

Cybersecurity: Week 1 Introduction

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



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.



2

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

3

Series Housekeeping - Outline

- **Week One – Welcome – Explanations of why and what's wrong**
 - 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 Three - Making Your Library Defensible & Resilient**
 - What and why of things around the library
 - Hardware, networks, ransomware
- **Week Four – Wrapping It All Up**
 - Training, planning, vendors
 - Websites
 - Checklists and specific steps to take next.

4

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

5

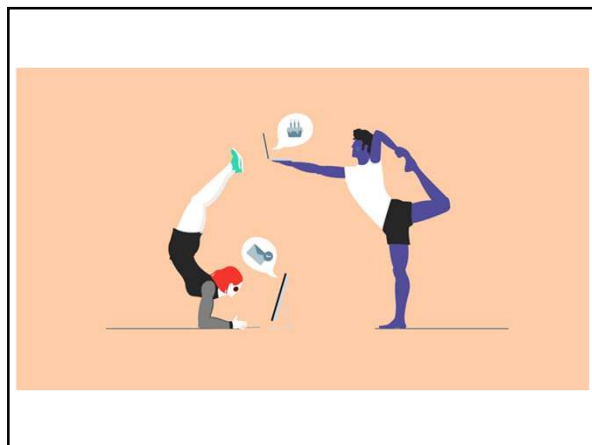
Series Housekeeping – Guidelines

- 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.

6



7



8

Today

- 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?

9

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

10

About LYRASIS

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




1000+
Members


\$500m
Services Provided


Millions
of Dollars Saved


11


Digital Technology Services: Hosting Services ✨



LYRASIS ArchivesSpace
Hosting Services


LYRASIS Islandora
Hosting Services


SimplyE



VIVO | connect share discover


LONE
ARRANGER

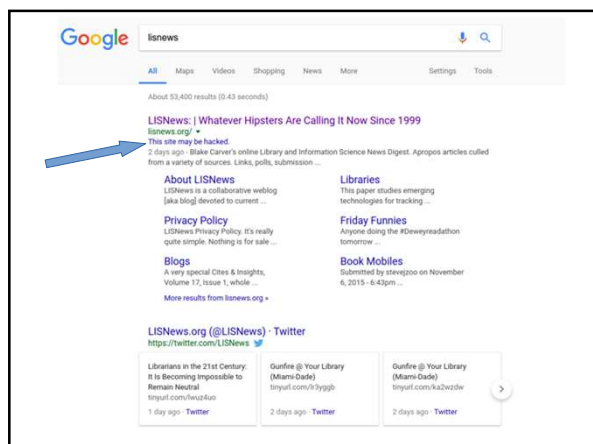

LYRASIS CollectionSpace
Hosting Services

Fedora™

DSPACE DIRECT


DSpace

12



13



14

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

15

Everything you need to know

Passwords: L E N G T H & Unique
Paranoia: Think Before You Click
Backups: Frequent and Automatic
Patches: Set to Auto
Upskill: Regular training
Protect: Review all settings

16

We are all targets

We all have something of value

17

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

18

“Security & Privacy can be two different things: They can be both a feeling & a reality ”

Bruce Schneier – TedxPSU

19

Understanding...
Information / IT / Data
Privacy

20

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



Privacy

21

Privacy Vs. Data Privacy

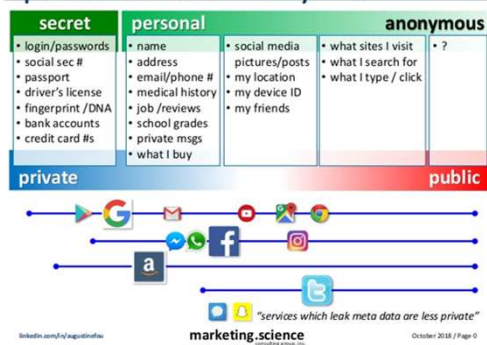
The rules of privacy are being defined and redefined today.

So much of what we do is for sale now.

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

22

Spectrum of Privacy –v2



23

Threats To Privacy?

1. The government threat
2. The criminal threat
3. The corporate threat

24

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

25

The new digital divide is between people who opt out of algorithms and people who don't

April 17, 2019 6:54am EDT

...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.

<https://theconversation.com/the-new-digital-divide-is-between-people-who-opt-out-of-algorithms-and-people-who-dont-114729>

26

Privacy is Getting Better!

But it's Getting Worse Faster

27

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

28



29

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.

<https://www.theguardian.com/content/privacy-404-personal>

30

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

31

Personal information is the
currency of the ***entire Internet***
economy

32

Angry Birds and the end of privacy

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

By Kaitlyn Tiffany | @kat_tiffany | kaitlyn.tiffany@vox.com | Updated May 14, 2019, 8:06am 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.

<https://www.vox.com/explainers/2018/5/7/44973355/angry-birds-iphone-games-data-collection-candy-crush>

33

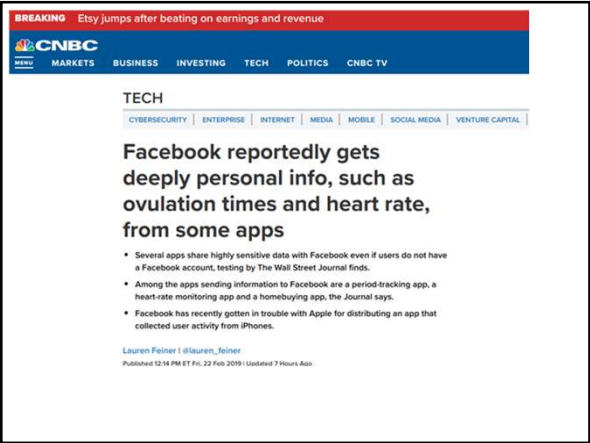
34

35





37



38

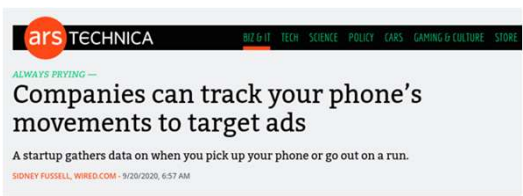


39

...your data is collected in ways you cannot reasonably prevent, no matter how carefully you or anyone you know behaves.

