CYBERSECURITY: WHO IS GUARDING YOUR NETWORK BUSINESS

Raj Goel, CISSP
raj@brainlink.com / 917-685-7731
www.RajGoel.com
@rajgoel_ny
YOUR KEY THREATS

Muggers
Thieves
Hackers
Spies
3 MUGGERS

- Crimes of opportunity
- Weak passwords
- Poor or disabled security
- Looking for a quick buck
4 THIEVES

- Motivated insiders
- Ex-employees
- Disgruntled employees
5 HACKERS

- They run a business…and their profitability exceeds yours.
- Attackers at scale
- They ARE persistent
SPIES

• Well-resourced attackers
• Foreign Governments
• Corporate Competitors
TO ERR IS HUMAN.

TO REALLY SCREWUP REQUIRES A COMPUTER
ELSEVIER LEFT USERS’ PASSWORDS EXPOSED ONLINE

- Due to a misconfigured server, a researcher found a constant stream of Elsevier users’ passwords.
- Elsevier, the company behind scientific journals such as The Lancet, left a server open to the public internet, exposing user email addresses and passwords. The impacted users include people from universities and educational institutions from across the world.

https://motherboard.vice.com/en_us/article/vbw8b9/elsevier-user-passwords-exposed-online
MONGODB CONFIGURATION ERROR EXPOSED 93 MILLION MEXICAN VOTER RECORDS

• A 132 GB database, containing the personal information on 93.4 million Mexican voters has finally been taken offline. The database sat exposed to the public for at least eight days after its discovery by researcher Chris Vickery, but originally went public in September 2015.

• Vickery, who works as a security researcher at Kromtech (the company behind MacKeeper), discovered the MongoDB instance on April 14, but had difficulty tracking down the person or company responsible for placing the voter data on Amazon's AWS. He first reached out to the U.S. State Department, as well as the Mexican Embassy, but had little success.

THE RNC FILES – LARGEST US VOTER DATA LEAK

• UpGuard’s Cyber Risk Team can now confirm that a misconfigured database containing the sensitive personal details of over 198 million American voters was left exposed to the internet by a firm working on behalf of the Republican National Committee (RNC)

• The data, which was stored in a publicly accessible cloud server owned by Republican data firm Deep Root Analytics, included 1.1 terabytes of entirely unsecured personal information compiled by DRA and at least two other Republican contractors, TargetPoint Consulting, Inc. and Data Trust. In total, the personal information of potentially near all of America’s 200 million registered voters was exposed, including names, dates of birth, home addresses, phone numbers, and voter registration details, as well as data described as “modeled” voter ethnicities and religions.

  https://www.upguard.com/breaches/the-rnc-files
EQUIFAX DATA BREACH

• Equifax says a 2017 data breach exposed the sensitive personal information of 143 million Americans.

• The company waited six weeks to disclose the breach.

  • FREE Credit freezes are coming
  • Eight state banking regulators imposed a consent order on Equifax in June, requiring security improvement, auditing, and reporting.
  • Senator Elizabeth Warren said, “At best you are incompetent; at worst you were complicit. Either way, you should be fired.” Smith [Equifax CEO] was joined soon after by the company’s chief information and chief security officers.
PREDATORY PUBLISHERS - OMICS GROUP

• Federal Trade Commission vs. OMICS Group, Inc.[edit]

• On 25 August 2016, the Federal Trade Commission (FTC) filed a lawsuit against the OMICS Group, iMedPub, Conference Series, and the individual Srinubabu Gedela, an Indian national who is president of the companies. In the lawsuit, the defendants are accused of "deceiving academics and researchers about the nature of its publications and hiding publication fees ranging from hundreds to thousands of dollars". The FTC was also responding to pressure to take action against predatory publishers. Attorneys for the OMICS Group published a response on their website, claiming "your FTC allegations are baseless. Further we understand that FTC working towards favoring some subscription based journals publishers who are earring [sic] Billions of dollars rom [sic] scientists literature," suggesting that corporations in the scientific publishing business were behind the allegations.[27] In March 2019, the FTC won the suit in a summary judgement and was awarded $50,130,811 in damages and a broad injunction of OMICS practices.

