The Daily Scam Newsletter - August 28, 2019

The Week in Review

Last week was the quietest week we've had all summer! We hope this is truly what our hundreds of weekly readers are experiencing. Not only were there far fewer scams and malicious emails last week than usual, but a multi-million dollar romance fraud gang got taken down by the Feds here in the United States and efforts are underway to arrest their compatriots in Nigeria! Hazzah! These bastards also targeted businesses and individuals with other types of scams. Faith Karimi, a CNN reporter, did a nice job presenting the details in her August 24 article titled "Men in California oversaw a romance scam that targeted women worldwide, feds say."

Phish Nets: Unexpected Source of Identity Theft

Neither we, nor our readers, found any phish in last week's ocean of emails or texts. What a breath of fresh air! However, we're sad to report that a Reddit user named **Kahnsg** gave a very detailed report on Reddit.com about an unusually complicated phone phishing scam that successfully targeted his girlfriend. It all started with a call to order a pizza from Papa Johns. Quite honestly, we never conceived of such a scam before! It was worrisome and fascinating how it happened. Kahn tells his story very well and it is worth reading it on the Reddit site to raise your awareness! Read the comments that follow it too!

https://www.reddit.com/r/personalfinance/comments/cu9oz0/our_identity_was_stolen_over_the_phone_the_case/

Your Money: Woodworking Projects

We often wonder how criminal gangs decide to target certain specific populations of people. Obviously, their broader motivation is that they believe they can trick this particular population of people to click a link based on the content of their weapon. Take, for example, this next malicious clickbait from August 22 with the subject line "**16,0000 woodworking plans inside…(2 days left).**" It is clearly targeting the do-it-yourselfer, that man or woman who likes carpentry projects. If you look closely at the email you'll clearly see that it references **"TedsWoodworking**" in both text and the picture.

We found multiple variations of **tedswoodworking** websites at DOT-co, DOT-com, and DOT-org. But this email didn't come from any of them. The first thing to notice is that it came from the domain name that follows the "@" symbol: **coundebb[.]us**. And of course, links in this clickbait point to that oddball domain. That's the most important "poker tell" that this is not likely what it appears to be. We used the Zulu URL Risk Analyzer to evaluate the link found in this email and confirmed our suspicions. This email is malicious. That wasn't surprising. What was interesting to see was that the malicious domain, **coundebb[.]us,** uses a forwarding script to send you to one of the real domains for Ted's Woodworking sites. This malicious clickbait first sends you to **coundebb[.]us** where your computer is hit with malware, and then forwards you to the real Ted's website so you aren't even suspicious or aware that you just got a computer infection!

16,000 woodworking plans inside...(2 days left) Inbox ×

Woodworking Carpentry <tedswoodwork@coundebb.us> Thu, Aug 22, 5:01 AM (2 days ago)

to me

The Complete Woodworking Carpentry Guide..

Hey,

This is important:

Have you secured TedsWoodworking yet?

If not, go immediately to do so...

PRICE IS GOING UP IN 24 HOURS

As I've said, this is the *EASIEST* way to start your woodworking projects - and it's still at a ridiculous low price:

If you're just starting out or you're a seasoned carpenter, you'll find out just how simple it is to build projects using TedsWoodworking step-by-step plans.

