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

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


The 1981 book *School, Work and Play (World of Tomorrow)*

Computer criminals

Computers will make the world of tomorrow a much safer place. They will do away with cash, so that you need no longer fear being attacked for your money. In addition, you need not worry that your home will be burgled or your car stolen. The computers in your home and car will guard them, allowing only yourself to enter or someone with your permission.

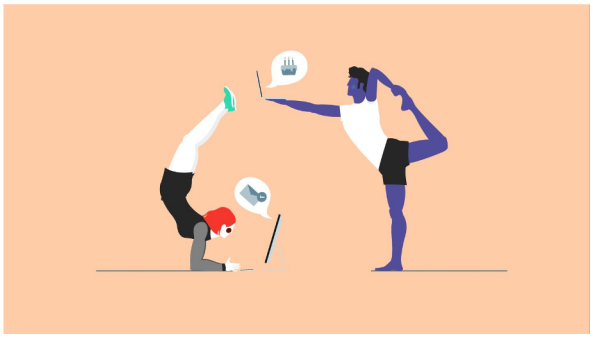
However, there is one kind of crime which may exist in the future – computer crime. Instead of mugging people in the streets or robbing houses, tomorrow's criminal may try to steal money from banks and other organizations by using a computer. The computer criminal works from home, using his own computer to gain access to the memories of the computers used by the banks and companies. The criminal tries to interfere with the computers in order to get them to transfer money to his computer without the bank or company knowing that it has been robbed.

Computer crime like this in fact exists already. However, it is very difficult to carry out a successful robbery by computer. Many computers have secret codes to prevent anyone but their owners from operating them. As computers are used more and more, it is likely that computer crime will become increasingly difficult to carry out.

Nevertheless, a computer criminal may succeed now and then and the detectives of the future will have to be highly skilled computer operators. There will probably be police computer-fraud squads, specially trained to deal with computer crime. Here you can see a squad arriving at the home of a computer criminal and arresting him as he makes a dash for it. He is clutching a computer cassette that contains details of his computer crimes, and the police will need this as evidence to prove that he is guilty.

27

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

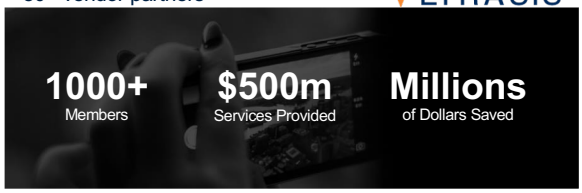
blake.carver@lyrasis.org

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

LYRASIS



11

Digital Technology Services: Hosting Services

LYRASIS ArchivesSpace
Hosting Services

LYRASIS Islandora
Hosting Services

Simply E

VIVO connect share discover

LONE ARRANGER

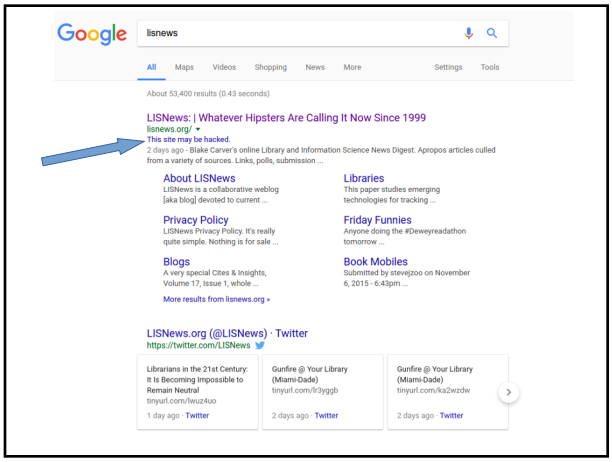
LYRASIS CollectionSpace
Hosting Services

Fedora™

DSPACEDIRECT

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

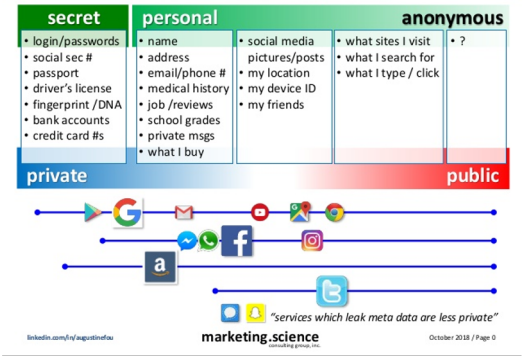
The rules of privacy are being defined and redefined today.

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



https://www.linuxjournal.com/content/privacy-mine-right-individual-persons-not-data

23

Threats To Privacy?

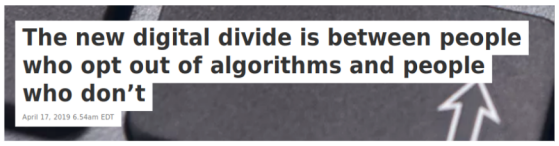
1. **The government threat**
2. **The criminal threat**
3. **The corporate threat**

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



...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-114719

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.linuxjournal.com/content/privacy-still-personal

30

We don't know how our information is used, stored or shared and for how long.

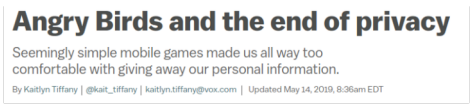
We don't know who has access

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

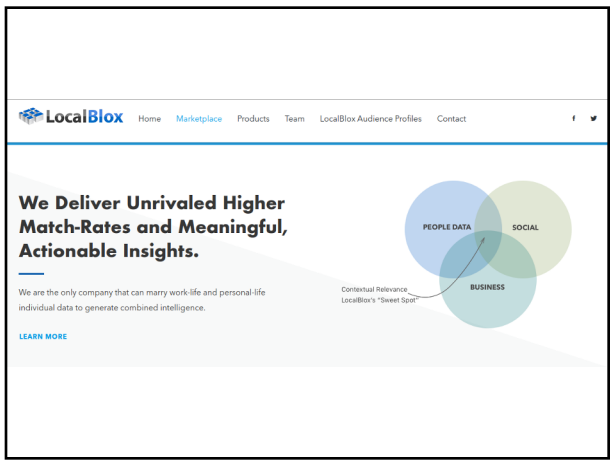
Seemingly simple mobile games made us all way too comfortable with giving away our personal information.

By Kaitlyn Tiffany | @kait_tiffany | kaitlyn.tiffany@vox.com | Updated May 14, 2019, 8:36am EDT

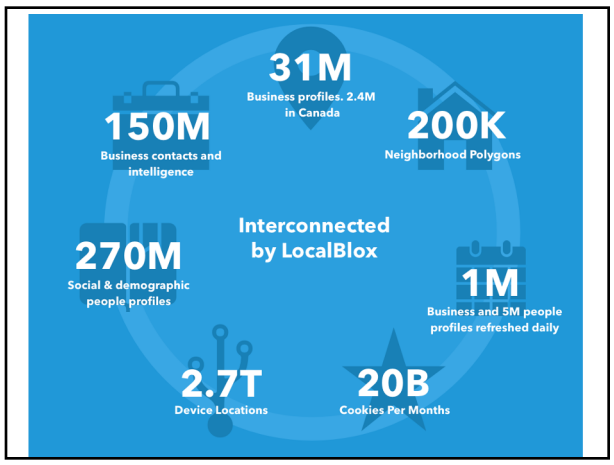
The business model that holds up the mobile gaming industry, digital advertising, and most major social media platforms is persistent and ravenous, very good at holding on to the information you've given it and even better at finding ways to enrich that information and keep it fresh, even after you've 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/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

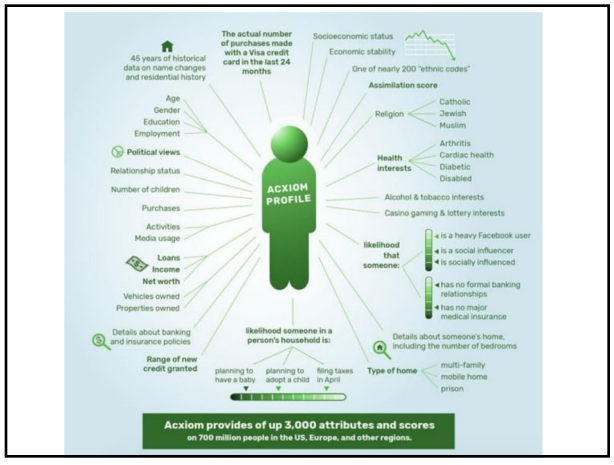
33


LocalBlox
Home
Marketplace
Products
Team
LocalBlox Audience Profiles
Contact
We Deliver Unrivaled Higher Match-Rates and Meaningful, Actionable Insights.
We are the only company that can marry work-life and personal-life individual data to generate combined intelligence.
LEARN MORE
PEOPLE DATA
SOCIAL
BUSINESS
Contextual Relevance
LocalBlox's "Sweet Spot"

34


31M
Business profiles. 2.4M in Canada
150M
Business contacts and intelligence
200K
Neighborhood Polygons
Interconnected by LocalBlox
270M
Social & demographic people profiles
1M
Business and 5M people profiles refreshed daily
2.7T
Device Locations
20B
Cookies Per Months

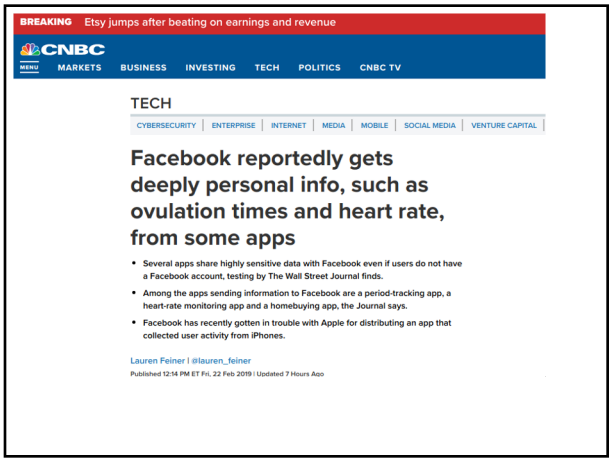
35


ACXIOM PROFILE
45 years of historical data on name changes and residential history
The actual number of purchases made with a Visa credit card in the last 24 months
Socioeconomic status
Economic stability
One of nearly 200 "ethnic codes"
Assimilation score
Religion
Catholic
Jewish
Muslim
Health interests
Arthritis
Cardiac health
Diabetic
Disabled
Alcohol & tobacco interests
Casino gaming & lottery interests
likelihood that someone:
is a heavy Facebook user
is a social influencer
is socially influenced
has no formal banking relationships
has no major medical insurance
Details about someone's home, including the number of bedrooms
Type of home
multi-family
mobile home
prison
Age
Gender
Education
Employment
Political views
Relationship status
Number of children
Purchases
Activities
Media usage
Loans
Income
Net worth
Vehicles owned
Properties owned
Details about banking and insurance policies
Range of new credit granted
likelihood someone in a person's household is:
planning to have a baby
planning to adopt a child
filing taxes in April
Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.

36


BBC
Sign in
News
Sport
Weather
Shop
Earth
Travel
NEWS
Home
Video
World
US & Canada
UK
Business
Tech
Science
Magazine
Technology
Google plans to track credit card spending
26 May 2017
Technology
Share

37


BREAKING Etsy jumps after beating on earnings and revenue
CNBC
MENU
MARKETS
BUSINESS
INVESTING
TECH
POLITICS
CNBC TV
TECH
CYBERSECURITY
ENTERPRISE
INTERNET
MEDIA
MOBILE
SOCIAL MEDIA
VENTURE CAPITAL
Facebook reportedly gets deeply personal info, such as ovulation times and heart rate, from some apps
Several apps share highly sensitive data with Facebook even if users do not have a Facebook account, testing by The Wall Street Journal finds.
Among the apps sending information to Facebook are a period-tracking app, a heart-rate monitoring app and a homebuying app, the Journal says.
Facebook has recently gotten in trouble with Apple for distributing an app that collected user activity from iPhones.
Lauren Feiner | @lauren_feiner
Published 12:14 PM ET Fri, 22 Feb 2019 | Updated 7 Hours Ago

38


FACEBOOK
Turning Off Facebook Location Tracking Doesn't Stop It From Tracking Your Location
Kashmir Hill
12/18/18 12:20pm
Filed to: YOU CAN RUN BUT YOU CAN'T HIDE
160.5K
170
4
When asked about this, Facebook said that's exactly what it's doing and that it considers this a completely normal thing to do and that users should know this will happen if they closely read various Facebook websites.
"Facebook does not use WiFi data to determine your location for ads if you have Location Services turned off," said a Facebook spokesperson by email. "We do use IP and other information such as check-ins and current city from your profile. We explain this to people, including in our Privacy Basics site and on the About Facebook Ads site."
On Privacy Basics, Facebook gives advice for "how to manage your privacy" with regards to location but says that regardless of what you do, Facebook can still "understand your location using things like... information about your Internet connection." This is reiterated on the "About Facebook Ads" site that says that ads might be based on your location which is garnered from "where you connect to the Internet" among other things.

39

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

https://fivethirtyeight.com/features/you-cant-opt-out-of-sharing-your-data-even-if-you-didnt-opt-in/

40

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS 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 - 9/20/2020, 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

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

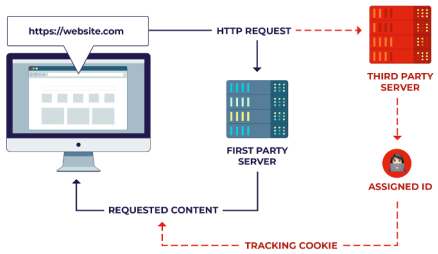
Web identifiers	Unique	Persistent	Available
Cookies	Yes	Until user deletes	In some browsers without tracking protection
IP address	Yes	On the same network, may persist for weeks or months	Always
TLS state	Yes	For up to one week	In most browsers
Local storage super cookie	Yes	Until user deletes	Only in 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



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

46

47

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

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

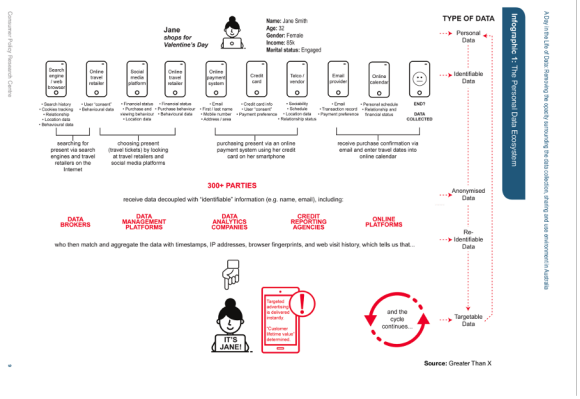
In a privacy experiment, we bought one banana with the new Apple Card — and another with the Amazon Prime Rewards Visa from Chase. Here's who tracked, mined and shared our data.

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.conradakunga.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. Obfuscation may be our best digital weapon.

By: Finn Brunton & Helen Nissenbaum

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://thereader.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://tnw.to/9fvH0

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://thenextweb.com/insights/2021/03/28/i-tried-to-use-the-ad-tech-industrys-tool-to-opt-out-of-personalized-ads-did-it-work-syndication/

55

What can we do?

Opt-Out / Log Out

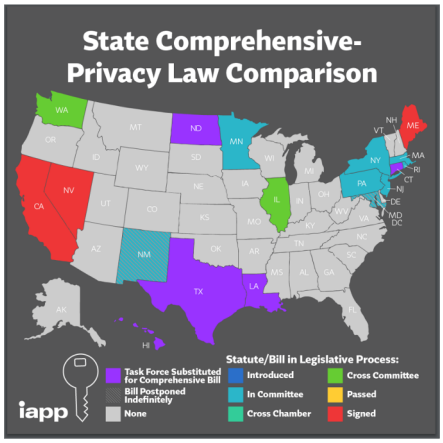
Decentralization & Self-hosting

Open-Source

Encryption

Awareness & Education

56



57

58

59

Web Browser Privacy: What Do Browsers Say When They Phone Home?

Douglas J. Leith
School of Computer Science & Statistics,
Trinity College Dublin, Ireland
24th Feb 2020

***Abstract*—We measure the connections to backend servers made by six browsers: Google Chrome, Mozilla Firefox, Apple Safari, Brave Browser, Microsoft Edge and Yandex Browser, during normal web browsing. Our aim is to assess the privacy risks associated with this back-end data exchange. We find that the browsers split into three distinct groups from this privacy perspective. In the first (most private) group lies Brave, in the second Chrome, Firefox and Safari and in the third (least private) group lie Edge and Yandex.**

We study six browsers: Google Chrome, Mozilla Firefox, Apple Safari, Brave Browser, Microsoft Edge and Yandex Browser. Chrome is by far the most popular browser, followed by Safari and Firefox. Between them these browsers are used for the great majority of web access. Brave is a recent privacy-orientated browser, Edge is the new Microsoft browser and Yandex is popular amongst Russian speakers (second only to Chrome). Notable omissions include Internet Explorer, since this is a largely confined to legacy devices, browsers specific to mobile handsets such as the Samsung browser, and the UC browser which is popular in Asia.

I. Introduction

From a privacy perspective Microsoft Edge and Yandex are qualitatively different from the other browsers studied. Both send persistent identifiers than 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

60

WIRED Technology | Science | Culture | Gear | Business | Politics | More

Privacy

Google's next big Chrome update will rewrite the rules of the web

Google's impending takedown of third-party cookies in Chrome is a big win for privacy. And Google

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

61

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?

62

63

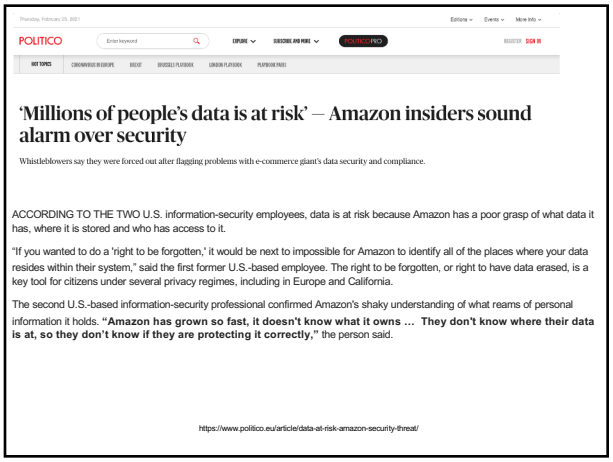
Bloomberg Businessweek

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



POLITICO

'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

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://osf.io/v2c3m/

68

We don't want to collect and save EVERYTHING.

Collect & communicate with transparency.

Give people a choice.

