Cybersecurity: Week 1
Introduction

Blake Carver
Senior Systems Administrator, LYRASIS
April 2021
Cybersecurity Training for Libraries
Week #1

This project was supported in whole or in part by the U.S. Institute of Museum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. The opinions expressed herein do not necessarily reflect the position or policy of the U.S. Institute of Museum and Library Services or the California State Library, and no official endorsement by the U.S. Institute of Museum and Library Services or the California State Library should be inferred.

Today’s Schedule

10:00 – 10:20 Welcome & course housekeeping
10:20 – 10:45 Training
10:45 – 10:50 Break
10:50 – 11:25 Training
11:25 – 11:30 Wrap up
Series Housekeeping - Outline

- Week One – Welcome – Explanations of why and what’s wrong
  - Week Three – Making Your Library Defensible & Resilient
    - What and why of things around the library
    - Hardware, networks, ransomware
- Touch on some privacy issues.
- Why are libraries, and all of us, targets?
- Why is security important?
- Professionals and Incentives, big money.
- What are they after and where are they working?
- Passwords
- Week Two – Securing our things
  - What things do we have to secure?
  - Hardware, software, etc.
  - How do things actually get infected? How can we spot it?
  - Email, phishing, browsers, VPNs, Tor, desktop, mobile, everything else.
- Week Four – Wrapping It All Up
  - Training, planning, vendors
  - Websites
  - Checklists and specific steps to take next.

Series Housekeeping – Expectations

**Online Sessions**
- 90 minutes/week for 4 weeks
- Lecture
- Small and large group discussions
- Exercises

**Optional Basecamp Work**
- 30 to 60 minutes/week
- Readings
- Discussions
- Exercises

Series Housekeeping – Guidelines

- When you disagree, challenge or criticize the idea, not the person.
- Speak from your own perspective.
- Be mindful of the time.
- One speaker at a time.
- What is said in this space, stays in this space unless you have permission.
The 1981 book *School, Work and Play World of Tomorrow*

- All about me, myself and LYRASIS
  - How did I get here?
  - How did any of us get here?
  - Why are we here?
- Privacy
  - The Fundamentals
  - Incentives & Players
  - The industry & how trackers work
  - What can we do?
- Security
  - Who is after us & who do we worry about?
  - Why does this matter?
  - What are the incentives?
- Passwords?

Today
I'm Blake! I'm a “librarian” - I have an MLS!

I’m an LJ Mover & Shaker (2001)
Library Director
Teacher
Programmer at a .com startup
Web Librarian
Records Manager
Business Owner / Sysadmin / Support
LISNews, LISHost & LISWire
Senior Systems Administrator

In the past decade I’ve done this ~40 times.

@blakesterz & @lisnews

blake.carver@lyrasis.org

About LYRASIS
• 80 years of deep history with information professionals
• Non-profit
• Community focused
• Devoted to serving members
• 1000+ members strong
• 80+ vendor partners

Digital Technology Services: Hosting Services

LYRASIS ArchivesSpace Hosting Services
LYRASIS Islandora Hosting Services
Simply VIVO
LYRASIS CollectionSpace Hosting Services
 Lone Arranger
DSpaceDirect
Fedora

1000+ Members
$500m Services Provided
Millions of Dollars Saved

11

12
Before We Start - My Assumptions

You're interested in or working in IT
You're willing to invest time (and money?)
You're working in a library
You have little to no experience with itsec
You have little to no security in place now
You're going to be doing some training
  Your staff/coworkers
  Your friends/family
  Your patrons/users/customers
  Your boss
  Your board
  Your self
Everything you need to know

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passwords:</strong></td>
<td>LENGTH &amp; Unique</td>
</tr>
<tr>
<td><strong>Paranoia:</strong></td>
<td>Think Before You Click</td>
</tr>
<tr>
<td><strong>Backups:</strong></td>
<td>Frequent and Automatic</td>
</tr>
<tr>
<td><strong>Patches:</strong></td>
<td>Set to Auto</td>
</tr>
<tr>
<td><strong>Upskill:</strong></td>
<td>Regular training</td>
</tr>
<tr>
<td><strong>Protect:</strong></td>
<td>Review all settings</td>
</tr>
</tbody>
</table>