<https://livesixtyeight.com/features/you-cant-opt-out-of-sharing-your-data-even-if-you-dont-opt-in/>

40



ars TECHNICA BIT'S & BYTES · TECH · SCIENCE · POLICY · GEAR · GAMING & CULTURE · STORE

ALWAYS PRYING —

Companies can track your phone's movements to target ads


A startup gathers data on when you pick up your phone or go out on a run.

SIDNEY FUSSELL, WIRED.COM · 5/29/2020, 6:57 AM

"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.**

41



SwiftOnSecurity
@SwiftOnSecurity

Equifax stole your data, China just copied it without paying them.

1:21 PM · Feb 10, 2020 · Twitter for iPhone

42

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.

43

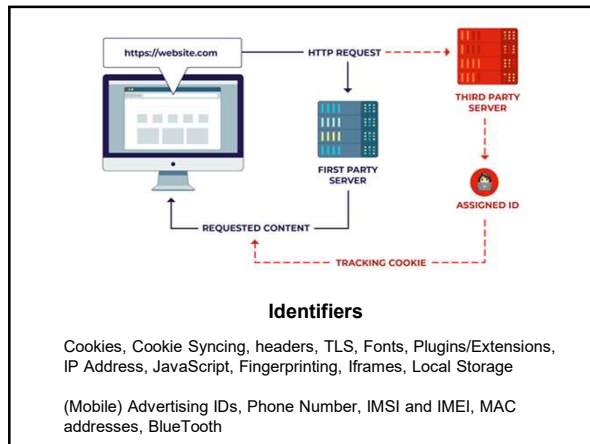
Web Identifiers	Unique	Persistent	Available
Cookies	Yes	Until user deletes	In some browsers without tracking protection
IP address	Yes	On the same network, may persist for weeks or months	Always
TLS state	Yes	For up to one week	In most browsers
Local storage super cookie	Yes	Until user deletes	Only in third-party IFrames; can be blocked by tracker blockers
Browser fingerprint	Only on certain browsers	Yes	Almost always; usually requires JavaScript access, sometimes blocked by tracker blockers

44

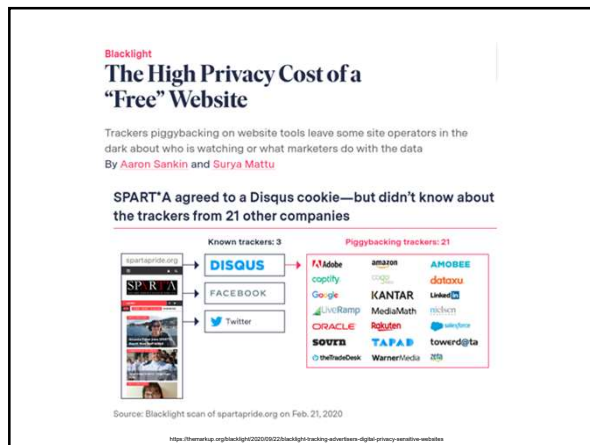
Phone Identifiers	Unique	Persistent	Available
Phone number	Yes	Until user changes	Readily available from data brokers; only visible to apps with special permissions
IMSI and IMEI number	Yes	Yes	Only visible to apps with special permissions
Advertising ID	Yes	Until user resets	Yes, to all apps
MAC address	Yes	Yes	To apps only with special permissions To passive trackers: visible unless OS performs randomization or device is in airplane mode

Other Identifiers	Unique	Persistent	Available
License plate	Yes	Yes	Yes
Face print	Yes	Yes	Yes
Credit card number	Yes	Yes, for months or years	To any companies involved in payment processing

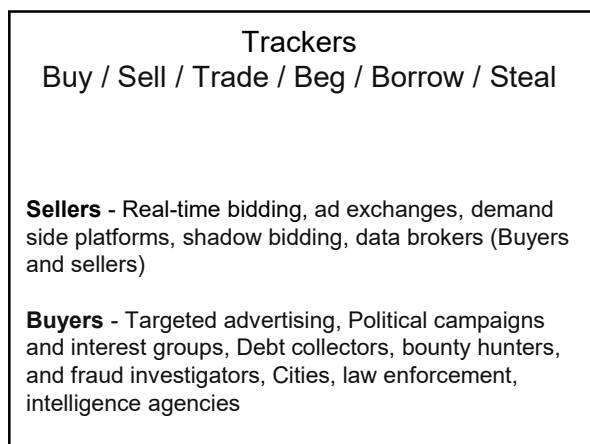
45



46



47



48

Sections

The Washington Post

Democracy Dies in Darkness

Sign In

Consumer Tech • Perspective

The spy in your wallet: Credit cards have a privacy problem

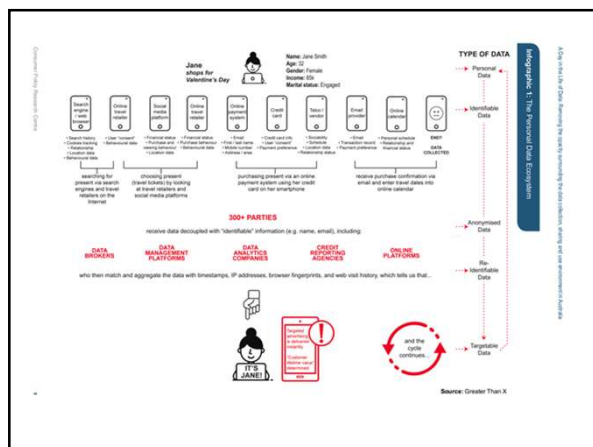
In a privacy experiment, we bought one banana with the new Apple Card — and another with the Amazon Prime Rewards Visa from Chase. Here's who tracked, mined and shared our data.

