Protect Your Business from Money Mules Transcript
Transcript

Part 1: How Organized Crime Uses Money Mules and Malicious Code

Julia Allen: Welcome to CERT's podcast series: Security for Business Leaders. The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. I'm pleased to welcome Chad Dougherty, a member of CERT's Cyber Threat and Vulnerability Analysis Team.

Today Chad and I will be discussing the rise in small businesses that have had their bank accounts cleaned out by organized criminals, using approaches where people are recruited to receive and transmit stolen funds from their country of origin to another, to protect the identity of the criminal. We'll also discuss what to do if you find yourself caught by one of these schemes. So welcome Chad. Really glad to have you with us today.

Chad Dougherty: Oh, it's good to be with you.

Julia Allen: So to get us off and running, could you just say a little bit about what this money mule scheme is, and in particular why it seems to be hitting small businesses?

Chad Dougherty: Sure. So the recent activity really is just a new take on some traditional online financial fraud that we've seen before. But in the most recent activities, the small business owners are the targets. And there's really a couple of reasons why that is. As opposed to individuals, small businesses typically, or frequently, have more cash in their accounts that can be transferred to a criminal. And unlike the larger organizations, they may not have a formal security policy or their defenses may be lower than a larger commercial organization.

Likewise, one of the reasons why it hits small business owners the hardest is because for many business banking accounts, the business owners don't enjoy the same account protections against liability that individuals do. So some of the listeners may be familiar with online credit card fraud against individuals. In many of those cases, the individual is not liable for the fraudulent transactions; whereas the small business bank account holders are responsible for the funds, and in many cases if the fraudulent transactions are completed, they're stuck with the entire loss.

Julia Allen: So how does this actually work? I know that we hear this term 'money mule', and there are people that are recruited to participate in these schemes. But could you walk us through the steps of how this actually happens, and how these folks get involved?

Chad Dougherty: Sure. There are a lot of different ways that these fraudulent activities can go, can be played out, obviously. But one of the most common, especially recently, involves money mules. And these are individuals whose job it is to receive money, receive bank transfers into a personal account, and then withdraw the funds from that account and send it via some payment transfer service, like Western Union, to an account where the criminals can then withdraw it and essentially cash out that transaction.

In many cases, these money mules are unwittingly involved in the transaction because they've signed up for some -- they may have received a spam email saying “Work at Home,” or something like that. And in those cases their job, the job that they've been recruited into is to give their personal bank account credentials to the criminals. And then basically sit by their computer and wait for a signal that funds have been transmitted into that account. And when the funds have been transmitted, then they're instructed to withdraw those funds and then complete the transaction through the payment service, like I mentioned.

Julia Allen: So they're not actually involved in targeting the small business and taking the funds from the small business. They're involved in moving it the next step down the chain, right?

Chad Dougherty: Right, that's correct. They're basically the last mile in the transaction. And what they get from that is at the point where they've withdrawn the money from their account, they're instructed to keep a certain percentage and send the rest via Western Union or other payment transfer service to the criminals.

Julia Allen: So is the whole idea behind this to obscure the identity of the criminal; just put somebody else in the loop so that the association with the criminal is more hidden?

Chad Dougherty: I think that's one reason, yes. And another reason is to keep the amount of the withdrawals small.

So if you can imagine a victim organization having a single transfer of let's just say $100,000.00 into another account that was then attempted to be withdrawn, that would raise a lot of alarms. What the organized criminals do in these cases is if they have an assortment of different accounts that they can transfer money to, they'll do it in smaller batches, and these smaller batches are less likely to raise alarms.

So in those cases, it is one way to obscure the criminal's identity. But it's also sort of a resiliency effort by the criminals to make sure that they can get smaller batches of funds, instead of losing out on one big transaction.

Julia Allen: So this is kind of interesting. And you may not know, but how many money mules -- let's say that a criminal absconds with a certain amount of funds from a number of different organizations. But how many people might they recruit to be involved in a single transaction or a number of transactions against a small business? Do you know?

Chad Dougherty: No I don't know offhand. Like I said though, it will typically be based on how much they're trying to transfer. So if the target is to keep the transfers under $9000.00, just by using simple arithmetic you can guess how many money mules are going to be involved, based on the total that they're trying to transfer.

Julia Allen: And am I correct in understanding that once a criminal uses a money mule, they typically use them only once? Or do they use them a repeated number of times?

Chad Dougherty: No that's right. The typical process is to use a money mule only one time. And then once that individual's account is cleared out, these individuals that believe they've accepted a legitimate business opportunity to work at home, they're just dropped cold and they never hear from that organization again.

Julia Allen: Very effective. So let's dig into the technology a little bit. Can you describe some of the tools, techniques -- perhaps malicious code or other types of attack strategies -- that criminals use to take funds from small businesses?

Chad Dougherty: Sure. As I did mention once before, there are a lot of possible ways that this can play out. But again, one of the most common is that a PC that the victim account holder uses to do their online banking will be compromised through a lot of the same means that home users and corporate users get compromised.

The listeners may be familiar with the term 'drive-by download', in which in that situation the victim is browsing to a website that contains some malicious code. It may exploit a vulnerability in the user's browser, or some other piece of software installed on their computer, and then allow a more sophisticated piece of malware to be installed on the system. And in these cases, the small business owner may have just a single PC that the employees use to browse the web, or do general purpose computing tasks -- read email or things like that. And in the course of doing those other things, the system becomes compromised. And then the next time the account holder or the accountant or the business owner at that business goes to do their online banking, that gives the attackers an in to the bank account.