We are all targets

We all have something of value

List O' Libraries In The News

- The Kokomo-Howard Public Library
- Northampton Area Public Library
- Wilmer, Texas
- The Bartlett Public Library District
- Contra Costa library system
- Volusia library
- Pittsburg Unified School District
- Denver Public
- Onondaga County library
- Spartanburg County
- Brownsburg Public Library
- Hardin County Schools
- Daviess County Public Library
- Bartlett Public Library
- St. Louis Public Library
- Butler County
- Baltimore County Public Schools
- Tillamook County
"Security & Privacy can be two different things: They can be both a feeling & a reality."

Bruce Schneier – TedxPSU

Understanding...
Information / IT / Data
Privacy

When it comes to Privacy...
Librarians are different.
Privacy Vs. Data Privacy

The rules of privacy are being defined and redefined today.

So much of what we do is for sale now.

Things that used to be ephemeral are now permanent(ish).

Spectrum of Privacy –v2

Threats To Privacy?

1. The government threat
2. The criminal threat
3. The corporate threat
Privacy is about control...your loss of control over that information is the issue. We may not mind sharing our personal lives and thoughts, but we want to control how, where and with whom. A privacy failure is a control failure.

https://www.schneier.com/blog/archives/2010/04/privacy_and_con.html

Privacy is Getting Better!

But it’s Getting Worse Faster

...savvier users are ... becoming aware about how algorithms affect their lives. Meanwhile, consumers who have less information are relying even more on algorithms to guide their decisions.

Why?

Devices: There's an exponential proliferation of devices.

Data: With all those devices, comes an avalanche of data.

People: There just aren't enough focused on privacy.

Surveillance is the business of the Internet

Privacy Policies

1) They can be changed whenever the company pleases.
2) They are not an agreement between you and the company.
3) They are theirs, not yours.
We don’t know how our information is used, stored or shared and for how long.

We don’t know who has access

We don’t know if it’s safe

Personal information is the currency of the entire Internet economy

**Angry Birds and the end of privacy**

Seemingly simple mobile games made us all way too comfortable with giving away our personal information.

By Katie Whitney | Updated: May 4, 2016, 6:44 PM EDT

The business model that holds up the mobile gaming industry, digital advertising, and most major social media platforms is persistent and ravenous, very good at holding on to the information you’ve given it and even better at finding ways to enrich that information and keep it fresh, even after you’ve moved on to a different app. In other words, you may be over the phase of your life that involved Angry Birds, but Angry Birds isn’t over you.
...your data is collected in ways you cannot reasonably prevent, no matter how carefully you or anyone you know behaves.


"We see Apple’s announcements, consumers getting more conscious of privacy, and the death of the cookie," says Abhishek Sen, cofounder of NumberEight, a "contextual intelligence" startup in the UK that infers user behavior from sensors in their smartphone.

Sen describes NumberEight’s chief product as “context prediction software.” The tool helps apps infer user activity based on data from a smartphone’s sensors: whether they’re running or seated, near a park or museum, driving or riding a train.

Equifax stole your data, China just copied it without paying them.
How Does This Work?

Browsing history, app usage, purchases, and geolocation data, data about our clicks, impressions, taps, and movement goes into sprawling behavioral profiles, which can reveal political affiliation, religious belief, sexual identity and activity, race and ethnicity, education level, income bracket, purchasing habits, and physical and mental health.

