

Cybersecurity: Making Your Library Defensible and Resilient

Blake Carver
Senior Systems Administrator, LYRASIS
April 2021
Cybersecurity Training for Libraries
Week #3



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 Librarian.



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

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.

4

Making Your Library Defensible & Resilient

5

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

6

Defensible

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

7

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

8

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

9

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 databreach or ransomware either

10

“Security is always excessive until it’s not enough.”

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

11

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?

12

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)

13

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/infocis/change-management-cisp/>

14

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/questions-attackers-ask-exploit/102051/>

15

But We're Just A Small Library!

16

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

17

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

18

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

Every Single Security Report Ever

19

It's Easier Being Bad

20

Security Is More Difficult

21

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

22

While we need to catch every
single thing...

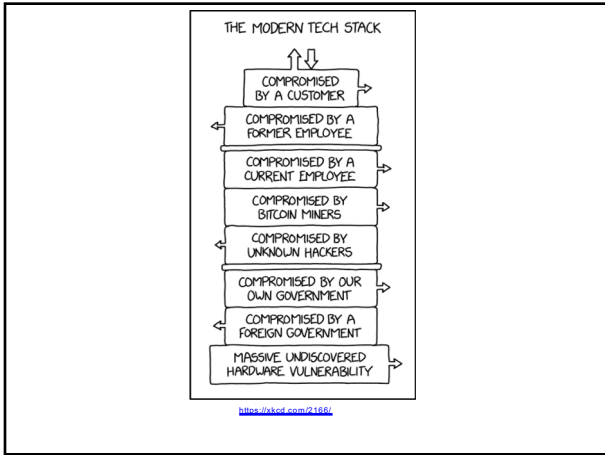
23

“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>

24



25

**Libraries Live Below
The Security Poverty Line**
(Windy 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...

26

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

27



28

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

29

What is the most important stuff in your library?
 What can you not live/work/function without?
 Is there only one thing?

30

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

31

Step 1 – Inventory & Prioritize

Step 2 – What could go wrong?

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

<https://www.fishbase.org/2020/02/20/2020-survey-of-fisheries-and-aquaculture-security-practices/>

32

An attacker will always pick the weakest point of entry...

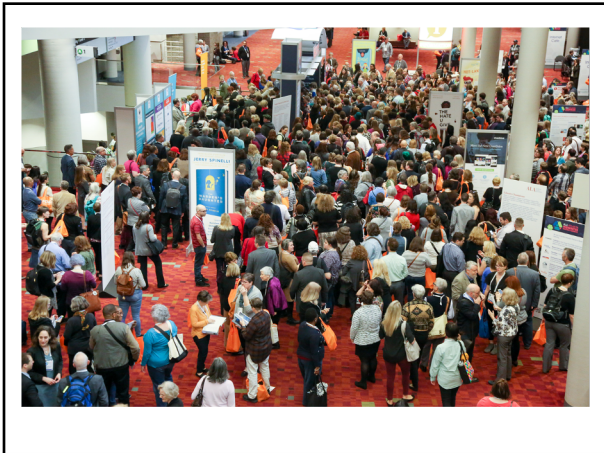
...but you can't know which point that is

33

The Weakest Point In A Library?



34



35

Public Access Computers



36

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

37

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

38

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...?

39

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://www.checkpoint.com/2020/02/05/...>

40

Cybersecurity

Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals

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

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>

41

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?

42

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

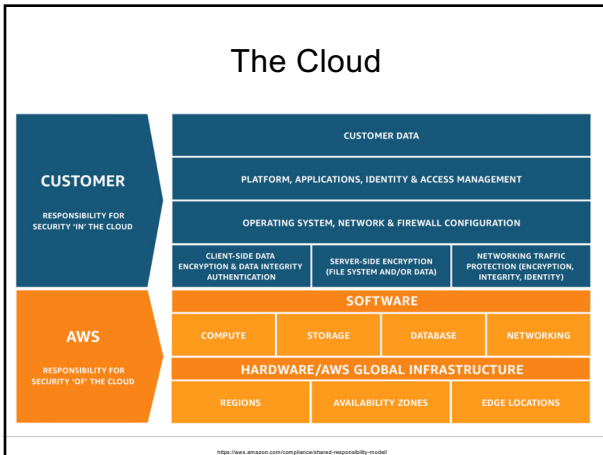
Secure your data

- Groups and Users
- Data loss prevention

Harden your environments

- Updates
- Password Managers
- Settings
- Training

43



44

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 applistrucre failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

45

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

46

The "Insider Threat" In Libraries

Insider threat program checklist

- 1 Research cybersecurity requirements in your industry
- 2 Form a group of interested stakeholders
- 3 Determine critical assets
- 4 Perform an insider threat risk assessment
- 5 Create a written insider threat policy
- 6 Appoint a manager responsible for dealing with insider threats
- 7 Conduct employee background checks
- 8 Educate your employees
- 9 Monitor user access
- 10 Monitor user actions
- 11 Form a remediation strategy
- 12 Revise your insider threat program

