


Cybersecurity: Tying it all together

Blake Carver
Senior Systems Administrator, LYRASIS
April 2021
Cybersecurity Training for Libraries
Week #4



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

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

5

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.

6

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

7

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)

8

Innovative World Headquarters
5850 Shellmound Way
Emeryville, CA 94608

510.655.6200
info@iii.com

[Our Company](#)
About
History
Executive Leadership
Strategic Partnerships
Careers

© 2018 Innovative Interfaces, Inc.
Privacy Policy | Terms of Use | Security

ISO 27001 CERTIFIED by schellman

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

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

9



10

- ### Securing Your Files
- . Backups
 - Local & Remote
 - WORM storage
 - . Updates
 - . Permissions
 - . Encryption
 - . Passwords

11

- ### 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

12

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
Versign DNS

https://media.defense.gov/2021/Mar/03/202590059/11-10/CS_P/PROTECTIVE%20DNS_L0011763-21.PDF

13

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

14

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/25/202588479/11-10/CS_E/EMBRACING_ZT_SECURITY_MODEL_L00115131-21.PDF

15

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/25/202588479-1-10/CS_EMBRACING_ZT_SECURITY_MODEL_U00115131-21.PDF

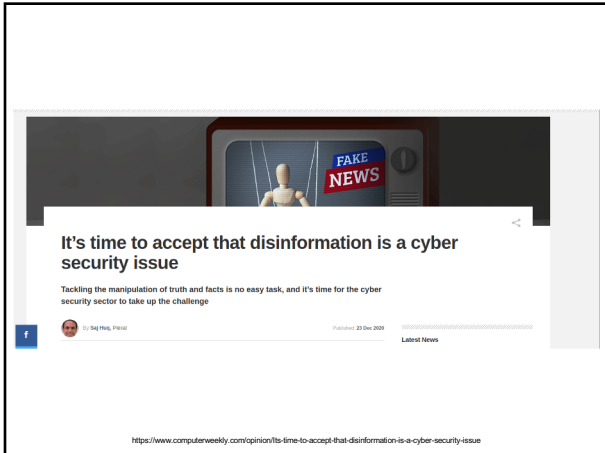
16

Training

17



18



19

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

20

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.

21

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.

22

----- Original Message -----
 Subject: "SPAM" [redacted]@mary.org
 Date: 09/04/2012 11:59
 From: "Name" <[redacted]@[redacted].info>
 To: [redacted]@mary.org

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]@ORK
 (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 immediately. 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.

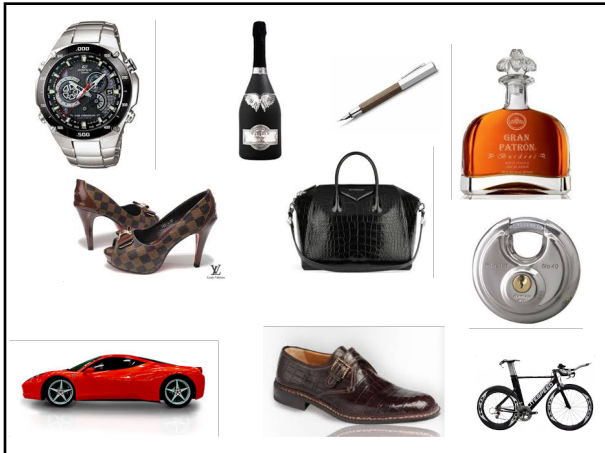
23

Understanding awareness, training, and development

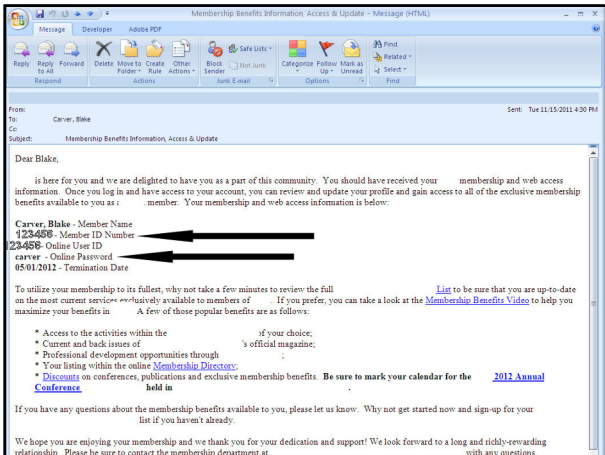
What we want is policies that reinforce good security principles that will foster over time a **new instinct** in people, a **new way of looking at things**, a new way of acting in a more secure way.

