Cyber Security Newsletter

03/2018

HELP THE CU BE A SAFER PLACE FOR OUR MEMBERS

Threat Categories

by Josh Silva

With the advent of information technology and the convenience it brings to us every day we can forget about the dangers of it as well. We hope that this newsletter will serve as an avenue for you to get good information about how to better safeguard yourself and our members from any cyber security dangers.

The Major Categories

There are a growing number of cyber security threats out in the wilds of the internet but we will focus on the following categories:

1. Viruses
2. Phishing
3. Vishing
4. USBs

Viruses

We have all heard of a virus and how dangerous it can be to get infected by one. Viruses give an avenue for hackers to gain control of systems with the end user not knowing what is happening most of the time. Here are some modes of transportation that are used to deliver viruses to unsuspecting end users.

E-mail

Hackers have gotten very good at masking the true nature of emails coming into your inbox. This method of transportation also ties into another category of cyber security threats called phishing, but we will go over that category later in this article.

There are 24 million households that have been infected by viruses via E-mail. That is a huge number of people that have been infected because they opened an email they shouldn't have.

Tips to help

1. Never open emails from people you do not recognize.
2. If you are not expecting an attachment from someone it is always best not to open it.
3. In the event you find an email you are suspicious of please call IT for further assistance.

STATISTICS

-8 million households infected
-Spyware makes up 2.89% of the most common threats in the world

-6.83 million new strains in 2016
-Cyber Crime to his $6 trillion annually in damages by 2021
-Ransomware expected to exceed $5 billion in damages in 2017.

Phishing

Phishing is a very common method for hackers and cyber criminals to try and gain access to information illegally from end users.

The most common method is E-mail. These emails are very well made and look almost exactly like emails you would get from legitimate business or agencies.

For instance, you may receive an email from the “IRS” saying that you owe back taxes and need to pay them immediately. They will use the IRS logo and even try and make the email look like the IRS website as much as possible.

In the email you will be asked to perform a task in order to pay your bill. They will either provide you a link that says “Click here to pay” or “Click here for assistance”. Both of these will lead to a website that will require you to “identify” yourself by entering your personal information. Once you have done this you will then be redirected somewhere else for further instructions or it will lead you nowhere.

At this point you have now given these criminals your personal information such as your name, address, and even SSN. In other cases they will ask you to “login” to the site with your credentials. Now they have your legitimate login information to login to the IRS website to retrieve whatever information they need.

These types of emails have caused havoc for many users across the world.

Tips to help

1. The IRS and other government agencies will never ask your personal information since they already possess it.
2. Always check the URL to make sure you are actually access the REAL agencies or entities website.
3. If you are unsure why you are getting any email from an agency or entity make sure to always call them directly to verify the emails authenticity.
4. Contact your IT department for any suspicious emails you are unsure of and they will assist you.
5. Always error on the side of caution when it comes to emails you are unsure of.

Vishing

Vishing is a newer method that has been on the rise. This method of attack uses text messages or cold calling.

There have been many cases in the US where an end user will receive a call or text from the “IRS”

An “agent” will answer the call and tell the end user that they owe a certain amount of taxes that need to be paid immediately. They will ask for a payment over the phone either by credit card or even instructing the end user to go to a retail store and pay via gift cards. I know this sounds ridiculous but they have caused millions in dollars in damages to unsuspecting people.

In the case of enterprises an end user will receive a call from “IT” telling them their account is locked. The “Help Desk” representative will ask for the end users user name. Upon them “verifying” their identity they will ask them for their password to further assist them.

Upon successfully obtaining this information an attacker now has the means to gain access to the enterprises network and sensitive data.

Tips to help

1. IT will never ask for password information or username information.
2. If you are ever unsure of who you are really talking to on the phone tell the “agent’ on the other end that you will can the main number for further assistance. In most cases they will just hang up.
3. Never give out any personal or payment information on the phone without verifying that the person you are speaking to is actually legitimate.

STATISTICS

-Business lost an average of $43,000 per account
-Individuals have lost an average of $4,200

-48% of people who find a USB plug it in to their PC
-20% of them plug it in within 1 hour of finding it.
-50% of them plug it in within 7 hours of finding it.

-24 million households experience heavy spam.
-16 million households experience a serious virus problem in the past 2 years.
-8 million of households have had spyware in the past 6 months
-1 million households lost money or compromised accounts from misused phishing.
-40% of households are affected by viruses.
-32% of the world’s computers are infected with some type of malware.

USBs

USBs can be our friend and our enemy. We use USBs now for an array of functions. Anywhere from file transport to saving and sharing pictures or files. This handy gadget can also be a wolf in sheep's clothing.

A common tactic used by criminals is called a "USB Drop". They will leave a USB in a common are at a business in plain sight. There have been cases where a USB Drop will be done with a label on it saying "Top Secret" or "Confidential" to entice someone to pick it up.

As is human behavior we tend to be curious and want to know what is hidden on this gem of information we have found in the open.

Unbeknownst to the end user that hidden gem is in fact a virus or information gathering program.

Here is a scary statistic for you: 48% of people who find a USB in a parking lot or common area do plug-in the drive to their work PCs.

So out of 12 out of 25 people will plug it in to a PC. Those odd of infection are very high and have caused criminals to rely on this method with great success.

Out of that 48% it has been found that 20% of those individuals connected their USB within the first hour of pickup and 50% within 7 hours of picking it up.

Tips to Help

1. Never plug in any USBs that you do not know the origin of.
2. Never plug in USBs at the office as it violates policy.
3. If a USB is found please turn it in to IT for examination.

Cyber Security Informational Websites

1. Drebsonsecurity.com
2. Info.wombatsecurity.com/blog
3. Blog.erratasec.com
4. Securityboulevard.com

Cyber Security Newsletter

03-2018