MACC
MID AMERICA COMPUTER CORP

May 2018 eMessage

In this issue...

Billing Info

Transmit day for June 1st of the month billing is Wednesday, May 23rd.

2018 MACC Events

SAVE THE DATE!

2018 MBTC
Session 1: September 5-7
Session 2: September 10-12

****NEW LOCATION!****
DoubleTree Hotel
Omaha, NE

www.maccmbtc.com

MACC Trivia April Winner

Congratulations to **Michelle Van Heuvelan from HTC Communications** for winning March's MACC Trivia Challenge Contest.

Watch for MACC Updates for more chances to win, along with helpful tips & tricks and other important information!

MACC Success Story:

Check clearing is a breeze with this Accounting Master feature

The import feature is phenomenal for anyone who has to clear more than 100 checks per month, and if you have to clear more than 1,000, it is invaluable.

That's how Laura Gullickson, Office Manager and Accountant for Ntec, describes her use of Accounting Master's **bank reconciliation import feature**. The feature allows her to reduce work effort on an annual project from six to eight hours down to 30 minutes.

The import feature works by allowing users to upload a file from a bank into Accounting Master to easily identify records needing to be cleared. Laura has used the bank reconciliation process in Accounting Master for years and always liked the tool. It was the addition of the import feature in 2016's release of Accounting Master 16.1 that made all the difference in terms of saving time.

Put the import feature to work at your office
To learn how to best implement the bank reconciliation import feature – and others – MACC's Training Team has a 30-minute web session during which we will walk you through set-up, and answer any questions you have.

Please contact your Client Relations Manager or Account Manager for details.

Version 18.1 is now available!

Version 18.1 is the latest edition of Customer Master and Accounting Master. Visit the Client Pages for highlights of this edition, each product's Update Letter and links to online training that can help you get the most out of Customer Master and Accounting Master 18.1.

MACC Mobile and TMS Enhancements

MACC Mobile and TMS were also enhanced in conjunction with the 18.1 release.Visit Client Pages for the products' Enhancement Summaries.

Featured MACC employee for May

Payton Shaw is this month's featured employee. She is an Accounting Master Software Support Representative. As a MACC client, if you call in for assistance using Accounting Master, there is a good chance you'll be visiting with Payton.

Q. When did you start at MACC?
A. August 2014

Q. What's your favorite part of your job?
A. I love being able to interact with our customers and assist them with their daily questions.

Q. Can you please tell us about your family?
A. My husband, Austin, and I have been married for almost three years. We have a crazy cat named Mocha and an outdoor loving dog name, Mollie, who lives back on our family farm.

Q. What do you do for fun in your free time?
A. Anything that gets me outdoors! I love to spend the summer down at the lake with our friends and family.

Q. If you could travel anywhere to spend a week on vacation, where would it be?
A. Anywhere with a beach and sunshine!

Q. What's your favorite quote?
A. "Twenty years from now you will be more disappointed by the things that you didn't do than by the ones you did do." Mark Twain

Q. If you could add any food to the MACC vending machines, what would it be?
A. String cheese or dill pickle sunflower seeds

Avoid Becoming a Crypto-Mining Bot: Where to Look for Mining Malware and How to Respond

by MACC's Technical Support Team

There's a lot of speculation in cryptocurrency right now. People are mining coins all over the place, and even though it's getting harder and harder to make money mining coins, interest is still high. All it costs is money for the power bill.

Why is This Important? What's the Deal?

It's sort of funny; there's a feeling that cryptomining malware isn't malicious, and therefore it must be really hard to find. But look closer. The assets being attacked in the cryptomining threat are:

•System integrity •Compute •Power

Yes, that's less harmful than ransomware or APT, but in the end, it's still just malware, and you use the same methods to find cryptomining malware as you do anything else. But let's concentrate on three that are specific to this situation.

continued on page 4

Are you ready for a road trip?

by JoEllen Maras, Creative Services Designer

We are already very busy mapping out an itinerary for the 2018 MACC Billing and Technology Conference (MBTC). This year's conference will be held over the course of two weeks making it convenient for everyone in your office to attend.

Session One will be held Wednesday, September 5th through Friday, September 7th. Session Two will be held Monday, September 10th through Wednesday, September 12th. As always, the 2018 MBTC will be filled with informative sessions, valuable training, product updates…and plenty of great food and fun!