<table>
<thead>
<tr>
<th>Web Identifiers</th>
<th>Unique</th>
<th>Persistent</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies</td>
<td>Yes</td>
<td>Until user deletes</td>
<td>In some browsers without tracking protection</td>
</tr>
<tr>
<td>IP address</td>
<td>Yes</td>
<td>On the same network, may persist for weeks or months</td>
<td>Always</td>
</tr>
<tr>
<td>TLS state</td>
<td>Yes</td>
<td>For up to one week</td>
<td>In most browsers</td>
</tr>
<tr>
<td>Local storage</td>
<td>Yes</td>
<td>Until user deletes</td>
<td>Only in third-party iFrames, can be blocked by tracker blockers</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Only on certain browsers</td>
<td>Yes</td>
<td>Almost always, usually requires JavaScript access, sometimes blocked by tracker blockers</td>
</tr>
</tbody>
</table>

How Does This Work?

<table>
<thead>
<tr>
<th>Other Identifiers</th>
<th>Unique</th>
<th>Persistent</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number</td>
<td>Yes</td>
<td>Until user changes</td>
<td>Ready available from data warehouses, only mobile to apps with special permissions</td>
</tr>
<tr>
<td>Advertising ID</td>
<td>Yes</td>
<td>Until user changes</td>
<td>Yes, for all apps</td>
</tr>
<tr>
<td>Email address</td>
<td>Yes</td>
<td>Yes</td>
<td>To apps only with special permissions</td>
</tr>
<tr>
<td>License plate</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credit card number</td>
<td>Yes, for months or years</td>
<td>To any computers involved in payment processing</td>
<td></td>
</tr>
</tbody>
</table>
Identifiers
Cookies, Cookie Syncing, headers, TLS, Fonts, Plugins/Extensions, IP Address, JavaScript, Fingerprinting, Iframes, Local Storage
(Mobile) Advertising IDs, Phone Number, IMSI and IMEI, MAC addresses, BlueTooth

Trackers
Buy / Sell / Trade / Beg / Borrow / Steal

Sellers - Real-time bidding, ad exchanges, demand side platforms, shadow bidding, data brokers (Buyers and sellers)

Buyers - Targeted advertising, Political campaigns and interest groups, Debt collectors, bounty hunters, and fraud investigators, Cities, law enforcement, intelligence agencies
The spy in your wallet: Credit cards have a privacy problem

What I learned: The card data business is booming for advertisers, for aiding investors and for helping retailers and banks encourage more spending. And there are many ways a card swipe can be exploited that don’t always require a transaction being “sold” or “shared” in a way that fully identifies you. Data can be aggregated, anonymized, hashed or pseudonymized (given a new name), or used to target you without ever technically changing hands.

1) The bank
2) The card network
3) The store
4) Point-of-sale systems and retailer banks
5) Mobile wallets
6) Financial apps

What can we do?

Opt-Out?
On Reuters, there are 647 different partners, each with its own privacy policy that you are somehow expected to read. Nobody is going to read all of those.

Remember that these vendors provide the same services to multiple websites, and as they are uniquely identifying your browser and devices, they can analyze and cross-reference you and build surprisingly accurate models of you, as this post from Privacy International outlines.

In summary:
1. There are hundreds of entities processing your data whenever you visit a website.
2. Largely, you have little say of what constitutes 'essential cookies' for the functionality of the websites.
3. Vendors see your data as a gold mine for new products, analysis, mining and cross-reference your data.
4. These organizations potentially deal with each other.
5. Among these vendors are some very familiar names - Adobe, Amazon, Google, Huawei, Oracle, Salesforce.


https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/
“If you need Exhibit A for why you shouldn’t let the ad industry regulate itself,” Cyphers added, “this is it.”

What can we do?
Opt-Out / Log Out
Decentralization & Self-hosting
Open-Source
Encryption
Awareness & Education
From a privacy perspective Microsoft Edge and Yandex are qualitatively different from the other browsers studied. Both send persistent identifiers that can be used to link requests (and associated IP address/location) to back end servers. Edge also sends the hardware UUID of the device to Microsoft and Yandex similarly transmits a hashed hardware identifier to back end servers. As far as we can tell this behaviour cannot be disabled by users. In addition to the search autocomplete functionality that shares details of web pages visited, both transmit web page information to servers that appear unrelated to search autocomplete.