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

24



25

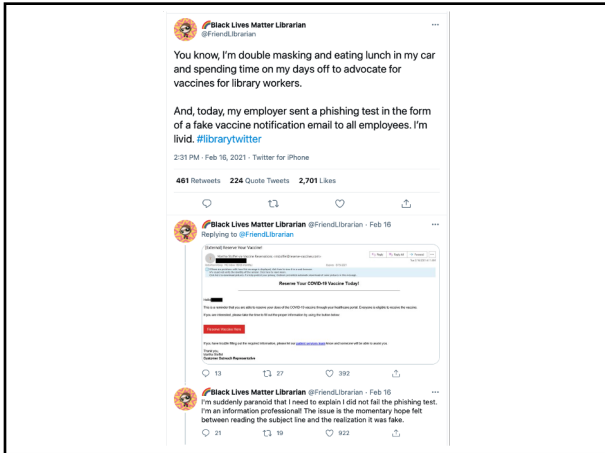


26

Training

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

27



28



29

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

30



31

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.

32

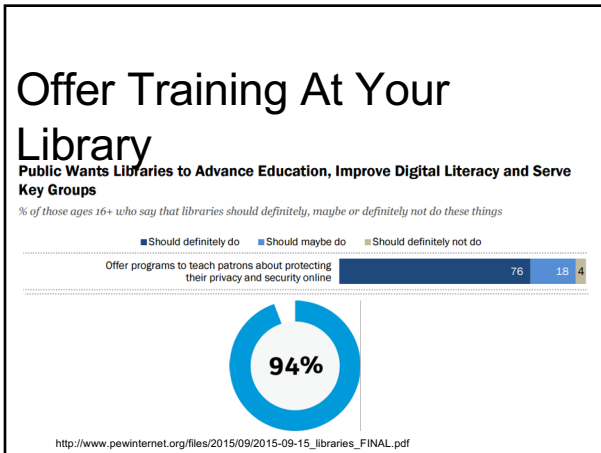
Training.... Patrons?

- 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

33



34

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.

35

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

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

36

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.

37

Don't Be Afraid To Brag



38

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...

39

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-safety-checks-2017/>

40

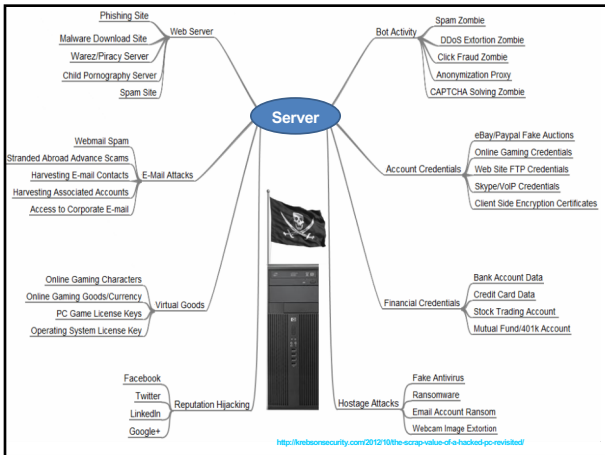
Treat security like a special collection

LFI: Privacy & Security in Public Libraries:

41

Securing Your Library's Website

42

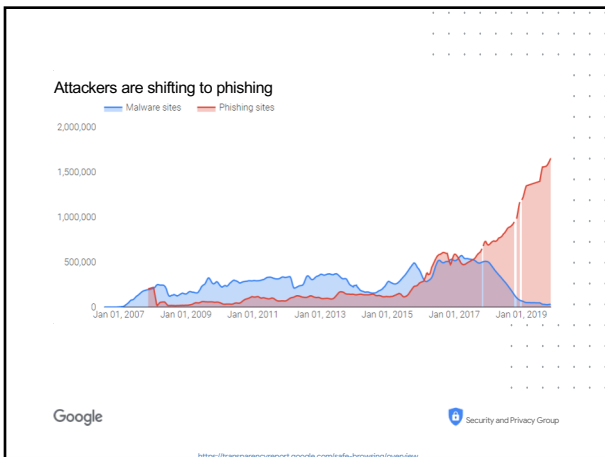


43

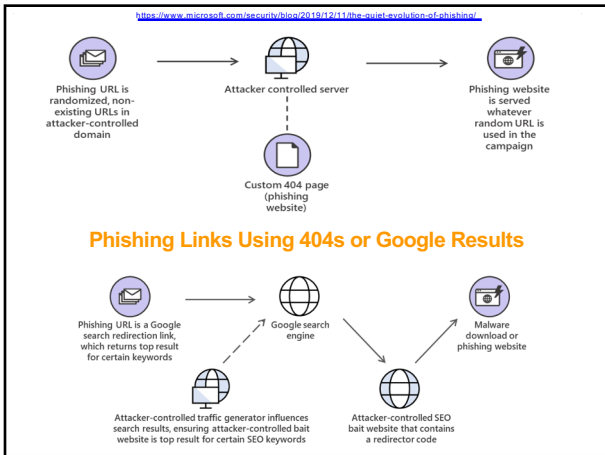
Servers Are Better!

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

44



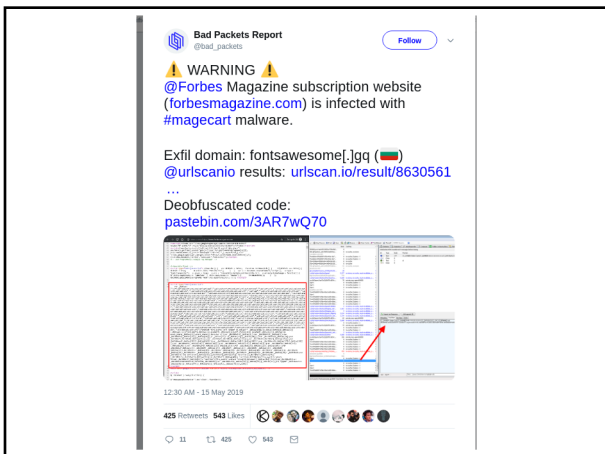
45



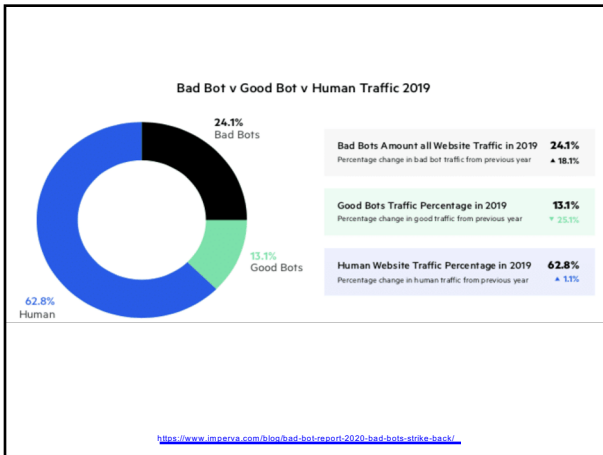
46

Any Good Web Site Can Go Bad At Any Time

47



48



49

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.

