**Overcoming Cybersecurity Challenges During the COVID-19 Pandemic**

Thanks Alexa, we appreciate you having the time to spend with you today. I have about 15 minutes. I'm going to be covering some of the threat trends we have seen in the first half of this year. This data is going to come from trend micro customers information that we have received back and through threat intelligence network to give you kind of an idea of what we have seen, what trends we have seen that have gone on in the first half. Let's get started here. Obviously, the first thing to talk about is COVID, and the global pandemic. I have been in cyber security for over 24 years now. One of the things we have learned very early on is that news is used by cyber criminals on a regular basis. Any new news that comes up, any big event that happens in the world, they tended to utilize those as information to use in allures and the socially engineered tech. This has been just an unbelievable opportunity for several criminals to take advantage of. One, because this is a global pandemic. Their victims are everywhere in the world. They can utilize this information as often as possible. The second thing is that the news is constantly changing and there's a lot of different types of news associated with the pandemic that they are able to utilize. So, whether it is updates to infection rates, updates to death rates, vaccine information, or other types of ways to prevent. All that stuff will be utilized in the attacks and social engineers threat. So, this has been one of the biggest shift that we saw this year, we did not expect this, but it did happen and I will be relaying some of that information. If you look at the number again, this comes from our customer network. We have blocked almost 20 three blocks, you can see the second quarter was a bigger number, which is kind of expected because COVID hit back in February and cyber criminals really just a start to do utilize COVID in their attacks starting in March, you will see these and some of the results that we all share here in a minute. But certainly 28 billion, that is a couple billion extra that we saw same time of last year. So definitely had an increase year over year in terms of threat locked. Let's talk about some of the threats related to COVID. First of all you can see here, if you break down the threats we saw based on whether they were web threats, URLs, E threats or malware. Email threats dominated. 92% of the 9 million threats that were associated with COVID, if it was an email, there was mention of COVID in the subject line, if it was URLs, there were types of URLs associated with organizations dealing with the COVID threat like the CDC or the World Health Organization, etc. Malware, this malware is actually the name of the file tended to have COVID in it or some sort of COVID or coronavirus in the name. But you can see here email was by far the dominant threat. When we break down where we saw these threats, it is global, obviously, like I mentioned. But, the United States shows the biggest number at just over 38%. Germany down at almost 15%, France at 9%, Belgium 4.7. Obviously Europe is where it sort of started and we have started see big outbreaks in Europe early on. So, the threat actors were targeting that region. But the United States predominately has the bulk of the challenge here where the victims were located. If we look at messaging threats you can just see here as I mentioned, January and February, very few. March, we started to see an increase. April was the biggest. You can see almost 3 million messaging based threats, and it has dropped off since then, but certainly still a pretty significant number even in June at almost 2 million messaging related threats that we saw. The one other interesting thing that we saw with the messaging threat is, in the past what we saw was one a message that came into an organization, normally the malicious actors behind would either include a weapon eyes detachment or they would include a link inside the message, directing the them to a malicious webpage. But, what we saw was actually a combination we are seeing an attachment and a link included. They are utilizing both ways to get the victim to either open it up or click on the link. That was a little bit of a different change that we had seen in the past, and will probably continue to see that moving forward, which also means we will be talking to you about protection leader, but also just means in the messaging and security we want to make sure you can cover both weapon eyes the task as well as malicious URLs. On the website, you can see here on the overall thing, we had almost 1 billion malicious URLs, but COVID related ones, these are domains that were swept up for COVID or coronavirus. We had about 743 thousand of those malicious URLs that we saw, a lot of them are fishing, they will pop up the page and ask for your login credentials for your email or account information that is where we see these malicious actors trying to obtain account information. On the file side, you can see it is a little different. It started off in January and February, very small, and was supposed to grow up, in June it was the biggest number. Again, these are malware files that have the name either coronavirus or COVID or COVID-19 in the name. So people would receive these, again usually these are going to be weapon eyes detachments that may pop up and say hey, coronavirus vaccine.dock or PDF or something. When you look at the malware in general, we have, you can see here the top five malware's that we saw in the first half. Number one was want to cry, the rent somewhere they hit a number of years ago. What is interesting is that if you look at number one and three, a lot of people don't remember down at. It was actually a warm that was using a vulnerability that was back in 2008. It actually got patched in 2008. One cry actually was associated with the eternal blue vulnerabilities available. But the interesting thing about both of these is that both works. The challenge we have with worms in the industry is that worms sit on the system and they beacon out and try to infect other systems in the network or other systems on the Internet. It is very difficult to kill off warms. That is why we continue to see WannaCry , because still there's infection sources out there that are still trying to be propagated. The good news is that most of these are detection forces actual infections. People are not getting effective with WannaCry