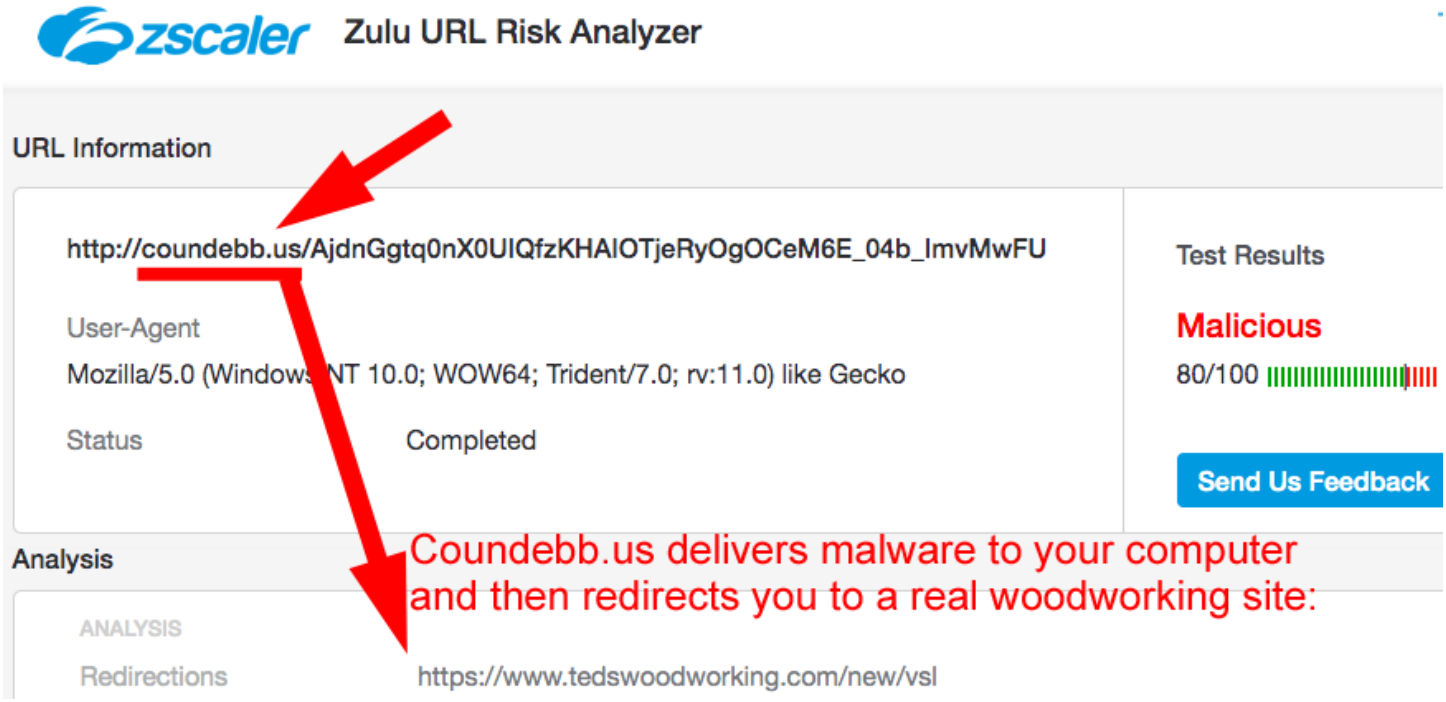
With over 16,000 plans, it covers a ton of projects. Check it out and see why I endorse it so much.

You'll love it.

So hurry...before this offer ends:

Take care and talk soon.
Shawn

coundebb.us/AjdnGgtq0nX0UlQfzKHAlOTjeRyOgOCeM6E_04b_lmvMwFU



Top Story: Sextortion Again :-(

We have written many times about sextortion. It is one of the most frightening and brutal online scams. In the past we've reported that at least one man had committed suicide as a result of being targeted by this type of scam (in December, 2017) and we've helped a few others step away from that cliff by exposing that what they thought was a real threat was, in fact, a scam. Last week, we had an unusual trifecta of three different variations of sextortion come to our attention. Though we've written about these scams before, it is important to raise awareness in our readers and their friends or families about this brutal, and effective collection of scams.

Our first example targeted us at The Daily Scam! During the last year we've twice received emails like this extortion email. It can be VERY intimidating to hit someone who is not very tech savvy and fits the circumstances described by the sender. Knowing that "Anonymous Hacker" sends out thousands of these emails at a time, it is highly probable that dozens of them hit a mark somewhere. In a nutshell…

1. Anonymous hacker claims to have installed malware on your computer that can turn on the video camera and record you without your knowledge.
2. Anonymous hacker claims to have captured a video of the computer owner masturbating while viewing pornographic images of teenagers.
3. Anonymous hacker claims to have stolen "all your email contacts and a list of your friends on Facebook."
4. Finally, the anonymous hacker threatens to publish the video he/she claims to have UNLESS you pay $2000 in Bitcoin to his untraceable Bitcoin account.

To increase your anxiety, and add to the pressure recipients of this trash will feel, the anonymous hacker claims to be monitoring your activities as you decide how to handle this threat. He/she implies that if you attempt to research what's just happened to you, the embarrassing video will be released. But there is no video. This extortion threat is a complete hoax. There was no malware recording the computer owner and it is just an empty threat. But the recipient WILL RECEIVE a follow up email giving him one more chance to

comply, or he can request an additional “48 hours” to get his money by opening “notepad and write ‘48h more’.” Take our word for it, this is total BS. Delete this bad boy!

▽ **IMPORTANT! You have been recorded masturbating! I have Iamspecial.mp4!**

From: Anonymous Hacker
Date: Today, 11:24:36 AM CDT
To: iamspecial@thedailyscam.com

ATTN: iamspecial@thedailyscam.com

The last time you visited a porn website with teenagers, you downloaded and installed the virus I developed.

My program has turned on your cam and recorded the act of your masturbation..

