CYBER THREATS

November 2022

AGENDA

- Common Misconceptions
- Corrections to Misconceptions
- Cyber Crime Trends
- News Around the U.S.A.
- Targeting Colleges and Universities
- Incoming Help

Common Misconceptions

"My organization is so small, no one would target us."

"We don't have any valuable intellectual property on our systems, we are not a research institution."

"We are entirely cloud-based and the application encrypts our data in the cloud."

"We have back-ups and insurance, so we are not very concerned about cyber events."

Corrections to Common Misconceptions

"My organization is so small, no one would target us."

- ***Correction: Bad actors will target you because you are small. It's easy to them.***

"We don't have any valuable intellectual property on our systems, we are not a research institution."

- ***Correction: Bad actors do not pick targets exclusively because of intellectual property. Many just cast a wide-net for victims, indiscriminately to see what value, of any kind that can be extorted.***

"We are entirely cloud-based and the application encrypts our data in the cloud."

- ***Correction: If the bad actor finds the correct credentials for the application, all encryption melts away.***

"We have back-ups and insurance, so we are not too concerned about cyber attacks."

- ***Correction: Back-ups are often encrypted or infection at the same time, or immediately after, the primary network is attacked. And, insurance coverage does not guarantee a painless, easy, or complete restoration. Sometimes, insurance may only cover minimal costs associated with the event. It is entirely dependent on the type of coverage.***

Trends Identified in Cyber Crime

Statistics from the Louisiana State Police Cyber Crime Unit Honeypots:

- Honeypots are fake networks, designed to look like various types of businesses in Louisiana with technological vulnerabilities to attract bad actors to study their behavior and tactics.

- **During last 6 months, the Honeypots saw:**
  - 31,922,944 Denial of Service Attacks
  - 12,729,848 File Server Brute Force attacks
  - 9,031,750 Web Site/Web Database attacks
  - 1,046,807 attacks on unpatched networking equipment
  - 622,087 attacks on unpatched Microsoft exchange servers
  - 4831 malicious files/viruses uploaded to honeypot fileserver (~3 a day)

- **Bad Actors' Endgames**
  - Build a botnet army
  - Steal credentials
  - Remote access systems
  - Crypto-mining

- Ransomware/Encryption is the **LAST STEP** in an attack after all other value is extracted.

Trends Identified in Cyber Crime

Top 5 Types of Malware Uploaded:

- Mirai A (botnet)
- Xorddos (Denial of service botnet)
- Zeus (Credential Stealing)
- Trickbot/Ryuk (credential stealing, remote access backdoor)
- BITRAT (remote access trojan)

Top origins of attack

- Brazil
- US
- Netherlands
- Russia
- UK
- China

24 Hours worth of Attack Data:

- 779,793 Fileserver attacks
- 285,867 Remote Access Attacks
- 200,238 Cisco networking equipment attack attempts
- 9,948 Microsoft Exchange Server attacks
- 3,948 Internet Connected Device Attacks (thermastats, security cameras, power management)

Trends Identified in Cyber Crime

What does this small business data have to do with a university?
If a small business is hit this hard, imagine how hard a university is hit by malicious actors, outside the network AND FROM WITHIN the network (students and faculty).

How can the University collect and study data like this?
ASK! The Louisiana State Police Cyber Crime Unit can monitor this type of activity on a university network by establishing its own Honeypot. The Honeypot is separate from the University network and does not create known opportunities for cross-contamination. Honeypots generate mass amounts of data for raw research and analytics studies.

Point of Contact for Honeypots:
IST Darrell Miller
Darrell.Miller@la.gov
225.892.8795

News Around the Country

August 2022
Cyber attack on an art college in the USA
Savannah College of Art and Design (SCAD) - Savannah, Georgia, Georgia, USA (Chatham County)

SCAD suffers data breach, 'limited number' of current and former students, employees impacted
https://eu.savannahnow.com/story/news/20...

September 30, 2022
Cyber attack at a private university in Mississippi
William Carey University - Hattiesburg, Mississippi, USA (Forrest County)

William Carey comes under ransomware attack
https://www.wdam.com/2022/10/01/william-...

August 12, 2022
Facebook account of a university in Kentucky hijacked
Thomas More University - Crestview Hills, Kentucky, USA (Kenton County)
An alternative account was put into operation.

The Thomas More University Facebook account 'Thomas More University' was hacked.
https://www.facebook.com/ThomasMoreUnive...

July 29, 2022
Ransomware at a US university
Whitworth University - Spokane Valley, Washington, USA (Spokane County)

Whitworth University Confirms Data Breach Was Ransomware
https://www.govtech.com/education/higher...

January 2022
Cyber attack on a university in Colorado
University of Colorado Boulder - Boulder, Colorado, USA

University is victim of cyberattack, prompting campus-wide password changes
https://www.cuindependent.com/2022/02/10...

March 2022
Ransomware at a university in North Carolina
North Carolina A&T State University (N.C. A&T) - Greensboro, North Carolina, USA

Ransomware sent North Carolina A&T University scrambling to restore services
https://arstechnica.com/information-tech...

Targeting Colleges & Universities

Why are Educational Institutions Targets of Cyber Crime?