For Brave with its default settings we did not find any use of identifiers allowing tracking of IP address over time, and no sharing of the details of web pages visited with backend servers. Chrome, Firefox and Safari all share...
Google will start trialling FLoC in March – but will only use websites that have tracking enabled or are already serving display advertising. The company also says it is against its ad policies to serve personalised ads based on sensitive categories. FLoC groups that reveal people’s race, sexual orientation and other categories will be blocked or, if that’s not possible, Google says it will change its algorithm to “reduce the correlation”.

https://www.wired.co.uk/article/google-chrome-cookies-third-party-ads

Practical Privacy
Browsers - Brave, FireFox, Safari
Browser Privacy Plugins
  Privacy Badger – uBlock Origin - uMatrix(?)
Use a VPN or Tor
  httpS
  Linux
  DuckDuckGo
Uninstall Apps
Check your settings
Pi-hole
Change DNS Provider
Don’t use Gmail?
The recordings she and her co-workers were listening to were often intense, awkward, or intensely awkward. Lonely sounding people confessing intimate secrets and fears: a boy expressing a desire to rape; men hitting on Alexa like a crude version of Joaquin Phoenix in Her. And as the transcription program grew along with Alexa’s popularity, so did the private information revealed in the recordings. Other contractors recall hearing kids share their home address and phone number, a man trying to order sex toys, a dinner party guest wondering aloud whether Amazon was snooping on them at that very instant. “There’s no frickin’ way they knew they were being listened to,” Slatis says. “These people didn’t agree to this.” She quit in 2016.

ACCORDING TO THE TWO U.S. information-security employees, data is at risk because Amazon has a poor grasp of what data it holds, where it is stored and who has access to it.

“If you wanted to do a ‘right to be forgotten,’ it would be next to impossible for Amazon to identify all of the places where your data resides within their system,” said the first former U.S.-based employee. The right to be forgotten, or right to have data erased, is a key tool for citizens under several privacy regimes, including in Europe and California.

The second U.S.-based information-security professional confirmed Amazon’s shaky understanding of what reams of personal information it holds. “Amazon has grown so fast, it doesn’t know what it owns … They don’t know where their data is at, so they don’t know if they are protecting it correctly,” the person said.


Libraries and Patron Data - Usual Suspects

- Integrated Library Systems
- Database backups
- Print management systems
- Server logs
- Reference chat/desk logs
- Public computer/wireless traffic logs
- Interlibrary Loan requests
- Anything else with PII
- Security camera footage
- Card reader logs
- Meeting room reservations
- Authentication system logs
- Library programs
  - Attendance logs
  - Feedback responses
- Vendor & other app data
- Paper forms
- Staff email

Library Data and You - A Brief Primer – Becky Yoose
Starting a Privacy Audit

ALA Resources
EFF’s How to Assess Vendor’s Data Security
LFI presentation by Becky Yoose
[https://vimeo.com/357307133]
LFI Presentation by Erin Berman
[https://vimeo.com/353128722]

From LFI’s excellent slide deck: Privacy & Security in Public Libraries

A Practical Guide to Performing a Library User Data Risk Assessment in Library-Built Systems

Libraries collect data about the people they serve every day. While some data collection is necessary to provide services, responsible data management is essential to protect the privacy of our users and uphold our professional values. One of the ways to ensure responsible data management is to perform a Data Risk Assessment.

A Data Risk Assessment is a process of identifying data the library collects about users, understanding how it manages that data, identifying the risks associated with that data, and then selecting an appropriate risk mitigation strategy.

[https://osf.io/v2c3m/]

We don’t want to collect and save EVERYTHING.

Collect & communicate with transparency.