• https://en.wikipedia.org/wiki/Predatory_open-access_publishing
This past year, when an undergraduate biology student at the University of the Fraser Valley approached dean of science Lucy Lee for $2,000 to publish a paper in an academic journal, Dr. Lee had immediate concerns about the request. She’d had a bad experience with the journal in question, the International Journal of Environmental Research and Public Health, while doing a review for the publication. She discovered a lack of rigour in some of the journal’s articles, was alarmed at its many retractions and corrections, and had concerns with the journal’s practice of publishing an “acknowledgement” issue with a very long list of reviewers to make it look credible.

The publisher, Multidisciplinary Digital Publishing Institute (MDPI), churns out nearly 160 scholarly journals a year, many of them of mediocre quality, according to Jeffrey Beall, an associate professor and librarian at the University of Colorado Denver, and one of the world’s leading experts on what he calls “predatory” open access publishing.

https://www.universityaffairs.ca/features/feature-article/beware-academics-getting-reeled-scam-journals/
HACKERS TAKE CONTROL OF CONSTRUCTION EQUIPMENT

“hack into devices that controlled cranes, excavators, scrapers and other large machinery. In every case, their prepared attack code worked.”

Jan 15, 2019 -
FLAW IN HID & PREMISYS CONTROLLERS

April 1, 2016 -

Most critical of these flaws could allow unauthorized attackers to access the Premisys badge database, thereby giving them the ability to create fake security badges or even disable building locks at the user organization’s facilities

RANSOMWARE IS REAL

- Del Rio, Texas Offline – back to pen & paper days
- Hackers threaten to dump law firm’s 9/11 files unless they pay bitcoin
- Atlanta ransomware attack leaves court systems offline
- Maersk Shipping lost $300M due to NotPetya
- Merck Pharmaceuticals lost $870M
- Oreo cookies cost more - Mondelez lost $150M
- Lysol & Durex Condoms cost more – Reckitt lost $129M
GIFT CARD SCAMS HAVE ALREADY HIT YOU

- On Thursday morning EMPLOYEE received an e-mail from “BOSS” that asked her for a big favor for me, that I needed gift cards from Amazon or WalMart for my employees “up here” and that I needed them fast so I needed her to buy them on the company amex card and then scan images of them after she scraped off the paste covering the security codes.

- Employee spent a lot of time on Thursday trying to get them online and was unsuccessful because of different fraud issues, but “BOSS” was patient but persistent that this was very important to him and that it needed to be done secretly so that he could surprise his employees.

- Company lost $ 9,000

- Another client, office manager walked to Apple Store to buy $5000 in gift cards.
PATCO CONSTRUCTION

- A Maine-based construction firm got infected with the Zeus Trojan virus and $588,851.26 was transferred from their accounts. Their bank recovered $243,000 but Patco was on the hook for $345,000. Patco was dragged through three years of lawsuits by their bank before the case settled.

  "We had hundreds of thousands of dollars in legal fees," says Patterson. "So even after we got the $345,000 back, we lost hundreds of thousands."
CHINA-BASED HACKERS TARGET LAW FIRMS TO GET SECRET DEAL DATA

- China-based hackers looking to derail the $40 billion acquisition of the world’s largest potash producer Potash Corp (Ca) by an Australian mining giant BHP Biliton Ltd (Aus) zeroed in on offices on Toronto’s Bay Street, home of the Canadian law firms handling the deal.

- Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada’s Finance Ministry and the Treasury Board.

- Bloomberg.com
GOOGLE’S DOORS HACKED OPEN – OPENED WITHOUT RFID

- Tomaschik looked at the encrypted messages the Software House devices (called iStar Ultra and IP-ACM) were sending across the Google network, he discovered they were non-random; encrypted messages should always look random if they’re properly protected. He was intrigued and digging deeper discovered a “hardcoded” encryption key was used by all Software House devices. That meant he could effectively replicate the key and forge commands, such as those asking a door to unlock. Or he could simply replay legitimate unlocking commands, which had much the same effect.