- Zero-Trust
  - Ability to back-door into another system (Federal agencies, larger university networks, corporate systems)
    - Private corporate entity or federal agency may be conducting research there.
  - Pivot or escalate access
    - Bad actors use easiest point of access to escalate to higher-value targets.
  - Ability to access teaching hospitals (nursing or medical schools)
- Fresh Batches of Unscathed Credit Reports
  - University and K-12 students often have unfrozen credit – easily accessible and rarely check their credit reports for unauthorized activity.

United States Department of Justice

FOR IMMEDIATE RELEASE — Wednesday, May 11, 2022

Man Charged with Using Stolen Identities of UCSD Students in Bank and Pandemic Unemployment Insurance Fraud Schemes

Assistant U. S. Attorney Eric R. Olah (619) 546-7540

NEWS RELEASE SUMMARY – May 11, 2022

SAN DIEGO – Nehemiah Joel Weaver was indicted by a federal grand jury for using stolen personal information of University of California San Diego students in furtherance of bank and pandemic unemployment insurance fraud schemes.

Weaver is charged with 60 felony counts, including bank fraud, mail fraud, wire fraud, aggravated identity theft, extortion, and obstruction of justice.

Weaver's co-defendant, Mia Nikole Bell, entered a guilty plea last week to one count of felony bank fraud. In her plea agreement, Bell admitted that when she was an employee at UCSD, she stole the personal identifiable information ("PII") of at least eight students and shared it with the intent to facilitate a bank fraud scheme. Bell's sentencing is set for August 15, 2022.

The indictment charges Weaver with using identities he obtained from Bell and other sources. Specifically, Weaver used stolen identities to apply for accounts and loans at a financial institution, to obtain more than $200,000 in benefit payments from the State of California's Employment Development Department ("EDD"), and to defraud the State of Arizona's Department of Economic Security ("DES") out of more than $27,000.

As part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020, Congress provided new unemployment benefits for those affected by the COVID-19 pandemic who would not otherwise qualify for unemployment insurance. The EDD administers unemployment insurance benefits in California, and DES does the same in Arizona.

Targeting Colleges & Universities

Why are Educational Institutions Targets of Cyber Crime?

- Theft of Research Data
  - Agricultural
  - Petroleum
  - Cybersecurity products
- Obtain credentials for future Brute Force Attacks
  - Cyber criminals conduct their own password analytics
- Blanket Attacks from Zero-Day Exploits
- Cybersecurity is often underfunded
  - So, attacking small institutions is sometimes easy
  - Often find flat networks, so bad actors can access entire network system without much impediment
- Financial Motivations –
  - Account numbers
  - Wiring Instructions

The Hacker News

Why Ransomware in Education on the Rise and What That Means for 2023

October 24, 2022 The Hacker News

The rise of ransomware attacks on education this year

Ransomware groups often target education, with effects including unauthorized access and theft of staff and student PII. The uptake of teachers, staff, and students working and learning online has expanded the threat landscape, with ransomware attacks on education trending upward since 2019. .

The FBI confirmed compromised education passwords for sale, including a dark web ad for 2,000 US university usernames and passwords on the .edu domain suffix, in 2020. In 2021, the FBI identified 36,000 email and password combinations for accounts on .edu domains on a publicly available instant messaging platform.

This year, the FBI found multiple Russian cybercriminal forums selling or revealing network credentials and VPN access to "a multitude of identified US-based universities and colleges, some including screenshots as proof of access."

Beefing up security for 2023

Attackers buy and sell breached passwords on the dark web by the millions, knowing that, due to password reuse, the average credential grants access to many accounts. Criminal hackers count on it so they can stuff breached passwords into login pages to gain unauthorized access. That illicit access to accounts allows hackers to gain access to sensitive data, exploit an open network, and even inject ransomware.

Incoming Help

- The Division of Administration, Office of Technology Services (OTS) is working with Board of Regents to offer Endpoint Detection and Response Software (EDR Software) to all 31 institutions of Higher Education for all (approx.) 113,000 IHE endpoints.
  - EDR Software comes with commercial 24/7 monitoring.
  - EDR Software to treat individual IHE as its Client (not OTS).
- OTS and Louisiana Military Department creating Office of Cyber Readiness to offer cyber readiness assessments for all public entities
  - *Similar to vulnerability assessments.*
- OTS and Board of Regents in **very early stages of** developing pilot program to create franchise-like LONI-enabled Security Operations Centers for Louisiana IHEs
  - Details TBD.

Recommended Self-Help Measures:

- Get a Cyber Incident Management and Response Plan
- Create network map.
- Invest in or accept free Endpoint Detection and Response Software.
- Identify vulnerabilities and start prioritizing remedial measures by budget and impact.

QUESTIONS?

CONTACT INFORMATION

Dustin Glover
Chief Cyber Officer
225.773.6719
Dustin.Glover@la.gov

LTC Stephen Durel
Co-Lead of ESF-17
504.418.0957
Stephen.Durel@la.gov

Corey Bourgeois
OTS Cyber Incident Manager
225.279.4877
Corey.Bourgeois2@la.gov

CMSgt Don Hermann
Infosec Expert
504.237.7841
Don.Hermann@la.gov

Sarah Anderson
ESF-17 Counsel
225.615.0810
Sarah.Anderson@la.gov