<https://www.ekran.com/en/blog/insider-threat-program>

47

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

Not every asset in your organization is equally valuable

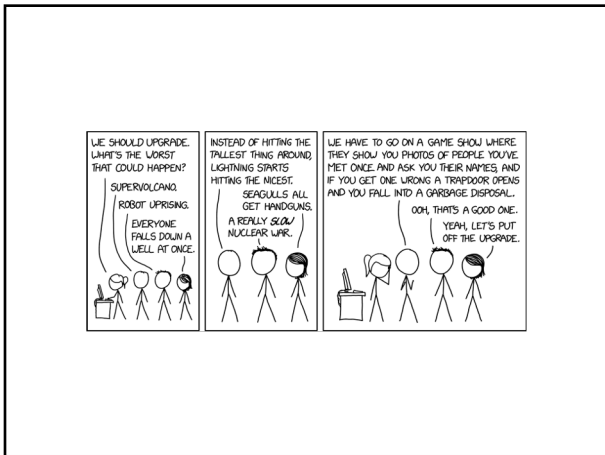
48

Locking Down Computers

- Patching and Updating
 - OS and *ALL* Applications



49



50

How-To Geek

Windows 10's Bugs Are Teaching the Importance of Backups



CHRIS HOFFMAN | @chrishoffman
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

51

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? 

52

LEHIGH VALLEY NEWS [HERE](#)

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 
- Send us your Lehigh Valley Christmas light display nominations 
- MAP: Where coronavirus is in Pennsylvania 

53

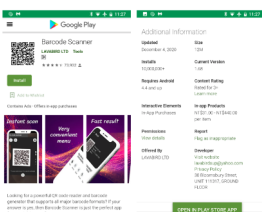
Barcode Scanner app on Google Play infects 10 million users with one update

Wired | February 3, 2021 by [Nehal Shah](#)

Late last December we started getting a distress call from our forum patrons. Patrons were experiencing calls that were opening up their devices to ransom attacks. The calls came in from people who had recently installed any apps, and the apps they had installed came from the Google Play store. Then one patron, who goes by username Amr00, 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 asked the developer, 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 a sudden, after an update in December, Barcode Scanner had gone from an innocent scanner to full on malware. Although Google has since pulled this app, we predict from a leaked 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/>

54

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.

55

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/>

56

Ransomware
&
Extortionware

57

A massive data breach has hit US Universities including Stanford University, University of California, University of Miami, University of Colorado Boulder, Yeshiva University, Syracuse University, and University of Maryland. Hackers have stolen terabytes of student, prospective student, and employee personal information including transcripts, financial info, mailing addresses, phone numbers, usernames, passwords and Social Security Numbers. These breaches are part of the larger Accellion FTA leak which has affected ~50 organizations. Students who applied to these colleges (or even have an account in the case of UC) are at risk of having their personal and financial information leaked publicly online including their **Social Security Numbers**. The hackers have sent emails to some victims. If you receive one of these emails, do not click the attached link unless you understand how to use Tor. The hackers are holding the universities at ransom. **Unless the universities pay the ransom, the hackers will continue publishing student information.**

https://twitter.com/itsnotastaticleak/status/1336816761428922368

58

Ransomware gangs made at least \$350 million in 2020

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

By Catalan Company to 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.

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 31% 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."

ZDNET RECOMMENDS

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

SECURITY

- Apple will deny Safe Browsing traffic on iOS 13.5 to hide user IP's from Google
- Yandex said it caught an employee selling access to users' inboxes
- Microsoft said the number of valid shells has doubled since last year
- Accellion to retire product at the heart of recent breach

NEWSLETTERS

ZDNet Security

59

Avatar @lozthing · In

Bitcoin #Blockchain #BTC

What if ransomware launched a service to contact to news media, companies for the best pressure at no cost, and DMG G.L 17 on a part service.

Also, they intend about developing support for VM ESX and a cybercrime engine to ransom.

| Profile | Following | Followers | Reposts |
|---------|-----------|-----------|---------|
| Avatar | 4 | 1 | 0 |
| Avatar | 1 | 0 | 0 |
| Avatar | 1 | 0 | 0 |
| Avatar | 1 | 0 | 0 |

We know how the opportunities to get their networks (DGA) to the media, contacts of companies to speak through press. To do this, the company's domain in the network operations, who 4 weeks with and to do up you can think to the data contacts or signs and images of the network.