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

<https://www.washingtonpost.com/technology/2019/08/26/spy-your-wallet-credit-cards-have-privacy-problem/>

49



50

What can we do?

Opt-Out?

51

How we use cookies

We use cookies to improve the site, measure performance, understand our audience, enhance your experience and provide you with advertising based on your browsing activities and interests on this and other sites. You can always change your preferences or opt out at the bottom of the site. Please note some of the cookies we use are essential for the parts of the site to operate. See "Manage Cookies" for details.

[Manage cookies](#) [Accept cookies](#)

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. There is a vibrant ecosystem of data vendors who collect, analyze, mine 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

<http://www.conradakanga.com/blog/what-do-you-actually-agree-to-when-you-accept-all-cookies/>

52

The Fantasy of Opting Out

Those who know about us have power over us. Opting out may be our best digital weapon.



Learn to do digital

By Peter Bracken & John Thompson

There is no simple solution to the problem of privacy, because privacy itself is a solution to societal challenges that are in constant flux.

<https://theater.mitpress.mit.edu/the-fantasy-of-opting-out>

53

I tried to use the ad tech industry's tool to opt out of personalized ads. Did it work?

by **THE MARKUP** — 1 day ago in **INSIGHTS**

51 SHARES <https://tne.to/9vH0>

Last year, while reporting a [story](#) about how the digital advertising industry burrowed its tracking technology into scores of websites serving vulnerable and marginalized communities, I did something counterintuitive, especially for a reporter who writes about tech for a living: I surrendered to the surveillance economy.

This decision to inject pure, uncut internet directly into my veins came as I was using and helping to create The Markup's [Blacklight](#) tool, which opened my eyes even further to the plethora of companies that sought to grab my data from the websites I used on a daily basis. Until then, I had mostly used Google's Chrome browser with the Privacy Badger extension, which blocks many forms of tracking, or Mozilla's Firefox, which has strict privacy controls set by default.

54

“If you need Exhibit A for why you shouldn’t let the ad industry regulate itself,” Cyphers added, “this is it.”

<https://thetechweb.com/insights/2021/03/28/why-to-use-the-ad-tech-industry-to-opt-out-of-personalized-ads-did-it-work-syndicator/>

55

What can we do?