69

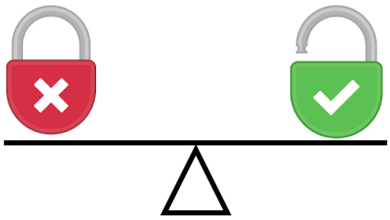
- Load third-party scripts only when needed
- Don’t run Google Analytics
- Remove social widgets
- No email tracking
- Do not log or ask PII data when it’s not needed

70

We need to find balance between…

private / secure / hard to use

open / harvested / easy



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/i-tried-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://stratechery.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 /

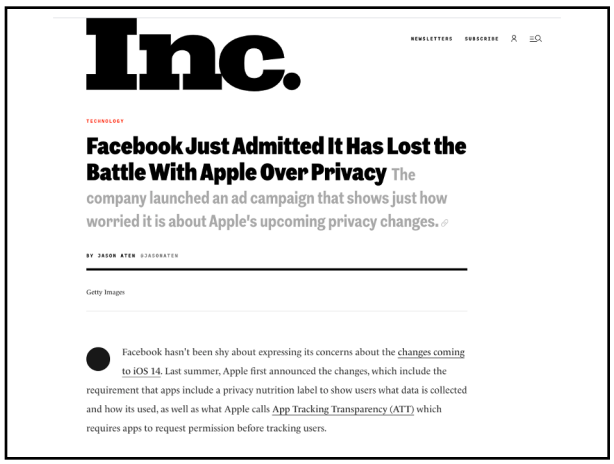
While Facebook's fourth quarter earnings report included solid user and revenue numbers, the company sounded a note of caution for 2021.

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 SUBSCRIBE

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 ATEN @JASONATEN

Getty 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 its used, as well as what Apple calls App Tracking Transparency (ATT) which requires apps to request permission before tracking users.

76

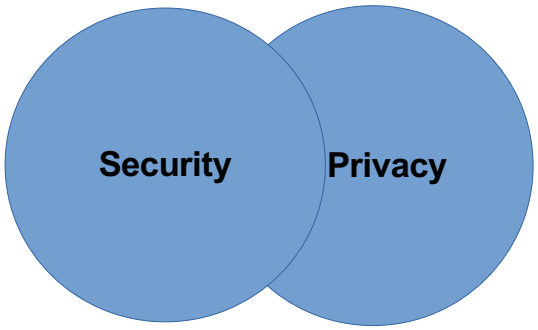
77

Security

Cyber Security?
IT Security?
Safety?
Information Security?
Information Literacy?
The Digital Divide?
ITSec

78

79

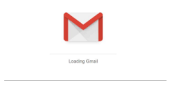


80

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

Somethings are IFs, somethings are WHENs

Perhaps things are Likely and Possible

82

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

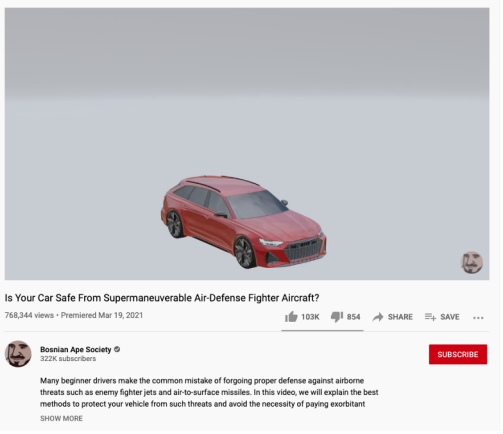
83

84

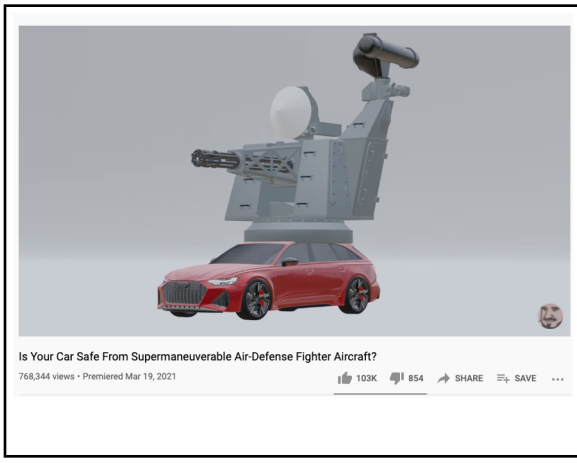
APTs - State Level Actors

- **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

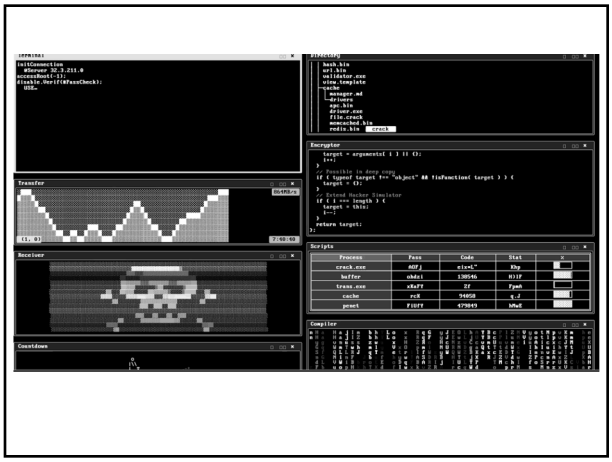


86



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/security/blog/2020/10/13/becoming-resilient-by-understanding-cybersecurity-risks-part-1/

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/82095/xkcd-936-short-complex-password-or-long-dictionary-passphrase/611686116

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

97

And Everyone Else

98

99

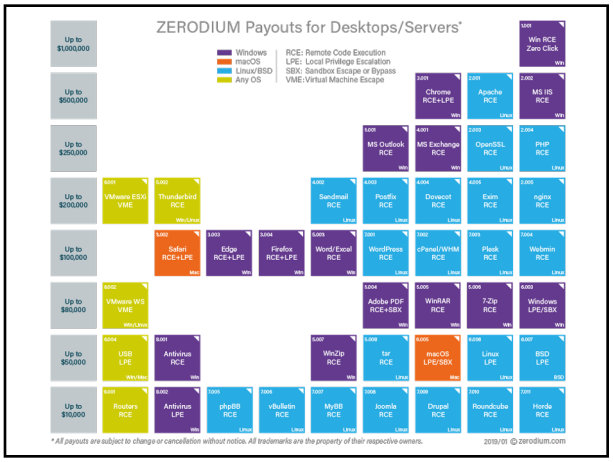
Security is about incentives.

100

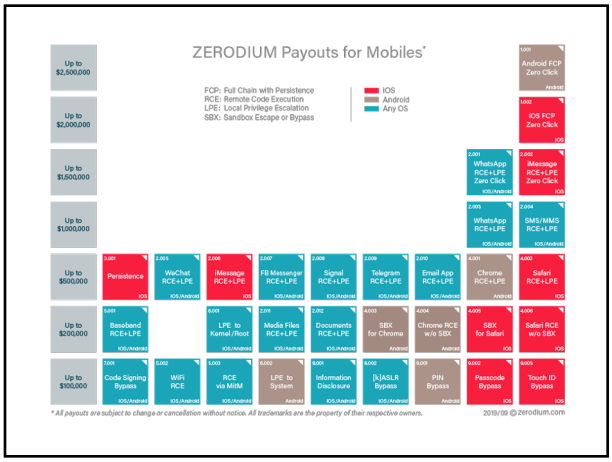
As the economics writer Matt Stoller has suggested, **cybersecurity is a natural area for a technology company to cut costs because its customers won't notice unless they are hacked – and if they are, they will have already paid for the product.** In other words, the risk of a cyberattack can be transferred 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-late-stage-capitalism.html

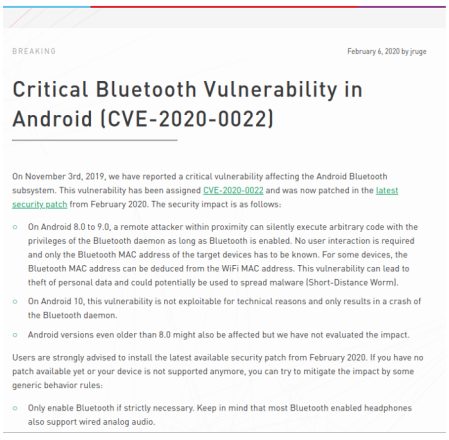
101



102



103



BREAKING February 6, 2020 by jruge

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 WiFi 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.

104

"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.**"

LILY HAY NEWMAN SECURITY 07.21.19 07:00 AM

ADWARE IS THE MALWARE YOU SHOULD ACTUALLY WORRY ABOUT

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

105

Ransomware gangs made at least $350 million in 2020

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

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 DDoS 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 – .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.")

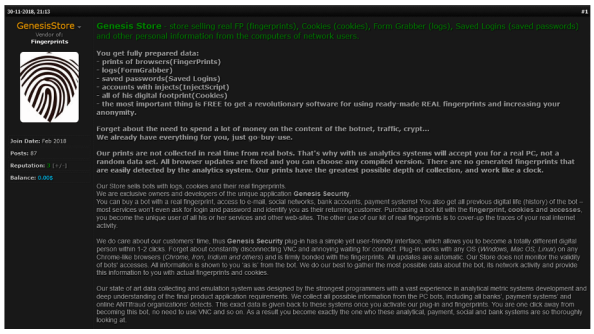
108

Bad Guys

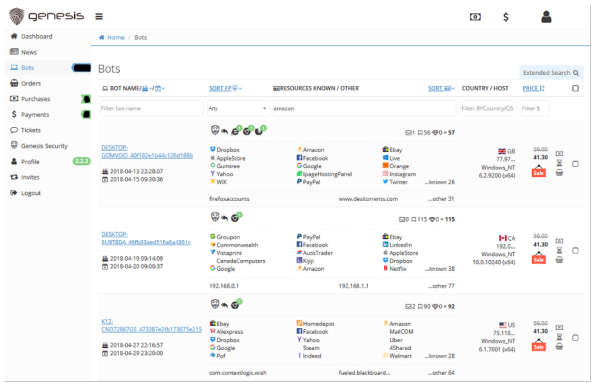
Skill
Focus
Tools
Time
Training

Highly Incentivized

109



110



111

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

112

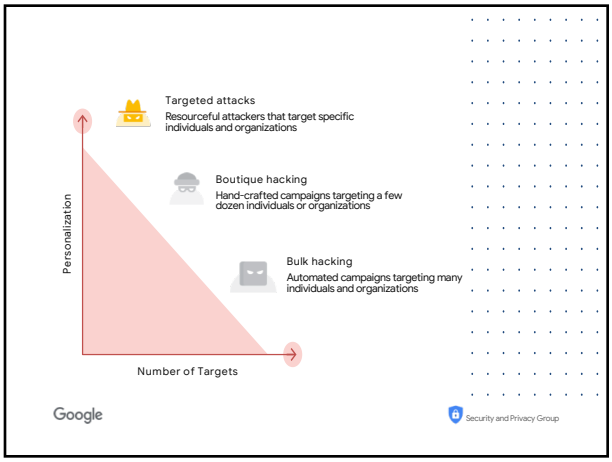
It's Safe Behind The Keyboard

Hacking is a really *safe* crime.

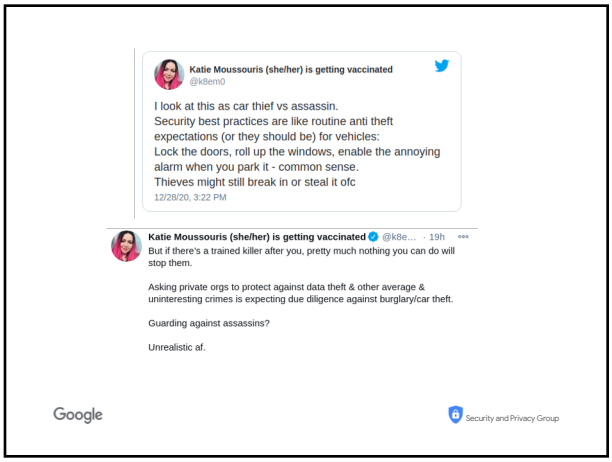
113

Who?	**Cybercrimials**	**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	Misson	Profit / Mission	Programming
Sophistication	Low-High	Low-High	High	Medium	Low
Numbers	Allota	Not Many	Fewer	Some	∞
Targets...					

114



115

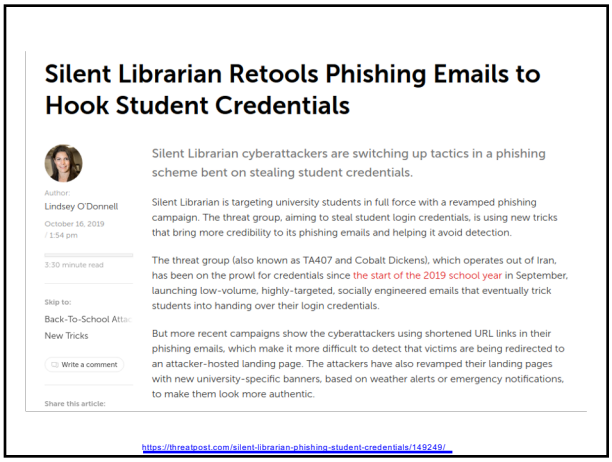


116

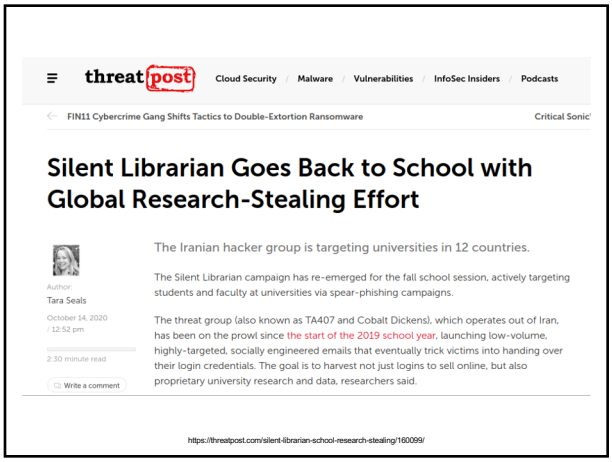
Where Are They Working?

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

117



118



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.**

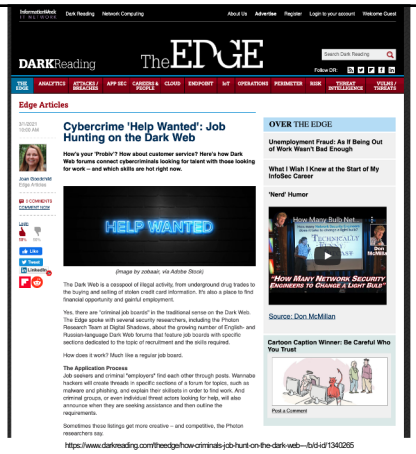
- CVE-2019-19871: Citrix Application Delivery Controller (ADC)
- CVE-2018-20062: NoneCMS ThinkPHP Remote Code Execution
- CVE-2006-1547: ActionForm in Apache Software Foundation (SAF) Struts
- CVE-2012-0391: ExceptionDelegator component in Apache Struts
- CVE-2014-6271: GNU Bash Command Injection
- CVE-2019-0708: '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/

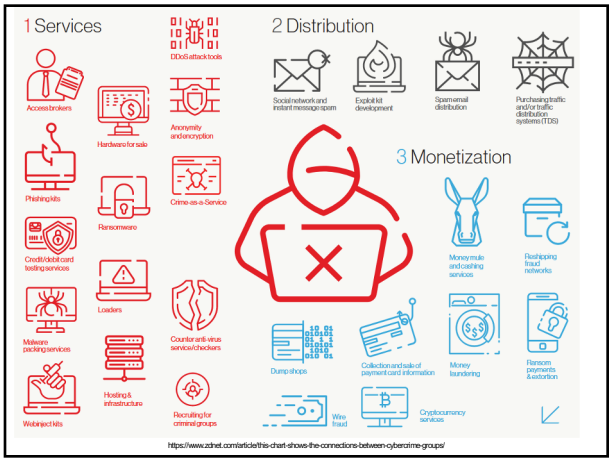
121

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

122



123

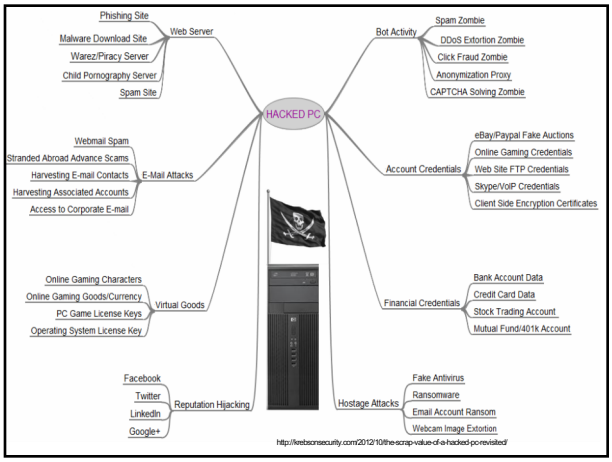


124

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

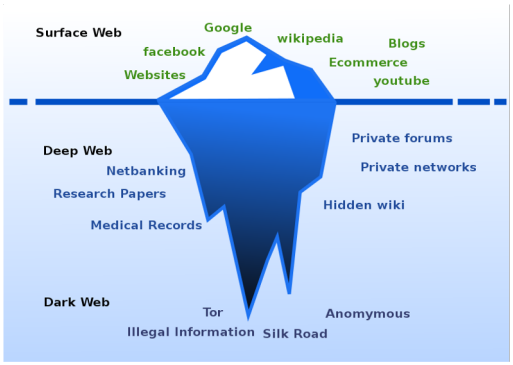
RDP with global admin access	$10
RDP, country-specific	$26
Hacked RDP	$35
Bank drop RDP via PayPal	$575

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

https://threatpost.com/rdp-server-access-payment-card-data-in-high-cybercrime-demand/162476/

128



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

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

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

131

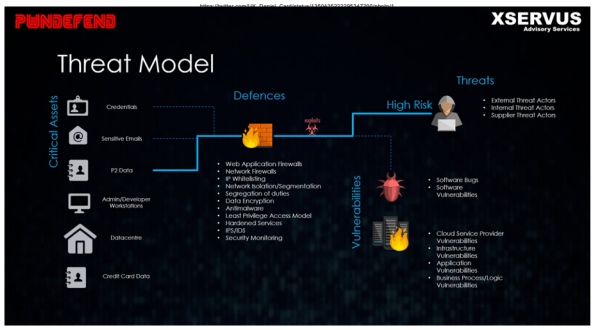
Next Week

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



Start Thinking About…

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

133

Cybersecurity: Week 2 Securing Our "Things"

Blake Carver
Senior Systems Administrator, LYRASIS
April 2021
Cybersecurity Training for Libraries
Week #2

Pacific Library Partnership

134

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.

INSTITUTE of Museum and Library SERVICES

135

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

136

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**
- Passwords
- 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

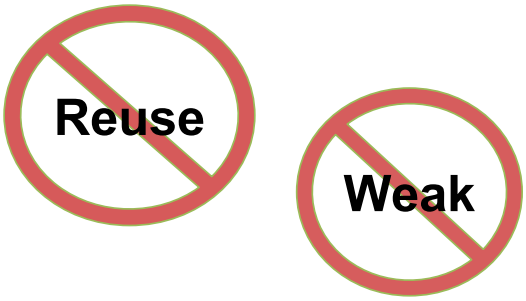
- **Week Four – Wrapping It All Up**
- Training, planning, vendors
- Websites
- Checklists and specific steps to take next.