50

Analyzing a malicious site

Use a VPN

Use the command line - wget / curl

VirusTotal.com

UrlScan.io

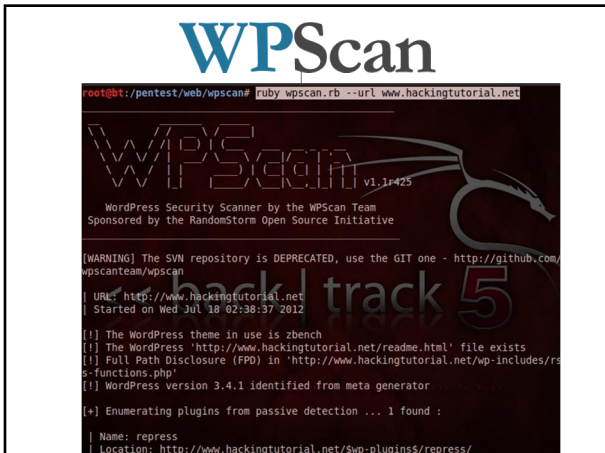
Google Safe Browsing

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

51



52

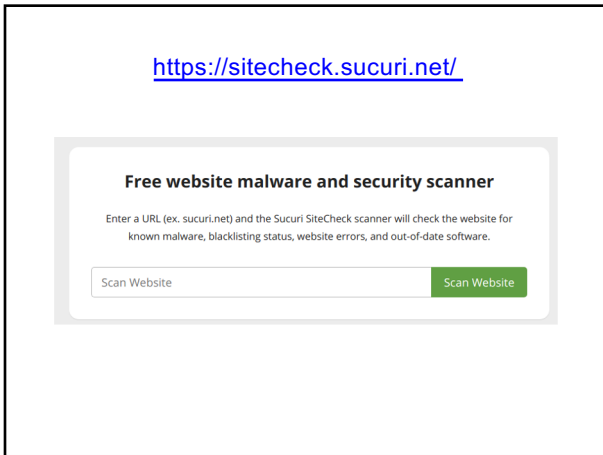


53

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

54



55



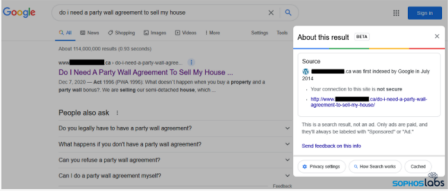
56



57

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://www.sophos.com/en-us/2021/03/01/gootloader-expands-to-pay-per-delivery-option/>

58



Sophos News

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

Corporate • Bug bounty • Security • 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://www.sophos.com/en-us/2021/02/08/have-a-domain-name-beg-bounty-hunters-may-be-on-their-way/>

59



Subject: Vulnerability in your Website
To: [redacted]

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 [redacted]. I was able to do this because of the following DMARC record:

DMARC record lookup and validation for: [redacted]
"No DMARC Record found"

Details:
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 spoofing and other cyber threat scenarios. 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; ml6480; rua=mailto:[redacted]@domain.com"

POC:
This can be done using any php mailer tool like this,
+@php
\$a = "mailto:[redacted]@domain.com";
Subject = "Password Change";
\$a["Change your password by visiting here (LURUS LINK HERE)";
\$headers = "From: mail@[redacted].com; Subject: [redacted]";
?>

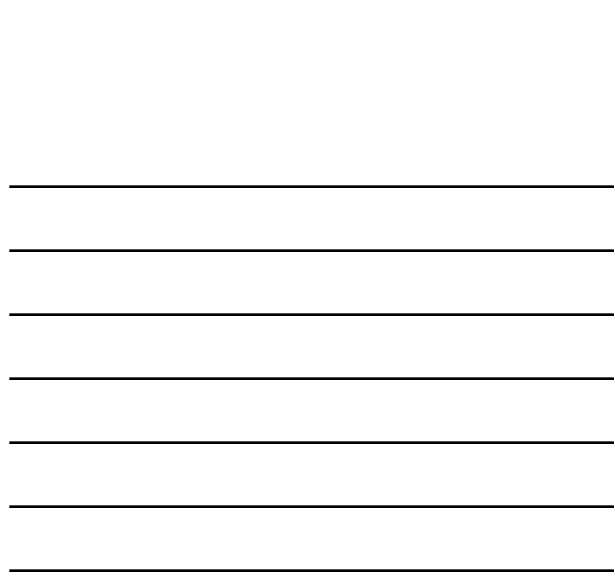
You can check your DMARC record from here : <https://mxtoolbox.com/DMARCS.aspx>