Give people a choice.
**Checklist: Privacy Best Practices**

- Load third-party scripts only when needed
- Don’t run Google Analytics
- Remove social widgets
- No email tracking
- Do not log or ask PII data when it’s not needed

---

**We need to find balance between...**

- private / secure / hard to use
- open / harvested / easy

---

“I don’t think the fix to privacy is something that can be done by an individual alone, in the same way I can’t solve the pollution problem by recycling on my own.”

Daniel Gillmor of the American Civil Liberties Union
None of this means Google, Facebook and the rest are evil. But let's focus on three things

1. Accept that privacy online entails trade-offs

2. Keep in mind that the widespread creation and spread of data is inherent to computers and the Internet

3. We all both benefit from the spread of data BUT let's also be aware of implications

2. Awareness & Education

https://stratechery.com/2019/privacy-fundamentalism/

Privacy is the new competitive battleground

It's not clear how soon the technology will become ubiquitous, but it is clear that privacy is quickly emerging as the next competitive battleground. Newly passed regulations like CPRA codify the measures companies need to take, but it's consumer expectations that will drive long-term shifts within the companies themselves.

For those ahead of the curve, there will be significant cost savings and growth — especially as customers start to shift their loyalty toward those businesses that respect and protect their privacy. For everyone else, it will be a major wake-up call as consumers demand to take back their data.

https://techcrunch.com/2020/12/16/privacy-is-the-new-competitive-battleground/

Facebook predicts ‘significant’ obstacles to ad targeting and revenue in 2021

Anthony No - 01/25/2021

Image Credits: TechCrunch

While Facebook's fourth quarter earnings report included solid user and revenue numbers, the company sounded a note of caution for 2021.

In the “CFO outlook” section of the earnings release, Facebook said it anticipates facing “more significant advertising headwinds” this year.

“This includes the impact of platform changes, notably iOS 14, as well as the evolving regulatory landscape,” the company wrote. “While the timing of the iOS 14 changes remains uncertain, we would expect to see an impact beginning late in the first quarter.”

https://techcrunch.com/2021/01/27/facebook-q4-earnings-2/
Security and privacy are *sometimes* mutually exclusive.

To get the best security you may have to sacrifice some privacy, and vice versa.

- Windows 10
- Windows Defender
- Gmail
If vs. When

Somethings are IFs, somethings are WHENs
Perhaps things are Likely and Possible

Bad Guys?
Hackers?
Crackers?
Attackers?
Threat Actors?
Black Hats
Flexible: A big ol’ tool belt of awesome tools
Objective driven: You could just be a step or convenient stop
Stealthy: Super quiet and hard to spot
Patient: Move slow, endless time
Well-resourced and skilled: Smart with endless budgets
Experienced: Established techniques and tools
Not APTs - Lower Level Actors

- Flexible: Small tool belt of lame tools
- Rules driven
- Stealthy: Eh, maybe
- Patient: Not at all.
- Well-resourced and skilled: Dumb and predictable
- Experienced: Obvious techniques and tools
Cybersecurity is both old and new

As you work to make security part of your library conversation, it is critical to keep in mind that:

- Cybersecurity is still relatively new.
- Cybersecurity is about human conflict.
- Cybersecurity evolves fast (and has no boundaries).
- Cybersecurity requires asset maintenance.

Security...

The opposite of secure...

Convenient & easy to use.

*Security at the expense of usability comes at the expense of security.*


https://security.stackexchange.com/questions/6095/xkcd-936-short-complex-password-or-long-dictionary-passphrase/6116#6116
Security...

Isn’t Either / Or.
Isn’t the goal.

Defensibility is our goal.

Thorough understanding…
how, what, and why we’re defending our Cybers.

“In security, you almost never go from making something possible to impossible,” Cappos told ProPublica. “You go from making it easy to making it hard...”

Security is Getting Better…

But it’s Getting Worse Faster
Why?

Professionals

And Everyone Else
Security is about incentives.

