Securing Your Shack Computer

By

B.A. Lynch
KB3YFS

Disclaimers

- I am not here representing my employers.
- I do not speak for any past or present employers.
- I am receiving no remuneration.
- Specific product recommendations are because I use them myself. I'm not getting anything for those recommendations.

(There, Legal – this good? Good.)

Who am I?

- Name: Bryce A. Lynch (KB3YFS)
- Ham radio operator seven years
  - APRS
  - High altitude ballooning
  - SDR (Software Defined Radio)
- Security practitioner: 24 years
  - System administration and architecture
  - Penetration testing
  - C&A, IV&V
- Human rights work
  - Training of journalists and activists in hostile regions
- Open source community: 1995
  - Slackware Linux v3.0

Overview

- Basic Internet security and safety
- Windows 7 and 10
- Specific security procedures and recommendations
- Software I use and why
- Links to helpful resources

Why my computer?

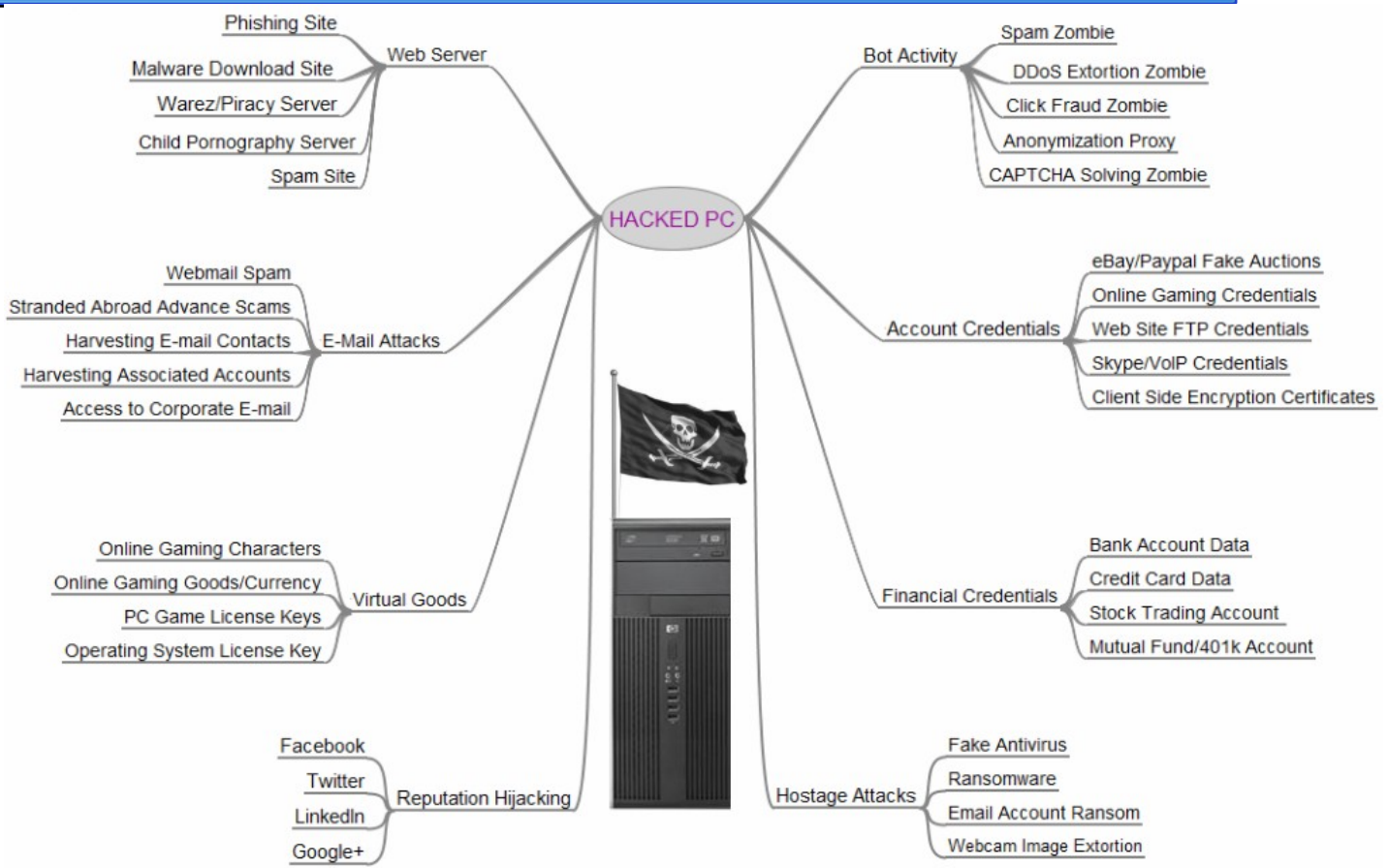


Image source: Brian Krebs https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Why my computer?