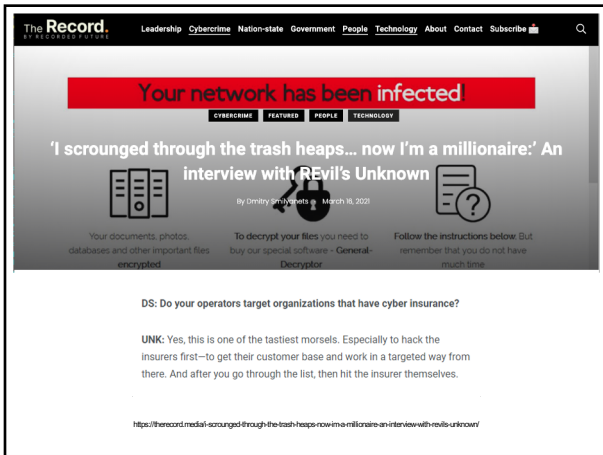
DMG is a G.L 17 on law, and network, DMG (network) services are also being tested. For more information, use the "news" service.

DMG is a G.L 17 on law, and network, DMG (network) services are also being tested. For more information, use the "news" service.

There is one place available, we will also take in the "Test Team" 1 team of network suppliers and 1 team of network developers. Experience is required. Maximum rate work weekly.

DMG - 1 Team - 1/2021

60



61

Never get into a position where you have to pay

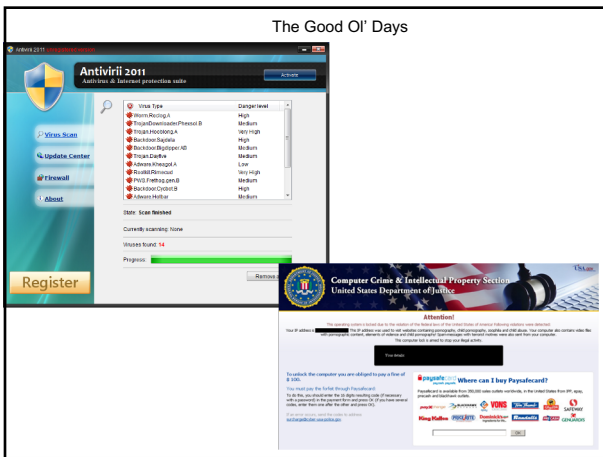
Two different types of backups

Multiple 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.

62



63

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)

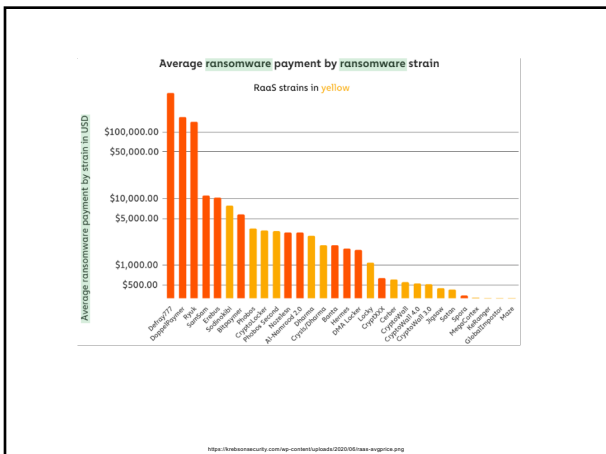
64

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.

65



66

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

67

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.

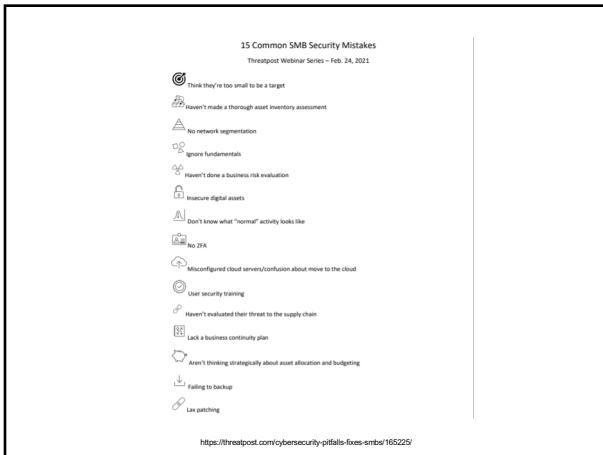
68

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

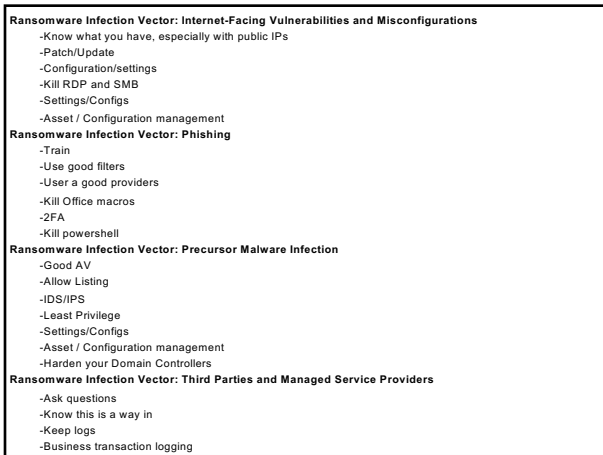
1. Keeping Legacy Systems on the Infrastructure
2. Having Limited Visibility Into Assets and Their Vulnerabilities
3. Forgetting to Implement System Hardening Policies
4. Relying on Perimeter Protection and Antivirus
5. Keeping a Flat Network Topology
6. Relying on Online Backups
7. Exercising Limited 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/>