My software also downloaded all your email contact lists and a list of your friends on Facebook.

I have the - Iamspecial.mp4 - with you jerking off to teens, as well as a file with all your contacts on my computer.

You are very Perverted!

If you want me to delete both files and keep the secret, you must send me the Bitcoin payment.
I give you 72 hours only to transfer the funds.

If you don't know how to pay with Bitcoin, visit Google and search - how to buy bitcoin.

****
Send 2,000 USD (0.2011839 BTC)
to this Bitcoin address as soon as possible:

35gEfEUU2gPsj3Fu1XcHF3QLo8tZh8UjLm
(copy + paste)
****

1 BTC = 9,970 USD right now, so send exactly 0.2011839 BTC to the address above.

Do not try to cheat me! As soon as you open this Email I will know you opened it.
I am tracking all actions on your device..

This Bitcoin address is linked to you only, so I will know when you send the correct amount.
When you pay in full, I will remove both files and deactivate my program.

If you choose to not send the btc I will send your masturbation video to ALL YOUR FRIENDS AND ASSOCIATES from your contact lists that I hacked.

Here are the payment details again:

Send 2,000 USD (0.2011839 BTC)
to this Bitcoin address:

****
0.2011839 BTC

to: 35gEfEUU2gPsj3Fu1XcHF3QLo8tZh8UjLm

(copy + paste)
****

You can visit police but nobody can help you. I know what I am doing. I don't live in your country and I know how to stay anonymous.

Don't try to deceive me - I will know it immediately - my spy software is recording all the websites you visit and all your key presses. If you do - I will send this ugly vid to everyone you know, INCLUDING YOUR FAMILY MEMBERS.

Don't cheat me! Don't forget the shame and if you ignore this message your life will be ruined.

I am waiting for your Bitcoin payment. You have 72 hours left.

Anonymous Hacker

P.S. If you need more time to buy and send BTC, open your notepad and write '48h more'.
This way you can contact me. I will consider giving you another 48 hours before I release the vid,
but only when I see that you are really struggling to buy bitcoin. I KNOW you can afford it - so don't play around...

One of our readers told us about this Forbes Magazine article published in early August to inform people that criminal gangs are using stolen email lists of millions of people to perpetrate these “anonymous hacker” scams. You are read their article here: https://www.forbes.com/sites/zakdoffman/2019/08/05/200m-email-addresses-held-by-sextortion-attackers-is-yours-on-their-list/amp/

You can also check a database created by the security firm Cofense to see if your email address is amongst those stolen and has the potential to be used by this group of criminals. For example, the criminals have more than 49 million Gmail account addresses to contact!

The second type of extortion we heard about last week is also well known to us. Over the last few years we’ve heard from about 50 men who’ve been targeted by women via Facebook. These women (or men playing women) entice the men into engaging in online sexual stimulation via video chat. However, what the men don’t realize is that they are being video recorded during this exchange. Here is a story told to us on August 23 by a young man about this form of extortion…

“I was recently friended my someone on Facebook who went by the name Balinder Gaud. "She" messaged me later on and like a naive fool, I messaged back. Now I have been single for over 3 years and having some beautiful woman message me out of the blue caught me by surprise but I kind of figured what's the harm it could do. So we talked and told a little bit about ourselves when ahe asked me if I like sex, and I replied, "Who doesn't." She then later offered to video chat with me and show me her breasts. I didn't think she was serious so I was like, "Sure, ok." She then gave me a video call on Facebook messenger and started exposing herself. She kept asking me to expose myself as well until I finally gave in. Next thing I know they were claiming that they were 15 years old and that they were going to expose me, making quotes from law books stating on how what I did was wrong. I will admit that what I did was completely reckless and stupid and I do not know what I was thinking. I made a really foolish mistake. They then said that they would delete the video if I sent $5000 to a hospital in West Africa saying that I would be doing a good deed. They say that they do this to help people and to teach people online not to expose themselves. They shortly opened a group chat and my family was in it, the mother of my children and a few others. The chat had a picture of my face from that video and I immediately told them [my family] *that it was a scammer and not to respond. I also messaged them and lied to them saying that I did my research and I tracked them and know who they are and to leave me alone. I haven't heard back from them but they did threaten to contact my employer and wreck my life. This was a lesson learned on how you should never trust anyone online.”*

A footnote to this awful circumstance: We don’t believe for a moment that these scammers donate the extorted money to a “hospital in West Africa.” That bit of manipulation is simply meant to lower the anger that the victim might feel about being extorted. Also, we do not believe this scammer has acted alone, or that the victim may even be interacting with a “live” feed from a “woman.” Men reporting this scam to us do not give us the details of their video chat interaction. It is quite possible that it is a recording designed for the purpose of getting a victim from point A to B, with little communication besides a few pre-recorded messages. We believe that it may be a criminal team involved in at least some of these sextortion scams because of the quick turn-around by which the “women” gather contact information, create and post a threatening Messenger group along with an image taken from the video that was captured. These criminals generally strike fast and give little opportunity for the victim to think, conduct research or figure out how to respond to this threat.