- It doesn't matter that it's your machine.
- What matters is that it's *a* machine, one of thousands on the Net.
- Even half a percent of all the computers out there is still a sizeable number of machines that can be abused.
- Cast a big enough net, catch an expensive fish.

What to do?

- Exercise a little caution
- Due diligence
- Best practices
- Helpful tools

Windows Update

- https://support.microsoft.com/en-us/help/12373/windows-update-faq
- Windows 7
  - Start -> Search box: Update -> Windows Update
  - Change settings -> Important Updates -> Install updates automatically
  - Recommended Updates -> Give me recommended updates the same way I receive important updates -> Ok
  - Click to checkmark every update in the window.
  - Click OK
  - Click Install Updates

Windows Update, cont'd.

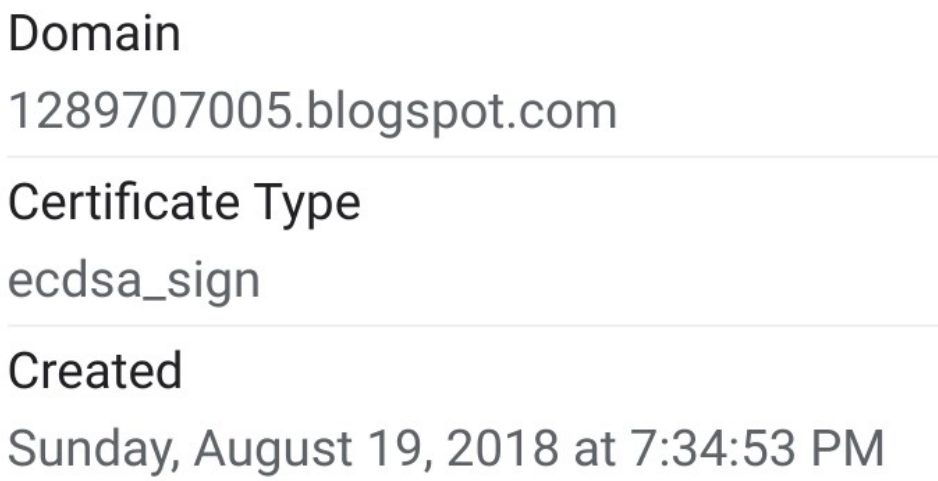
- Windows 10
  - Updates are supposed to be installed automatically.
  - Start Menu -> Settings -> Update & Security -> Windows Update -> Check for updates
- Both versions
  - Let Windows Update run until it asks you to reboot. Let it reboot your machine.
  - Go back into Windows Update and repeat until there are no updates left.

Web Browser

- Probably *the* software that all of us use all the time.
- Chromium - https://www.chromium.org/
- Google Chrome - https://www.google.com/chrome/
- Google Chrome is built on top of Chromium.
  - Microsoft Edge will be soon.
- Probably the most secure browsers out there today.
- Regularly downloads curated blacklists of known compromised and dangerous websites.
- Tabs are sandboxed so they can't access each other.

Cookies

- Small text files set by a website that your browser holds onto.
- If you log into a website it manages your session so you stay logged in.
  - ID pass
- As common as it gets.



Tracking cookies

- Cookies set by third parties on websites for the purpose of user tracking.
  - User tracking data is part of advertising revenue.
- Tracking cookie set on site A, requested on site B.
- If it is retrieved successfully it means the same user on the same browser looked at both sites.
- The reason why certain types of advertisements follow you across the web.
- Security software likes to play up the threat, just a minor privacy nuisance.

Privacy and cookie warnings

- Basically means "legal told us we have to warn you about cookies because of GDPR." Even if that site doesn't set any cookies.
  - Ignore the "close and accept" button.
  - Click it anyway. Adblocker will probably stop it.

Adblockers

- Software that plugs into your web browser to block advertising and tracking cookies.
- Available for just about every browser on every platform.
- No ads means pages load faster.
- Minimizes possibility of browser compromise.
- Ghostery - https://www.ghostery.com/
- uBlock Origin - https://github.com/gorhill/uBlock
- Search in the addon collection for your browser, install.

Malware

- Software that tries to make your computer do something you don’t want it to.
  - Join a botnet
  - Harvest credentials
  - Ransom your files back to you (cryptolockers)
- Most of the time they try to catch you in a moment of inattention.
  - Link sent in a spoofed e-mail or instant message.
  - Pop-up windows that mimic antivirus warnings and ask you to download "updates" that are actually malware.