As the economics writer Matt Stoller has suggested, cybersecurity is a natural area for a technology company to cut costs because its customers won’t notice unless they are hacked – and if they are, they will have already paid for the product. In other words, the risk of a cyberattack can be transferred to the customers. Doesn’t this strategy jeopardize the possibility of long-term, repeat customers? Sure, there’s a danger there – but investors are so focused on short-term gains that they’re too often willing to take that risk.
"You’re starting to see actors realizing that just regular adware won’t do these days," Check Point’s Hazum says. **"If you want the big money you need to invest in infrastructure and research and development."**

https://www.wired.com/story/adware-most-common-malware/
Retail, Finance, Healthcare, and Education

1. Piles of treasure!
   - PI; IP; Espionage, Ransomware, proprietary research data
2. An easier target
   - Older equipment, crowds, students
3. (Sometimes) Not the Most Protected
   - Tight budgets and limited technical staffs
   - Students / Patrons
   - Large and complex
   - Lack of focus and budget on security
4. Lots of Users
5. Perimeter-Focused
6. Lack of Research Visibility for IT Staff
   - The IT department cannot take measures to secure research data it does not know about.
7. Open Culture
8. Third-Party Vendors

But... Is edu is more likely to report problems than private sector targets?

Not much of this crime is new

Automation
Distance
"Technique Propagation"

("Only the first attacker has to be skilled; everyone else can use his software.")
Bad Guys

Skill
Focus
Tools
Time
Training

Highly Incentivized
The technology of the internet makes the bad guys vastly more efficient.

It's Safe Behind The Keyboard

Hacking is a really safe crime.

<table>
<thead>
<tr>
<th>Who?</th>
<th>Cybercriminals</th>
<th>State-Affiliated Bad Guys (APT)</th>
<th>Nation State Bad Guys</th>
<th>Hacktivists</th>
<th>Bot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivation</td>
<td>Economic</td>
<td>Economic / Political</td>
<td>Political</td>
<td>Social / Political</td>
<td>Social / Political / Economic</td>
</tr>
<tr>
<td>Driven By</td>
<td>Profit</td>
<td>Profit / Mission</td>
<td>Mission</td>
<td>Profit / Mission</td>
<td>Programming</td>
</tr>
<tr>
<td>Sophistication</td>
<td>Low-High</td>
<td>Low-High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Numbers</td>
<td>Akira</td>
<td>Not Many</td>
<td>Fewer</td>
<td>Some</td>
<td>0</td>
</tr>
<tr>
<td>Targets...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Resourceful attackers that target specific individuals and organizations.

Hand-crafted campaigns targeting a few dozen individuals or organizations.

Automated campaigns targeting many individuals and organizations.

Social Networks
Search Engines
Advertising
Email
Web Sites
Web Servers
Home Computers
Mobile Devices
Silent Librarian Retools Phishing Emails to Hook Student Credentials

Silent Librarian cyberattackers are switching up tactics in a phishing scheme bent on stealing student credentials.

Silent Librarian is targeting university students in full force with a revamped phishing campaign. The threat group, aiming to steal student login credentials, is using new tricks that bring more credibility to its phishing emails and helping it avoid detection.

The threat group (also known as T5075 and Cobalt Chieftain), which operates out of Iran, has been on the prowl for credentials since the start of the 2020 school year in September, launching low-volume, highly-tailored, socially engineered emails that eventually trick students into handing over their login credentials.

But more recent campaigns show the cyberattackers using shortened URL links in their phishing emails, which makes it more difficult to detect that victims are being redirected to an under-hosted landing page. The attackers have also revamped their landing pages with new university-specific banners, based on weather alerts or emergency notifications, to make them look more authentic.

What Are They Using?

Keyloggers
Data Stealers
Ram Scrapers
Bots, Aka Zombies
Banking Trojans
Rats (Remote Access Trojans)
Ransomware
Bugs / Holes / Flaws / CVEs
IBM Security X-Force ranked the top 10 CVEs of 2020 based on how frequently threat actors exploited or attempted to exploit them. The ranking is based on both IBM X-Force incident response (IR) and IBM managed security services (MSS) data for 2020. According to our findings, attackers focused on common enterprise applications and open source frameworks that many businesses use within their networks.