Opt-Out / Log Out

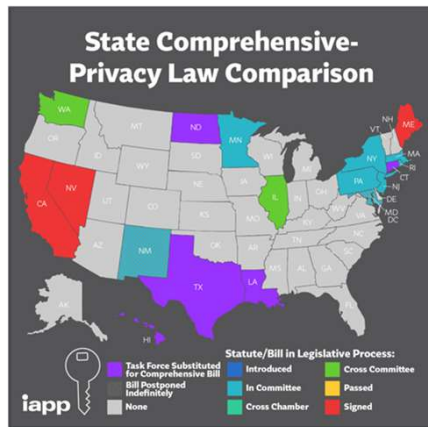
Decentralization & Self-hosting

Open-Source

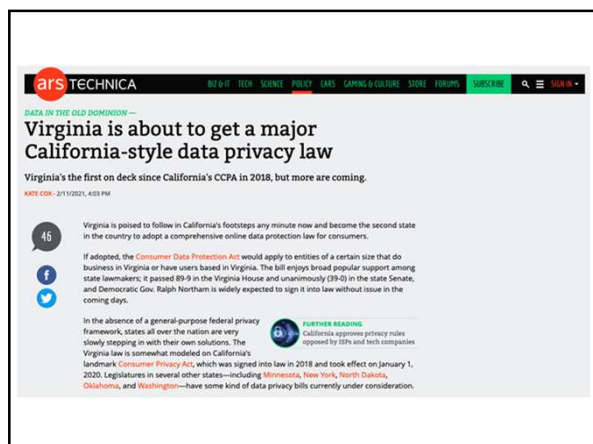
Encryption

Awareness & Education

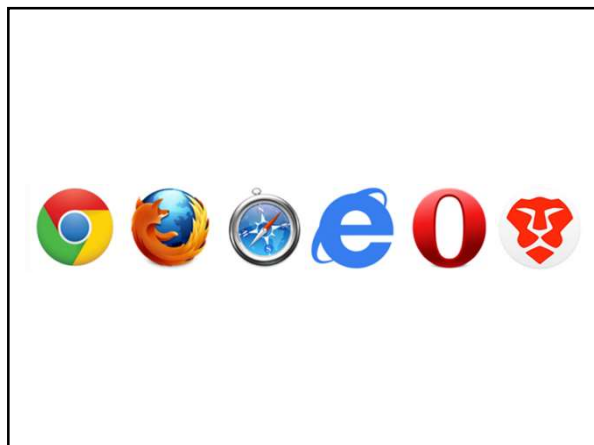
56



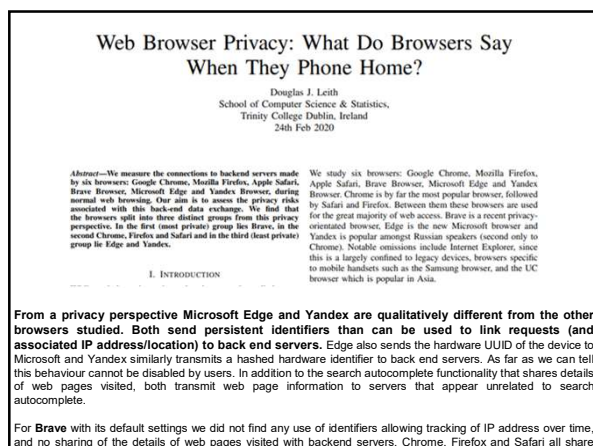
57



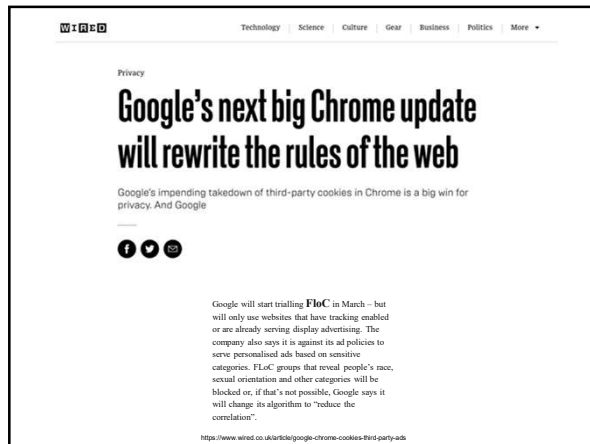
58



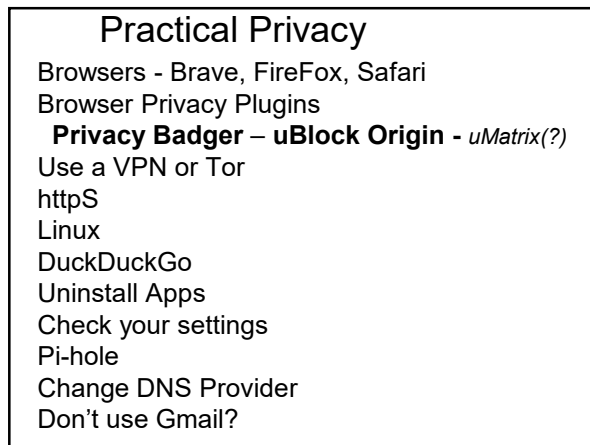
59



60



61



62



63

Bloomberg Businessweek

Silicon Valley Is Listening to Your Most Intimate Moments

How the world's biggest companies got millions of people to let temps analyze some very sensitive recordings.

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.

64

Thursday, February 26, 2021

POLITICO

NET TOPICS

'Millions of people's data is at risk' — Amazon insiders sound alarm over security

Whistleblowers say they were forced out after flagging problems with e-commerce giant's data security and compliance.

ACCORDING TO THE TWO U.S. information-security employees, data is at risk because Amazon has a poor grasp of what data it has, 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.

<https://www.politico.eu/article/data-at-risk-amazon-security-threat/>

65

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

66

Starting a Privacy Audit

ALA Resources
 EFF's *How to Assess Vendor's Data Security*
 LFI presentation by Becky Yoose (<https://vimeo.com/357367133>)
 LFI Presentation by Erin Berman (<https://vimeo.com/353126702>)

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

Data Lifecycle Quick Reference Map

Phase	Question	Best Practice
Collection	What data are you collecting? Why are you collecting that data?	Only collect data needed for demonstrated business cases. Practice "The Five Whys".
Storage	Where is the data stored?	Limit number of data storage sites. Limit storage of PII in both local and vendor systems.
Access	Who has access to the data?	Limit physical and electronic access to PII data. Audit vendor security and privacy practices.
Reporting	What data is published to staff and the public?	Aggregate and control access to data through dashboards, data tables, and other data visualization and reporting tools.
Retention	How long is the data kept?	Follow local, state, and federal retention regulations. Don't forget about backups and logs.
Deletion	What data is deleted and how?	Properly dispose of physical and electronic media that contained PII.

LDH Consulting Services
[CC BY-SA 4.0](https://ldh.com)

<https://libdataprivacy.com>
 LFI, August 2019

67

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://oef.io/v2c3m/>

68

We don't want to collect and save EVERYTHING.

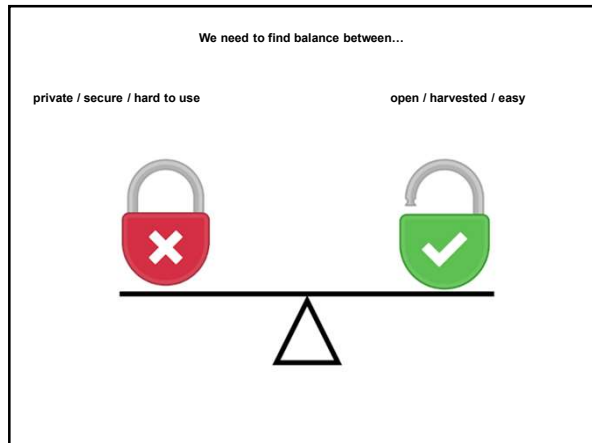
Collect & communicate with transparency.

Give people a choice.

69

- 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

70



71

"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

<https://www.bloomberg.com/news/features/2019-08-08/instead-hiding-from-silicon-valley-in-a-pile-of-privacy-gadgets>

72

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

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

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

2. Awareness & Education

<https://stratichery.com/2019/privacy-fundamentalism/>

73

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/>

74

Facebook predicts 'significant' obstacles to ad targeting and revenue in 2021

Anthony Ha @anthonyha / 4:49 PM EST • January 27, 2021

 Comment

 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/>

75

Inc.