References:
1) <https://www.knowbe4.com/wiki/en/all/lookup/setting-up-and-using-dmarc-records>
2) <https://blog.credentia.com/news/the-advantage-of-email-verification-how-to-run-dmarc-check-and-your-campaign-in-light-of-covid-19/>
3) <https://sai010.com/blog/2020-02-18-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.

60



Now What??

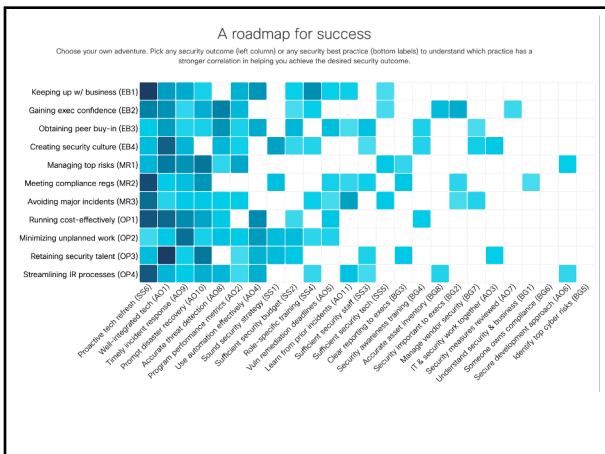
Horizontal lines for notes.

61

Strategies to Mitigate Cyber Security Incidents:
https://goo.gl/ctaex
Now What?
https://goo.gl/Xavh6s

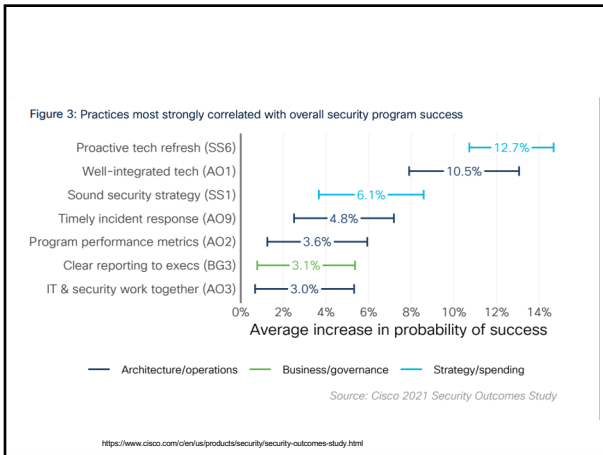
Horizontal lines for notes.

62

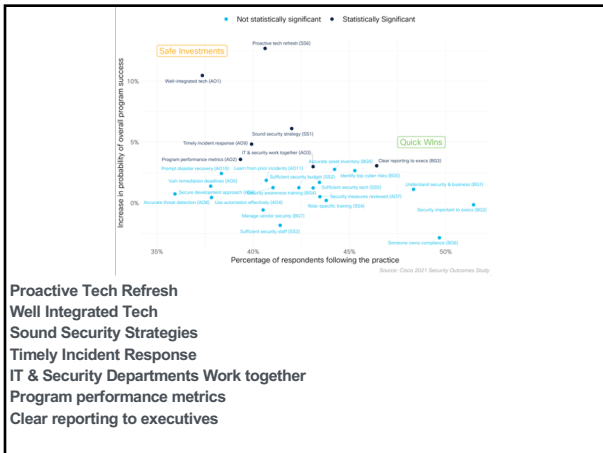


Horizontal lines for notes.

63



64



65

- 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

66

Your Library

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

67

Your Library

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

68

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

69

Questions \ Feedback?

**Blake Carver
LYRISIS
Systems
Administrator**