Our advice may be a bit uncomfortable, but it is always the same…. DO NOT PAY! Experience has taught us that if you pay those who extort money from you, they will usually come back for more! Here is our advice to the men:

1. Immediately delete or suspend ALL your social media accounts to make it harder for the scammer to contact you. - Facebook, Snapchat, Twitter, Instagram, etc.

2. If you are being pressured heavily that the scammer will contact your friends/family with your photos, then YOU SHOULD contact friends/family yourself via email/text or better yet... in person. Inform your immediate family that you are being targeted by an online extortion scam and you've had to shut down your social media accounts (temporarily)
Facebook Deactivation: https://www.facebook.com/help/214376678584711?helpref=faq_content
Instagram Deactivation: https://help.instagram.com/728869160569983

3. Respond to the scammer that you don't care what they do. You aren't paying them any (more) money. Be firm but not vulgar. Then block them. Keep it short and simple. Don't swear or threaten them.

4. Contact your local police and inform them what is happening and ask their advice. Also, report this scam on the IC3.gov website. We know for a fact that the FBI monitors reports to this site so feel free to ask them for help or call your local FBI office.

5. To make it harder for the extortionist to contact you, some men have decided to immediately change their phone numbers and accounts on apps like WhatsApp.

Finally, we've been reporting on the "underage girl (or boy) sext" scam since September, 2016. In November, 2018 fifteen individuals were arrested as the primary perpetrators of this scam and for several weeks victims reporting this scam to us dropped to zero! But in 2019, we began to hear from victims again, though fewer in number. However, by late Spring 2019 the number of victims reaching out to us for help has nearly returned to the same level as before the November arrests. On August 24, an anxious young man contacted us to ask for advice. As he described it... *"I just got a phone call from an angry father saying their daughter is out of hand and wants money to fix damages or they are calling the cops! Does this sound like a scam! I sent a text to the number and said I'm calling the cops! They responded with see you in the courts! Does this sound like a scam to you?"* He then goes on to say that the "girl's" profile on the dating app said she was 18, but "she" later revealed herself to be 16, at which point the man quit communicating with her. As you might foresee, the "father" contacts the victim saying that he has discovered the sexts his daughter sent the man, and sexts sent by the victim to the presumed underage daughter (if any were sent.) But it is all a lie. There is no girl. The dating profile is VERY quickly removed by the scammer so the victim can't even go back and screenshot it to say that "she" pretended to be 18 or older. You can read lots of details and examples of this awful scam in our article "Plenty of Fish Has Plenty of Sharks." (Plenty of Fish is a popular online dating app most often used by criminals to entrap their victims.)

We especially encourage our readers to share this information with the young men (typically age 18 - 28) in their circle of friends and families. These young men are the ones most commonly victimized by this scam. Below are links to our other articles about sextortion scams.

Sextortion by Email
Sextortion Scam via Facebook
Phone Malware Recording You
Sextortion by Bot?
Your Worst Nightmare: Sexting a Minor…. Or so you think.

For Your Safety: Adobe Flash Player Popup
One of our readers told us about his experience while watching an instructional video on a tennis website:

"Recently while watching a tennis instruction video online, the video was interrupted by a notice that I needed to update Adobe Flash Player in order to continue watching. I clicked a few boxes to install the update and suddenly the screen was filled with an advertisement for ***Mac CleanUp Pro****. I had heard this was malware and did not fall for their hype. However, I couldn't get it into the trash. I subsequently noticed that there was another new icon on my dock for Booking Rental Cars. I could not get it into the trash either. I called Apple and they showed me how to turn the apps off and get them into the trash and then empty the trash. So, I guess there was no harm done to my computer but the question I have is, is it common that Adobe Flash Player is used to transport malware into a computer?"*

For Apple computer owners who may not know, **"Mac CleanUp**" is scumware! You do NOT want to install it on your computer, ever! Here are two links describing why this software is unnecessary, deceptive, and how to remove it:

https://malwaretips.com/blogs/remove-mac-cleanup-pro/
https://www.pcrisk.com/removal-guides/13775-mac-cleanup-pro-unwanted-application-mac

Until next week, surf safely!

info@thedailyscam.com

Free Newsletter Every Wednesday