For the past 10 years MBTC has been held at the Embassy Suites in the Old Market District of Omaha, Nebraska. Due to renovations being done on the hotel, this year's conference will be held at the DoubleTree Hotel in downtown Omaha. Our new location is still a short distance from the airport and just six blocks from the historic Old Market District. With ample meeting space and lots of great amenities, we know you'll enjoy your stay!

Watch for future editions of this newsletter for up-to-date information, as well as periodic emails with more details on the conference. If you are not receiving our MBTC emails, please contact Kristi Rounds at KRounds@maccnet.com and she will get you added to our list.

We look forward to seeing you in September!

Strawberry Shortcake Delight

1 loaf (14 ounces) angel food cake, cut into 1" slices

½ cup cold milk

1 package (5.1 ounces) instant vanilla pudding mix

1 pint vanilla ice cream, softened

1 package (6 ounces) strawberry gelatin

1 cup boiling water

2 packages (10 ounces each) frozen sweetened sliced strawberries

Sliced fresh strawberries (optional)

Arrange cake slices in a single layer in an ungreased 13-in x 9-in x 2-in dish. In a mixing bowl, beat milk and pudding mix for two minutes or until thickened; beat in ice cream. Pour over cake. Chill. In a bowl, dissolve gelatin in boiling water; stir in frozen strawberries. Chill until partially set. Spoon over pudding mixture. Chill until firm. Garnish with fresh strawberries if desired.

Recipe courtesy:

Stacie Finken, Training Conversion Analyst II

Avoid Becoming a Crypto-Mining Bot

continued from page 2

How to spot mining malware:

Method #1 – Monitor the Network

Miners typically use mining pool platforms. Stratum, for example, likes ports 3333, 1333, 8333, etc. Decent "established-only" SNAT firewalls should block incoming mining requests. For outbound stratum connections, you should be getting alerts on network anomalies like these using the same tools you'd use for outbound inspection of any other type of malware. Note that many of these connections will be encrypted and may require SSL inspection where possible.

Peer-to-peer (P2P) mining pools may use DNS to locate other hosts. If you're lucky enough to have a threat feed that includes common pool servers as Indicators-of-Compromise (IOCs), great. But if you don't, use one of the ones listed below or find the malware another way. When you find it, check its config for "pool_address" and then watch for other machines on your network connecting to it. That will lead you to more infections.

Prevent employees running their own hardware cryptominers at their desks. The most powerful policy you can adopt is the one used by the most secure networks today; don't let unknown MAC addresses on your network. Yes, this is harder than just looking the other way, but for god's sake people, it's 2018 we need to get our heads out of the sand. If that's too much of a challenge for now (and I get it, not everyone has a fully-staffed security team), an addendum to the company policy is appropriate, as is an email as a start.

Method #2 – Monitor the Servers

Recall from our threat list that power is the third asset under attack in the threat surface. You're already monitoring your servers. Make sure you're monitoring their CPU usage and temperature. Many data centers monitor fan speed, a jump of which is another indicator of compromise. If any machine goes to 100% in the middle of the night and stays there, well that's suspicious and should be checked out. Even if a malicious miner is not consuming 100% of the CPU, the load itself will likely stay constant versus sawing around, so monitor for that.

Mature tools can tell you if new files have been installed on servers; maybe it's time to revisit TripWire if you haven't lately.

Method #3 – Protect Users via Block Lists

Drive-by cryptomining is JavaScript that affects browsers. Imagine a user visiting a site that hosts malicious JavaScript. The script mines coins while the user is on the site. The user's system integrity isn't affected, but her CPU is, and so is her power consumption. MalwareBytes wrote about variants that keep the mining going even after the user has closed the browser, which is really rude.

Fixing this problem is harder for administrators; most don't monitor network, CPU usage, or fan speed for their users, especially for remote users.In these cases, try to block access to sites that host mining JavaScript.

Conclusion – Get Back to the Basics

Take a step back and realize that cryptocurrency mining is really just another form of malware, which is something you should be good at finding already. Look at graphs, just like you always do, for DDoS, or malware, or anything else. Find the anomalies and track them down. It's the same with cryptomining.

Article by David Holmes in Security Week

https://www.securityweek.com/avoid-becoming-crypto-mining-bot-where-look-mining-malware-and-how-respond

We take security very seriously at MACC and have been working hard to develop a culture of security awareness. We are committed to offering our best to help you strengthen your defenses. If you have any questions or if there is anything we can do for you, please don't hesitate to contact your MACC Tech Support Team and we will be happy to help! We can be reached at 402-533-5300 or via email at macctechs@maccnet.com.