NEWSLETTERS SUBSCRIBER R 50A

TECHNOLOGY

Facebook Just Admitted It Has Lost the Battle With Apple Over Privacy The company launched an ad campaign that shows just how worried it is about Apple's upcoming privacy changes.

BY JASON ATEK ILLUSTRATION

Cathy Images

Facebook hasn't been shy about expressing its concerns about the changes coming to iOS 14. Last summer, Apple first announced the changes, which include the requirement that apps include a privacy nutrition label to show users what data is collected and how it is used, as well as what Apple calls App Tracking Transparency (ATT) which requires apps to request permission before tracking users.

76

Security



77

Security

Cyber Security?

IT Security?

Safety?

Information Security?

Information Literacy?

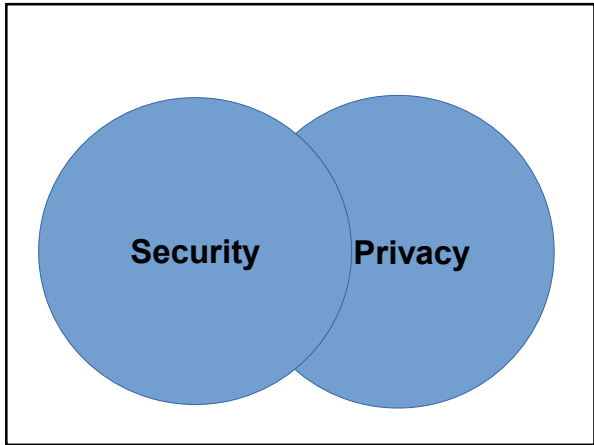
The Digital Divide?

ITSec

78



79




80

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







81

If vs. When

Some things are IFs, some things are WHENs
Perhaps things are Likely and Possible

82

Bad Guys?
Hackers?
Crackers?
Attackers?
Threat Actors?
Black Hats

83




84

APTs - State Level Actors

- **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

85



Is Your Car Safe From Supermaneuverable Air-Defense Fighter Aircraft?

768,344 views • Premiered Mar 19, 2021


103K


854

SHARE

SAVE

...



Bosnian Ape Society 


222K subscribers

SUBSCRIBE

Many beginner drivers make the common mistake of forgoing proper defense against airborne threats such as enemy fighter jets and air-to-surface missiles. In this video, we will explain the best methods to protect your vehicle from such threats and avoid the necessity of paying exorbitant

SHOW MORE

86



Is Your Car Safe From Supermaneuverable Air-Defense Fighter Aircraft?

768,344 views • Premiered Mar 19, 2021

103K

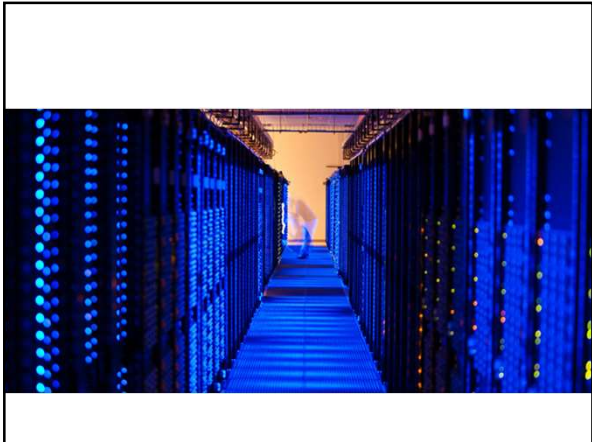
854

SHARE

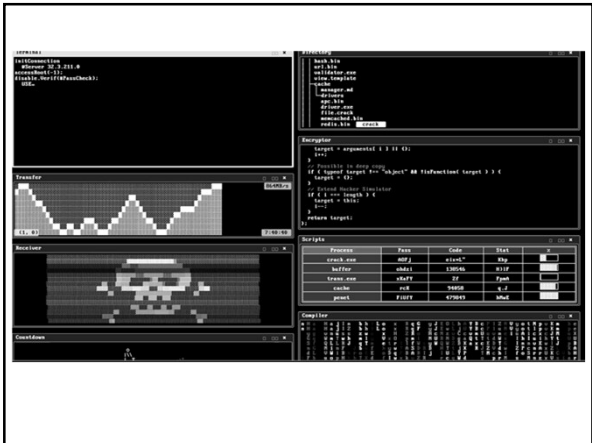
SAVE

...

87



88



89

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

90

HAZARD RISK ASSESSMENT MATRIX				
Frequency of Occurrence	Hazard Categories			
	1 Catastrophic	2 Critical	3 Serious	4 Minor
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Unacceptable
 High
 Medium
 Low

91

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.

<https://www.microsoft.com/news/cyberlog/2020/01/30/steering-resiliently-understanding-cybersecurity-risk-part-2>

92

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/9099/should-i-use-a-short-complicated-password-or-long-dictionary-password/118961#118961>

93

Security...

Isn't Either / Or.

Isn't the goal.

Defensibility is our goal.

Thorough understanding...

how, what, and why we're defending our Cybers.

94

"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...***"

<https://www.propublica.org/article/solarwinds-cybersecurity-system>

95

Security is Getting Better...

But it's Getting Worse Faster

Intro

96

Why?

Professionals

Intro

97

And Everyone Else



98



Krebs on Security
In-depth security news and investigation

29 Career Choice Tip: Cybercrime is Mostly Boring

When law enforcement agencies tout their latest cybercriminal arrest, the defendant is often cast as a brazen outlaw engaged in sophisticated, lucrative, even exciting activity. But new research suggests that as cybercrime has become dominated by pay-for-service offerings, the vast majority of day-to-day activity needed to support these enterprises is in fact mind-numbingly boring and tedious, and that highlighting this reality may be a far more effective way to combat cybercrime and steer offenders toward a better path.