Malware, cont'd.

- Email with attachments that pretend to be from tax preparers, lawyers…
  - something.docx.exe
  - But Windows shows you something.docx
- Double-click to open, but Windows executes it.
- Windows can be configured to show you the entire filename. If it looks like it has more than one file extension, don't open it.
  - https://www.howtohaven.com/system/show-file-extensions-in-windows-explorer.shtml
- Don't open documents unless you're sure of what they are and where they came from.
  - If you have to call someone and ask if they sent you a document, do so.

Yet more malware

- Can take the form of software that pretends to be something else, or gets bundled with an installer.
  - Adware bundled with installers
    - If you look carefully, there might be a checkbox to opt out.
  - Download sites that look legit but are copies of the real thing.
- Usually installs browser extensions you don’t want or adware.
- Most of the time pretty annoying, but there are exceptions.
- Detected and removed by most anti-malware and anti-spyware utilities.

Antivirus software

- Constant defense against viruses, worms, and malware.
- Windows Defender / Windows Defender Antivirus (Win10)
  - https://www.microsoft.com/en-us/windows/windows-defender/
- Install it.
- Turn it on.
- Let it run.

Accounts and credentials

- Obvious examples like bank accounts aside.
- Email addresses are useful for
  - Scamming people the real owner corresponds with.
  - Resetting passwords on other services to gain access.
  - Mischief like cancelling utility services.
  - Gaining access to bank accounts.
  - Gaining access to services that might have saved payment information, e.g., Amazon.
    - Shopping spree, anyone?
  - Sending spam.

Passwords

- The secret you need to log into an account.
- Used to be fairly simple - single words.
  - Attackers started using dictionaries to try to log in.
- Password complexity requirements
  - Capital and lowercase letters, numbers, and punctuation marks.
  - Attackers started trying the same variations on dictionary attacks.
  - Attackers started keeping lists of passwords they knew worked.
    - People like to re-use their passwords, after all.

Data breach abuse

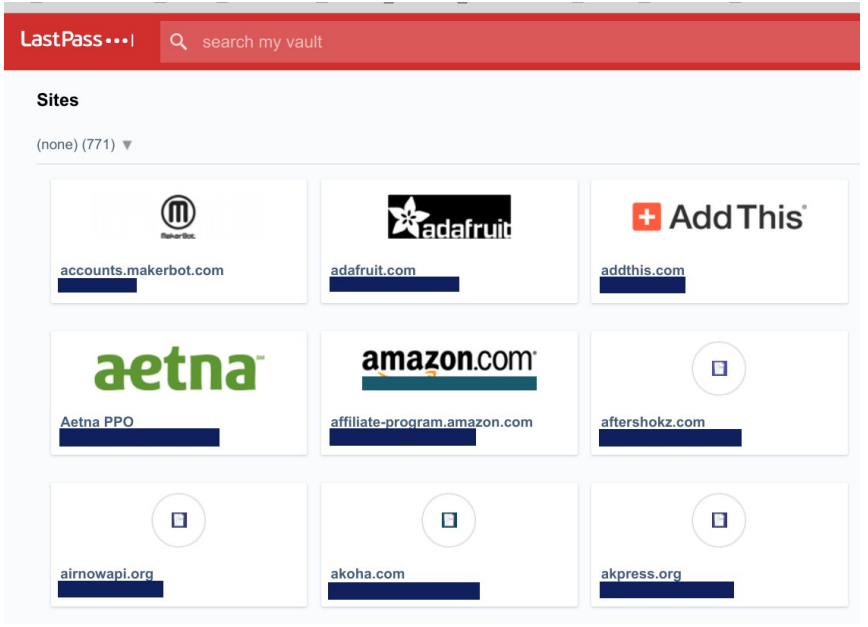
- Attacker collects a bunch of dumps from data breaches.
- Search for email addresses that appear in every database, pick out passwords.
- Try that address and every password for it at every service they can think of to see which ones work.
  - Relatively simple piece of software.
  - More sophisticated attackers do this when going after corporate networks, because people re-use passwords.
- This is why you should never, ever re-use passwords.

Password organizers

- Keep track of your passwords for you, so you don't have to memorize them.
- Strong passwords are hard to guess so they're also hard to remember.
- Some can enter them for you automatically.
- Can also generate passwords for you.

