected machines can sometimes send random messages with links.

⇒ Look out for fraudulent e-mail messages that have excessive characters in the subject line, or that use names similar to popular services, such as PayePal instead of PayPal, or use popular service names without commas.

Sources:
https://fossbytes.com/adylkuzz-miner-monero/
http://www.pbs.org/newshour/rundown/everything-need-know-wannacrypt-ransomware-attack/
https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/
https://answers.microsoft.com/en-us/windows/forum/windows_10-security/wanna-cry-ransomware/5afdb045-8f36-4f55-a992-53398d21ed07
https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

More Help Is On The Way

Cybersecurity risk is at an all-time high. We are living in an era when everything is hackable: cars, TVs, computers, phones and pretty much any device that has an Internet connection. It can be extremely overwhelming, not just for average citizens, but especially for small businesses that have been entrusted with consumers' most valuable information. Most small businesses do not have the number of resources as big corporations and the Federal Trade Commissions (FTC) has recognized this and is now trying to do something about it.

Earlier this month, the FTC created a website designated to helping small businesses combat cyberattacks and scams. This is an important step in ensuring that public and private institutions are protected. The website ftc.gov/SmallBusiness features videos, articles and other information to help small businesses protect their networks and assets. According to Symantec's 2016 Internet Security Threat Report, 43% of small businesses are the subject of some type of cyberattack. Cybercriminals are very strategic about who they attack and know that most small businesses do not have the means to fully protect their organizations, therefore they go after them with a vengeance, knowing their attacks will most likely be successful.

This website could not come at a better time. Small businesses have been the backbone of our economy, accounting for 63 percent of the net new jobs created between 1993 and mid-2013 despite the slowdown during the recession. A cyberattack could be extremely devastating to a small business resulting in major financial loss that may be hard to recover from. The new website will highlight specific ways small businesses can protect themselves as well as protect their customers' data by providing tools such as a Small Business Computer Security Basics Guide which focuses on computer safety and how to protect mobile devices. It also addresses how to deal with a possible data breach.

In the end, small businesses need as many tools in their arsenal as they can get to protect them from hostile actors, more today than ever before. The events in the past two weeks have put a major spot light on the need for everyone to be prepared for not if there is a cyber attack but when there is an attack. This new website adds to the commitment of an "all hands on deck" approach to help fight against cybercriminals and is definitely worth taking a look at.

Sources:
https://www.ftc.gov/SmallBusiness
http://www.lexology.com/library/detail.aspx?g=ae12a7ad-0afa-4ac3-a372-c32c5cfb2c6a
https://www.us-cert.gov/ncas/current-activity/2017/05/09/FTC-Announces-Resources-Small-Businesses