Burrus
Research®

Connected Objects Will Become Your New Problem

Just as we have started to get used to the idea of ourselves always being online, it seems that many of our homes and an increasing number of objects inside them will soon be connected and have the ability to talk to each other. Although there is a growing realization of our responsibilities around our lifestyle choices and the environmental carbon footprint we leave behind, we are only just starting to think about the impact of our digital footprint and how it could affect our future selves.

The threat of terrorist attacks has led to heightened security and it seems that the dirty secrets of both the good and bad guys online could be exposed at any moment. We seldom stop to think about the internet itself and that your phone, laptop, and tablet always connected to your home Wi-Fi actually represents four connected devices when including your router.

This is just one person with a conservative number of connected devices to the internet, but a quick look on your routers settings will quickly reveal just how many devices now connect to your internet family plan, and we just expect it to work. Try to imagine the world's four billion devices for a moment and how many are probably connected to the internet right now and how many are insecure or are broadcasting information publicly.

There is a new threat to our privacy and security that many reading this have never considered which is the rapidly growing list of connected hardware or shiny new gadgets themselves. The big elephant in the room is that many connected devices are no longer created only by software giants, but by companies who do not automatically think about threat modeling or security issues and this could be quite concerning as we embrace the concept of the smart home or even smart city with open arms.

Allow me to introduce you to a Google-powered search engine called "Censys" that was launched in October 2015 by researchers at the University of Michigan, and allows computer scientists to ask questions about the devices and networks that compose the Internet. In a nutshell, it's a search engine for the so-called Internet of Things that could expose vulnerabilities in many devices that we trust implicitly.

Researchers teamed up with Duo Security and learned how Dell laptops were being shipped with a preloaded self-signed root digital certificate that could allow attackers to spy on traffic to any secure website. There are countless other stories including one worrying tale about the discovery of Internet-connected gadgets from over 70 vendors contradicting their own security standards by the method in which they create and store passwords.

Last year, problems with personal data being leaked through our online behavior were highlighted by the Ashely Maddison hack that put many users in the public eye for the wrong reason. This year we are already starting to see the wealth of dirty secrets that have been hiding on devices connected to the Internet.

Malicious hackers are always searching for vulnerabilities that can be exploited and these latest tools that are being used for the greater good could also be used to expose companies that have previously been negligent or naive at best with their responsibilities. This kind of unwelcome attention could leave them in a very damaging situation.

Our Kickstarter economy now allows anyone with an idea to bring it to the mass audience regardless of any technical expertise. Both corporate and personal security is increasingly becoming paramount online and despite investing considerable time and money on securing software, it seems that many have been blindsided by the hardware itself.

The harsh reality is websites, software, hardware or anything that is connected to the internet could unleash a pandoras box of secrets at any moment. Thankfully this digital wake-up call has ensured that scanning the entire internet for weak spots is being recognized as being vital to our online safety and seen as an important step forward in shutting down criminal behavior online.

Now that nearly every aspect of our lives is available online along with a growing number of home appliances such as Televisions, refrigerators, thermostats and even toasters, maybe its time that we all began to take a holistic view of security rather than just assuming everything will be ok.

Expect the boring and safe IT guys that famously said no to many of the modern requests to say I told you so in the very near future. Traditionally IT has taken their thankless roles as custodians or guardians of networks incredibly seriously, and there is an argument that it’s only since we started lowering our guard and going our own way that we are starting to realize the error of our ways.

Is the threat of malware or online security starting to make you a little more cautious about the amount of security built into the many devices you hook up to the internet?

Please share your thoughts and experiences by commenting below.

About the Author:

DANIEL BURRUS is considered one of the world's leading technology forecasters and innovation experts, and is the founder and CEO of Burrus Research, a research and consulting firm that monitors global advancements in technology driven trends to help clients understand how technological, social and business forces are converging to create enormous untapped opportunities. He is the author of six books including The New York Times best seller Flash Foresight. This article is reprinted with permission. Reproduction without permission is strictly prohibited. For reprint permission, contact Burrus Research, Inc. at office@burrus.com.

INOVA BUSINESS SCHOOL

INOVA CONSULTING