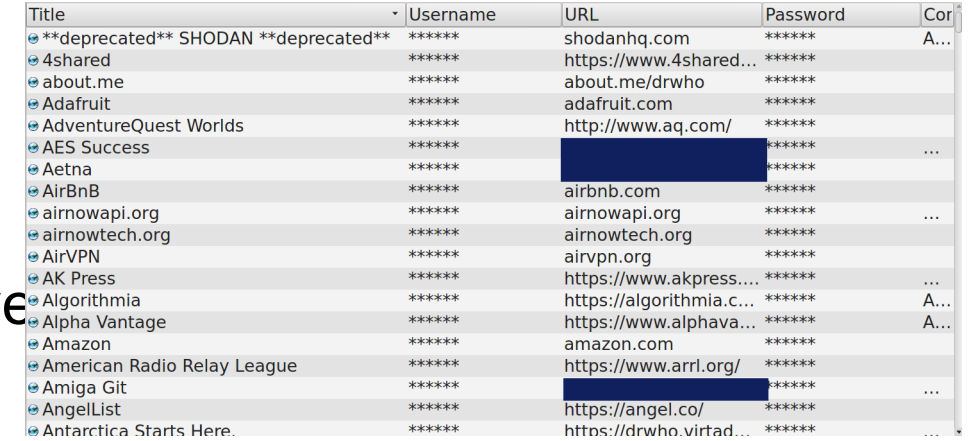
Lastpass

- https://www.lastpass.com/
- Web browser plugin, mobile app.
  - Available for just about everything.
- Lastpass-the-company has no idea what your passwords are, they're encrypted before being uploaded.
- Create an account, log in from every device, sync your passwords to each.
- Can export and back up your passwords.
- Can also store and securely share notes and other kinds of credentials.



KeepassX

- https://keepass.info/
- Application available for every platform and mobile devices.
- Passwords and notes are encrypted before they hit storage.
- Does not sync across devices, you have to do that yourself.
  - Google Drive
- Can copy and paste credentials with mouse (right-click) or keyboard (^B for username, ^C for password, ^v to paste)



Title	Username	URL	Password	Cor
deprecated SHODAN **deprecated**	******	shodanhq.com	******	A...
4shared	******	https://www.4shared...	******	
about.me	******	about.me/drwho	******	
Adafruit	******	adafruit.com	******	
AdventureQuest Worlds	******	http://www.aq.com/	******	
AES Success	******	[redacted]	******	...
Aetna	******		******	
AirBnB	******	airbnb.com	******	
airnowapi.org	******	airnowapi.org	******	...
airnowtech.org	******	airnowtech.org	******	
AirVPN	******	airvpn.org	******	
AK Press	******	https://www.akpress....	******	...
Algorithmia	******	https://algorithmia.c...	******	A...
Alpha Vantage	******	https://www.alphava...	******	A...
Amazon	******	amazon.com	******	
American Radio Relay League	******	https://www.arrl.org/	******	
Amiga Git	******	[redacted]	******	...
AngelList	******	https://angel.co/	******	
Antarctica Starts Here	******	https://drwho.virtad...	******	...

Multi-factor authentication

- Some thing you have that is used as a secondary credential.
  - Something you have, something you know, something you are.
- New passcodes are generated every sixty seconds.
- Between six (average) and eight digits in length.
- Your username and password for a site can be compromised, but without the secondary code the attacker can't log in.
- At the very least, buys you some time to change your password.
- Sometimes a hardware token, more commonly a smartphone app these days.
- Multiple implementations that all do the same thing.
  - Google Authenticator - https://www.google.com/landing/2step/
  - Lastpass Auth - https://lastpass.com/auth/
  - Authy - https://authy.com/

MFA setup

- An account setting on the service.
- Google "<name of service> mfa"
  - Gmail
  - Facebook
- It'll show you a barcode or a string of letters and numbers.
- Photograph the barcode or type in the string.
  - Note: The barcode also requires a barcode reader app, available in the appstore.
- Synchronizes the app on your phone to the service.
- For every account, it will generate a new code every sixty seconds.
- To log in, enter your username, password, and the current code.

SMS as MFA?

- Some services will insist on texting you that MFA code.
  - (Too many) banks
  - Twitter
  - LinkedIn
- If possible, don’t use this feature. Use an actual MFA app.
- This isn’t really secure.
- SIM swapping attacks used to redirect those text messages.
  - Multi-million dollar a year scam.
  - https://krebsonsecurity.com/tag/sim-swapping/

How to contact me

- Email: drwho at virtadpt dot net
  - PGP: 4d7d5c94 fa44a235
- WWW: https://drwho.virtadpt.net/
- Fediverse: https://hackers.town/@drwho
- Github: https://github.com/virtadpt
- Profile: https://about.me/drwho