Security Collaboration for Library Resource Access

Corey Roach, CISO
University of Utah

SNSI Security Summit
October 2020

Corey Roach

- Chief Information Security Officer (CISO)
- Joined the University of Utah in 1998
- 18+ years of Information Security Experience in Higher Ed
- Information Security Office - 34 Employees
  - Enterprise Security (Engineering, Incident Response)
  - Security Assurance (Security Operations Center)
  - Governance, Risk, and Compliance
  - Identity and Access Management
An Interesting Challenge

Unique Privacy Requirements
Fragile Assets
Limited Resources
Limited Legal Support

Threat Vector

Phishing
Social Engineering
Credential Re-Use
Hacktivism

Technology alone does not solve “People Problems”
Technology Overview

Web Server Automation Analysis
Multi-Factor Identity Log Storage
Customer Web Proxy Web App Firewall

Typical Library Proxy Service

Typical Logs

Library Logs:
- Timestamps
- Basic Browser Info (UA)
- Username
- Customer IP
- URLs Requested

Publisher Logs
- Timestamps
- Proxy IP
- URLs Requested
Typical Library Proxy Service

Typical Web App

Typical Web App - Logs

**Web App Owner Logs:**
- Timestamps
- Extensive Browser Info
- Username
- Account Information
- Customer IP
- URLs Requested
- 2-Factor Device Info
- Geographic Location

- User Behavior
- Biometric Data
- Threat Correlation / Info Sharing
Modern Library Design

**Library Logs/Info:**
- Timestamps
- Extensive Browser Info
- Username
- Account Information
- Customer IP
- URLs Requested
- 2-Factor Device Info
- Geographic Location

- User Behavior
- Biometric Data
- Threat Correlation / Info Sharing

**Publisher Logs:**
- Timestamps
- Proxy IP
- URLs Request
Obstacles?

Privacy
Expertise
Cost

Publisher / SNSI Support

• Develop or subsidize a low-cost proxy or plug-in
• Facilitate threat information sharing
• Provide administrator training
• Promote community
• Provide pricing incentives to share risks

Other Opportunities

• Foster security advocates, provide materials
• Educate leadership on shared risks
• Educate users on personal risks
• Promote to customers the value of publishers
The threat presented by Sci-Hub and other state-sponsored or individual bad actors

Crane Hassold
  • Sr. Director, Threat Research, Agari Data Inc.

AGARI

Silent Librarian, Sci-Hub, and State-Sponsored Actors

Crane Hassold
Sr. Director of Threat Research, Agari

Who Am I?

• 11 years in the FBI
• Helped create the FBI’s Cyber Behavioral Analysis Center (CBAC)
• Built two phishing threat intelligence teams
• Currently oversee the Agari Cyber Intelligence Division
• Focus is Business Email Compromise (BEC)
Silent Librarian: An Overview

- Active since 2013
- Linked to Iranian threat actors
- Targets global colleges/universities
  - 300+ schools in 22 countries
- Phishing pages mimic library login pages
- Purpose is to compromise student/faculty credentials
- Motivation?
  - Theft of academic journal articles
  - Theft of other sensitive research

Silent Librarian: Attack Process

- Lure emails from university "library"
- Consistent for years
- Direct spoofing of university addresses
- Use of shortened URLs behind look-alike URLs
- Phishing URLs very similar to legitimate URLs

Dear Student,

This is an automatically generated email from IT Services, Carleton University.

IT standards for computer passwords and system access controls state that an appropriate library access must be enabled in order to use the library at Carleton University. Our records indicate that your library account has not been used for a period of time.

Please click the URL link below to update your library account for access.