137

The Importance Of Passwords For You & Your Library

138

Passwords



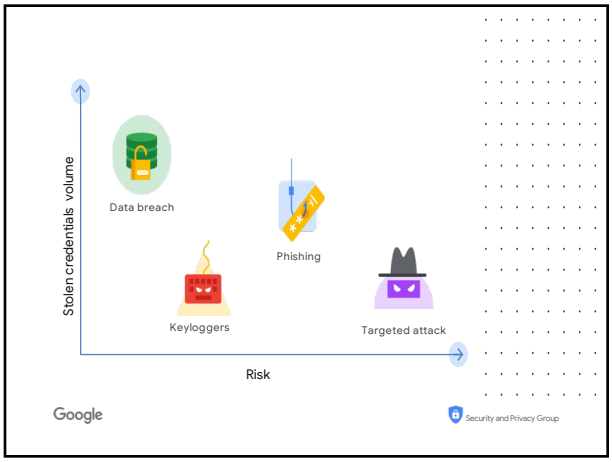
139

140

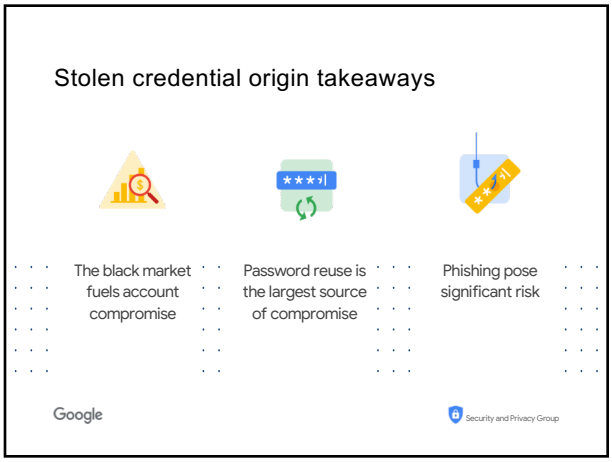
How Did They Get My Password?

Guessed
Password Reset
Stolen Mobile Device
Phishing
Trojans/Virus/Malware
API Exploitation
Third Party App Exploitation
Website Breach

141



142



143

people respond to policies,
perversely

ZAQ!@#$
P@5sw0rd1!

Passwords

144

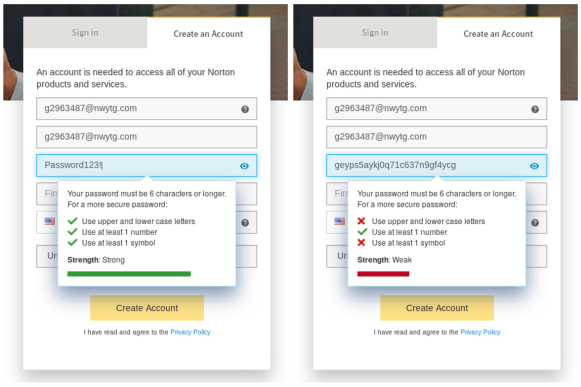
49% of workers, when forced to update their password, reuse the same one with just a minor change

Graham Cluley
11:15 am, December 11, 2019

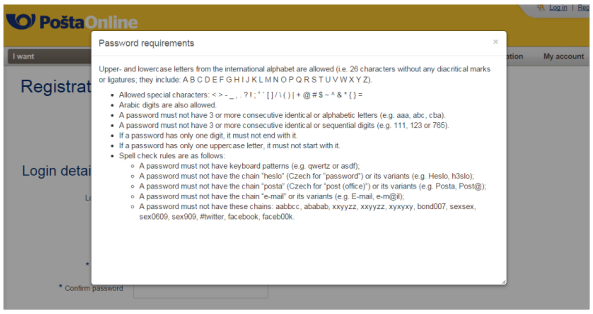
For instance, not only did 72% of users admit that they reused the same passwords in their personal life, but also 49% admitted that when forced to update their passwords in the workplace they reused the same one with a minor change.

Furthermore, many users were clearly relying upon their puny human memory to remember passwords (42% in the office, 35% in their personal lives) rather than something more reliable. This, no doubt, feeds users' tendency to choose weak, easy-to-crack passwords as well as reusing old passwords or making minor changes to existing ones.

145



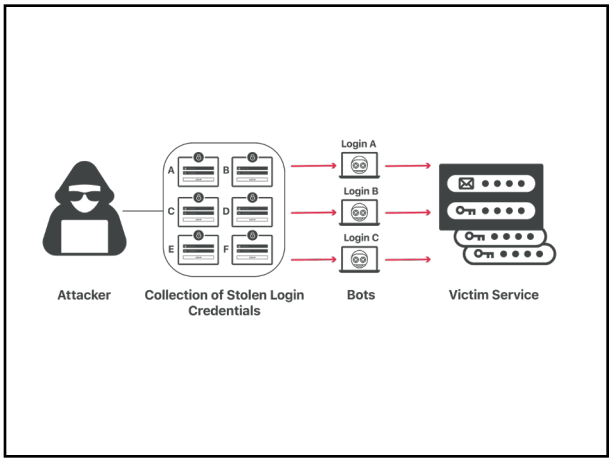
146



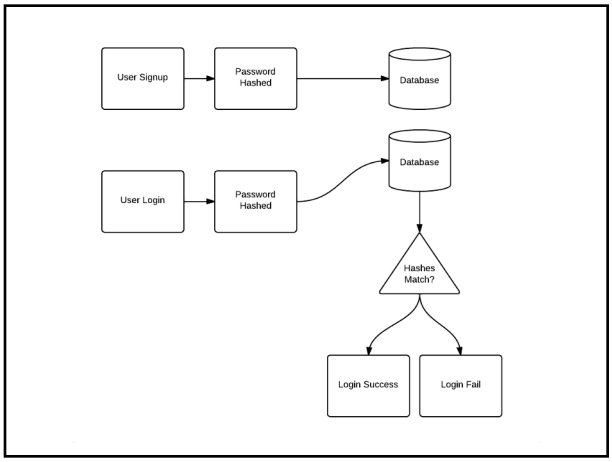
147


Set password
Password too long

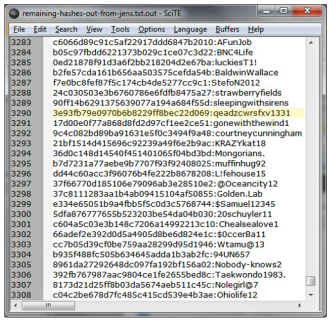
148


A
B
C
D
E
F
Login A
Login B
Login C
Attacker
Collection of Stolen Login Credentials
Bots
Victim Service

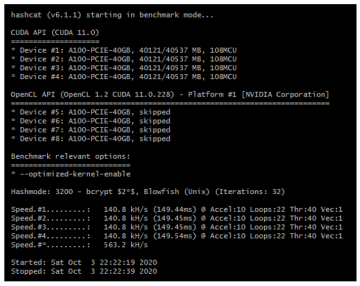
149


User Signup
Password Hashed
Database
User Login
Password Hashed
Database
Hashes Match?
Login Success
Login Fail

150

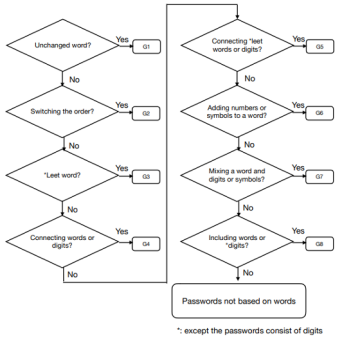


151



152

PCFG Cracker - Probabilistic Context Free Grammar (PCFG) Password Guess Generator



*: except the passwords consist of digits

153

- **Traditional Brute-Force Attack**: A dedicated, purpose-written software package generates all combinations of letters, numbers, and other characters such as punctuation and symbols, in progressively longer strings. It tries each one as the password on the account under attack. If it happens to generate a combination of characters that matches the password for the account under attack, that account is compromised.
- **Dictionary Attack**: A dedicated, purpose-written software package takes one word at a time from a list of dictionary words, and tries them as the password against the account under attack. Transformations can be applied to the dictionary words such as adding digits to them and substituting digits for letters.
- **Password Look-Up Attack**: Similar to a dictionary attack, but the word lists contain actual passwords. Automated software reads a password at a time from a huge list of passwords collected from data breaches.
- **Intelligent Password Look-Up Attack**: Like a password attack, but transformations of each password are tried as well as the "naked" password. The transformations emulate commonly used password tricks such as substituting vowels for digits.
- **API Attack**: Instead of trying to crack a user's account, these attacks use software to generate strings of characters they hope will match a user's key for an Application Programming Interface. If they can get access to the API they may be able to exploit it to exfiltrate sensitive information or intellectual copyright.

https://www.cloudsavvyit.com/7132/how-to-protect-your-organization-against-password-dictionary-attacks/

154

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

155

https://johnopdenakker.com/every-day-should-be-worldpasswordday/

156

Simple Things Make Strong Passwords (*Slow Them Down*)

- DO Make it as _l o n g_ as you can
- Do not reuse it on multiple sites
- Do not use numb3r5 1n pl@c3 of l3tt3rz
- Some Letters – UPPER and lower case
- Use some numbers
- Have a something else <>(*%$@!-+=)
- S P A C E S

157

Don't Test Your Memory

Anything dependent on memory doesn't scale

- Use a password manager
  - Bitwarden, LastPass, KeePass[X], 1Password, Dashlane..
- Use A Pass Phrase
- Nobody – *nobody* – is immune from getting hacked

158

Should You Change Your Passwords Every X # of Months?

- Email?
- Bank Account?
- Network? Server? Router?
- Facebook & Twitter?
- code4lib.org?
- ala.org?

159

Assume Your Password Will Be Stolen

Most of your passwords should be almost worthless. Some will be very important.

160

What Else Ya Got?

- Biometrics
- Hardware
- Your face
- Iris scans
- Voice files
- Your DNA
- Your voice
- 2 Factor Authentication
- Security Questions

...More Confusion ...More Work ...More Money

161

Here's Why [Insert Thing Here] Is Not a Password Killer

05 NOVEMBER 2018

Every single solution I've seen that claims to "solve the password problem" ***just adds another challenge in its place thus introducing a new set of problems.***

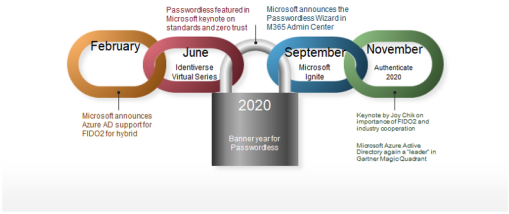
This is why [insert thing here] is not a password killer and why, for the foreseeable future, we're just going to have to continue getting better at the one authentication scheme that everyone knows how to use: passwords.

https://www.troyhunt.com/heres-why-insert-thing-here-is-not-a-password-killer/

162

Microsoft: Next steps for passwordless in 2021

Our team has been working hard this year to join these partners in making passwords a thing of the past. Along with new UX and APIs for managing FIDO2 security keys enabling customers to develop custom solutions and tools, we plan to release a converged registration portal in 2021, where all users can seamlessly manage passwordless credentials via the My Apps portal.



https://www.microsoft.com/security/blog/2020/12/17/a-breakthrough-year-for-passwordless-technology/

163

Securing The "Things"

164

165

It's not about what's most secure…
it's about what the bad guys focus on

166

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS

*INTERNET OF SH*T —*

When coffee makers are demanding a ransom, you know IoT is screwed

Watch along as hacked machine grinds, beeps, and spews water.

DAN GOODIN - 9/26/2020, 10:58 AM

Additionally, this case also demonstrates one of the most concerning issues with modern IoT devices: **"The lifespan of a typical fridge is 17 years, how long do you think vendors will support software for its smart functionality?"** Sure, you can still use it even if it's not getting updates anymore, but with the pace of IoT explosion and bad attitude to support, we are creating an army of abandoned vulnerable devices that can be misused for nefarious purposes such as network breaches, data leaks, ransomware attack and DDoS.

https://arstechnica.com/information-technology/2020/09/how-hacker-turned-a-250-coffee-maker-into-ransom-machine/

167

Share of IoT infections has increased by 100%

IoT devices now make up 32.72% of the infected devices observed. Compared with 2019, the share occupied by IoT devices in the overall device breakdown has increased by 100%, from a previous share of 16.17%.

With the widespread proliferation of IoT devices, it is to be expected that the number of IoT infections will grow dramatically. As Figure 3 demonstrates, in 2020 this led to the increase of the share that IoT infections have in the overall device breakdown.

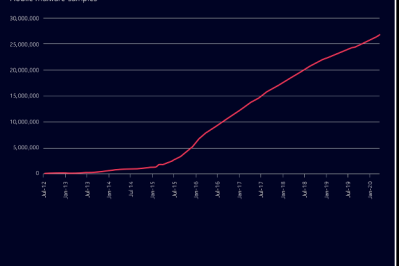
The rate of success in infecting IoT devices depends dramatically with the visibility of the devices to the internet. In networks where devices are routinely assigned public facing internet IP addresses, we find a high IoT infection rate. In networks where carrier grade NAT is used, the infection rate is considerably reduced, because the vulnerable devices are not visible to network scanning.

With the introduction of 5G well underway, it is expected that not only the number of IoT devices will increase dramatically, but also the share of IoT devices accessible directly from the internet will increase as well. A separate section of this report analyzes the security challenges in the 5G environment and highlights the important role that Threat Intelligence can play in addressing security issues in multiple systems of the 5G architecture.

Android malware samples continue to grow in 2020

Figure 4 shows the increase in the mobile malware samples that were collected and analyzed in the Threat Intelligence Lab. There are now close to 27 million Android malware samples, which represents a 17.4% year-over-year increase.

Figure 4. Mobile malware samples in Threat Intelligence Lab's database



9 Threat Intelligence Report 2020

Nokia_Threat_Intelligence_Report_2020_Report_EN.pdf

168

How Do You Know If You Are Infected?

- Fans Spinning Wildly
- Programs start unexpectedly
- Your firewall yells at you
- Odd emails FROM you
- Freezes
- Your browser behaves funny
- Sudden slowness
- Change in behavior
- Odd sounds or beeps
- Random Popups
- Unwelcome images
- Disappearing files
- Random error messages

169

How Do You Know If You Are Infected?

- Fans Spinning Wildly
- Programs start unexpectedly
- Your firewall yells at you
- Odd emails FROM you
- Freezes
- Your browser behaves funny
- Sudden slowness
- Change in behavior
- Odd sounds or beeps
- Random Popups
- Unwelcome images
- Disappearing files
- Random error messages

You Don't

170

Your Browser Goes Rogue
If your browser has acquired new Toolbars/Extensions that you didn't install

People Receive Fraudulent Invitations/Emails From You
Threat actors set up fraudulent and copycat profiles on social media platforms and send invitations to the friends of the person with the real profile, or they gain access to the real profile probably through a phishing attack.

Passwords Mysteriously Change
If you cannot log in to an online service or platform, make sure the service is operational.

Software Materializes On Your Computer
If software appears on your computer and you have no idea where it came from, it might be enemy action.

The Cursor Flies Solo
A moving mouse pointer without your hand on the mouse may indicate hardware issues or be due to "drift" in the software drivers.

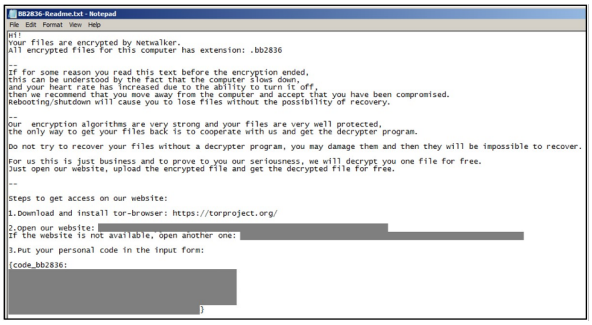
Your Shields Are Down And Won't Come Up
If your defensive software such as personal firewall, anti-virus, and anti-malware are turned off and refuse to come back into service, you've been infected with a virus or other malware.

Your Own Systems Tell You So
Any and all alerts from your intrusion detection system (IDS) or other monitoring software should be treated as genuine incidents until an investigation proves otherwise.

https://www.cloudsavvyit.com/7259/have-you-been-hacked-10-indicators-that-say-yes/

171

172



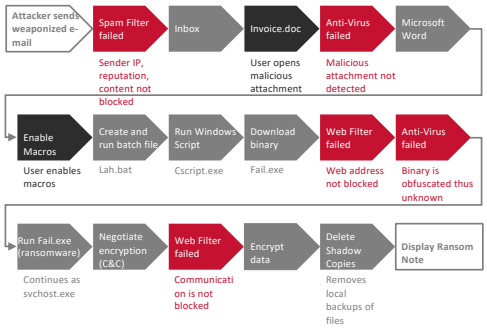
173

Your antivirus software is a seat belt – not a force field.

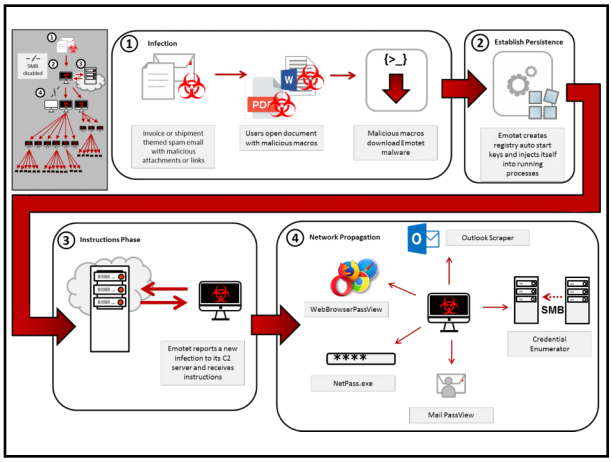
- *Alfred Huger*

174

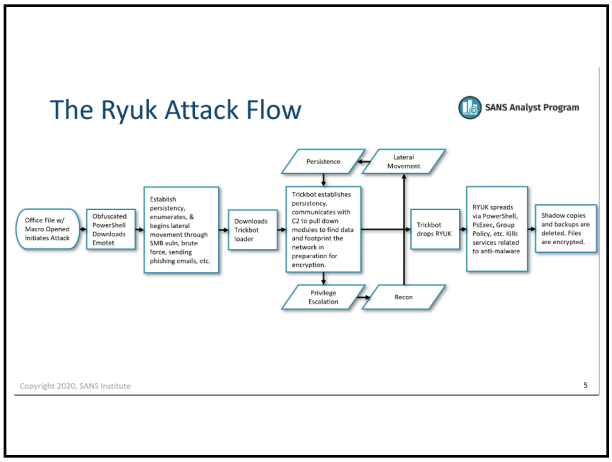
Infection Flow



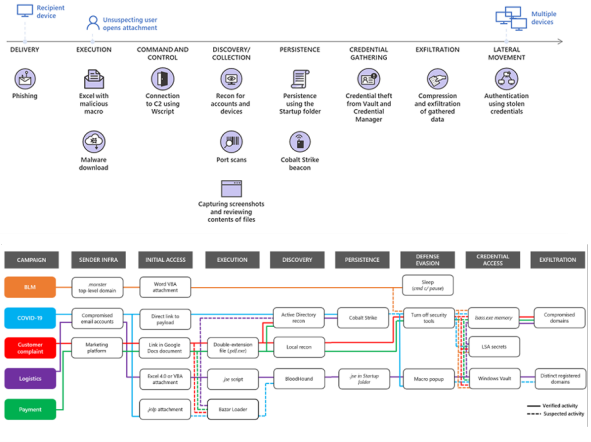
175



176



177



178

Phishing

IT experts...