but it is still out there trying to attack organizations, same with DownAd, it is 12 years old but we still see 40 or 50,000 hits every month from our network out there. There are different resources out there. Others, we see crypto currency regular being shared out there. Powell load is one that we see regularly out there. Again, these files and criminals are using COVID all the time to name their malware so that people are unsuspecting and may click on them. The other thing we saw the phenomenon is that everybody is still working at home. We definitely saw targeted attacks on home users users. In this case you can see some of the tools that people are using, in this case on the lower left you will see actually we saw Zoom installers being shared, malicious zoom installers. You can see here the legitimate Zoom installer which is about 11 1/2 kilobytes. Very similar, you can see the two above it are actually malicious installers but still use a similar type of name. Size wise, they are pretty similar as well, there's only a little bit of size increase to include the malicious content. So, that is also a challenge that we have when these types of events happen. The actors will target the applications that people are using on a regular basis and Zoom certainly was one of them, as well as some of the other communication tools that people are utilizing. Rent somewhere, some interesting thing is we saw 68% decrease in overall Ransomware detections . We will talk about that. We did see some increase in Ransomware family. Some of the new families that came out that we saw. Cold lock was one of the new one that hit, a Taiwanese organization aimed at systems that held very critical information like databases, servers, email servers. New one that looks like it came out that is a successor in one of the tactics was actually to steal the files from an organization and threaten them with exposing that data to the public. The other interesting thing, one of the reasons why I think we are seeing a decrease in the number of Ransomware attacks is the Ransomware demands are going up pretty significantly. In this case, the Ransomware demand is up from 800,000 to almost 1.3 million. You can see here at the bottom right the Ransomware demand increases to around 62.5%. Actually the actors behind Ransomware are targeting organizations more selectively, but they are also increasing the ransom demands significantly. And the big change is it went from opportunistic where they, like I mentioned earlier, spray and pray. They spray and pray tons of stuff out there to try to get as many victims as possible, to the more targeted breach were now they are selecting the organizations and looking at what system can they expect that will have the biggest damage inside the organization or cause the biggest challenge for an organization for day-to-day operations, targeting those and getting those inspected. Then there also stealing data before they even start the process so that they will have a double whammy against an organization where they can say if you don't pay the ransom to decrypt all of these, maybe you have done your due diligence in terms of doing building a backup processing and rebuilding systems very quickly. Now we will ransom you for the data that you stole prior to encryption. So, they are for seeing this shift where they are definitely doing a more selected approach to who they are targeting with Ransomware. Some of the other notable threats we are seeing we will compromise increase as well you can see on the chart that there are COVID related attempts. They are using this as a way to propagate business value compromise attacks. But this threat continues to be a challenge and the FBI is seeing some insignificant increases in these attacks around the world. Another we saw a Windows vulnerability. Microsoft has been releasing on average over 106 for vulnerabilities this month. You can see starting in March, and even in July and August we have about 100 as well. There is also a significant window vulnerability that had just recently if you are monitoring that, the zero login ability that just hit. Microsoft, we are seeing a lot more patches for Microsoft. Some notable ones, we also saw VPN vulnerabilities being targeted. Again, this is probably due to a lot of the work from home users utilizing VPN into the organization, they will be targeting that infrastructure. Our Bugs Bunny program saw a 74% increase in the number of bugs that were submitted to us in the second half of last year through the first half. Definitely bugs and vulnerabilities are continuing to be utilized and exploited by criminals and their attacks as well. One interesting trend with file threats have gone down significantly. So the use of file less technology seem to be diminishing. We will see if that is an anomaly or that is something that continues to trend in the second half. The other thing that was interesting, these are my two final slides I wanted to highlight and mention work from home is a big one. So the threat actors are definitely targeting work from home users. We have technology that runs on home routers and smart home routers and smart home networks. We are able to identify inbound and outbound and different types of attacks associated with home networks. You can see here in the left-hand bar chart the number of inbound attacks we saw increased dramatically from just last year to the first half of this year. We are seeing very big attacks against home networks. And again, likely because they realize that everyone is now working from home. If we actually break it down into what types of attacks we are seeing, by far the biggest one is brute force logins. They are trying to get your login account from your routers and your devices inside your home network so that they can compromise those, then use them in outbound attacks in many cases, or doing attacks against organizations, we see these attacks in the first half of last year. So, they are looking for these IOT devices inside home networks to watch attacks. WannaCry continues to be seen, infectious sources inside homes that are helping WannaCry attempts outside the home. These are some of the attacks and trends we have seen. We have published a first-half security Roundup if you want to see more information about all of the different types of threats that we saw in the first half, you can go to our website and download that report. With that, I will send it over to the next speaker. Thanks everybody, have a great day.

