The Security Section
Society of American
Archivists

Protect to Preserve

January 2021
Second Encounter

Information, Observations, and Things to Ponder

Secure Your Stuff

- By Jeff Lundgren

Didn't do your New Years' systems review?

I shouldn't admit this, but perhaps like you I'm cyber vulnerable. When my employer went to a work-from-home platform last spring, some of us brought our computers home; I didn't ('cause I knew I would drop it on the way to my car) and have been doing work and school and volunteer assignments for the Security Section on the same device.

That means that if one of the eighty-one people I work with opens the wrong email, I could be in a bad place. Theoretically. You see, we were hacked in 2019 and I assume we're stronger and better prepared now. But we are, like your employer perhaps, a non-profit so how much post disaster defense spending vis-à-vis cybersecurity was there?

In part one of his article on "cyber distancing", Tim Bandos keeps it simple and clear what we all should have done months ago, but indicates it is not too late to protect yourself.

I thought his article, linked below, would be a good selection for multiple reasons, both as a reminder (I can be a nag) and if you are reading my stuff, I automatically like you and here's my kindness in written form. By the way, if you read the article and don't know what *IoT* refers to, check my security term for the week.

Enjoy and upgrade!

https://www.securityweek.com/covid-19-requiring-us-implement-cyber-distancing

Some tips for further focus on protecting your stuff

Protect your device

- **Set PINs and change passwords frequently**
- **Backup and secure your data. Do this yourself or find a product to do it for you (https://www.nytimes.com/wirecutter/reviews/how-to-back-up-your-computer/).**
- **Wipe data from your old phone before you dispose of it. With so many new versions of phones constantly entering the market, you may forget that your old phone is going somewhere after you get rid of it. Let it go, but leave nothing behind**

Protect your data

- **Discuss with your employer the classification level for the type of data you handle and what type and extent of security precautions are required**

Quote for this Day

"The good we secure for ourselves is precarious and uncertain until it is secured for all of us and incorporated into our common life."

Jane Addams

(https://tinyurl.com/y6fas4lg)

Archival Term for this Week

Certificate authority

A trusted third party that supports authentication infrastructures by registering individuals and organizations, and then issuing them an X.509 digital certificate attesting to their identity.

Explanation/notes: A certificate authority issues public and private keys in the form of digital certificates for message encryption and decryption. By issuing, managing, and validating these certificates, a certificate authority guarantees the authenticity of the user.

https://dictionary.archivists.org/entry/certificate-authority.html

Addendum:
Digital certificates must meet strict standards. They not only are used for encryption, and providing verification of identity, but they record session and data information, such as time, that assure a message has come directly from the sender to the recipient without having been diverted to unauthorized entities that could copy or alter communication. They make possible a secure (as much as can be) connection between parties, designated by the https:// in the URL on a browser, and usually symbolized by a "lock" at the beginning of the address.

Certificate authorities (CA), (not to be confused with Certified Archivist) hold the trust of the technical community involved in such things, and that trust is what gives them their authority. If the trust varies from CA to CA, the value of the certificates may also vary in the view of parties involved in communication. Some CAs are not accepted by everyone.

-Addendum by James Havron, CA, Security+, CEH [Certified Ethical Hacker]

Quiz

- By Jeff Lundgren
  (with Jim Havron)

True or false. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, quality of service, up-times and reduce costs of operation in all infrastructure related areas.

The Criminal Hacker: Tools of the Trade

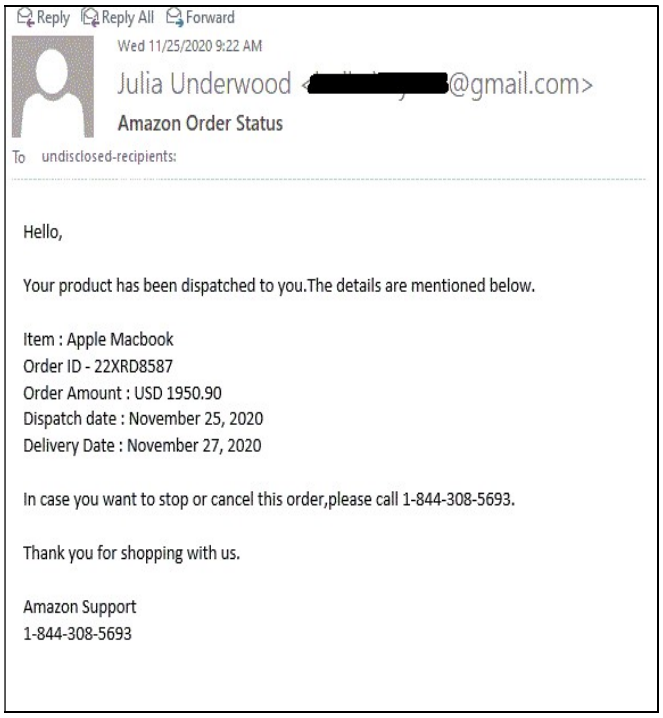
Many people do not understand the cybercriminal's area of expertise. They envision the kid in the basement breaking codes and stealing credit card numbers. Well, the basement may or may not be present, and while the credit card numbers may be an object of theft, theft itself is just one of the objects of a criminal hacker.