University Library

If you have not renewed your library account by the date mentioned above, your access to the library and its services will expire. If you have any questions arising from this notice, contact the Library Helpdesk. For a list of the current library online services, please visit:

https://library.carleton.ca

Yours sincerely,

MacOwen Library - Carleton University
1125 Colonel By Dr. Ottawa, ON, K1S 5B6, Canada
library.services@carleton.ca

Legitimate URLs
shibboleth.mcgill.ca
libproxy.library.unt.edu
librarryssso.vu.edu.au

Phishing URLs
shibboleth.mcgill.ca.ifttt.tk
libproxy.library.unt.edu.itlib.me
librarryssso.vu.cvr.it
Silent Librarian: Links to Mabna Institute

- March 23, 2018: USDOJ indicts 9 Iranian individuals connected to the Mabna Institute
  - $3.4 billion in intellectual property loss
  - 31.5 TB of academic data stolen
  - ~8000 university account compromised
  - Also targeted government agencies, private companies, and international NGOs
- Silent Librarian = Mabna Institute

Silent Librarian: Indictment Aftermath

- Worked with REN-ISAC to mitigate phishing sites
- April 11, 2018: Testified at House committee on foreign threats to US research and academic institutions
  - Other witnesses focused on physical threats
- Indictments have had no impact on deterring future attacks
Sci-Hub

- Launched in 2011 by student in Kazakhstan
- Contains pirated copies of academic journal articles
  - 81 million+ articles
- Top countries using Sci-Hub: India, China, US, Brazil, Iran
- How do they get articles?
  - "Donated"
  - Phishing?
  - Potential link to Silent Librarian?

Motivations for Cyber Attacks

ECONOMIC
- Cybercriminals
- State-affiliated contractors

POLITICAL
- Nation-state actors

SOCIAL
- Hacktivists
What Motivates Silent Librarian and Sci-Hub?

**ECONOMIC**

**Silent Librarian**
- Access to journals sold on Iranian marketplaces

**Sci-Hub**
- Created in response to high cost of journal paywalls
- “Napster for journal articles”

**POLITICAL**

**Silent Librarian**
- “Acted at the behest of the Iranian government”
- Potential for intelligence gathering

**Sci-Hub**
- Potential backing by Russian government?
Nation-State Actors: Myths vs. Reality

- Biggest difference between cybercriminals and nation-state actors:
  - Cybercriminals driven by **profit**
  - Nation-state actors driven by **mission**
- Not all nation-state attacks are **technically** sophisticated
- DNC Compromise – basic Google Accounts phishing page

**vs.**

-Recent GRU indictments – NotPetya, Olympic Destroyer, BlackEnergy, etc.

---

Thank You

**Crane Hassold** | Sr. Director of Threat Research
chassold@agari.com
@CraneHassold

Agari Cyber Intelligence Division (ACID)
https://acid.agari.com
Polling Question 2

How much do you know about the different kinds of cybersecurity threats to the scholarly infrastructure (how peer reviewed literature and open access content is shared, funded and trusted)?

Library patron security and why it’s important

Linda Van Keuren
  • Assistant Dean for Resources & Access Management
  • Dahlgren Memorial Library at Georgetown University Medical Center
Library patron security and why it’s important

Cybersecurity Landscape: Protecting the Scholarly Infrastructure
Scholarly Networks Security Initiative
October 22, 2020

Linda Van Keuren,
Assistant Dean for Resources and Access Management
Dahlgren Memorial Library, Georgetown University Medical Center

Patron security

- Credentials
- Institutional networks
- Personally identifiable information and confidentially
- Intellectual property
Minimizing risks

- Easy access
- Collaborate
- Educate
- Policies
- Federated authentication

DML case study

Dahlgren Memorial Library (DML)
- Graduate Health and Life Sciences Research Library at Georgetown University Medical Center

- 99.9% online collections
- Serves the 6,500 FTE of Schools of Medicine, Nursing, Biomedicine, a Cancer Center and Hospital
Federated authentication

- 5 years ago - IP based authentication for library resources
  - Security concerns
  - Acquisitions model
  - Minimal statistics
  - Hospital access

Federated authentication

- Created logic
- Added attribute
- Configured connection
- Provisioned resources
- Contacted publishers
- Updated URLs
Federated authentication

- Robust security
- Precise response to misuse
- Better identity management
- Streamlined license term compliance
- Integrates resource access into user workflow

Thank you

Contact:
Linda Van Keuren
lav30@georgetown.edu
Foreign interference in academia

Joseph DeMarco
- Partner, DeVore & DeMarco LLP