High audience. This is Mitchell Chang. I am responsible for our global education at Trend Micro and very happy to share with you some of the latest development on how do you protect yourself for small business. I think one thing, as John had mentioned, we see, as far as the number, quantity -wise, we have seen quite a bit of increase on the hacker or cyber activity in the past six months. But overall, the technique they are using like Ransomware and emails and something like a business in a compromise, that has not changed. And I think hackers have more opportunity now because a lot of people have started working from home and taking classes from home, and also there is a lot of confusion like the whole slide change and a the PPE equipment and also companies usually the centralized organization, they may set up a business running from a location where you have a lot more remote work and how best to protect your data and access information, you create a lot more app opportunities for hackers. So, overall, the parts of cyber security for small business, I think the thing, we are advising the customers and users in community to do is still, we always communicated which I will go through, as Jon had mentioned , the email is probably the most used attacking method among all of the different ways to attack a. And especially like phishing. Some of the phishing email may and may not be malicious or spam email. So we saw an increase. And I think Jon shared this data. We see overall in the first half of the year and is going to the second half of the year, we have seen over 28 billion. But the majority of that is email. I think the reason email is widely used is because sending out malicious email and spam and phishing email is relatively low . So, the best way to protect yourself and to use security products or tools is to try to scan the malicious activity and emails gateway or server in such that the user will probably never see the malicious email, so you don't have to make a decision at your endpoint or your laptop computer whether to click on the email link or not. So, there's a different layer of protection. Since I lived in California, the example I want to give is that we have a lot of fires out there right now. And when you go outside you tend to wear a mask. But when you are home, you worry about the crack for the air may come in. So, there's different tools and a certain level of threat and you kind of have to be aware, which we will go through in a minute here. So, this is kind of review of the cyber security hygiene that we have always talked about in the past several years when we reach out to the community, and I kind of put in two different categories about security, and a kind of want to go through, device wise you have computer server or mobile devices and the cases are getting more diverse in a way protect yourself. We do have security vendors that do provide like IOT monitoring devices that protect the network. But overall, I think on the right side of the slide, vulnerability, the vulnerability windows that can be discovered, that is how we can update the operating system or app to better protect yourself when you apply these patches. And also, you do want to be familiar with security and privacy features of any devices, like the home routers. Each one has slightly different setup, and also may be slightly different settings. So, you take advantage of the features. And one thing I do want to mention, I think I saw it coming out there. If you are a small business sometimes you don't really have the time to understand all of these. In that case he may want to leverage a consultant or I.T.s system integrated to help you set up. I mentioned this before, it is kind of like fixing your automobile or your car. Some people like to work on their cars and do the oil change in the maintenance, but some people just rely on a good mechanic. So for small business we recommend you sort of make the decision which way you wanted to go to protect your network and your business is quite essential these days, with cyber security issues that we are seeing. And you do want to minimize application and location access. Wi-Fi is a good technology, but what can you are out in the public you want to be careful with what kind of access and unsecure Wi-Fi network, we usually don't recommend people access info access that information. And also, Bluetooth is something you don't want to have on all the time by default, if you can help it. And download apps and all of the devices, they have a security with the recommended change. For example, your Wi-Fi routers full password for administrative purpose that way you can put in an additional factor or two to protect yourself. Also, last but not least, this is actually quite important. You can use it to protect your business. There's a lot out there from micro where, we have a lot of projects for small business as well. And you wanted to get more of a commercial grade cyber security tools versus a consumer grade and free programs out there, there's a different layer of protection that you cannot. For example you can have email security added at a level that will filter your email before you have to make a decision whether you click on a phishing email or not. Okay, and the user security, I think the device is only part of it. But the user, it is up to you or your staff to help yourself. First of all, I think this has become a very essential, it is what we call to go factor or multifactor indication. One good example that is very popular now is using Facebook or when you want to change something on your user account level, it will ask you or send a text message to your phone or your device. That is adding a factor to indicate who you are. Usually the factors are something you know, something you have, this can be a text message to your phone or using a fingerprint system or facial recognition to get in in addition to the password. And also, speaking of passwords, I think definitely you want to use a strong password. I think quite a few of the product tools out there today, they are in your bank account they require a certain number of characters or special characters to make a strong password. And on the Internet, there's quite a few public sites that help you check customer your password is. You