The expert... **tries to make sense of the email**, and understand how it relates to other things in their life. As they do this, they notice discrepancies: little things that are "off" about the email. As the recipient notices more discrepancies, they feel a need for an alternative explanation for the email. At some point, some feature of the email — usually, the presence of a link requesting an action — triggers them to recognize that phishing is a possible alternative explanation.

At this point, **they become suspicious** (stage two) and investigate the email by looking for technical details that can conclusively identify the email as phishing.

Once they find such information, then they move to stage three and **deal with the email by deleting it or reporting it**.

https://dl.acm.org/doi/10.1145/3415231

179

Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender

Lee Hadlington, Jens Binder, and Natalia Stanulewicz

Published Online: 10 Jul 2020 https://doi.org/10.1089/cyber.2019.0703

Abstract

The role of human factors in employee information security awareness (ISA) has garnered increased attention, with many researchers highlighting a potential link between problematic technology use and poorer online safety and security. This study aimed to present additional evidence for this by exploring the relationship between of Fear of Missing Out (FoMO) and ISA in employees. A total of 718 participants completed an online questionnaire that included a measure of FoMO, ISA, as well as the Big Five personality inventory. Participants who reported higher levels of FoMO had lower overall ISA, as well as having poorer knowledge, a more negative attitude, and engaged in riskier behaviors in relation to ISA. **FoMO was also demonstrated to be the largest single negative predictor for ISA**, above that of age, gender, and the key personality traits tested. The potential reasons for the influence of FoMO over ISA are discussed, as well as the implications for organizational information security.

180

Locking Down Computers

- Keep Things Updated
  - The Operating System
  - All Applications (Browsers!)
- Application Allowlisting (whitelisting)
- Reboot to restore
- Secure Microsoft Office Macros
- Don't use Windows?
- What About Anti-virus Applications?

181

12,970 views | Dec 9, 2019, 09:13am

Are You One Of Avast's 400 Million Users? This Is Why It Collects And Sells Your Web Habits.

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Avast, the multibillion-dollar Czech security company, doesn't just make money from protecting its 400 million users' information. It also profits in part because of sales of users' Web browsing habits and has been doing so since at least 2013.

182

Securing The Other "Things" We use

183

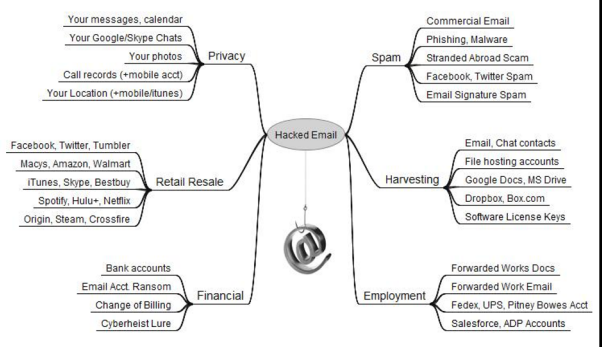
Which of your online accounts is most valuable?

- Email
- Bank
- Social Network
- Shopping
- Gaming
- Blogs

184

Own the Email, Own the Person

185



186

Second Factor Authentication

187

Types of additional information

Who you are | What you have | What you know

Google | Security and Privacy Group

188

Not all 2FA technologies are equal

	Secondary email	SMS verification	Device prompt	Security key
Boutique phishing	68%	96%	99%	100%
Spear-phishing	53-100%	76%	90%	100%

Evaluating Login Challenges as a Defense Against Account Takeover - WWW19

Google | Security and Privacy Group

189

The Consumer Authentication Strength Maturity Model (CASMM)

1	Token2FA	**Token-based 2FA** *Examples: Yubikey, RSA Token* In addition to quality passwords in a manager, you authenticate using a physical token that only you have.	VULNERABLE TO: TOKEN KEY SYSTEM COMPROMISE LIVE SOCIAL ENGINEERING
2	App2FA	**App-based 2FA** *Examples: Google Authenticator, Authy* In addition to quality passwords in a manager, you authenticate using an application that only you can access.	VULNERABLE TO: LIVE SOCIAL ENGINEERING MOBILE DEVICE COMPROMISE
3	SMS2FA	**SMS-based 2FA** *Examples: Any SMS-based auth* In addition to quality passwords in a manager, you authenticate using a text sent to your mobile device.	VULNERABLE TO: SIM-SWAPPING SMS-HIJACKING ATTACKS
4	Password Manager	**Password Manager** *Examples: 1Password, LastPass* In addition to having unique passwords, you also store them securely in an encrypted archive.	VULNERABLE TO: ACCOUNT RESET/TAKEOVER
5	Quality Passwords	**Quality Passwords** *Examples: A0!2-2vOo-?1sM.* Your passwords are not just unique, but they're long, random, and they include special characters.	VULNERABLE TO: PASSWORD DUMPS / CRACKING
6	Unique Passwords	**Unique Passwords** *Examples: DOBs, Towns, Schools* Your passwords are unique, but they're too short, simple, or contain personal information.	VULNERABLE TO: LIVE PASSWORD GUESSING
7	Shared Passwords	**Shared Passwords** *Examples: Gmail, Wells Fargo, Netflix* You use the same password in multiple places across the internet.	VULNERABLE TO: CREDENTIAL STUFFING

DANIEL MIESSLER 2021

https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model-2/

190

Hacking

A Hacker Got All My Texts for $16

A gaping flaw in SMS lets hackers take over phone numbers in minutes by simply paying a company to reroute text messages.

By Joseph Cox

Looking down at my phone, there was no sign it had been hacked. I still had reception; the phone said I was still connected to the T-Mobile network. Nothing was unusual there. But the hacker had swiftly, stealthily, and largely effortlessly redirected my text messages to themselves. And all for just $16.

I hadn't been SIM swapped, where hackers trick or bribe telecom employees to port a target's phone number to their own SIM card. Instead, the hacker used a service by a company called Sakari, which helps businesses do SMS marketing and mass messaging, to reroute my messages to him. This overlooked attack vector shows not only how unregulated commercial SMS tools are but also how there are gaping holes in our telecommunications infrastructure, with a hacker sometimes just having to pinky swear they have the consent of the target.

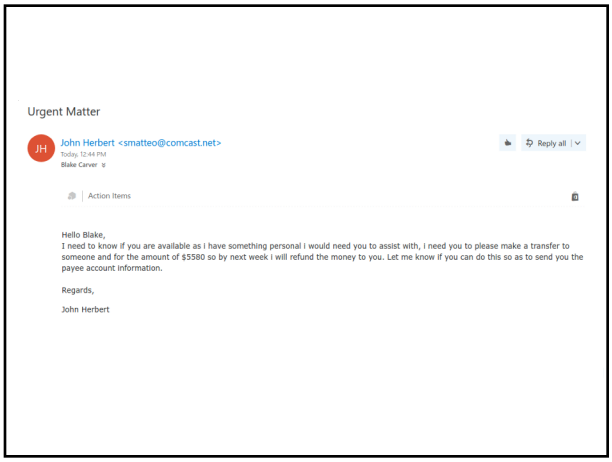
https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

191

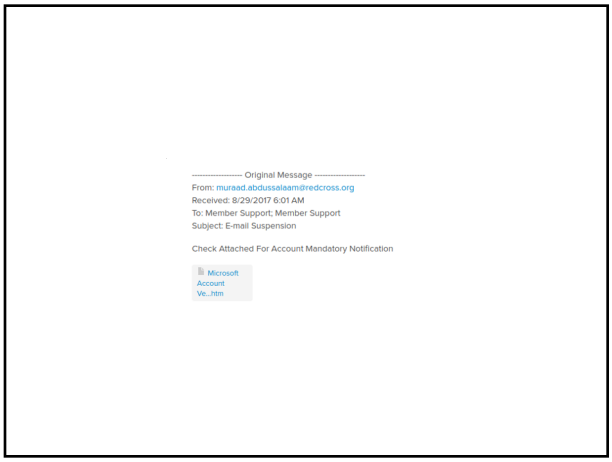
Phishing:

Fake email, telephone or text messages

192


Urgent Matter
JH
John Herbert <smatteo@comcast.net>
Today, 12:44 PM
Blake Carver
Reply all
Action Items
Hello Blake,
I need to know if you are available as i have something personal i would need you to assist with, i need you to please make a transfer to someone and for the amount of $5580 so by next week i will refund the money to you. Let me know if you can do this so as to send you the payee account information.
Regards,
John Herbert

193

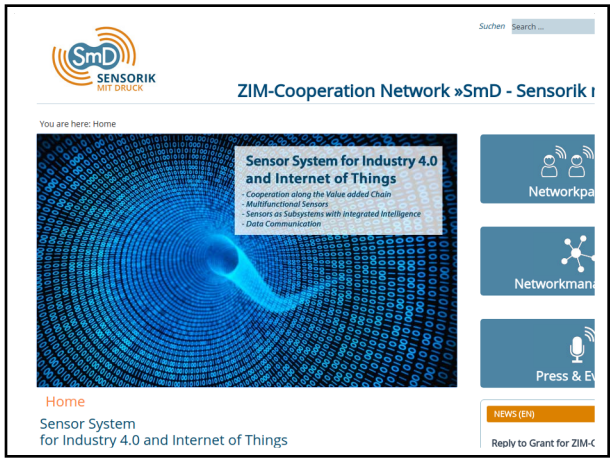

---------- Original Message ----------
From: muraad.abdussalaam@redcross.org
Received: 8/29/2017 6:01 AM
To: Member Support; Member Support
Subject: E-mail Suspension
Check Attached For Account Mandatory Notification
Microsoft Account Ve...htm

194


of the below and protect your mailbox </p>
<table width="100%" style="font-family: calibri; letter-spacing: normal; orphans: 2; text-indent: 0px; text-transform: none; widows: 2; word-spacing: 0px; -webkit-te
rgb(255, 255, 255); text-decoration-style: initial; text-decoration-color: initial;">
<tr>
<td width="50%" align="left">
<a rel="nofollow" target="_blank" style="width: 223px; display: block; float: left; height: 41px; color: rgb(255, 255, 255); font-size: 15px; font-weight: bo
padding: 10px; background: green" href="http://www.
CONFIRM ACCOUNT VERIFICATION</td>
<td width="50%" align="left">

<a rel="nofollow" target="_blank" style="width: 107px; display: block; float: left; height: 41px; color: rgb(255, 255, 255); font-size: 15px; font-weight
padding: 10px; background: red" href="http://www.
VISIT ACCOUNT DASHBOARD
</td>
</tr>
</table>
<p style="color: rgb(0, 0, 0); font-family: calibri; font-size: 15px; font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; font-weight: nor

195



196

Email

- Don't trust anything
- Don't leave yourself logged in
- 2 Factor Authentication
- Passwords
- Email is not a secure storage facility
- OpenPGP

197

Surfing The Web

198

The majority of encounters happen in the places that online users visit the most—and think are safe.

2013 Cisco Annual Security Report

199

Browsers

- Use Two & Keep Updated
- Know Your Settings
  - –Phishing & Malware Detection - Turned ON
  - –Software Security & Auto / Silent Patching - Turned **ON**
- A Few Recommended Extensions:
  - –Something to Limit JavaScript
  - –Something to Force HTTPS
  - –Something to stop trackers
  - –Something to Block Ads

200

Privacy Badger

uBlock Origin

uMatrix
???

HTTPS Everywhere

Disconnect

BROWSER

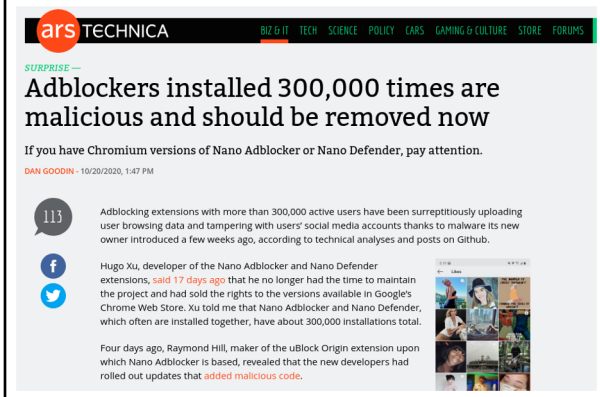
Ghostery

201

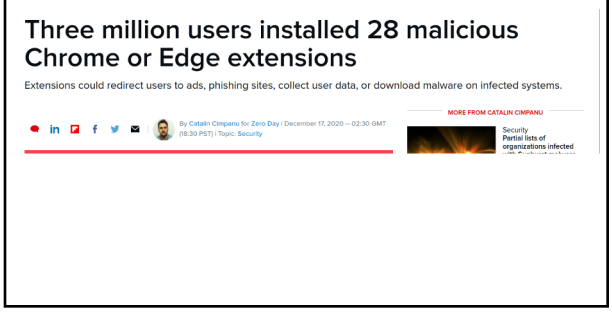
But The Internet Is Free Because Of Ads...

- Malicious content is 27 times more likely to be encountered via search engines than counterfeit software
- Online ads were 182 times more likely to deliver malware than an adult site

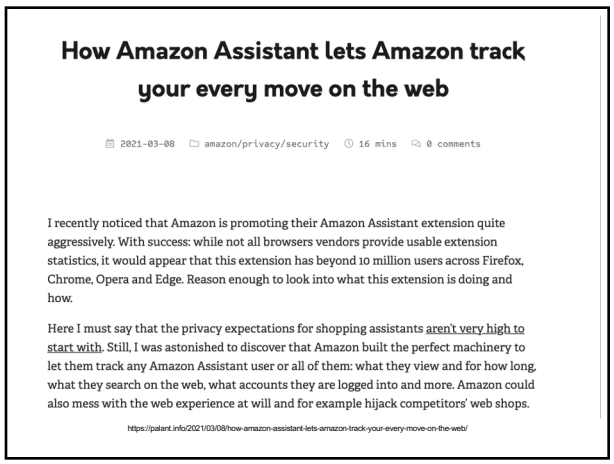
202



203



204



How Amazon Assistant lets Amazon track your every move on the web

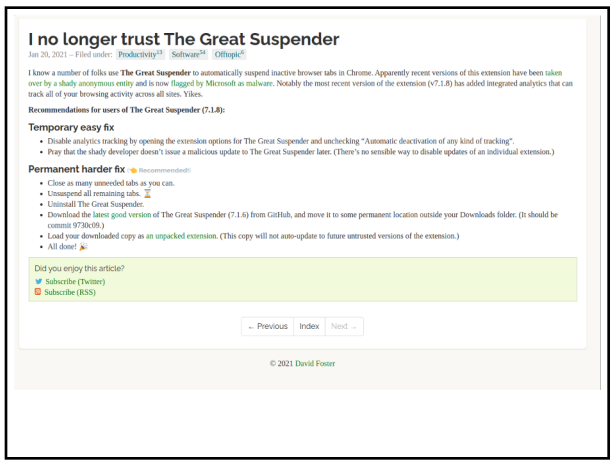
2021-03-08 amazon/privacy/security 16 mins 0 comments

I recently noticed that Amazon is promoting their Amazon Assistant extension quite aggressively. With success: while not all browsers vendors provide usable extension statistics, it would appear that this extension has beyond 10 million users across Firefox, Chrome, Opera and Edge. Reason enough to look into what this extension is doing and how.

Here I must say that the privacy expectations for shopping assistants aren't very high to start with. Still, I was astonished to discover that Amazon built the perfect machinery to let them track any Amazon Assistant user or all of them: what they view and for how long, what they search on the web, what accounts they are logged into and more. Amazon could also mess with the web experience at will and for example hijack competitors' web shops.

https://palant.info/2021/03/08/how-amazon-assistant-lets-amazon-track-your-every-move-on-the-web/

205



I no longer trust The Great Suspender

Jun 20, 2021 – Filed under: Productivity[13] Software[54] Offtopic[6]

I know a number of folks use **The Great Suspender** to automatically suspend inactive browser tabs in Chrome. Apparently recent versions of this extension have been taken over by a shady anonymous entity and is now flagged by Microsoft as malware. Notably the most recent version of the extension (v7.1.8) has added integrated analytics that can track all of your browsing activity across all sites. Yikes.

Recommendations for users of The Great Suspender (7.1.8):

Temporary easy fix

- Disable analytics tracking by opening the extension options for The Great Suspender and unchecking "Automatic deactivation of any kind of tracking".
- Pray that the shady developer doesn't issue a malicious update to The Great Suspender later. (There's no sensible way to disable updates of an individual extension.)

Permanent harder fix Recommended!

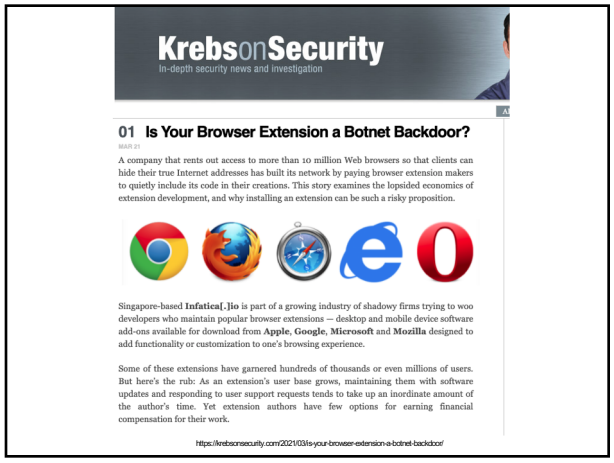
- Close as many unneeded tabs as you can.
- Unsuspend all remaining tabs. ⏳
- Uninstall The Great Suspender.
- Download the latest good version of The Great Suspender (7.1.6) from GitHub, and move it to some permanent location outside your Downloads folder. (It should be commit 973fc09.)
- Load your downloaded copy as an unpacked extension. (This copy will not auto-update to future untrusted versions of the extension.)
- All done! 🎉

Did you enjoy this article?
Subscribe (Twitter)
Subscribe (RSS)

← Previous Index Next →

© 2021 David Foster

206



KrebsonSecurity
In-depth security news and investigation

01 Is Your Browser Extension a Botnet Backdoor?

MAR 21

A company that rents out access to more than 10 million Web browsers so that clients can hide their true Internet addresses has built its network by paying browser extension makers to quietly include its code in their creations. This story examines the lopsided economics of extension development, and why installing an extension can be such a risky proposition.

Singapore-based **Infatica[.]io** is part of a growing industry of shadowy firms trying to woo developers who maintain popular browser extensions — desktop and mobile device software add-ons available for download from **Apple**, **Google**, **Microsoft** and **Mozilla** designed to add functionality or customization to one's browsing experience.

Some of these extensions have garnered hundreds of thousands or even millions of users. But here's the rub: As an extension's user base grows, maintaining them with software updates and responding to user support requests tends to take up an inordinate amount of the author's time. Yet extension authors have few options for earning financial compensation for their work.

