Cyber Attacks for Ransom: Exponentially Growing Problem

Anatomy of a Ransomware Attack

NEW YORK, NY, UNITED STATES, May 11, 2021 /EINPresswire.com/ -- In view of the recent ransomware attack of Colonial Pipeline in the United States, it's useful to get a clearer understanding of how these attacks work and how the stakes have been raised.

Four years ago, when I started to follow the progression of ransomware attacks, two of the prominent examples of that time were the 2016 hack of Uber, which captured 57 million driver and rider accounts in which Uber paid a $100,000. ransom.

Another example was when HBO was hacked and several scripts for “Game of Thrones” was stolen. HBO offered $250,000., according to press reports.

> “Hackers have taken their ransom demands to a whole new level.”
>
> *Ron Alvarez*

Well, hackers have taken their ransom demands to a whole new level. Now, hackers are routinely paid hundreds of thousands of dollars and sometimes millions for companies to regain access to their files.

RECENT EXAMPLES

In June, the University of California paid $1.4 million to unlock files at their medical school;

In July, the U.S. travel management company CWT reportedly paid $4.5 million to get their files back;

And it has been reported that Garmin Ltd. paid as much as $10 million to solve their hacking

episode in July.

For the next few posts, I will discuss various issues related to ransomware attacks.

ANATOMY OF A HACK AND $4.5 MILLION DOLLAR PAYOUT

As I mentioned above, in July of this year, the travel management company, CWT, was reportedly hacked and paid $4.5 million to get back access to their files.

What makes this episode particularly instructive is that the communications between the hackers and CWT were made public.

In a View from the Wing article, written by Gary Leff and published on August 13th, titled, "Travel Management Firm Pays $4.5 Million Data Ransom, The Negotiation is Online For All To Read," we get to witness the sobering and disturbing exchange between CWT and the criminals.

I urge you to read the following partial and disturbing transcript of the EXTORTION (including grammar and spelling errors) between CWT (victim-company) and the hackers:

Sunday, July 26, 2020

CWT – Hello? What do we need to do to get our data deleted from your servers and unlock our files?

Monday, July 27, 2020

HACKERS – You have 30,000 infected and locked devices from different countries. Our price is consists of the services, decryption software and deleting all downloaded data from our servers. If you need both of them you have to pay $10,000,000. in Bitcoins, before the timer on main page will ends. As a bonus we will provide you with the details about how we break your security perimeter and give you recommendations about improving security measures to help your admins avoid such issues in future.

HACKERS – For sure we understand your worries about this deal, that's why we will decrypt two random files for Free, just to prove that our decryptor is working properly!

CWT – So in your message that you left us, you mentioned a "Very SPECIAL PRICE" if we reached out to you within 2 days, which we did. There's no way that $10M is a "very SPECIAL PRICE" right?

HACKERS – This price isn't a Special price, correct! However, it is a standard amount for company of your size and it's probably much cheaper than lawsuits expenses, reputation loss cause by leakage.

Yes we did offered a special price and you are eligible for it, so if you are ready to process the payment promptly, we can make a step forward to your direction and give you a discount

CWT – I appreciate the discount and kind words here, but to be honest, we were hoping for something that we actually have available cash for. I completely understand that this is a business for you, but right now I'm tasked with trying to keep our business afloat. In all honesty, $8M puts us in a spot where we would need to double current revenue to keep our doors open. We were willing to get you $3.7M potentially today if we could have found common ground. I don't mean to belittle you and your team's work here. I'm just trying to help prevent further layoffs on our side.

HACKERS – We appreciate your offer, but understand us too, this is the market and you have been offered an adequate price. unfortunately, the amount you offered is not enough to close our deal with you, we gave you 20% not because we are ready to bargain heavily, but because we see your business spirit and immediately gave you a good discount, we can offer 5% discount more and payment by installments. For example fore $4M you will get the Decryptor and after you will pay the rest amount, we will delete all the private Data.

Reportedly, after the ransom was paid, the hackers provided the security advice. (See the above linked article for details.)

Tuesday, July 28, 2020

CWT – Thank you for all of this in a very timely manner.

HACKERS – You are welcome it's a pleasure to work with professionals. If there be any questions, please feel free to ask.

Please confirm that you wrote down all important information from this Chat, we we could clear it. However we will keep the chat room and will be here for your support if necessary

FINAL THOUGHTS

This transcript shows how efficient and malicious these criminals continue to be.

Ron Alvarez
IP PI Blog
email us here

---

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.