can see that by adding a symbol or character, it can take much longer for a heck her to crack your password. And I think also, another area that's important, cyber defense, when we work for a company, and usually use their protection to protect their network and servers. But that strategy is no more validated by itself. It's know about protecting data you can be anywhere anytime protecting data from your map and your mobile phone or your PC at home. So, how do you protect that? There's probably some additional work you need to consider. And also another important factor, because with all the rent somewhere out there, we recommend you pay the ransom, so having regular backup is quite important. And I think there are some questions on the VPN that I saw in the chat box. VPN is encryption technology, and we probably don't have time to get into more detail, but you understand what limitation for example, is for when you're working for a company, you want to access the company network and you have to connect sessions between yourself and your company. So, there is less chance of getting hacked or even having the hacker see the traffic and having to decipher what the messages. And minimize personal data, we will discuss more about that. One area I want to spend a little bit of time on is the email compromise. This is the perfect example where the actors are using both technology and social engineering to try to commit a crime, or try to attack the network. And I think the FBI has strong warnings, especially for small businesses about that tag. And first of all, most of what we see comes from email, and combining with technology and the hacker will usually try to find out their target's personal information, such as who was the potential target, let's say it was the company CEO or CFO or the family information so they can sort of create fake emails and we were you to click on the attachment. Once they establish that communication, you may think if you are a CEO or CFO you can have your email to wire some money to a supplier. But [ Indiscernible ] these organized crime outfits. And some of the recommendation that we have, I think for most, is trying to identify information on the Internet, that these are for your birthdays or the security. That is a must. Also important that you some people post internal company information, or their friends list on social network. And I think you can sort of minimize those activities to only your friends group or internal to your company employees only, that would be the best because social engineering cannot, they will not be able to make sense and create some sort of email for you to click. So we're used to have an eight security tool that is quite important. You have to process a system that only requires authorized suppliers to get paid and the chances of having a fake authorization to pay a vendor will be lessened. So, very quickly, I kind of want to give you a feel of what takes place. Because we see the number one hacking system is through email, phishing or spam. Spam may not be malicious , where they just have a lot of information that you don't care to read. If you are on the right side and you are a company where you have a lot of data back on the server or in the cloud, and where things get started is on the phishing side with there is malicious activity is that you will get an email and it may have some attachment, I think Jon demonstrated that already , such as installers for zoom or some kind of file that may alter the email adding malicious components. And we see a lot of this called snitching, they will come through a text message through your mobile phone for you to click on the response. One example that we see is very popular is like your bank will use, a fake email will send you a text message saying you need to contact the bank for some credit card fraud information. Once you click on it, essentially what it is trying to do is establish a channel between the hacker actor and you. At that point they may already compromise your account, so they can release your information like your login and these types of things. So, that will give them opportunity to do that that thing. So, I think what we mentioned earlier is about protecting the data. If you use a commercial grade antivirus or protection software, there's different layers and it will try to filter such as your email or even text messages that will prevent you from having to do with these issues. But, most importantly is also user awareness and education and behavior. So, we can talk about for a person or organization, a user gets some training, but the user tries to click on the malicious email, they open up a backdoor even the best protection software will not protect you. User behavior education is quite important. And to summarize, again. It is about overall security hygiene from these points that I mentioned. Also, I want to share with you two other thoughts. The Ransomware, we do run into this issue that these are the reason why you should not pay the ransom. First of all there is no guarantee that the folks will actually unencrypted or file. They basically encrypt your disk and asking for ransom. And it is almost impossible to on decrypt a file that is Artie encrypted. Unless the attacker left a key somewhere so a software vendor can be tagged. And also paying ransom is funding a criminal. And also if you pay the ransom, they would probably come back to you again because you have become a lucrative target. And last, but not least, I think some things to consider moving forward is something called IOT Internet, these are smart devices at home or in the factory. There is a convergence in the factory side, something called Industry 4.0, where the operation technology and the manufacturing I.T.s department where things are converging we are seeing a lot more devices out there giving the hackers opportunity. Also another area that I think is interesting is quite a bit of info misinformation out there sometimes including fake news, that will be becoming more and more prevalent, and also fraud and cybercrime. So, with that, here are some additional resources on the slides here you are welcome to reference to. But I want to give the floor to Kristin judge to talk more about cybercrime in the next section, thank you.. Smack