Mailing List
[Subscribe here](#)

99

Security is about incentives.

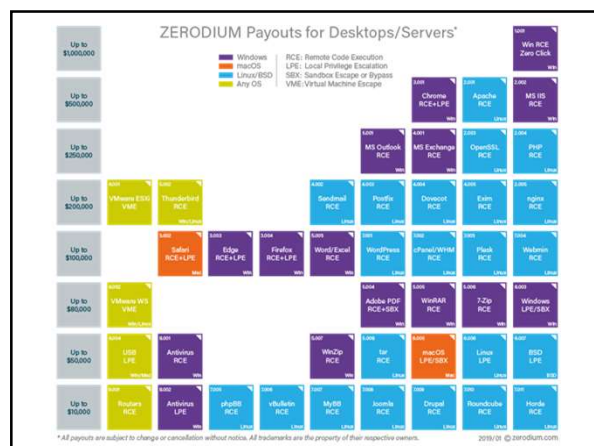
100

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.

<https://www.schneier.com/blog/archives/2021/03/national-security-risks-of-zero-stage-capitalism.html>

101



102

BREAKING

February 6, 2020 by jrgue

Critical Bluetooth Vulnerability in Android (CVE-2020-0022)

On November 3rd, 2019, we have reported a critical vulnerability affecting the Android Bluetooth subsystem. This vulnerability has been assigned [CVE-2020-0022](#) and was now patched in the [latest security patch](#) from February 2020. The security impact is as follows:

- On Android 8.0 to 9.0, a remote attacker within proximity can silently execute arbitrary code with the privileges of the Bluetooth daemon as long as Bluetooth is enabled. No user interaction is required and only the Bluetooth MAC address of the target devices has to be known. For some devices, the Bluetooth MAC address can be deduced from the Wi-Fi MAC address. This vulnerability can lead to theft of personal data and could potentially be used to spread malware (Short-Distance Worm).
- On Android 10, this vulnerability is not exploitable for technical reasons and only results in a crash of the Bluetooth daemon.
- Android versions even older than 8.0 might also be affected but we have not evaluated the impact.

Users are strongly advised to install the latest available security patch from February 2020. If you have no patch available yet or your device is not supported anymore, you can try to mitigate the impact by some generic behavior rules:

- Only enable Bluetooth if strictly necessary. Keep in mind that most Bluetooth enabled headphones also support wired analog audio.

"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."**

LOU HATZENDORN / SECURITY 07.21.10 07:00 AM

**ADWARE IS THE MALWARE YOU
SHOULD ACTUALLY WORRY
ABOUT**

<https://www.wired.com/story/adware-most-common-malware/>

Ransomware gangs made at least \$350 million in 2020

The figure represents a 311% increase over ransomware payments recorded the previous year, in 2019.

By Catalin Cimpanu for Zero Day | February 2, 2021 | 10:48 GMT



Ransomware gangs made at least \$350 million in ransom payments last year, in 2020, blockchain analysis firm Chainalysis said in a [report](#) last week.



MORE FROM CATALIN CIMPANU

- Security: Blockchain transactions confirm murky and interconnected ransomware scene
- Security: Security firm Stormshield discloses data breach, theft of source code
- Security: Android devices ensnared in OObS botnet
- Security: Google: Proper patching would have prevented 25% of all zero-days found in 2020

106

Retail, Finance, Healthcare, and Education Retail, Finance, Healthcare - Obvious Education / Libraries?!

1. Piles of treasure!
PII, 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
Target-rich environment.
Students / Patrons
Large and complex
Less 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?

107

Not much of this crime is new

Automation Distance "Technique Propagation"

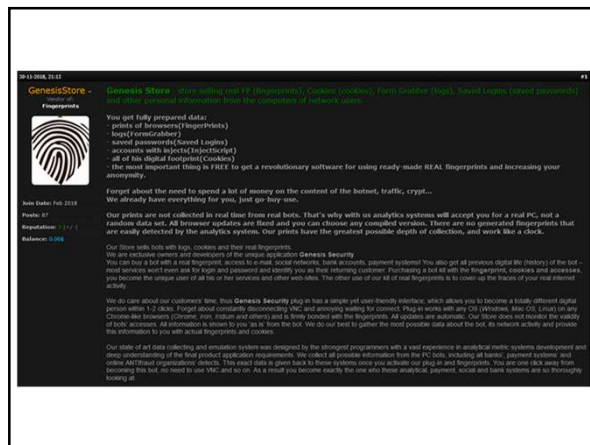
("Only the first attacker has to be skilled; everyone else can use his software.")