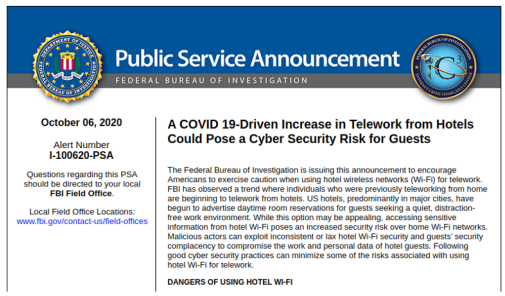
https://krebsonsecurity.com/2021/03/is-your-browser-extension-a-botnet-backdoor/

207

Never Trust Public Wi-Fi

Use A PAID VPN

208



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 06, 2020

Alert Number
I-100620-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

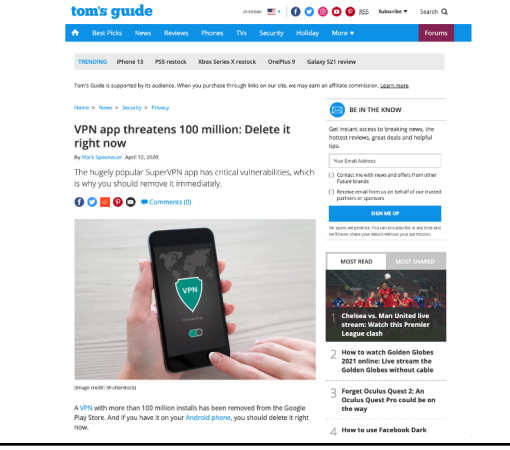
Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

A COVID 19-Driven Increase in Telework from Hotels Could Pose a Cyber Security Risk for Guests

The Federal Bureau of Investigation is issuing this announcement to encourage Americans to exercise caution when using hotel wireless networks (Wi-Fi) for telework. FBI has observed a trend where individuals who were previously teleworking from home are beginning to telework from hotels. US hotels, predominantly in major cities, have begun to advertise daytime room reservations for guests seeking a quiet, distraction-free work environment. While this option may be appealing, accessing sensitive information from hotel Wi-Fi poses an increased security risk over home Wi-Fi networks. Malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests. Following good cyber security practices can minimize some of the risks associated with using hotel Wi-Fi for telework.

DANGERS OF USING HOTEL WI-FI

209



tom's guide

Best Picks | News | Reviews | Phones | TVs | Security | Holiday | More | Forums

TRENDING iPhone 13 | PS5 restock | Xbox Series X restock | OnePlus 9 | Galaxy S21 review

Tom's Guide is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more

Home > News > Security > Privacy

VPN app threatens 100 million: Delete it right now

By Mark Spoonauer April 10, 2020

The hugely popular SuperVPN app has critical vulnerabilities, which is why you should remove it immediately.

Comments (0)

(Image credit: Shutterstock)

A VPN with more than 100 million installs has been removed from the Google Play Store. And if you have it on your Android phone, you should delete it right now.

BE IN THE KNOW

Get instant access to breaking news, the hottest reviews, great deals and helpful tips.

Your Email Address

Contact me with news and offers from other Future brands

Receive email from us on behalf of our trusted partners or sponsors

SIGN ME UP

MOST READ | MOST SHARED

1 Chelsea vs. Man United live stream: Watch this Premier League clash

2 How to watch Golden Globes 2021 online: Live stream the Golden Globes without cable

3 Forget Oculus Quest 2: An Oculus Quest Pro could be on the way

4 How to use Facebook Dark

210

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action

Why Public Wi-Fi is a Lot Safer Than You Think

BY JACOB HOFFMAN-ANDREWS | JANUARY 29, 2020

The advice stems from the early days of the Internet, when most communication was not encrypted. At that time, if someone could snoop on your network communications—for instance by sniffing packets from unencrypted Wi-Fi or by being the NSA—they could read your email. They could also steal your passwords or your login cookies and impersonate you on your favorite sites. This was widely accepted as a risk of using the Internet. Sites that used HTTPS on all pages were safe, but such sites were vanishingly rare.

However, starting in 2010 that all changed. Eric Butler released Firesheep, an easy-to-use demonstration of "sniffing" insecure HTTP to take over people's accounts. Site owners started to take note and realized they needed to implement HTTPS (the more secure, encrypted version of HTTP) for every page on their site. The timing was good: earlier that year, Google had turned on HTTPS by default for all Gmail users and reported that the costs to do so were quite low. Hardware and software had advanced to the point where encrypting web browsing was easy and cheap.

211

Social Media

- Understand and adjust your privacy settings
- Be skeptical of everything –especially ANYONE asking you for money

212

Free Services Are Expensive

"...if you're not the customer you're the product being sold"

metafilter.com/95152

Staying Safe Online

213

Mobile Devices - Threats

- Trojans, Viruses & Malware
- Lost and/or Stolen
- Opaque Apps Permissions
- Access To Everything
- Open Wi-Fi Networks and Public Hotspots
- Data leakage
- Insecure Wi-Fi
- Network spoofing
- Phishing and social engineering attacks
- Spyware
- Poor cyber hygiene, including weak passwords and improper or no use of multifactor authentication (MFA)
- Poor technical controls, such as improper session handling, out-of-date devices and operating systems, and cryptographic controls

214

Mobile / Portable / Cellular

Solid Operating Systems
Encrypted
Super Secure Hardware (secure enclave)
End to end secure apps available
Biometrics

215

But...

Endless Apps means endless points of insecurity

OS design can hide really bad practices

lack of TLS, client app no longer validates certs, bad coding, basic security stuff

You don't see it in the UI

216

The privacy is even worse...

More apps collecting more stuff storing it in more places and sharing widely

217

Current attacks are generally tough & against High Value Targets

High value most often means rich financial gains for the threat actors.

They require significant financial backing, top-tier technical skills, a lot of man-power, and operational guidance and control.

Riskware is the name used for free apps that offer to do something entertaining or useful—and actually deliver on that promise—but secretly siphon off information and send it back to the app publishers to be sold to advertisers or criminals.

- Smishing Attacks
- Loss / Swiper got swiped
- SIM Swapping
- Public Wi-Fi and Network Spoofing

https://www.cloudsavvyit.com/8514/why-cyber-criminals-love-cellphones/

218

Set up a mobile carrier PIN

SIM hijacking is a process where a hacker socially engineers or bribes a mobile carrier to transfer your phone number to a SIM card they own.

If you use text messages as a two-factor authentication method, this gives hackers the ability to bypass 2FA and in most cases the ability to reset your passwords completely.

219

Mobile Devices

1. Encrypt it
2. Password it
3. Backup it
4. Case it
5. Know those settings
6. Watch your Wifi
7. It is not forever

220

How do you know if you have malware on your phone?

- You see ads all the time.
- You install an app and it disappears immediately.
- Your battery drains much faster than usual.
- You see apps that you don't recognize.
- Data usage through the roof.
- Random charges on your phone bill.
- Slow.
- Your friends get weird messages/emails from you

221

Carry A Safe
Not A Suitcase

222

Cybersecurity

Week Three

223

Making Your Library Defensible & Resilient

224

Able To Be Defended

- **Defensible** does not mean secure
- There are more things to defend than there are resources to defend with
- Defensibility focuses on what, why, how, when and from whom

225

Defensible

A change in mindset
Awareness of limitations & weaknesses
Awareness of threats
An admission of inconvenience
A lot of hard, detailed work.

226

Cyber Resilience

Your ability to keep operating when bad things happen to your IT.

The ability to withstand all types of cyber events.

- Prevention
- Detection
- Containment
- Response

227

What's security?

Gets in the way for patrons & fails for administrators

For us, it's critical

So it's important for us to remember what others think

We need to keep in mind how security affects users

228

What's security?

This is more than just tech, it's about

1. People
2. Processes
3. Technology

In the end, we want to have trained people using solid technology

We can't afford a security team, or even a person, we can't afford a databareach or ransomware either

229

"Security is always excessive until it's not enough."

Robbie Sinclair, Head of Security, Country Energy, NSW Australia

230

We've been thinking…

- What do we have to secure?
- Who wants it?
- How could they acquire it?
- How could they benefit from its use?
  - –Can they sell it?
  - –Can they hold it hostage?
  - –Can they use & abuse it?
- How damaging would the loss of data be?
- How would this change operations?
- How secure do we really need to be?

231

What's Plugged In?

It's important to know what you have & when it should be renewed

Identifying your assets needs to be a regular exercise

Shadow IT, forgotten things, outdated things, you need to know what's around the library.

Knowing what you have will **hopefully** lead to getting new stuff.
Getting new stuff is important from a security standpoint.

How's that budget looking!?

Are cloud hosted things better at being updated? You don't host it, you don't need to update it?

Our risk tolerance keeps getting higher because we can't afford to buy new stuff. Keep putting it off.
There's always a good reason to put it off

cost, time, expertise, capability, influence (how do YOU influence it to get done)

232

Change Management

When a business begins to use a change information resource (software, hardware, networks, system documentation, and operating procedures and environment) for any reason, it should be managed according to a specific process called a "control process" fixed in advance so that the transition is accomplished in an organized way in all its steps from the review to the authorization, test, implementation, and release of the changed resource.

In addition to the change management procedures, the control process should assign responsibilities and authorities to all the business staff involved.

https://resources.infosecinstitute.com/certification/change-management-cissp/

233

Think Like A Bad Guy

1. What useful information can I see about a target from the outside? (Enumerability)
2. How valuable is this asset to the adversary? (Criticality)
3. Is the asset known to be exploitable? (Weakness)
4. How hospitable will this asset be if I pwn it? (Post-exploitation potential)
5. How long will it take to develop an exploit? (Research potential)
6. Is there repeatable ROI developing an exploit? (Applicability)

https://threatpost.com/6-questions-attackers-ask-exploit/162651/

234

But We’re Just A Small Library!

235

You can’t assume no one cares about what is in your library

236

We (*libraries*) are targets because we're large (*ish*) and complex (*ish*) and hard to defend, often we are part of larger organizations, (*city/county*, *campus*), and those other things could have way more than just the library that's way more valuable

237

83% targets of opportunity
92% of attacks were easy
85% were found by a 3rd party

Every Single Security Report Ever

238

It's Easier Being Bad

239

Security Is More Difficult

240

The attacker only needs to succeed once…
or just keep trying

241

While we need to catch every single thing...

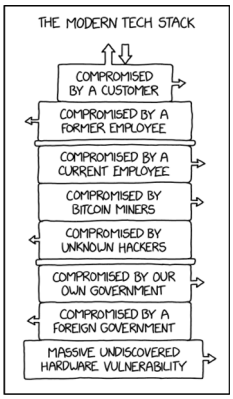
242

"In security, you almost never go from making something possible to impossible… You go from making it easy to making it hard…"

We want to make things hard on the bad guys.

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

243



https://xkcd.com/2166/

244

Libraries Live Below The Security Poverty Line

(Wendy Nather)

We simply can't afford to reach a great level of security

Few or no IT People
Few or no Security People
Hard to keep up with technology and security
Maintenance, planning, strategy are 2nd to OMG
Depend on consultants, vendors, family, patrons, friends, volunteers, etc...

245

Staying safe takes more than just a firewall & AV/AM...

246

247

Your security software / hardware is a seat belt – not a force field.

248

What is the most important stuff in your library?

What can you not live/work/function without?

Is there only one thing?

249

1. Know your organization

2. Know your threats. Know what's happened in your library, your neighbors, all over the world. Keep current. Ask around.

3. Prioritize. Match up what you see and hear with what you have. Give it some thought and time.

4. Review and improve. Build a real model and plan. Recommendations and costs and time

250

Step 1 – Inventory & Prioritize

Step 2 – What could go wrong?

Step 3 – How is it Protected, how could we do better?

251

An attacker will always pick the weakest point of entry…

…but you can't know which point that is

252

The Weakest Point In A Library?

253

254

Public Access Computers

255

Public Access Computers

Staying Safe On This Computer:

- **Make Sure You Log Out**
- **Don't Access Sensitive Sites**
- **Beware of the "remember me" option**
- **Don't send personal or financial information via email or insecure websites**

256

Public Access Computers

This Week's Stay Safe Tips

- **Never Trust Email**
- **Learn About Phishing**
- **Attend Our Security Class**
- **Always Check For A Secure Connection**

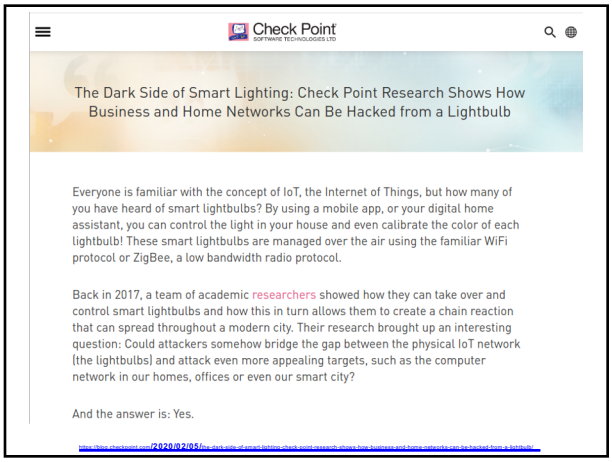
257

What Do We Need To Protect?

Staff Computers	Cell Phones
Databases	Wi-Fi Routers
Printers / Copiers	Routers
Website	Cell Phones
Servers	Tablets
Backups	Laptops
Toasters	Lightbulbs

Your Employees Homes / Phones / etc...?

258



Check Point
SOFTWARE TECHNOLOGIES LTD

The Dark Side of Smart Lighting: Check Point Research Shows How Business and Home Networks Can Be Hacked from a Lightbulb

Everyone is familiar with the concept of IoT, the Internet of Things, but how many of you have heard of smart lightbulbs? By using a mobile app, or your digital home assistant, you can control the light in your house and even calibrate the color of each lightbulb! These smart lightbulbs are managed over the air using the familiar WiFi protocol or ZigBee, a low bandwidth radio protocol.

Back in 2017, a team of academic researchers showed how they can take over and control smart lightbulbs and how this in turn allows them to create a chain reaction that can spread throughout a modern city. Their research brought up an interesting question: Could attackers somehow bridge the gap between the physical IoT network (the lightbulbs) and attack even more appealing targets, such as the computer network in our homes, offices or even our smart city?

And the answer is: Yes.

https://blog.checkpoint.com/2020/02/05/the-dark-side-of-smart-lighting-check-point-research-shows-how-business-and-home-networks-can-be-hacked-from-a-lightbulb/

259

Cybersecurity

Hackers Breach Thousands of Securit Cameras, Exposing Tesla, Jails, Hospit

By William Turton
March 9, 2021, 4:32 PM EST *Updated on March 10, 2021, 11:35 AM EST*

- Hacker group says it wanted to show prevalence of surveillance
- Video footage was captured from Sequoia-backed startup Verkada

SHARE THIS ARTICLE
Share
Tweet
Post
Email

In this article

163991D
VERKADA INC
Private Company

TSLA
TESLA INC
694.77 USD

A group of hackers say they breached a massive trove of security-camera data collected by Silicon Valley startup Verkada Inc., gaining access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons and schools.

Companies whose footage was exposed include carmaker Tesla Inc. and software provider Cloudflare Inc. In addition, hackers were able to view video from inside women's health clinics, psychiatric hospitals and the offices of Verkada itself. Some of the cameras, including in hospitals, use facial-recognition technology to identify and categorize people captured on the footage. The hackers say they also have access to the full video archive of all Verkada customers.

https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams

260

Remote Work / Working From Home

Thanks 2020!

Working from home means that employees:

- Will need to be able to access systems that were intended for internal use only
- Will heavily use video conferencing platforms

Assess

- How Are Your Users Working Remotely?
- What Devices Are They Using?
- What Software Are They Using?
- How Do They Connect?
- Do They Manage Sensitive or Protected Data?
- Do They Need Access to Specialized Tools or Line of Business Applications?

261

Remote Work / Working From Home
Thanks 2020!

Secure your identities
- 2FA
- conditional access
- impossible travel - contextually aware
- new devices - contextually aware
- disabling legacy authentication
- Time limits
- Permissions
- SSO

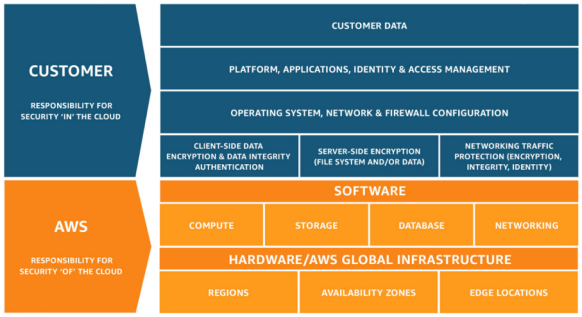
Secure your devices
- Updates
- Passwords
- Settings
- VPN

Secure your data
- Groups and Users
- Data loss prevention

Harden your environments
- Updates
- Password Managers
- Settings
- Training

262

The Cloud



https://aws.amazon.com/compliance/shared-responsibility-model/

263

CSA surveyed 241 experts on security issues in the cloud industry and came up with these top 11 threats:

1. Data breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access, and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

264

Top 10 Cloud Malware Threats

Written by **Intezer** - 16 March 2021

They all target Linux systems

For a long time Linux has not been seen as a serious target of threat actors. This operating system makes up such a small percentage of the desktop market share compared to Windows, it's no surprise why threat actors would focus most of their attention on attacking Windows endpoints.

Times are quickly changing though as the next major battleground moves from traditional on-premise Windows endpoints to Linux-based servers and containers in the cloud. For perspective 90% of the public cloud runs Linux.

Attackers are taking note. Some have started to write new malware from scratch exclusively for Linux, while others are adapting their existing Windows malware to target Linux.

Traditional endpoint protection platforms built to secure Windows are struggling to keep up with Linux threats. If you are in the cloud, make sure you have a security solution compatible with Linux systems, both in terms of threat detection and performance.

Below we highlight 10 Linux malware families targeting the cloud that should be on your radar.

1. TrickBot

265

OSINT

Open Source Intelligence

OSINT is a term that refers to a framework of processes, tools, and techniques for collecting data passively from open or publicly available resources (not to be confused with open-source software). Open source intelligence historically referred to open source information gathering via conventional channels such as newspapers, radio, TV, etc. Nowadays, to extract specific intelligence, we use:

- Blogs,
- Discussion boards,
- Social media,
- The dark web (accessible through TOR), and
- Deep web (pages not indexed by Google like a people search database).

https://osintframework.com/

266

The "Insider Threat" In Libraries

Insider threat program checklist

https://www.ekransystem.com/en/blog/insider-threat-program

267

There are more things to defend than there are resources to defend with

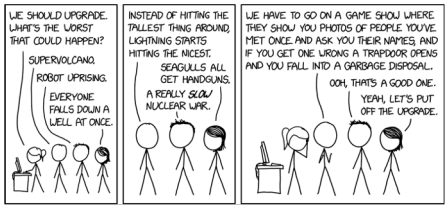
Not every asset in your organization is equally valuable

268

Locking Down Computers

- Patching and Updating
  –OS and *ALL* Applications

269



270

How-To Geek

Windows 10's Bugs Are Teaching the Importance of Backups

CHRIS HOFFMAN @chrisbhoffman
MARCH 31, 2020, 6:40AM EDT

Windows 10 has now had multiple automatic updates that accidentally deleted people's files. Buggy updates have caused problems with hardware drivers, too. Microsoft highlights the importance of having good backups and being prepared for anything.

ADVERTISEMENT

271

Locking Down Computers

- Patching and Updating
  –OS and *ALL* Applications
- Whitelisting
- BIOS passwords
- SteadyState / DeepFreeze / SmartShield
- Check for suspicious USB additions
- Don't use Windows?

272

LEHIGH VALLEY NEWS | NEWS

Ransomware attack temporarily closes Northampton Area Public Library

By ANDREW SCOTT
THE MORNING CALL | NOV 17, 2020 AT 8:20 PM

A ransomware attack forced Northampton Area Public Library to temporarily close, according to a message posted Monday on its website.

