Personal Digital Security and Privacy (2018)

December, 2018

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Robert Hurlbut

Threat Modeling Architect, Trainer

Microsoft MVP – Developer Security 2005-2009, 2015-2019

(ISC)2 CSSLP 2014-2020

Co-host with Chris Romeo – Application Security Podcast

MeetUp Leader: Boston .NET Architecture Group, Amherst Security Group

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

Introduction to Personal Digital Security and Privacy (2017)

See original slides here:

https://www.slideshare.net/RobertHurlbut/introduction-to-personal-privacy-and-security-80739776

What's new in 2018?

- Lessons from Marriott Breach
- Email scams
- Your Apps are tracking you
- Other / Discussion

Lessons from Marriott Breach

Brian Krebs wrote article on December 1, 2018: "What the Marriott Breach Says About Security"
https://krebsonsecurity.com/2018/12/what-the-marriott-breach-says-about-security/

- Data breach discovered in September, 2018 – 500 million guests of Starwood hotel properties – breach lasted *four* years! (Likely Chinese hackers per info on 12/12/2018)
- Article covers recommendations to Companies and Individuals

Lessons from Marriott Breach, continued

For individuals – two things to realize:

- **Reality #1:** Bad guys already have access to personal data points that you may believe should be secret but which nevertheless aren't, including your credit card information, Social Security number, mother's maiden name, date of birth, address, previous addresses, phone number, and yes — even your credit file.

- **Reality #2:** Any data point you share with a company will in all likelihood eventually be hacked, lost, leaked, stolen or sold — usually through no fault of your own. And if you're an American, it means (at least for the time being) your recourse to do anything about that when it does happen is limited or nil.

Lessons from Marriott Breach, continued

For individuals – good reminders / recommendations:

- Use a password manager
  - Your passwords exposed in data breaches are being used for credential stuffing attacks – make sure you are not using the same password everywhere
- Freeze credit files with all major credit bureaus
  - Get free copies regularly from annualcreditreport.com
  - See more here: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Lessons from Marriott Breach, continued

For individuals – good reminders / recommendations:

- Plant your flag – establish online identity
  - Bank accounts
  - Social Security - https://www.ssa.gov/myaccount/
  - US Postal Service - https://reg.usps.com/entreg/RegistrationPortalAction_input
  - IRS – https://www.irs.gov
  - Mobile provider and Internet Service Provider (ISP)
- Place very little trust in anything in email: links, etc.
- Multi-factor authentication with every service you use that offers it (Amazon, Microsoft, etc.)
  - Transition from SMS, use more secure app- or key-based options

Lessons from Marriott Breach, continued

For individuals – good reminders / recommendations:

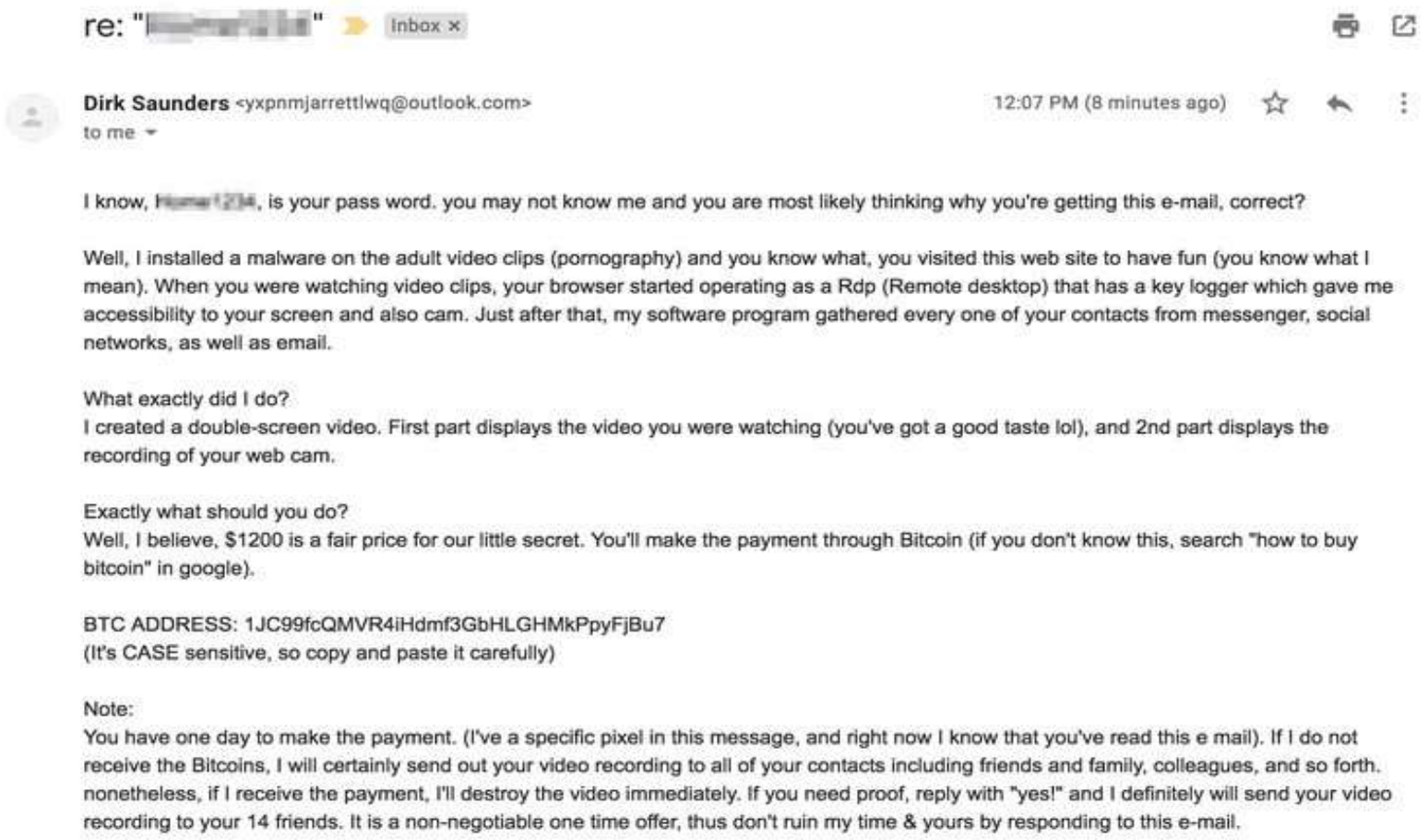
- Accept the inconvenient, unfair, and expensive life in living with Realities #1 and #2
- Difficult trade-offs of security, privacy, and convenience - you get to pick two out of the three.