- CVE-2019-19871: Citrix Application Delivery Controller (ADC)
- CVE-2018-20062: NoneCMS ThinkPHP Remote Code Execution
- CVE-2006-1547: ActionForm in Apache Software Foundation (SAF) Struts
- CVE-2012-0391: ExceptionDelegator component in Apache Struts
- CVE-2014-6271: GNU Bash Command Injection
- CVE-2020-8515: Draytek Vigor Command Injection
- CVE-2020-5722: HTTP: Grandstream UCM6200 Sql Injection

This is the work of a rogue industry, not a roguish teenager.
What Are They After?

- Databases and business information
- PINs
- Passwords
- Credit Cards
- Bank Accounts
- Usernames
- Contact Lists
- Emails
- Phone Numbers
- Your Hardware...
### Dark Web Price Index 2020

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Data</td>
<td>Cloned Mastercard with PIN</td>
<td>$15</td>
</tr>
<tr>
<td>Online banking logins</td>
<td>minimum $2000 on account</td>
<td>$65</td>
</tr>
<tr>
<td>Payment processing services</td>
<td>PayPal minimum $100</td>
<td>$198.56</td>
</tr>
<tr>
<td></td>
<td>PayPal $1000 – $3000</td>
<td>$320.39</td>
</tr>
<tr>
<td>Social Media</td>
<td>Hacked Facebook account</td>
<td>$74.5</td>
</tr>
<tr>
<td></td>
<td>Hacked Instagram account</td>
<td>$55.45</td>
</tr>
<tr>
<td></td>
<td>Hacked Twitter account</td>
<td>$49</td>
</tr>
</tbody>
</table>

#### 2020 Pricing (in USD) RDP Server Access

<table>
<thead>
<tr>
<th>Service</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP with global admin access</td>
<td>$10</td>
</tr>
<tr>
<td>RDP, country specific</td>
<td>$25</td>
</tr>
<tr>
<td>Hacked RDP</td>
<td>$35</td>
</tr>
<tr>
<td>Bank drop RDP via PayPal</td>
<td>$175</td>
</tr>
</tbody>
</table>

#### 2020 Pricing (USD) Ssh for hire Services

- Hack for hire of service entity: $60
- Remove SSID, add 10 days: $100
- White hat hack, 10 days: $300
- User Id, 10 days: $300
- Remove SSID hack, 10 days: $400
- Botnet attack, 10 days: $1,000
- SSH and private IP address: $200
- SSH and private IP address: $300

#### Deep Web

- Nethanking
- Research Papers
- Medical Records
- Private forums
- Private networks
- Hidden wiki
- Tor
- Illegal Information
- Silk Road

---

https://news.ycombinator.com/item?id=23818727

https://commons.wikimedia.org/wiki/File:Deepweb_graphical_representation.svg

What Happens On The Dark Web? (There’s no map)

- Buying/Selling of Data/Credentials
- Buying/Selling of digital goods (exploits, malware, ransomware as a service)
- Exfiltration

- Does my library need to monitor the Dark Web?
- Most places can benefit from SOME Dark Web monitoring
  - Know what you’re going to do with this stuff
- Some alerts are generally low quality, such as:
  - Lists of email addresses, some of which include the org’s domain
  - Username and password pairs for external things
- Interesting, but probably not actionable
- But if we discover someone selling access to our network, internal user/pass, other access, that’s actionable!

- Dark Web monitoring is one of those things where you shouldn’t try to do it yourself
- The legal and regulatory implications of DIY Dark Web monitoring can be significant
- Weigh these issues carefully before deciding on a strategy

Next Week

1) Pick A Podcast and/or a email newsletter or Twitter or OPML

1) Send me a ranked list of all the things in your library with an IP address

blake.carver@lyrasis.org
Start Thinking About…

- What You Have
- What are your defences
- What are the threats
- Confidence and Likelihood