"We hope to open to the public soon," the message states. "The affected [computer] servers were taken offline and some library services have already been restored. It may be several days before all library services are fully operational. We are working closely with our IT company to help prevent future attacks. All book drops are open at this time."

The library does not store Social Security numbers or credit card payment information in its computer system, according to the message. Patrons who have used the library's Wi-Fi are advised to change their passwords and regularly monitor their personal information.

LATEST LEHIGH VALLEY NEWS

How the Bethlehem Steel/Chrysler Building myth grew: 65 years passed before steelmaker got credit for skyscraper – by mistake
55m

Send us your Lehigh Valley Christmas light display nominations
2h

MAP: Where coronavirus is in Pennsylvania
NOV 28, 2020

273

ANDROID

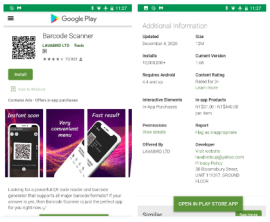
Barcode Scanner app on Google Play infects 10 million users with one update

Posted: February 5, 2021 by Nathan Collier

Late last December we started getting a distress call from our forum patrons. Patrons were experiencing ads that were opening via their default browser out of nowhere. The odd part is none of them had recently installed any apps, and the apps they had installed came from the Google Play store. Then one patron, who goes by username Anon00, discovered that it was coming from a long-time installed app, *Barcode Scanner*. An app that has 10,000,000+ installs from Google Play! We quickly added the detection, and Google quickly removed the app from its store.

Simple scanner turns evil

Many of the patrons had the app installed on their mobile devices for long periods of time (one user had it installed for several years). Then all of sudden, after an update in December, *Barcode Scanner* had gone from an innocent scanner to full on malware! Although Google has already pulled this app, we predict from a cached Google Play webpage that the update occurred on December 4th, 2020.



https://blog.malwarebytes.com/android/2021/02/barcode-scanner-app-on-google-play-infects-10-million-users-with-one-update/

274

Windows security baselines

https://aka.ms/baselines

What are security baselines?

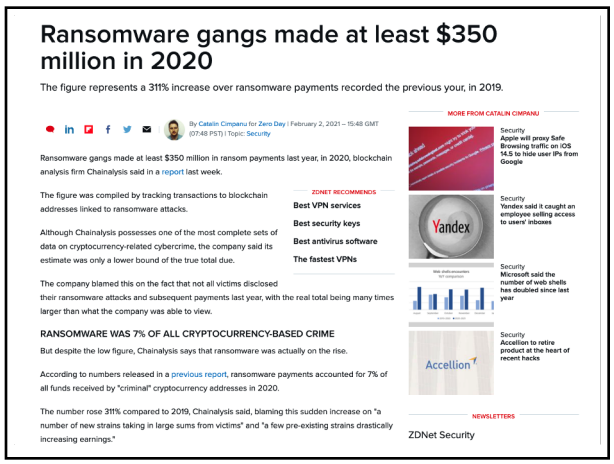
Every organization faces security threats. However, the types of security threats that are of most concern to one organization can be completely different from another organization. For example, an e-commerce company may focus on protecting its Internet-facing web apps, while a hospital may focus on protecting confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must be compliant with the security standards (or security baselines) defined by the organization.

A security baseline is a group of Microsoft-recommended configuration settings that explains their security impact. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

275

Ransomware

276



Ransomware gangs made at least $350 million in 2020

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

By Catalin Cimpanu for Zero Day | February 2, 2021 – 15:48 GMT (07:48 PST) | Topic: Security

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

The figure was compiled by tracking transactions to blockchain addresses linked to ransomware attacks.

Although Chainalysis possesses one of the most complete sets of data on cryptocurrency-related cybercrime, the company said its estimate was only a lower bound of the true total due.

The company blamed this on the fact that not all victims disclosed their ransomware attacks and subsequent payments last year, with the real total being many times larger than what the company was able to view.

ZDNET RECOMMENDS

Best VPN services
Best security keys
Best antivirus software
The fastest VPNs

RANSOMWARE WAS 7% OF ALL CRYPTOCURRENCY-BASED CRIME

But despite the low figure, Chainalysis says that ransomware was actually on the rise.

According to numbers released in a previous report, ransomware payments accounted for 7% of all funds received by "criminal" cryptocurrency addresses in 2020.

The number rose 311% compared to 2019, Chainalysis said, blaming this sudden increase on "a number of new strains taking in large sums from victims" and "a few pre-existing strains drastically increasing earnings."

MORE FROM CATALIN CIMPANU

Security
Apple will proxy Safe Browsing traffic on iOS 14.5 to hide user IPs from Google

Security
Yandex said it caught an employee selling access to users' inboxes

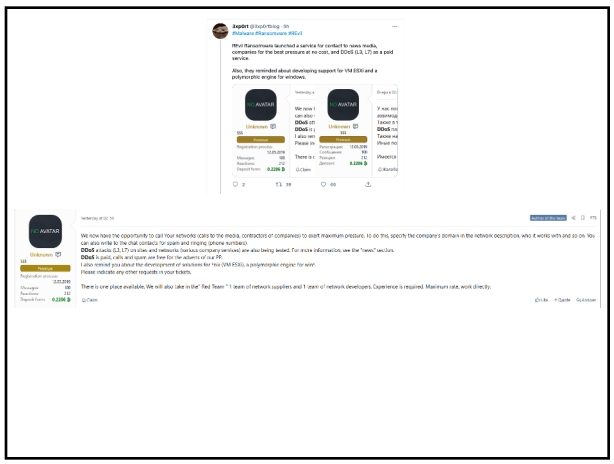
Security
Microsoft said the number of web shells has doubled since last year

Security
Accellion to retire product at the heart of recent hacks

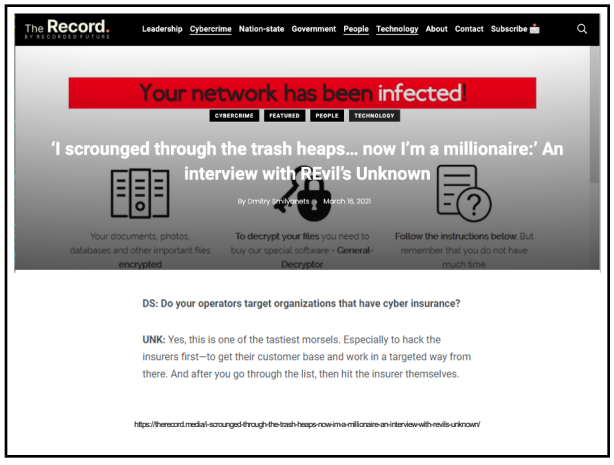
NEWSLETTERS

ZDNet Security

277



278



The Record. BY RECORDED FUTURE

Leadership Cybercrime Nation-state Government People Technology About Contact Subscribe

Your network has been infected!

CYBERCRIME FEATURED PEOPLE TECHNOLOGY

'I scrounged through the trash heaps... now I'm a millionaire:' An interview with REvil's Unknown

By Dmitry Smilyanets | March 16, 2021

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

DS: Do your operators target organizations that have cyber insurance?

UNK: Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves.

https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

279

Never get into a position where you have to pay

Two different types of backups

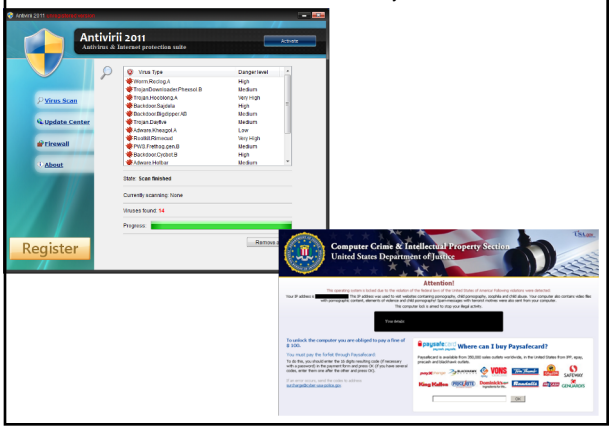
Mulitple network segments

Virtualizing local servers can be better than bare metal?

Remember, backups cover system critical processes as well. How do you do something with no computers? Backups for processes, how do you do it manually.

280

The Good Ol' Days



281

Ransomware is commonly deployed across an environment in two ways:

1. Manual propagation by a threat actor after they have penetrated an environment and have administrator-level privileges broadly across the environment:

- Manually run encryptors on targeted systems.
- Deploy encryptors across the environment using Windows batch files (mount C$ shares, copy the encryptor, and execute it with the Microsoft PsExec tool).
- Deploy encryptors with Microsoft Group Policy Objects (GPOs).
- Deploy encryptors with existing software deployment tools utilized by the victim organization.

2. Automated propagation:

- Credential or Windows token extraction from disk or memory.
- Trust relationships between systems — and leveraging methods such as Windows Management Instrumentation (WMI), SMB, or PsExec to bind to systems and execute payloads.
- Unpatched exploitation methods (e.g., EternalBlue — addressed via Microsoft Security Bulletin MS17-010)

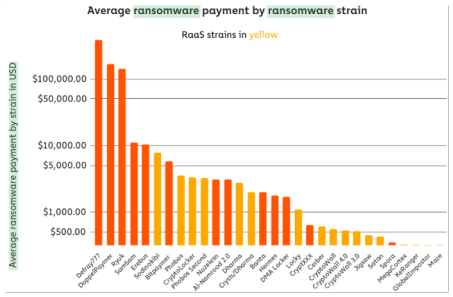
282

Targets of ransomware attacks

There are several reasons attackers first choose what kind of organizations they want to target with ransomware:

- Easy to evade defense. Universities, small companies that have small security teams are an easy target. File sharing and an extensive database make the penetration simple for attackers.
- Possibility of a quick payment. Some organizations are forced to pay a ransom quickly. Government agencies or medical facilities often need immediate access to their data. Law firms and other organizations with sensitive data usually want to keep a compromise a secret.

283



https://krebsonsecurity.com/wp-content/uploads/2020/06/raas-avgprice.png

284

The Hidden Costs

Opportunity Costs

System Downtime

Reduced Efficiency

Brand Damage & Loss of Trust

IP Theft

Incident REsponse

Outside Help

Insurance

Employee and Patron Moral

285

The obvious costs

Paying the ransom doubles the cost of dealing with a ransomware attack.

The average cost to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.) is US$732,520 for organizations that don't pay the ransom, rising to US$1,448,458 for organizations that do pay.

286

10 Reasons Your Library Is Potentially at Risk of a Ransomware Attack

1. Keeping Legacy Systems on the Infrastructure
2. Having Limited Visibility Into Assets and Their Vulnerabilities
3. Forgetting to Implement System Hardening Policies
4. Relying on Perimeter Protection and Antivirus
5. Keeping a Flat Network Topology
6. Relying on Online Backups
7. Exercising Limited Control Over User Access
8. Waiving Security Monitoring and Analytics
9. Underestimating Security Awareness
10. No Incident Response Plan or a Team to Lead It

https://securityintelligence.com/posts/10-reasons-your-organization-is-potentially-at-risk-of-a-ransomware-attack/

287

Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations
- -Know what you have, especially with public IPs
- -Patch/Update
- -Configuration/settings
- -Kill RDP and SMB
- -Settings/Configs
- -Asset / Configuration management

Ransomware Infection Vector: Phishing
- -Train
- -Use good filters
- -User a good providers
- -Kill Office macros
- -2FA
- -Kill powershell

Ransomware Infection Vector: Precursor Malware Infection
- -Good AV
- -Allow Listing
- -IDS/IPS
- -Least Privilege
- -Settings/Configs
- -Asset / Configuration management
- -Harden your Domain Controllers

Ransomware Infection Vector: Third Parties and Managed Service Providers
- -Ask questions
- -Know this is a way in
- -Keep logs
- -Business transaction logging

288

What to do when ransomware is happening:

1. Know Who Is Going To Be In Charge
2. Document EVERYTHING
3. Pull the plugs ASAP. (train people on this, **everyone**)
4. Assume ALL your usernames and passwords are in the wild
5. Identify the Infection
6. Make some calls! Vendors, FBI, Insurance, what about the bad guys?
7. Assess the damage, what's been affected, what is it, what still works, is the virus still growing or hidden, anything have PII
8. Communicate! staff, board, patrons, public? admins, give regular updates
9. Do you need to pay? tough call. When you're in this mess the decision can be very hard. Best to avoid being in this position. Maybe you need something back ASAP.
10. Reinstall your OS and software applications from the source media or the internet. (Make an image of the bad system first)
11. Restore from backups
12. Check and double check e.g. Check your email rules on infected machines

289

Treat the cause, not just the symptoms

Even with the ransomware removed and the system restored from backups, attackers:

- may have backdoor access to the network
- probably have administrator privileges
- could just as easily re-deploy the ransomware if they wanted to

290

Breach Containment

Creating Situational Awareness

Know what's going on

Know what normal looks like

strategies and procedures

Reducing the Attack Surface

strong patch management capabilities

vulnerability scanning

Network segmentation

least privilege

IPS/IDS/DLP

shut down a system, disconnect it from a network, disable certain functions)

291

Protect backups from ransomware!

Put in some roadblocks!

Protect Windows

Most (not all!) ransomware attacks are against Windows, and they spread to other Windows hosts. Try making backups to Linux-based media servers, or MacOS.

Get backups out of the library

Whatever backup solution you choose, copies of backups should be stored in a different location. Send them to the cloud! Cloud object-based storage that can't be changed. The idea is to get your backups—or at least one copy of your backups—as many hops away from an infected Windows system as they can be. Put them in a provider's cloud protected by firewall rules, use a different operating system for your backup servers, and write your backups to a different kind of storage. **(immutable backup)**

Remove file-system access to backups

If your backup system is writing backups to disk, do your best to make sure they are not accessible via a standard file-system directory. For example, the worst possible place to put your backup data is E:\backups. Ransomware products specifically target directories with names like that and will encrypt your backups.

292

Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again

A cautionary tale shows how organisations that fall foul of ransomware should concentrate on finding how it happened before anything else - or they could fall victim again.

By Danny Palmer | February 2, 2021 -- 09:56 GMT (01:56 PST) | Topic: Security

A company that fell victim to a ransomware attack and paid cyber criminals millions for the decryption key to restore their network fell victim to the exact same ransomware gang under two weeks later after failing to examine why the attack was able to happen in the first place.

The cautionary tale is detailed by the UK's National Cyber Security Centre (NCSC) in a blog post about the rise of ransomware.

The unnamed company fell victim to a ransomware attack and paid millions in bitcoin in order to restore the network and retrieve the files.

SEE: Network security policy (TechRepublic Premium)

However, the company just left it at that, failing to analyse how cyber criminals infiltrated the network – something that came back to haunt them when the same ransomware gang infected the network with the same ransomware less than two weeks later. The company ended up paying a ransom a second time.

"We've heard of one organisation that paid a ransom (a little under £6.5million with today's exchange rates) and recovered their files (using the supplied decryptor), without any effort to identify the root cause and secure their network. Less than two weeks later, the same attacker attacked the victim's network again, using the same mechanism as before, and re-deployed their ransomware. The victim felt they had no other option but to pay the ransom again," the NCSC

ZDNET RECOMMENDS

Best VPN services

Best security keys

Best antivirus software

The fastest VPNs

MORE FROM DANNY PALMER

Security: This old form of ransomware has returned with new tricks and new targets

Security: SolarWinds patches three newly discovered software vulnerabilities

Security: Ransomware payments are going down as more victims decide not to pay up

Security: Ransomware gangs now have industrial targets in their sights. That raises the stakes for everyone

NEWSLETTERS

ZDNet Security

https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/

293

A key cog in this growing operation is the interdependency between those who specialize in selling access to compromised systems or stolen information, and those looking to launch ransomware attacks.

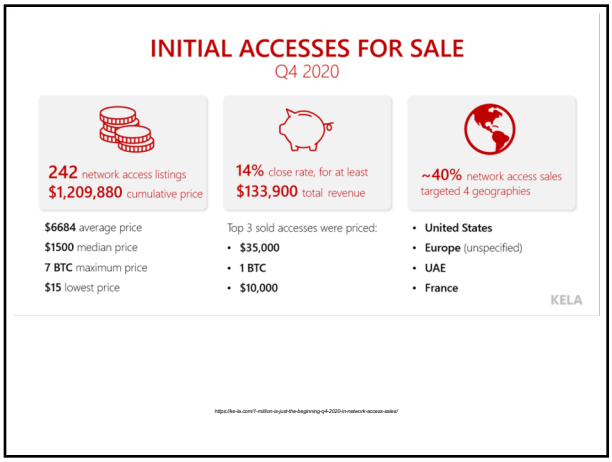
Data gathered by Intel 471 points to a pattern in numerous ransomware attacks that have occurred in the past 18 months: Criminals in underground forums will advertise access to various breached organizations, and quickly turn to sell access to the highest bidder or strike a deal with an ransomware affiliate in order to share in any profits pulled from a successful payment.

These partnerships have resulted in a flourishing submarket, where access to corporate networks is sold for six-figure sums directly or via a partnership and cut of paid ransoms.

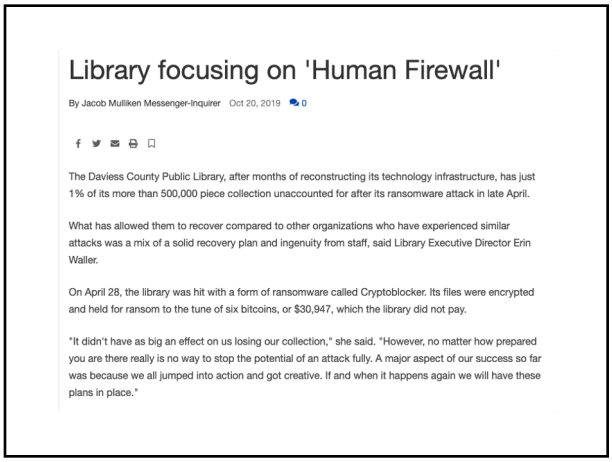
The compromised credentials are mostly obtained through attackers abusing flaws or security shortcomings in virtual private networks or remote desktop protocol endpoints, which provides the initial entry point into enterprise networks. Additionally, credential information can come from logs tied to infostealer malware, password spraying or other credential marketplaces in the criminal underground.

https://intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service/

294



295



Library focusing on 'Human Firewall'

By Jacob Mulliken Messenger-Inquirer Oct 20, 2019 0

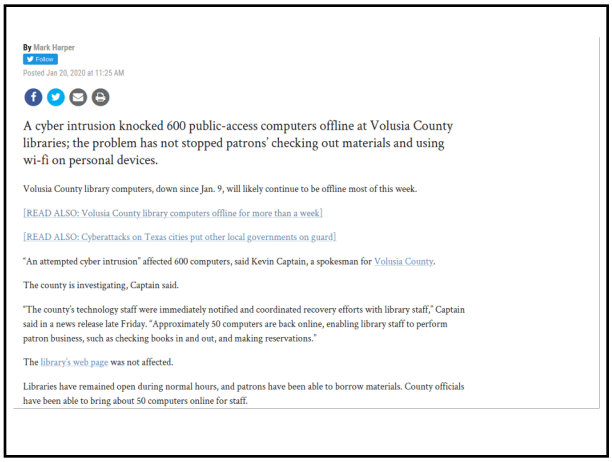
The Daviess County Public Library, after months of reconstructing its technology infrastructure, has just 1% of its more than 500,000 piece collection unaccounted for after its ransomware attack in late April.