thank you so much Mitchell, thank you to Trend Micro for supporting it. Thank you to Alexa for having me today. Really happy to talk about our services. We are a public private partnership and we exist to serve the individual of small businesses by cybercrime. We know there are people in the U.S. and small businesses who are struggling after they have been victims of cybercrime. We know also that we don't really know how many people are affected by cybercrime or how many small businesses, because we have not counted them as well as we probably can. We know that the Federal Trade Commission and the FBI Internet crimes complaint center probably combined get about 2 million complaints a year. We want to increase the number of people who are letting the authorities know they and hacked, or been a victim of an online fraud or cybercrime so we can work with Congress to let them know what kind of things are needed for the victim. When somebody is the victim of a cybercrime, small business consumer, where is the first place to go? Do you know what number to call? And where to go to get that help? Talk a little bit about that, that is the reason we make sure that becomes easier. And will share this slide from the Internet crimes complaint center just to make a point about how large of an issue this is. To people's pocketbooks and to our economy. In 2019, or hundred and 50,000 people reported to the FBI that they had been a victim of a cybercrime. And of those 450,000, either consumers or small businesses, they will have have lost $3.5 billion with a B. If you think about all the research showing at least one in four Americans is the victim of a cybercrime every year. That would be about 50 million attacks a year or someone is losing money. The real loss to the Americans and consumers and small businesses and the economy is closer to over $300 billion a year. This is another economic crisis on top of other crises that we are doing with that needs to be addressed people are losing money and many times they are afraid to come out in public because they are embarrassed. In their minds. The goal is really to make sure people are not shy about this. I worked with an amazing small business who had me on her podcast and she was willing to share what happened to her. She lost $200,000, but she shared her story. And hopefully when somebody else hears that story they are going to be paying attention if they are in a similar situation. The criminals are really, really smart. Is not that we are victims, it's that the criminals really know how to approach us. Many times will have people ask what is cybercrime? They understand online fraud as a term better than cybercrime. Cybercrime categories according to the Internet crime complaint Center can be seen here on your website. You probably care most about things like credit card fraud, identity theft, ransomware, phishing, and things like that that can impact your business. We really want to make sure that people know the answer to one question. Where do I start? From a victim of cybercrime, my business just got hit or my family got hit. Where do I go? This is an actual tweet from the Philadelphia police. People were calling YouTube excuse me, calling 911 because YouTube was not working. People were calling 911 because Facebook was not working. I know that can be a complete emergency to some people, but not a reason to call 911. But it shows the point that people really don't know where to go. And there are great resources. Here is an example right here on this slide, the hotline issue, because there are a lot of great resources. It is just hard to find how to get to those resources. That is where we come in. We have started some pilots in the following communities here where we have the existing 211 structure. Right now if you call 211 you can health and human services needs and referrals. We train 211 in these locations to help cybercrime victims get to where they need to go. It was not a surprise to us that most of the people calling in our calling about things like imposter scams, financial purchase scams and imposter scams can be this impersonation, you will see a dentist -- into devices which can include a website. So, what we did is we built fraud at support.org. This is a website you can go to right now and click on I am a business and get nine different categories to choose from. PowLoad -- Ransomware, accounts that have been hacked. To get the email you want, this very next page will have all of these following components. It will have a definition of what compromise is so you can make sure that is what happened to you, and some immediate steps you can take. And how do you report that business email compromise? What are some tools to recover? And how do you reinforce your security after the fact? You will notice here that we have some MICRA trend resources on here. Because one someone has been a victim of cybercrime, it's a really good time to educate and teach them how to secure their system. We also have a fantastic place that you can share with people in your life, especially seniors who are impacted by cybercrime. We have three golden rules that people can pay attention to like what left and right before you cross the street, slow down and stop or don't send gift cards or wire money to strangers. Don't -- if we can follow those three rules, we can follow and decrease cybercrime. For us increased reporting, increased recovering and increased resources so we can actually start decreasing cybercrime and victimization. We are a public-private partnership, we have funding from the private sector and also from federal agencies. We are very thankful for everybody coming together under one umbrella to really help make a difference. Here is some information about where to find our website, you can follows on Twitter and YouTube, we have some great free videos that are all under one minute. We have some graphs and infographics you can share. They are all vendor neutral, it is a great educational tool and if you want to engage and get some of these free posters or sent to you, you can give you this website cybercrime support.org. Thank you again for the opportunity to share and I hope people will visit our site and share with friends around you and your family and coworkers. Thank you.