One of my personal areas of expertise, part of what landed me on my first few security audit teams (i.e., professionals of various specialties with one in common, hacking skills, testing the security of an organization or system by overcoming the defenses wherever possible; then issuing a report with analysis and recommendations) was the little kit in the image above. Not the see-through practice/teaching lock, but the package of little tools. While they are more varied in name and use than this implies, most would call them lock picks.

Let's Go Phishing!

Did you figure out the phishing email from the November bulletin? Giveaways that it was a phish? Things that might have made it effective?

This message is actually extremely effective. Can you guess why? Can you spot reasons to suspect it is fake?



Reply Reply All Forward

Wed 11/25/2020 9:22 AM

Julia Underwood <[redacted]@gmail.com>

Amazon Order Status

To undisclosed-recipients:

Hello,

Your product has been dispatched to you.The details are mentioned below.

Item : Apple Macbook
Order ID - 22XRD8587
Order Amount : USD 1950.90
Dispatch date : November 25, 2020
Delivery Date : November 27, 2020

In case you want to stop or cancel this order,please call 1-844-308-5693.

Thank you for shopping with us.

Amazon Support
1-844-308-5693

Phish! ⌂

The image above is a cropped copy of a real message sent to an individual. The email of the "sender" has been redacted. The "UPDATE HERE" text did hold a link, but it has been rendered inactive by the transfer to a still photographic image.
How many clues can you find that this is not a legitimate message? Can you identify the techniques used to try to persuade the receiver to act as the sender would wish? You may include some assumptions, such as "If the were not received on Tuesday as is shown, it is likely bogus". [Hint: That is NOT a correct assumption, just an example of how one might point to a suspect piece of information as a clue].

This message has some obvious items if one is used to looking for such things, but everyone is not. Please post your ideas on the discussion page for the SAA Security Section, or email them to jimhavron@comcast.net.

If I am good at opening doors, cases, what-have-you, I am useful for accessing the server room and network closet for the entire building.
Individual offices? Usually not a problem. Storage lockers and cabinets, file drawers, hey cabinets, and display cases are particularly easy. Combination locks tend to be of similar difficulty.

That's okay. We just leave our business cards and lock them up again. The management and staff can see that we were in position to physically access their entire communication and environmental control system (the fact that this last was connected to the alarm system and we were there in the first place actually demonstrated some of that), offices, storage and displays (anything of interest in such places when found in a library, archives, or museum?). They were not as secure as they thought. And bad guys don't always come across the Internet.

Cybercrime, criminal hacking if you wish, is about gaining control, regardless of how. After that, it can be about corrupting data and hiding the evidence, hiding different security faults to programs that then might go undetected, denying access to the data to the owner, releasing the data, but hiding things in it so more damage can be done later, stealing copies of the data and threatening to release it if not paid to stop, releasing it anyway, using pieces of information acquired to help exploit individuals, particularly children and hospitals, vulnerable targets that can be very profitable, and on, and on, and on. And targets like that can be anyone, anywhere. The best are the ones that think themselves safe or able to deal with it all.

Ask your IT department how they evaluate locks to be sure they are secure. My guess is that is not their job. Security specialists do it and security auditors, in the form of hackers, test it all. (But only with contractual permission.)

I have other areas of expertise that are more valuable to audit teams than compromising locks. And that is not where my truest strengths lie. But do think about locks, and surveillance cameras that are part of IoT and can easily be taken down. Ask if there is anything YOU can do to make it safe.

Answer to Quiz:
True. See also footnote #66 in attached link to Wikipedia.
https://en.wikipedia.org/wiki/Internet_of_things

Addendum by James Havron, CA, Security+, CEH [Certified Ethical Hacker]

This statement is true.
It should be noted, however, that in almost all, if not all, situations in Information Systems, advantages, breakthroughs, and exciting new conveniences introduce new vulnerabilities, undefined surfaces for defense, and opportunities for cybercriminals. IoT provides all manner of data that feeds Automated or Artificial Intelligence (AI)/Machine Learning, making communication of needed data far more efficient in an emergency. AI can frequently respond in record-setting times, increasing the mitigation of and recover from emergency situations.

The other side of this is that a vast number of IoT sensors and other devices were deployed with no though whatsoever to securing them and the data they provide. Billions of devices are out in the world, connected to networks and the Internet, without being monitored by security systems. They create vulnerabilities, access points through devices few would think to guard. Many devices collect data, but do not appear to communicate it, even while they are exploited by cyber criminals. Baby monitors, surveillance cameras, and refrigerators were part of the exploits that took control of one of the largest stockpiles of personal credit data in the nation a few years ago. A spokesperson for the Executive Branch of the government was ridiculed as ignorant by opponents when she noted that microwaves were potential threats. The reality is she had been properly briefed on the fact that microwave ovens have been collecting and relaying data for over a decade, well before they included “smart” features to allow remote control. Publicized features that allow users to access and control devices, so-called “smart tech”, are not the only way devices can be gathering information.

So along with this great opportunity to gather and act upon data, protecting and responding to threats and emergencies, comes entire new ways that cybercriminals can attack and take control of these very systems. The new opportunities have created new challenges in cybersecurity.