What has allowed them to recover compared to other organizations who have experienced similar attacks was a mix of a solid recovery plan and ingenuity from staff, said Library Executive Director Erin Waller.

On April 28, the library was hit with a form of ransomware called Cryptoblocker. Its files were encrypted and held for ransom to the tune of six bitcoins, or $30,947, which the library did not pay.

"It didn't have as big an effect on us losing our collection," she said. "However, no matter how prepared you are there really is no way to stop the potential of an attack fully. A major aspect of our success so far was because we all jumped into action and got creative. If and when it happens again we will have these plans in place."

296



By Mark Harper
Follow
Posted Jan 20, 2020 at 11:25 AM

A cyber intrusion knocked 600 public-access computers offline at Volusia County libraries; the problem has not stopped patrons' checking out materials and using wi-fi on personal devices.

Volusia County library computers, down since Jan. 9, will likely continue to be offline most of this week.

[READ ALSO: Volusia County library computers offline for more than a week]

[READ ALSO: Cyberattacks on Texas cities put other local governments on guard]

"An attempted cyber intrusion" affected 600 computers, said Kevin Captain, a spokesman for Volusia County.

The county is investigating, Captain said.

"The county's technology staff were immediately notified and coordinated recovery efforts with library staff," Captain said in a news release late Friday. "Approximately 50 computers are back online, enabling library staff to perform patron business, such as checking books in and out, and making reservations."

The library's web page was not affected.

Libraries have remained open during normal hours, and patrons have been able to borrow materials. County officials have been able to bring about 50 computers online for staff.

297

Regular Volusia County Library users say they haven't been able to log onto the public computers since Jan. 8.

Lucinda Colee, director of library services, acknowledged the outage on Thursday, but would not discuss specifics, referring a questions instead to a community information director. Kevin Captain has only said he is "working on your request." Neither immediately responded to messages left on Friday.

Users say they have gotten little information, as well. Nothing is posted on the library's web page.

A librarian and her supervisor at City Island also referred all questions to Colee and simply said the outage is an "IT issue."

One, Marla Orlowski of Edgewater, said Colee returned her call and informed her the computers are out systemwide and might not be working until late next week.

Colee told her Volusia has reciprocal agreements with Flagler, Lake and Brevard counties, where Volusia library users can access materials and computers.

Ben DiGiovanni, a New Smyrna Beach resident, said he doesn't have internet access at home.

"So if I need to do something online, like ... I was looking to do something with my car insurance, the only other access I have is through my phone," DiGiovanni said. "It's much easier to use a desktop."

He said he's visited both the DeLand and New Smyrna Beach branches to no avail.

"It's a little upsetting," said Susan Griggs of Holly Hill. "Those computers are busy most of the time I go there. There are an awful lot of people who depend on these computers."

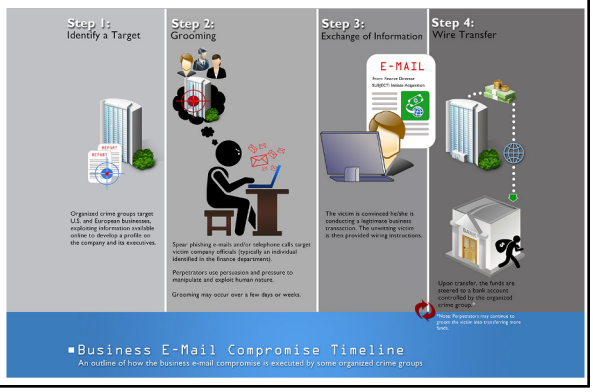
298

Email Threats

Business Email Compromise (BEC)
Phishing
Spam

299

BEC: Business Email Compromise
LEC: Librarian Email Compromise



300

Watch out for email messages that have subjects containing words like...

request, *payment*, *transfer*, and *urgent*, among others.

5 Common types of BEC scams:

- The Bogus Invoice Scheme- Attackers pretend to be known suppliers requesting fund transfers for payments to an account owned by fraudsters.
- CEO Fraud - Attackers pose as the company CEO or any executive and send an email to employees in finance, requesting them to transfer money to the account they control.
- Account Compromise - An executive or employee's email account is hacked and used to request invoice payments to vendors listed in their email contacts. Payments are then sent to fraudulent bank accounts.
- Attorney Impersonation - Attackers pretend to be a lawyer or someone from the law firm supposedly in charge of crucial and confidential matters.
- Data Theft – Employees under HR and bookkeeping are targeted to obtain personally identifiable information (PII) or tax statements of employees and executives. Such data can be used for future attacks.
- **Watch those forwarding rules in Outlook!**

301

1. Hit the IC3 Complaint Referral Form ASAP! (https://bec.ic3.gov/)
    i. include as much detail as possible. What was the account the scammer requested? What was the *name* used for the account wire? What were the other names of companies involved? Phone numbers called, email accounts used, URL's visited? Did they send you an invoice, and if so, do you have the original copy?
2. Report all accounts
    i. Email
    ii. Social Media
    iii. Domains (maybe)
3. Assume You've Lost Control
    i. Assume inbox = fully compromised
        1. all emails
        2. Rules
        3. Passwords
        4. Everything

A Complete BEC recovery guide: https://github.com/PwC-IR/Business-Email-Compromise-Guide

302

Microsoft 365 Defender Recommendations

- Educate end users
- Configure Office 365 email filtering settings to ensure blocking of phishing & spoofed emails,
- Set Office 365 to recheck links on click and delete sent mail to benefit from newly acquired threat intelligence.
- Disallow macros or allow only macros from trusted locations. See security baselines for Office and Office 365.
- Turn on AMSI for Office VBA.
- Check perimeter firewall and proxy to restrict servers from making arbitrary connections to the internet to browse or download files.
- Turn on network protection to block connections to malicious domains and IP addresses.
- Turning on attack surface reduction rules, including rules that can block advanced macro activity, executable content, process creation, and process injection initiated by Office applications, also significantly improves defenses. The following rules are especially useful:
    - Block all Office applications from creating child processes
    - Block Office applications from creating executable content
    - Block Office applications from injecting code into other processes
    - Block Win32 API calls from Office macros
    - Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - Block Javascript or VBScript from launching downloaded executable content
    - Block execution of potentially obfuscated scripts
    - Block executable content from email client and webmail

https://www.microsoft.com/security/blog/2021/02/01/what-tracking-an-attacker-email-infrastructure-tells-us-about-persistent-cybercriminal-operations/

303

Cybersecurity

Week Four

304

Reactive vs. proactive security: You want a proactive cybersecurity strategy

What is reactive security?

Reactive security requires that measures are put in place to spot the tell-tale signs of a breach and react to it, as it happens, or during a prolonged attack.

Examples of reactive cybersecurity measures include:

- Cybersecurity monitoring solutions: These solutions monitor a network looking for possible attacks as they happen.
- Forensic analysis of security events: It is extremely useful to understand the methods used in an attack to help make cybersecurity policy decisions.
- Anti-spam/ anti-malware solutions: Important, but can fail when new malware enters the landscape (e.g., fileless malware)
- Firewalls: Important, but configuration issues can leave organizations vulnerable

305

What is proactive security?

Proactive security is a more holistic approach to securing IT systems. It focuses on prevention rather than detection and response.

Proactive security measures include:

- **Security awareness training**: Preempting a social engineering or other phishing attacks by ensuring a user base knows how to spot the tell-tale signs and tricks of fraudsters. The CRAE report found that phishing was the biggest concern for 59% of US and 68% of Canadian respondents.
- **Penetration testing**: Using white-hat hackers to test IT systems to find exploitable vulnerabilities. Penetration tests will produce a report that can be used to close off potential exploits.
- **Proactive endpoint and network monitoring**: New technologies, such as machine learning, are helping to make reactive measures more proactive by reducing false positives and negatives.
- **Threat hunting and threat intelligence:** This is a set of complementary tasks performed by internal or external skilled staff. These tasks can be thought of as proactive digital forensics. An organization will engage an internal or external Red Team to hunt for vulnerabilities. These gaps in security can then be hardened against real attacks in a proactive way.

306

Filtering:
Email, Web, DNS, Firewall

Allow List: (AKA Whitelist)
Blocks every application from running by default, except for those you explicitly allow.

Patch:
Everything updated always

Hardening:
Browsers get locked down (no flash, java).
Office, macros off.
Segment your networks
RDP
File Shares
Privileged Accounts
PowerShell Bad!

Monitoring:
Automated monitoring of logs, network, file access, logins

307

What About Your Vendors?

- Ask them questions
  - Higher Education Community Vendor Assessment Toolkit (HECVAT)
- Ask other users
- Things to look for:
  - SSL on the website
  - Privacy Statement
  - Security Statement
  - A software bill of materials (SBoM)

308

https://www.iii.com/security/

https://www.iii.com/privacy-policy/

309

Securing Your Files

310

Securing Your Files

- Backups
  - Local & Remote
  - WORM storage
- Updates
- Permissions
- Encryption
- Passwords

311

The NetworkS

BIG S. At least TWO networks.

- Change all default passwords to something unique and strong.
- Patch all computers, routers, and other devices on the network.
- Enable 2FA
- Change your DNS to
  - 1.1.1.2, or 1.1.1.3, 9.9.9.9 etc
- Run a network scanner to inventory everything
- Run a canary or two
- Use professional equipment

312

Protective DNS

PDNS is a security service that uses existing DNS protocols and architecture to analyze DNS queries and mitigate threats. Its core capability is leveraging various open source, commercial, and governmental threat feeds to categorize domain information and block queries to identified malicious domains. This provides defenses in various points of the network exploitation lifecycle, addressing phishing, malware distribution, command and control, domain generation algorithms, and content filtering. PDNS can log and save suspicious queries and provide a blocked response, delaying or preventing malicious actions – such as ransomware locking victim files – while enabling an organization to investigate using those logged DNS queries.

OpenDNS
Cloudflare
Google Public DNS
Comodo Secure DNS
Quad9
Verisign DNS

https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_PROTECTIVE%20DNS_UOO117652-21.PDF

313

Canaries / Honey Pots

Security honeypots—systems that look like they contain valuable data and are ripe targets for attack, but which are really traps—are a well-known technique for detecting intrusions. Hackers will inevitably discover and explore the honeypot systems, unwittingly alerting their victims to their intrusion. However, they're not commonly used. Creating and maintaining a honeypot that looks authentic, but is reliably able to report intrusion attempts, isn't easy, and most organizations don't bother.

OpenCanary

314

Adopt a Zero Trust mindset

To adequately address the modern dynamic threat environment requires:

- Coordinated and aggressive system monitoring, system management, and defensive operations capabilities.
- Assuming all requests for critical resources and all network traffic may be malicious.
- Assuming all devices and infrastructure may be compromised.
- Accepting that all access approvals to critical resources incur risk, and being prepared to perform rapid damage assessment, control, and recovery operations.

Embrace Zero Trust guiding principles

A Zero Trust solution requires operational capabilities that:

- Never trust, always verify – Treat every user, device, application/workload, and data flow as untrusted.
- Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
- Assume breach – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
- Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.

Leverage Zero Trust design concepts

When designing a Zero Trust solution:

- Define mission outcomes – Derive the Zero Trust architecture from organization-specific mission requirements that identify the critical Data/Assets/Applications/Services (DAAS).
- Architect from the inside out – First, focus on protecting critical DAAS. Second, secure all paths to access them.
- Determine who/what needs access to the DAAS to create access control policies – Create security policies and apply them consistently across all environments (LAN, WAN, endpoint, perimeter, mobile, etc.).
- Inspect and log all traffic before acting – Establish full visibility of all activity across all layers from endpoints and the network to enable analytics that can detect suspicious activity.

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

315

Adopt a Zero Trust mindset

To adequately address the modern dynamic threat environment requires:

- Assuming all devices, people and all network traffic may be malicious and compromised.
- Be ready for things to fall apart.

Embrace Zero Trust guiding principles

A Zero Trust solution requires operational capabilities that:

- Never trust, always verify – Treat every user, device, application/workload, and data flow as untrusted.
- Don't let anyone/thing do anything that's not necessary.
- Assume you're breached.

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

316

Training

317

318

https://www.computerweekly.com/opinion/Its-time-to-accept-that-disinformation-is-a-cyber-security-issue

319

Good security awareness programs help everyone know where to get help

Who they should call when there is trouble

Where they can look for guidance & policies

They should know that they will not be looked down on for making a mistake

Someone's job is to help them through whatever difficulty they are having

320

We can't make everyone an expert

We do NOT need to train the non-technical employees about what the deep level geek employees already know.

321

How do we reach EVERYONE and do it in a way that teaches them without lecturing and/or yelling at them. They only care about their job, so we need to work with them, not tell them.

Meet them where they live and bring security up in their lives and make it part of their work and tell them why.

322

-------- Original Message --------
Subject:***SPAM***[redacted]
Date:08/04/2018 17:59
From:"Dianne" <[redacted]ull.lishost.info>
To:[redacted]

It appears that, ([redacted]), is your password. You may not know me and you are probably wondering why you are getting this e-mail, right?

in fact, I setup a spyware over the adult vids (porno) web site and you know what, you visited this web site to have fun (you know very well what I mean). While you were watching videos, your internet browser started out working like a RDP (Remote Access) which provided me accessibility to your screen and web camera. from then on, my computer software obtained all your contacts from your Messenger, Microsoft outlook, FB, as well as emails.

What did I actually do?

I created a double-screen video. First part shows the recording you are watching (you've got a good taste haha . . .), and Second part shows the recording of your webcam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for your little hidden secret. You will make the payment by Bitcoin (if you don't know this, search "how to purchase bitcoin" in Google).

BTC Address: [redacted]PQRk
(It is case sensitive, so copy and paste it)

Very important:
You have 1 day to make the payment. (I've a special pixel in this e mail, and at this moment I know that you have read this email message). If I don't get the BitCoins, I will certainly send your videos to all of your contacts including family members, coworkers, and so on. Having said that, if I get the payment, I'll destroy the recording immidiately. If you want evidence, reply with "Yes!" and i'll definitely send out your videos to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by answering this message.

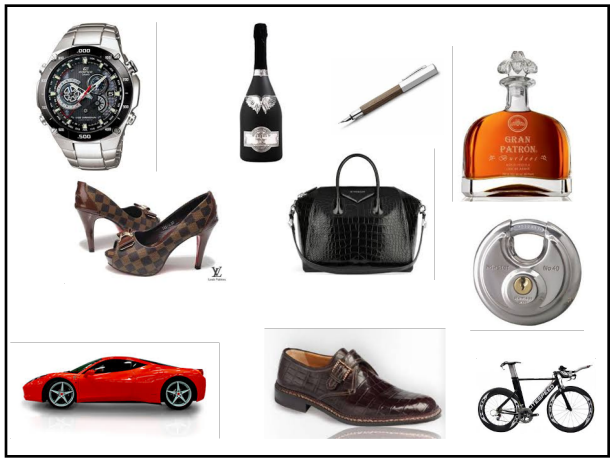
323

Understanding awareness, training, and development

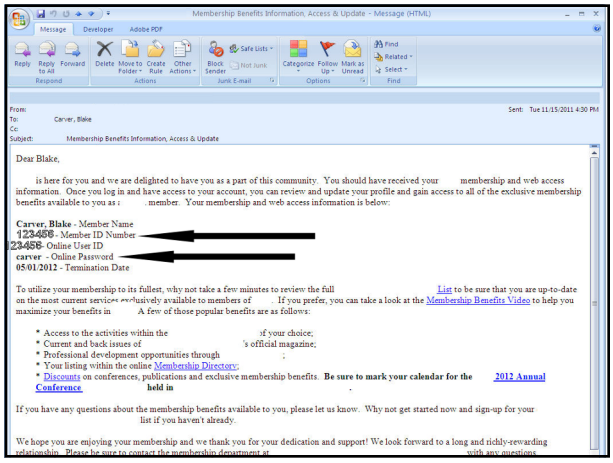
What we want is policies that reinforce good security principles that will foster over time a **new instinct** in people, **a new way of looking at things**, a new way of acting in a more secure way.

This will require a huge amount of patience and buy in from every at your library.

324



325

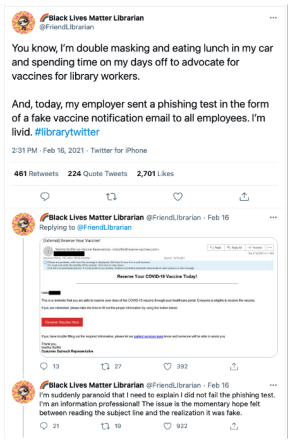


326

Training

- Phishing
- Social Engineering
- Privacy
- Passwords
- Email Attachments
- Virus Alerts
- Social Networking
- Updates

327



328

329

The goal is to make doing things **the right way** become the default in your library

330

331

Well then what?!

Criteria for good metrics.

1. Consistently measures (no subjective criteria).
2. Cheap to gather (preferably automated).
3. Expressed as a cardinal number or percentage.
4. Expressed using at least one unit of measure.
5. Contextually specific (i.e. relevant to decision makers so they can take action).

Two general categories for metrics. Categories that measure *who* took the training and metrics that measure the *impact* of the training.

- **WHO**: This measures how many people took the awareness training.
- **IMPACT**: This measures how effective the training was, are you getting a return for your investment.

Andrew Jaquith's book Security Metrics.

332

Training…. Patrons?

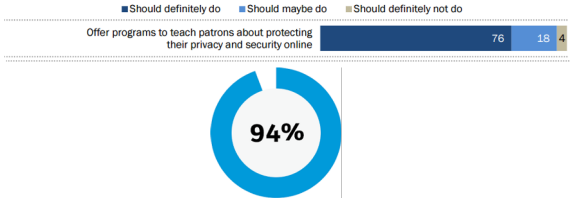
- Your patrons don't care much for security
- Their habits are inviting malware
- Look for ways to make things safer in ways that don't interfere with people's everyday tasks as much as possible.
- Principle of Least Privilege

333

Offer Training At Your Library

Public Wants Libraries to Advance Education, Improve Digital Literacy and Serve Key Groups

% of those ages 16+ who say that libraries should definitely, maybe or definitely not do these things



http://www.pewinternet.org/files/2015/09/2015-09-15_libraries_FINAL.pdf

334

What about training UP?

How do we communicate up?

Is your boss/director/board/dean/whatever aware of IT Security? If they were, would that help make the library more secure?

It may be up to you to help everyone at your library become Security Literate.

So how do you do it?

Start talking & training.

Make sure everyone understands that we are all targets.

If they ask "How secure are we? What's this going to cost?"… the answer will most likely scare them.

335

They (board/boss/whatever) need to know there's other costs attached to new technology.

- The technology costs $X
- Securing that also costs $X

336

Boards should discuss cybersecurity regularly.

A recent McKinsey survey of financial services companies suggests best practices.

Nearly 95% of the firms reported that one of their board committees discussed cybersecurity and technology risks four times or more per year. Almost half the companies involved the board in cybersecurity exercises, and nine in 10 provided regular updates on cybersecurity to the full board.

Financial services firms furnish a good model because they have long been targets of attacks and have advanced cybersecurity programs. Their approach hints at what shareholders, regulators and others are likely to demand from boards in other industries.