Julia Allen: I remember also in one of our earlier conversations as we were getting ready for this podcast, you said there's also approaches where the criminals have software in the browser, or have screens in the browser, that actually make it look like the balances and the transactions are legitimate, where there's other things going on behind the scenes. Have you seen occasions where that has happened?

Chad Dougherty: Yes, that's exactly right. In many cases, the malicious code that is installed is very sophisticated. And it can give the account holder the impression that everything is okay with their account. It basically shows them the balances that they expect. But in reality it's using what's referred to as a “man-in- the-browser attack,” where the fraudulent transactions are going on behind the scenes, either automatically by the malware or through remote control of the criminals. And so basically there are two books being kept: one is being kept by the malware and displayed to the user to give them the impression that nothing's wrong. And the other book is obviously the one where the malicious transactions are occurring and reflects the true withdrawals from the account.

Julia Allen: That's pretty darn sophisticated, isn't it?

Chad Dougherty: Yes, it's pretty impressive. It also illustrates the fact that once the user's system is compromised, it gives the attackers a lot of leverage in terms of what they can do to maintain that illusion of security.

Part 2: Actions Businesses Can Take to Protect their Accounts

Julia Allen: Okay, so that's all the bad news. Let's see if we can turn our attention to some of the good news. So first of all, how might a small business owner become aware that this is happening to them; other than getting an alarming call from their bank or a statement that doesn't look like they're expecting? How do they find out that they may be subject to this kind of attack?

Chad Dougherty: Well unfortunately the cases that I'm aware of have been the result of the business owner going to their bank account and finding that it's -- they're overdrawn on a particular transaction, or the funds simply aren't there. In the cases where they're lucky, they'll

receive a notice from their bank saying, "We detected this attempt to transfer some amount of money. Is this a legitimate transfer?" But yes, in most cases -- this is still on the bad news front, I guess -- but in most cases, the account holder is not notified until the money is gone or nearly gone. And in many cases those transfers can't be reversed. So at that point they're out of luck on those particular transfers.

Julia Allen: Is there something that their bank should be doing on their behalf? Is there something they should look for when deciding what to do business with, in terms of protections or thresholds? In other words, are there some actions, both in terms of running their own business and then in working with their financial institution, that they can take to be a little more proactive?

Chad Dougherty: Yes there are. And if there's some good news, I guess this is where it comes in.

Really what the small business owners should do is number one, make sure they understand upfront what protections their banks offer, and what their liabilities for fraudulent transactions are. In many cases, as I mentioned, the small business account holders are completely surprised to learn that they can't recoup any of those fraudulent -- the funds from those fraudulent transactions, after they've occurred.

The second is -- and this is an area where small businesses may have an advantage over a home user, for example -- they can opt to use a system specifically designated for online banking at the organization instead of using a general purpose PC. So, as I mentioned, a lot of times a system at their business can be compromised because someone's using it for general purpose web browsing or email or other applications. But if the small business owner keeps a system set aside, just for banking, and maintains the security of that machine, keeps it updated on patches and antivirus signatures, and uses it only to go to the site where their online banking is done, that can go a long way in preserving the security of their account.

And finally, the last thing is to have them set up with their bank certain security precautions that will be limits on how much money can be transferred. For example, if a fraudulent transaction is attempted that exceeds a certain threshold, they will get an alert about that and it won't -- they can set it up so that it won't go through automatically without their specific authorization. And this authorization for large transfers can be done in an out-of- band mechanism, to add more security. So it might be something like a call back, or a fax, or an SMS (short message service aka text message); something that doesn't involve the same system that may in fact be compromised. So those are some of the things that the business owners can do to sort of attempt to prevent this fraud.

Julia Allen: Are you finding that banks are offering services, or are perhaps doing things like profiling what is considered normal behavior versus abnormal behavior? In other words, they do work with a small business and they know the small business does their payroll at the end of every month, or they know certain accounts payable/accounts receivable transactions take place in the course of a month, and they profile that. And then they monitor for things; like we get with our own personal credit cards where sometimes we'll get a call from our credit card company and they say, "Is this really you doing this transaction because it's in a different country than we know that you live in?" Are you seeing those kinds of services, banks offering those kinds of services to small businesses?

Chad Dougherty: I don't have a lot of information to support that. I do know that some of the banks will register a particular IP address the transaction should be coming from. So an

obvious sign of fraud would be if the account holder's account is accessed from IP addresses that exist overseas or foreign internet service providers, or something like that. But as we discussed already, in many cases the fraud originates from an infected PC that the business owner has on-site. So in that case, from the bank's point of view, it would be difficult to detect malicious access, based on IP address. That's one of the things that business owners should discuss with their banks, to see in reality what security precautions they do offer, and opt into those services when they can.

Julia Allen: Excellent. Well this has been a great introduction Chad. I sure appreciate being able to explore this topic with you. Do you have some places, some resources, where our listeners can learn more on the subject, or keep up to date on what's happening?

Chad Dougherty: Sure. There's a reporter named Brian Krebs who previously worked for the Washington Post who's been doing a lot of work on this topic. His website is krebsonsecurity.com. And recently the Secret Service, in conjunction with multi-state ISAC, which is Information Sharing and Analysis Center, published an advisory about this type of fraud. It refers to this very type of fraud, including the most common form -- the most common malware that's associated with it, which is a Zeus trojan. And this is one of the sophisticated pieces of malware that can further this type of fraud.

Julia Allen: Well this is great. Again, I thank you so much for your time and expertise, and helping our listeners get up to date on this new form of attack. Thanks very much Chad.

Chad Dougherty: Sure, my pleasure.