Intro

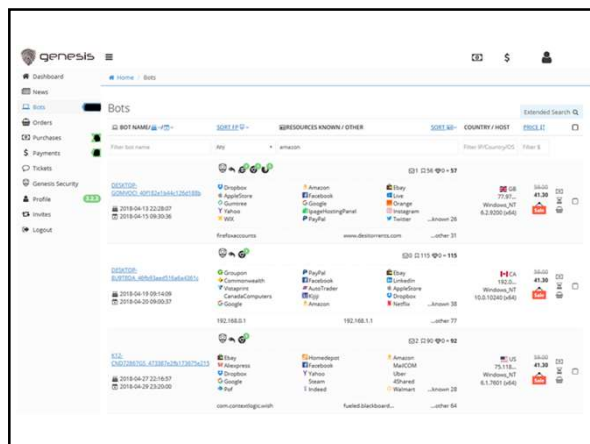
108

Highly Incentivized

109



110



111

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

112

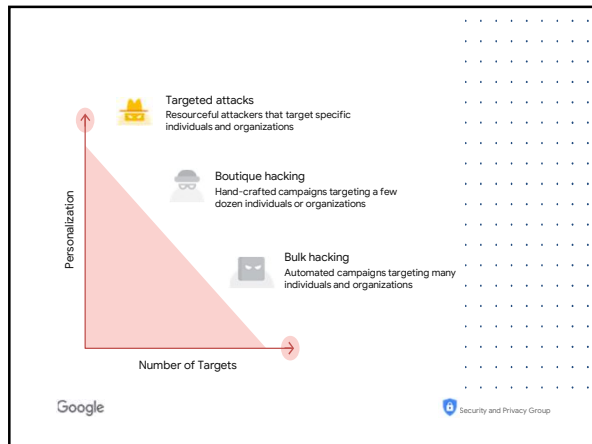
It's Safe Behind The Keyboard

Hacking is a really *safe* crime.

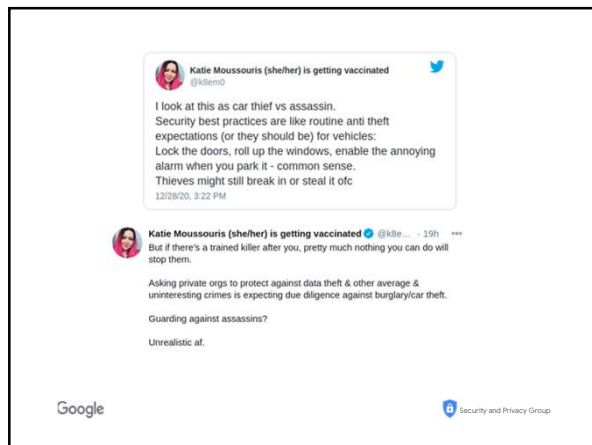
113

Who?	Cybercriminals	State-Affiliated Bad Guys (APT)	Nation State Bad Guys	Hacktivists	Bots
Motivation	Economic	Economic / Political	Political	Social / Political	Social / Political / Economic
Driven By	Profit	Profit / Mission	Mission	Profit / Mission	Programming
Sophistication	Low-High	Low-High	High	Medium	Low
Numbers	Allota	Not Many	Fewer	Some	∞
Targets...					

114



115



116

Where Are They Working?

- Social Networks
- Search Engines
- Advertising
- Email
- Web Sites
- Web Servers
- Home Computers
- Mobile Devices

117

Silent Librarian Retools Phishing Emails to Hook Student Credentials



Author
Lindsey O'Donnell
October 30, 2019
1:54 pm

3:30 minute read

Skip to:
Back-To-School Att...

New Tricks

Write a comment

Share this article:

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 TA407 and Cobalt Dickens), which operates out of Iran, has been on the prowl for credentials since the start of the 2019 school year in September, launching low-volume, highly-targeted, 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 make it more difficult to detect that victims are being redirected to an attacker-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.

<https://threatpost.com/silent-librarian-phishing-student-credentials/149249/>

118

threatpost Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

FIN11 Cybercrime Gang Shifts Tactics to Double-Extortion Ransomware

Critical Sonic

Silent Librarian Goes Back to School with Global Research-Stealing Effort



Author
Tara Seals
October 14, 2020
12:52 pm

2:30 minute read

Write a comment

The Iranian hacker group is targeting universities in 12 countries.

The Silent Librarian campaign has re-emerged for the fall school session, actively targeting students and faculty at universities via spear-phishing campaigns.

The threat group (also known as TA407 and Cobalt Dickens), which operates out of Iran, has been on the prowl since the start of the 2019 school year, launching low-volume, highly-targeted, socially engineered emails that eventually trick victims into handing over their login credentials. The goal is to harvest not just logins to sell online, but also proprietary university research and data, researchers said.

<https://threatpost.com/silent-librarian-school-research-stealing/160099/>

119

What Are They Using?

Keyloggers
Data Stealers
Ram Scrapers
Bots, Aka Zombies
Banking Trojans
Rats (Remote Access Trojans)
Ransomware
Bugs / Holes / Flaws / CVEs

120

Top 10 CVEs of 2020

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.**

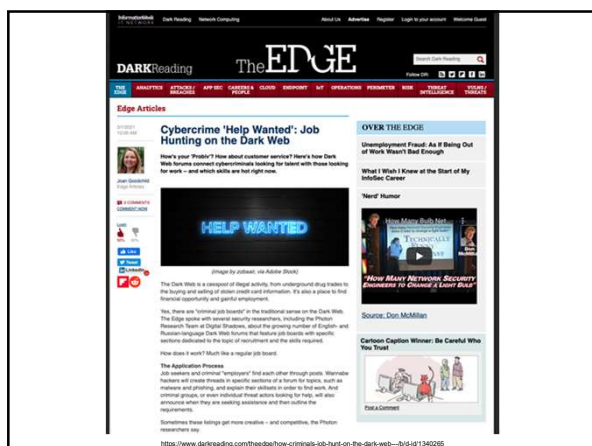
- CVE-2019-19871: Citrix Application Delivery Controller (ADC)
- CVE-2018-20062: NoneCMS ThinkPHP Remote Code Execution
- CVE-2006-1547: ActionForm in Apache Software Foundation (SAF) Struts
- CVE-2012-0391: ExceptionDelegator component in Apache Struts
- CVE-2014-6271: GNU Bash Command Injection
- CVE-2019-0708: 'Bluekeep' Microsoft Remote Desktop Services Remote Code Execution
- CVE-2020-8515: Draytek Vigor Command Injection
- CVE-2018-13382 and CVE-2018-13379: Improper Authorization and Path Traversal in Fortinet FortiOS
- CVE-2018-11776: Apache Struts Remote Code Execution
- CVE-2020-5722: HTTP: Grandstream UCM6200 SQL Injection