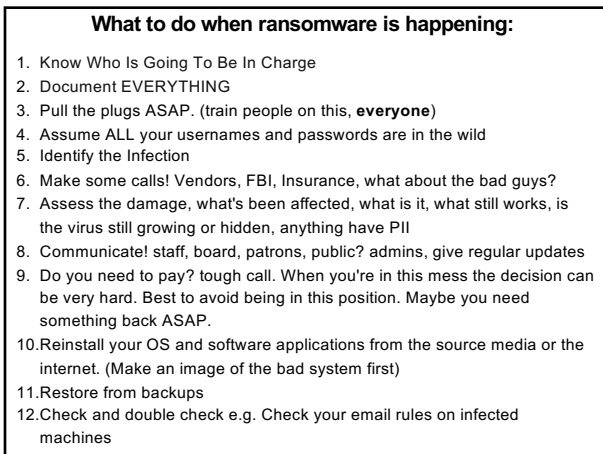
69



70



71



72

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

73

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)

74

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.

75

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

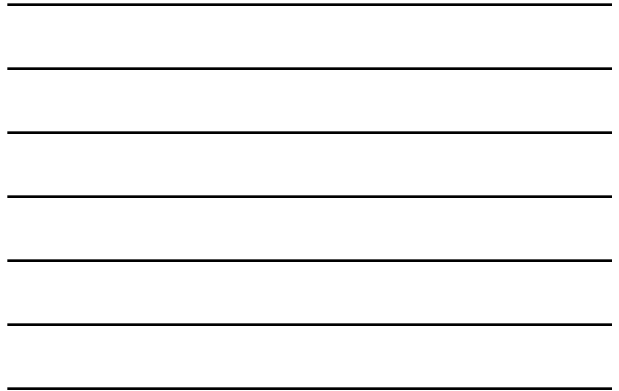
A cautionary tale shows how organisations that fall foul of ransomware should concentrate on finding how it happened before anything else - or they could fall victim again.

MORE FROM DANNY FALMER

- Security: The old form of ransomware has returned with new tricks and new targets
- Security: Enterprise 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

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

76



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/>

77



INITIAL ACCESSSES FOR SALE

Q4 2020

- 242** network access listings
\$1,209,880 cumulative price
- 14%** close rate, for at least
\$133,900 total revenue
- ~40%** network access sales targeted 4 geographies

\$6684 average price
\$1500 median price
7 BTC maximum price
\$15 lowest price

Top 3 sold accesses were priced:

- \$35,000
- 1 BTC
- \$10,000

• United States
 • Europe (unspecified)
 • UAE
 • France

KELA

<https://the-ny.com/7-million-a-pair-the-highest-q4-2020-in-network-access-sales/>

78



Library focusing on 'Human Firewall'

By Jacob Mulliken Messenger-Inquirer Oct 20, 2019

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."

79

By Mark Harper

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.

80

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 Orlovski 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.

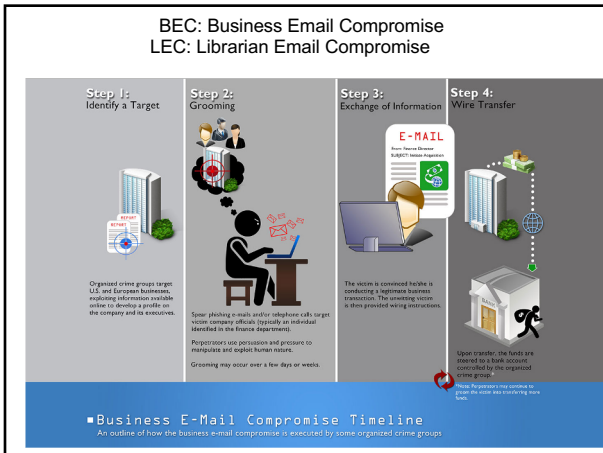
"It's a little upsetting," said Susan Griggs of Holly Hill. "Those computers are busy most of the time I go there. There are an awful lot of people who depend on these computers."

81

Email Threats

Business Email Compromise (BEC)
Phishing
Spam

82



83

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!**

84

1. Hit the IC3 Complaint Referral Form ASAP! (<https://www.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>

85

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/>

86