Email scams

- No longer fake emails from Nigeria with bad grammar and spelling
- More sophisticated emails, including good grammar and spelling, are targeted toward knowledge of you and/or who/what you know (various kinds of phishing attacks)

Email scams, continued

"They" are watching you (and supposedly what you watch …)



re: "[redacted]" Inbox ×

Dirk Saunders <yxpnmjarrettlwq@outlook.com> 12:07 PM (8 minutes ago)
to me

I know, [redacted], is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?
I created a double-screen video. First part displays the video you were watching (you've got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?
Well, I believe, $1200 is a fair price for our little secret. You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in google).

BTC ADDRESS: 1JC99fcQMVR4iHdmf3GbHLGHMkPpyFjBu7
(It's CASE sensitive, so copy and paste it carefully)

Note:
You have one day to make the payment. (I've a specific pixel in this message, and right now I know that you've read this e mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I'll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don't ruin my time & yours by responding to this e-mail.

Email scams, continued

What to do:

- Don’t send bitcoin to scammers
- Again, password managers and multi-factor authentication
- Turn off or cover any web cameras

Your Apps are tracking you

"Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret" (Jennifer Valentino-DeVries, New York Times, December 10, 2018)

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

- At least 75 companies receive anonymous, precise location data from apps
- 200 million mobile devices tracked in the United States
- Data reveals people's travels in detail – accurate within a few yards and in some cases updated 14,000 times a day

Your Apps are tracking you, continued

Who collects the data (and why)?

- Advertisers
- Retail outlets
- Investment / hedge fund companies
  - See https://www.fnlondon.com/articles/regulators-campaigners-sound-alarm-over-hedge-funds-data-use-20170904

All trying to understand consumer behavior.

Your Apps are tracking you, continued

What can you do?

- In Settings / Privacy / Location Services on your mobile device, check the app is using “While Using the App” (iOS)
- In Google Settings / Security & Location / Location / App-level permissions – determine which apps you want to track your location (Android) (see https://support.google.com/android/answer/6179507)
- In general – remove apps no longer in use

Other / Discussion

Facebook / LinkedIn / etc. data download

Mobile apps getting your contact list

IoT (The “S” is for Security) – be careful how you integrate it into your network, what it may be tracking

Resources - Books

Personal Digital Security: Protecting Yourself from Online Crime

Michael Bazzell

Hiding from the Internet: Eliminating Personal Online Information

Michael Bazzell

The Complete Privacy and Security Desk Reference: Volume 1: Digital

Michael Bazzell and Justin Carroll

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

Kevin Mitnick

Questions?

Contacts

Web Site:
https://roberthurlbut.com

Twitter: @RobertHurlbut