<https://securityintelligence.com/posts/top-10-cybersecurity-vulnerabilities-2020/>

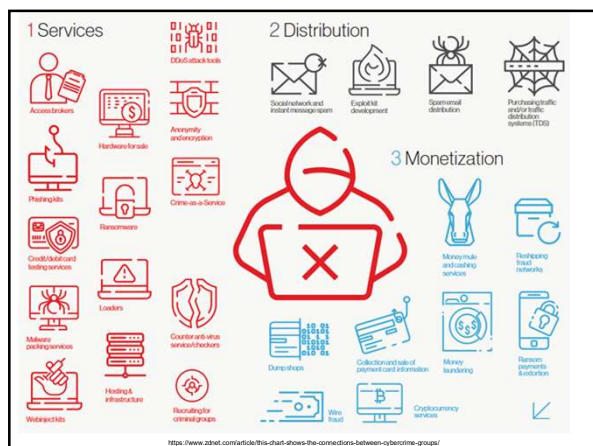
121

This is the work of a rogue industry, not a roguish teenager

122



123

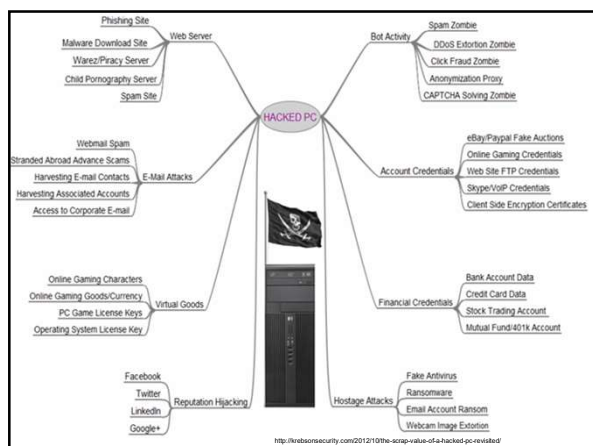


124

What Are They After?

- Databases and business information
- PINs
- Passwords
- Credit Cards
- Bank Accounts
- Usernames
- Contact Lists
- Emails
- Phone Numbers
- Your Hardware...

125



126

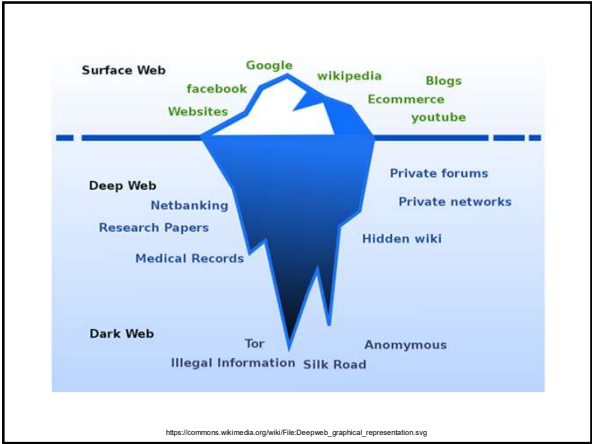
Dark Web Price Index 2020		
Credit Card Data		
Cloned Mastercard with PIN	\$15	
Online banking logins		
minimum \$2000 on account	\$65	
Payment processing services		
PayPal minimum \$100	\$198.56	
PayPal \$1000 – \$3000	\$320.39	
Social Media		
Hacked Facebook account	\$74.5	
Hacked Instagram account	\$55.45	
Hacked Twitter account	\$49	

127

2020 Pricing (in USD): RDP Server Access	
RDP with global admin access	\$10
RDP, country-specific	\$26
Hacked RDP	\$35
Bank drop RDP via PayPal	\$575

2020 Pricing (USD): DDoS-for-Hire Services	
Telephony Denial of Service (TDoS)	\$22
10-minute DDoS attack, 60 Gbps	\$45
4-hour DDoS Attack, 15 Gbps	\$55
Layer 7 bypass, 100 Gbps	\$85
30-minute DDoS Attack, 60 Gbps	\$90
DDoS attack, fully-managed	\$165
DDoS script private CloudFlare bypass	\$200
DDoS script private OVH bypass	\$250

128



129

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

130



COVID-19 BEST REVIEWS NEWS HOW TO FINANCE HEALTH SMART HOME C/

Your hacked Facebook account may be bankrolling scam ad campaigns

One campaign tried to use a person's credit card to spend \$10,000 a day on Facebook scam ads.



Alfred Ng · Nov 4, 2019 5:00 a.m. PT



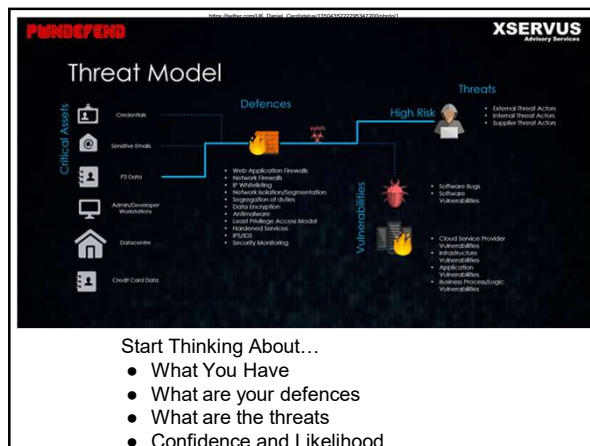
<https://www.cnet.com/news/your-hacked-facebook-account-may-be-bankrolling-scam-ad-campaigns/>

131

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

132



133