337

Don't Be Afraid To Brag

338

Security Exercises

It's Gone

Pick a system, any system. Think of a reason why it's completely hosed–failure of the entire RAID array, fire in the datacenter, evil script kiddies, sysadmin mistake–and see how your team copes.

Stowaway

Connect an unauthorized network device into your network and let it talk to something. See how your team tracks it down and removes it.

Blame the Mailman

A system that should never send mail starts sending

Naughty Ned

Choose a team member with elevated privileges (any member of your security or systems administration / ops team is usually a good choice, so might be a leadership team member or a developer). Pretend he or she has been fired, and revoke all of his or her privileges.

Evil Patron

You walk into your library as a patron with a Kali Linux laptop. Start exploring...

339

Create an Employee Offboarding Process

Your organization's HR department likely has an offboarding process. That process should include IT and security personnel from the very beginning. Their role in the offboarding process should begin as soon as notice is given or as plans are in place to terminate an employee. IT and security should work together to create a checklist of their offboarding responsibilities, which should include the following:

1. Create an inventory of the employee's digital life in the company. There should be a record of every company device in the employee's possession, accounts they have access to and any admin permissions and responsibilities. The more that is known about the employee's digital footprint, the easier it will be to delete it.

2. Set deadlines. Working with the employee's manager, IT can set up specific times to delete access to accounts or have devices returned. At this point, the employee should only be able to access the data they are currently using to finish up projects. Also, begin to revoke software licenses for the outgoing user.

3. Audit what users do. Security should keep watch over network activity to ensure the employee isn't downloading a high volume of files or moving them to personal clouds.

4. Deploy a data management solution that can easily silo employee data that must be retained.

5. Delete the employee's access before they leave the building for the last time. Whether it is during the exit interview or the goodbye party, access to email, software, cloud services, apps and other digital properties should be removed.

6. Create a thorough list of digital devices to make sure everything has been recovered.

7. Shut access to any apps on personal devices.

8. Change passwords and set up forwarding for email and voicemail.

9. Use a zero trust model for security. Once the person leaves, security should consider a zero trust model (if it isn't used already) as part of the offboarding process. They should also assume that any attempt to log in is a potential threat that means action is required.

https://securityintelligence.com/articles/offboarding-checklist-safely-closing-doors/

340

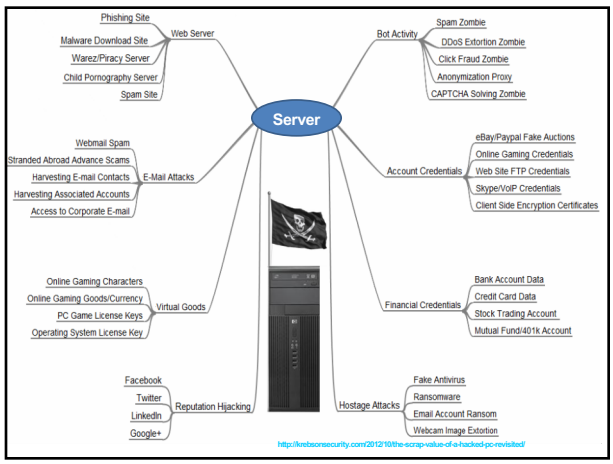
Treat security like a special collection

LFI: Privacy & Security in Public Libraries:

341

Securing Your Library's Website

342

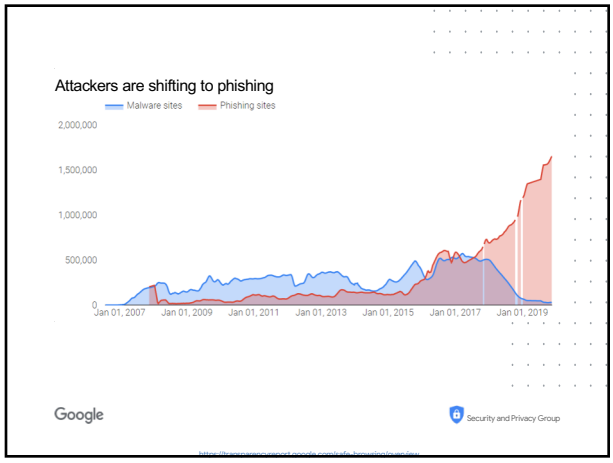


343

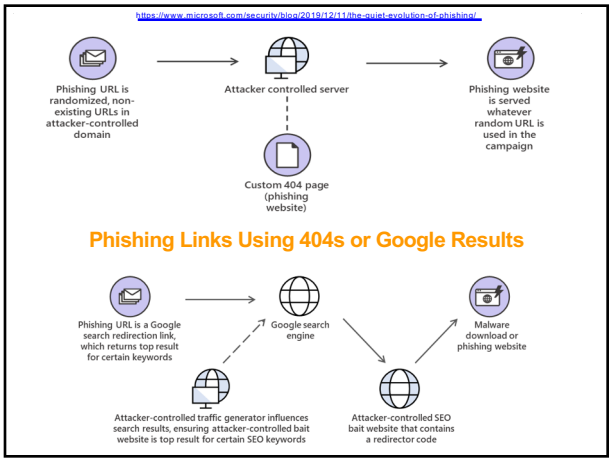
Servers Are Better!

- Bigger
- Better
- Faster
- Always On
- Unattended
- Bigger Pipes!
- Full of stuff!!
- People come to visit!!!

344



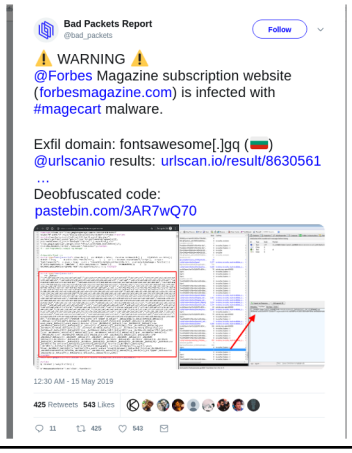
345



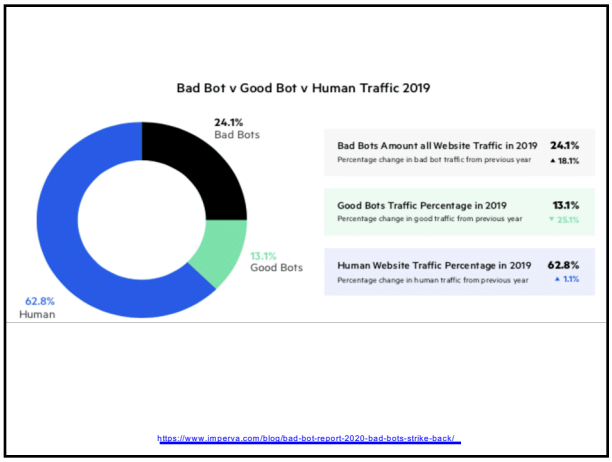
346

Any Good Web Site Can Go Bad At Any Time

347



348



349

Key Findings from the 2020 Bad Bot Report:

- Bad bot traffic rises to highest levels ever. In 2019, bad bot traffic comprised 24.1% of all website traffic, rising 18.1% from the year prior. Good bot traffic consisted of 13.1% of traffic—a 25.1% decrease from 2018—while 62.8% of all website traffic came from humans.
- Financial services industry hit hardest by bad bots. Every industry has a unique bot problem ranging from account takeover attacks and credential stuffing to content and price scraping. The top 5 industries with the most bad bot traffic include financial services (47.7%), education (45.7%), IT and services (45.1%), marketplaces (39.8%), and government (37.5%).
- Moderate to sophisticated bad bots make up almost three quarters of bad bot traffic. Advanced persistent bots (APBs) continue to plague websites and often avoid detection by cycling through random IP addresses, entering through anonymous proxies, changing their identities, and mimicking human behavior. In 2019, 73.7% of bad bot traffic was APBs.
- More than half of bad bots claim to be Google Chrome. Continuing to follow browser popularity trends, bad bots impersonated the Chrome browser 55.4% of the time. The use of data centers reduced again in 2019, accounting for 70% of bad bot traffic—down from 73.6% in 2018.
- For the third year in a row, the most blocked country is Russia. In 2019, 21.1% of country blocks were Russia, followed closely by China at 19%. Despite this, with most bad bot traffic emanating from data centers, the United States remains the "bad bot superpower" with 45.9% of attacks coming from the country.

350

Analyzing a malicious site

Use a VPN

Use the command line - wget / curl

VirusTotal.com

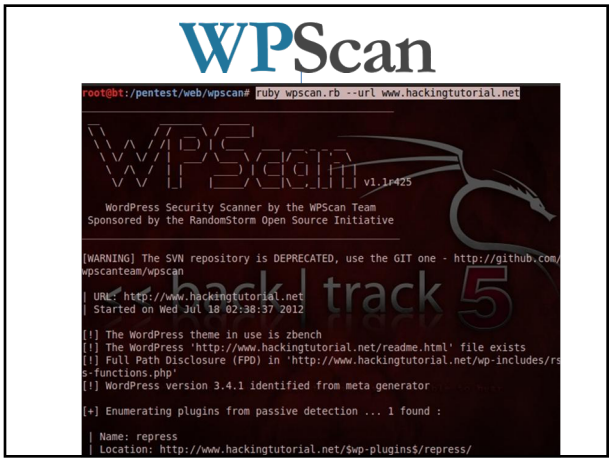
UrlScan.io

Google Safe Browsing

https://zeltser.com/lookup-malicious-websites/

351

352



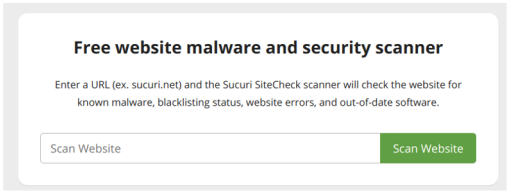
353

How Do I Know My Site's Been Hacked?

1. Errors on the pages
2. Errors In The Logs
3. New server side processes, users, jobs
4. Files have changed or appeared
5. You show up on black lists
6. Random things in your ad blocker
7. Weird redirects

354

https://sitecheck.sucuri.net/



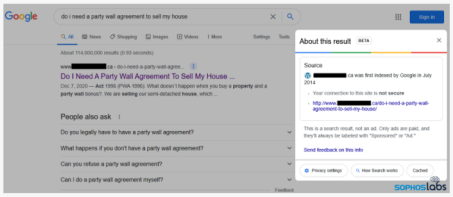
355

356

357

Search engine *deoptimization* as root cause

Gootloader uses malicious search engine optimization (SEO) techniques to squirm into Google search results. The way it accomplishes this task deserves some discussion, because it centers as much around technology as human psychology.



A malicious result that delivers Gootloader appears legitimate, even to Google

To accomplish this phase of the attack, the operators of Gootloader must maintain a network of servers hosting hacked, legitimate websites [we estimate roughly 400 such servers are in operation at any given time]. The example shown above belongs to a legitimate business, a neonatal medical practice based in Canada. None of the site's legitimate content has anything to do with real estate transactions – its doctors deliver babies – and yet it is the first result to appear in a query about a very narrowly defined type of real estate agreement. Google itself indicates the result is not an ad, and they have known about the site for nearly seven years. To the end user, the entire thing looks on the up-and-up.

https://news.sophos.com/en-us/2021/03/01/gootloader-expands-its-payload-delivery-options/

358

Sophos **News**

Have a domain name? "Beg bounty" hunters may be on their way

Corporate • bug bounty • extortion • Vulnerabilities

8 FEBRUARY 2021

By Chester Wisniewski

You are probably familiar with the popular practice of "bug bounty" programs in software security, where an organization offers rewards or bounties to security researchers who ethically disclose security vulnerabilities in their software. Organizations set terms for bugs they will reward. Typically, the more severe the flaw, the higher the bounty.

However, if, like myself, you have worked for a software company, then regardless of whether or not it had a bug bounty program in place, you will likely have been on the receiving end of what has become known as a "beg bounty." What are they and why are they such a menace?

The beg bounty playbook

"Beg bounty" queries run the gamut from honest, ethical disclosures that share all the needed information and hint that it might be nice if you were to send them a reward, to borderline extortion demanding payment without even providing enough information to determine the validity of the demand.

Just as in other areas of information security, ideas trickle down from experts to imitators. I began hearing from small businesses in the middle of 2020 about security researchers who had contacted them about vulnerabilities in their website. Should I worry? What do I do? Have I been hacked? Knowing these businesses did not have a bug bounty program and in fact probably didn't even know what code ran their website, it seemed odd for a legitimate researcher to be wasting their time on the smallest fish in the pond.

https://news.sophos.com/en-us/2021/02/08/have-a-domain-name-beg-bounty-hunters-may-be-on-their-way/

359

Subject: Vulnerability in your Website
To:

Hello Team ,

I am a security researcher and I founded this vulnerability in your website.

Vulnerability: No DMARC Record Found
I just sent a forged email to my email address that appears to originate from I was able to do this because of the following DMARC record

DMARC record lookup and validation for:
"No DMARC Record found"

Description:
DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities. DMARC Record contains the policy which determines how to handle unauthenticated/forged emails. Its lack can allow attacker to abuse the domain name.

Fix:
1)Publish DMARC Record.
2)Enable DMARC Quarantine/Reject policy
3)Your DMARC record should look like
"v=DMARC1; p=reject; pct=100; rua=mailto:info@domain.com"

POC:
This can be done using any php mailer tool like this ,
```
<?php
$to = "victim@example.com";
$subject = "Password Change";
$txt = "Change your password by visiting here - [VIRUS LINK HERE]!";
$headers = "From:
mail($to,$subject,$txt,$headers);

?>
```

You can check your DMARC record form here : https://mxtoolbox.com/DMARC.aspx

References:
1) https://www.knownhost.com/wiki/email/troubleshooting/setting-up_spf-dkim-dmarc_records
2) https://blog.redsift.com/email/the-resurgence-of-email-spoofing-how-to-run-impactful-and-secure-campaigns-in-light-of-covid-19/
3) https://easydmarc.com/blog/how-to-fix-no-dmarc-record-found/

Impact:
This is useful in phishing. The attacker can send forged emails from your domain granting him the ability to pose as the company's official and send scam emails to your website user asking them for money or credentials.

Let me know if you need furthermore assistance required, or if you have any other questions.

360

Now What??

361

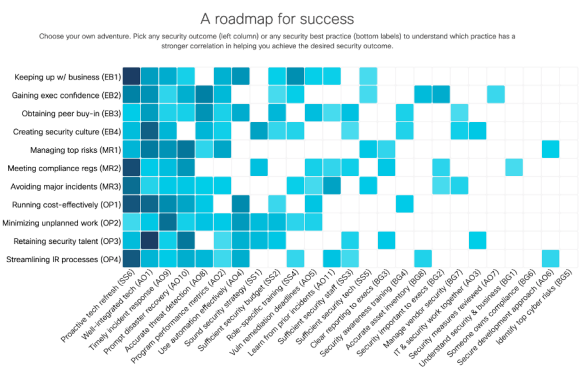
Strategies to Mitigate Cyber Security Incidents:

https://goo.gl/ctaecX

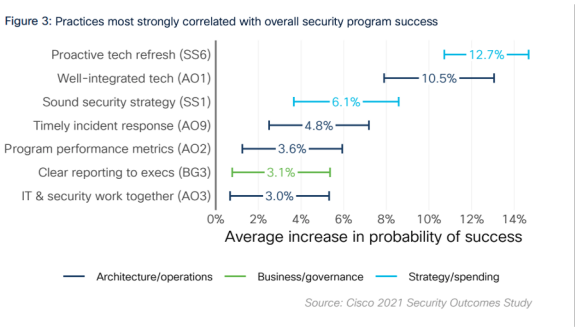
Now What?

https://goo.gl/Xavh6s

362

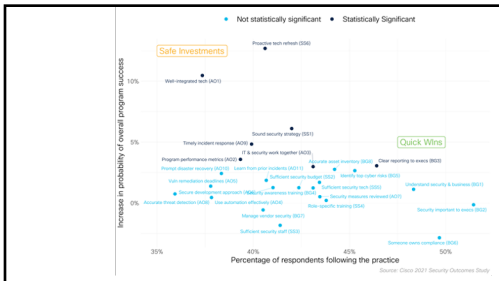


363



https://www.cisco.com/c/en/us/products/security/security-outcomes-study.html

364



Proactive Tech Refresh
Well Integrated Tech
Sound Security Strategies
Timely Incident Response
IT & Security Departments Work together
Program performance metrics
Clear reporting to executives

365

You

Use a password manager & 2FA
Encrypt your disks in portable devices
(FileVault, BitLocker, TrueCrypt)
Using a public network? Use a VPN
Browser Plugins
Updates / Patches
Don't run as root / admin
Firewalls
Remove Programs / Processes / Services
Clean Up Your Footprints
Stay Current

366

Your Library

- Threat Modeling
- Lock down all the “things”
- Hardware Security Checks
- Limit Users - Least Privilege
- Browser Plugins
- Updates / Patches
- Networks
- Training & Planning

367

Your Library

- Remove programs / Processes / Services
- Logging and auditing
- Backup & Encrypt
- Passwords
- Website

368

Stay Current

- https://ldhconsultingservices.com
- Schneier on Security
  http://www.schneier.com/blog/
- SANS Newsbites
  https://www.sans.org/newsletters/newsbites
- Naked Security – Sophos
  http://nakedsecurity.sophos.com/
- Troy Hunt :
  http://www.troyhunt.com/
- SANS Reading Room
  http://www.sans.org/
- Podcasts :
  http://grc.com/securitynow.htm Security NOW
  https://risky.biz/netcasts/risky-business/ Risky Business
  https://securityinfive.libsyn.com/ Security In 5

369

Questions \ Feedback?

Blake Carver
LYRASIS
Systems
Administrator

370

Pacific Library Partnership

Cybersecurity

371

Introduction: Why Cybersecurity, and What's Wrong?

Week One

372

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.

373

The reality is that your sensitive data has likely already been stolen, multiple times. Cybercriminals have your credit card information. They have your social security number and your mother's maiden name. They have your address and phone number. They obtained the data by hacking any one of the hundreds of companies you entrust with the data -- and you have no visibility into those companies' security practices, and no recourse when they lose your data.

https://www.schneier.com/blog/archives/2019/05/protecting_your_2.html

374

GOOGLE ADS

Charting a course towards a more privacy-first web

David Temkin
Director of Product Management, Ads Privacy and Trust

Published 03 Mar 2021

It's difficult to conceive of the internet we know today — with information on every topic, in every language, at the fingertips of billions of people — without advertising as its economic foundation. But as our industry has strived to deliver relevant ads to consumers across the web, it has created a proliferation of individual user data across thousands of companies, typically gathered through third-party cookies. This has led to an erosion of trust: In fact, 72% of people feel that almost all of what they do online is being tracked by advertisers, technology firms or other companies, and 81% say that the potential risks they face because of data collection outweigh the benefits, according to a study by Pew Research Center. If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web.

That's why last year Chrome announced its intent to remove support for third-party cookies, and why we've been working with the broader industry on the Privacy Sandbox to build innovations that protect anonymity while still delivering results for advertisers and publishers. Even so, we continue to get questions about whether Google will join others in the ad tech industry who plan to replace third-party cookies with alternative user-level identifiers. Today, we're making explicit that once third-party cookies are phased out, we will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products.

375

Cybersecurity

376