Thank you all so much. We want to use the remainder of the time to answer audience questions that have been coming in. So we will do that for the remainder of time during the live with webinar section. I want to go ahead and get started here and kick us off. The first question comes in and asking about when clicking on a webpage, it goes to a spam webpage like hijacking URL. Is is usually a malware on his machine? Or has somebody hacked the server that he was browsing? Can you discuss that a little bit more and what can be expected?

This is Jon. So, it could be a couple of things . If your computer is compromised, they can make modifications so that if you go to a website you will get redirected. But more likely, the culprit here is that they have compromised the site you are going to. They have added some script summa, some cross site scripts so that when you reach the website the browser is redirected to another site. The challenge you have is a person doing this in many cases, a lot of the stuff being done is in the background. So, you won't see often, you being redirected through, and it could be multiple sites you are being redirected to and from, where ultimately one of the webpages or web sites that get dropped will drop malware onto your system. So, it really just depends if you suspect something, you should run a scan on your computer. There are free skins out there. Housecalls is one area but there are lots of free skins out there that you can do if you don't have an Internet security product running that has web skinning for you. But certainly you want to do some scans on your computer to see if you have some malware or something showing up.

Next question, this comes from Terry. We have had other audience members asked something similar. This is around backup. If you could talk a little bit about backup options and small businesses should consider beyond the cloud, for example.

This is Mitchell. You said beyond the cloud?

Yes. So if somebody was using it cloud-based backup, are there other options?

Right. Well, certainly I think before the cloud the most popular thing you could use it was a USB drive or additional backup drive or home users. But now, I think the technology that is in all, there's a lot of vendors who stole one drive from Microsoft and all of these technology you can synchronize your home database without some sort of cloud provider and they use something that we refer to as public cloud there, like Amazon Web services. So, there seems to be less need of a premise sort of backup. But I think the caution point two consider, also, is that I think when you backup the data to these services and before you do that, you can create a vulnerability and accidentally share something you don't want to share on 70s network. So, it depends on the level of sophistication, for larger organizations we definitely

Reporter: Recommend the I.T.s department to backup. Backup is an must these days. If you do not is no longer an option anymore.