- Sep 03, 2018 -
A publisher in the Netherlands has retracted 13 published studies and withdrawn 52 that were under consideration (but not yet published) after learning that someone illegally accessed its workflows to add fake authors and manipulate text.

According to Seyyed Mohammad Miri, the founder, CEO, and managing director of Kowsar Publishing, the 13 retracted papers all included extra authors added by the same Internet Protocol (IP) address. Cyber police in Iran found the same IP address had also accessed the 52 other papers, which were in various stages of the publishing process (such as peer review) and not yet online, Miri told Retraction Watch.

YOU ONLY THOUGHT YOU WERE IN THE PUBLISHING BUSINESS

- *Nature News* revealed that a Brazilian citation cartel had been outed by Thomson Reuters. That’s right: a citation cartel.

- A scholarly version of SEO spamming
YOU ONLY THOUGHT YOU WERE IN THE PUBLISHING BUSINESS

• “I no longer believe that when I publish articles in journals with minuscule circulations I am contributing to the field—if by “field” we mean the thousands of well-meaning individuals who go to work each day in places called schools.” – Sam Waineburg, Professor of History & Education at Stanford

• He & his students made high-quality curricula available to 5 San Francisco high schools.

• HS teachers forwarded links – 200,000 downloads by year-end

• No Ranking, impact invisible to institution reviewers

REALIZE THAT DATA IS YOUR BUSINESS
Brainlink's Defense In Depth

- Security Awareness Training
- Email Protection
- Application Security
- Network Security
- Backup and Disaster Recovery

PLAY DEFENSE
USE PASSWORD MANAGERS & MULTI-FACTOR AUTHENTICATION
SHARE HISCOX’S SMALL BUSINESS HACK VIDEO WITH YOUR TEAM

https://www.youtube.com/watch?v=DeCL4TAi0CE
HOW DO YOU PROTECT YOURSELF FROM MUGGERS, THIEVES, HACKERS & SPIES?

Stay vigilant.

Two lawyers walking through the woods spotted a vicious looking bear. The first lawyer immediately opened his briefcase, pulled out a pair of sneakers and started putting them on. The second lawyer looked at him and said, "You're crazy! You'll never be able to outrun that bear!" "I don't have to," the first lawyer replied. "I only have to outrun you."

Your job is to outrun your competitors!
Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
C: 917-685-7731
raj@brainlink.com
www.RajGoel.com
www.linkedin.com/in/rajgoel
@ra الجو ال_ ny

Author of

UNPLUGGED Luddites Guide To Cybersecurity

The Most Important Secrets To Getting Great Results From IT
http://www.amazon.com/gp/product/0984424814
ABOUT BRAINLINK

✓ Founded in 1994
✓ Works Like An Extension of Your Firm
✓ Wide Range of Skills & Fun To Work With
✓ Dedicated To Increasing Your Productivity & Profitability
✓ 2015 SmartCEO Winner for our “SOP Culture”
✓ 2015/2016 Gotham City Networking “Networker Of The Year”
✓ Recognized as Sophos’ most heavily certified partner in NYC
✓ Brainlink’s CTO serves as the Cyber Security expert for WPIX-11, Bloomberg, CNN, CNBC, etc.
✓ Recognized as Top 100 Financial Focused MSPs in North America (2018)
✓ Recognized as Top 100 in MSP501 List (2018)
✓ Named Channelnomics Innovation Award – Most Progressive Partner (2018)
✓ We have a PROVEN Track Record for Construction DISASTER RECOVERY PLANNING

You Run Your Business And Leave The IT To Us.
HOW CAN WE HELP YOU?

- We assist clients in performing risk & threat analysis.
- We implement sane, effective security, governance & data protection solutions.