I would only add one point and that is to make sure one of the copies is off-line. In many cases, the Ransomware actors understand the backup is a great way to defeat them. So, they will actually encrypt a backup if it is online all the time, and then they will backup or encrypt all of the files in the backup, even on the web-based cloud-based backup. If they add action to it or they have ransom, it has access to the drive associated with the backup and will encrypt everything there. You also want to make sure you follow the principle of having a regular off-line backup of your backup.

All right, next question here is from Patricia. Patricia would like to know how do we know when our system is compromised? This is Mitchell, I think I answered a similar question for another viewer. I think some of the compromise is obvious, like when I read somewhere active attacks or system, is it going to be obvious that your disk is encrypted and you get a pop-up message. But some are not so obvious. They may even betray your system that they are stealing credentials and waiting for an opportune time to launch an attack. But, if you have any suspicious, especially, as Jon mentioned , you can always click on the link and you are not supposed to. So, you want to take the precaution to either consult your IT consultant or if there is a scanner doing something we call housecalls, and online scanner that you can put the scanner on your system and make sure nothing gets dropped in your filesystems or things like that. And yeah.

Also, just look for slowdowns. I think slowdowns. Crypto minors are notoriously resource hogs. You will see a lot of slowdown in your resources, your CPU utilization will go pretty high regularly. So, others things you can monitor your CPU and memories and see spikes and regular spikes and regular increases that are not normal operations that you want to take a look at them.

And I think also to your point, we mentioned the multifactor or two factor authentication. I think to post points Jon has made. Backup and system, that is actually very critical, multifactor authentication. Imagine a user has copper Mize to your system. And they don't want to get into additional credentials, your other credentials are multifactor. Are you doing a warning where let's say you do not try to change her password or access your account information and also you get a message from the vendor that you are trying to access and that could be also a warning sign.

Okay. Looks like we're going to have time for one or maybe two last questions here, this comes to us from Mike and Mike is asking should a home office or small office look into setting up virtual networks using a managed network switch to break up their devices.

This is Jon. I do believe that segmentation is one great way to defeat ransomware actors, for example, that they are encrypting a number of your devices if you are segmented out a few areas of your network that cannot get access to those other areas and we will certainly contain an attack better than if you have a flat network that is open to everything, especially small business where. And I know a lot of them may have a single business server and everybody connected to that, that might make it a little more difficult. But certainly, I do believe one of the ways that a lot of the bigger organizations certainly are looking to contain outbreaks inside the organization is through segmentation. That might be something to look into again, probably the best bet is to talk to your advisor or IT a professional that does this for a living and they can make a recommendation on how to do that most effectively. The good news is that a lot of technology has gotten much more improved and better to help support them.

All right. So, we are out of time to take additional questions. We realize there are a lot of questions that have been addressed. We did not have a chance to address your question, I would like to recommend a few options. One, you can reach out to your mentor after today's session who can assist you with further questions and your business needs if you're not already working with the mentor, you can get further information and request one by going to score website www.tran01.org/find mentor, it will also, as a reminder, we are sending out slight decks to all participants in the post event email is going out just after the webinar ends today that contains the speaker's contact information you can reach out to for further assistance there as well. So, before closing I do want to make sure that you are familiar with other available resources that are on the final slide and they are accessible by clicking on the respective link's here. SCORE has live, free webinars weekly , you can view and register for upcoming webinars by clicking the link on the screen. We also record the live webinars and the recordings are archived for you to do any time after the live session. The small business resiliency hub provides resiliency resources to help you during a crisis. So, on behalf of SCORE, I would like to thank you all for attending today and I would like to get a very special thanks to Trend Micro for sponsoring the webinar and our presenters Jon, Mitchell and Kristin. Thank you all so much for your time and sharing such value and critical information with the audience. thank you for the opportunity. Thanks everybody, have a great day.

Thanks again, everyone. Take good care and we look forward to seeing you back next time.

[ Event Concluded ]