Ransomware

Jim Basney
Director, Trusted CI
jbasney@ncsa.illinois.edu

MS-CC Cybersecurity Community of Practice

October 10, 2023

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Growing Ransomware Risk to Science

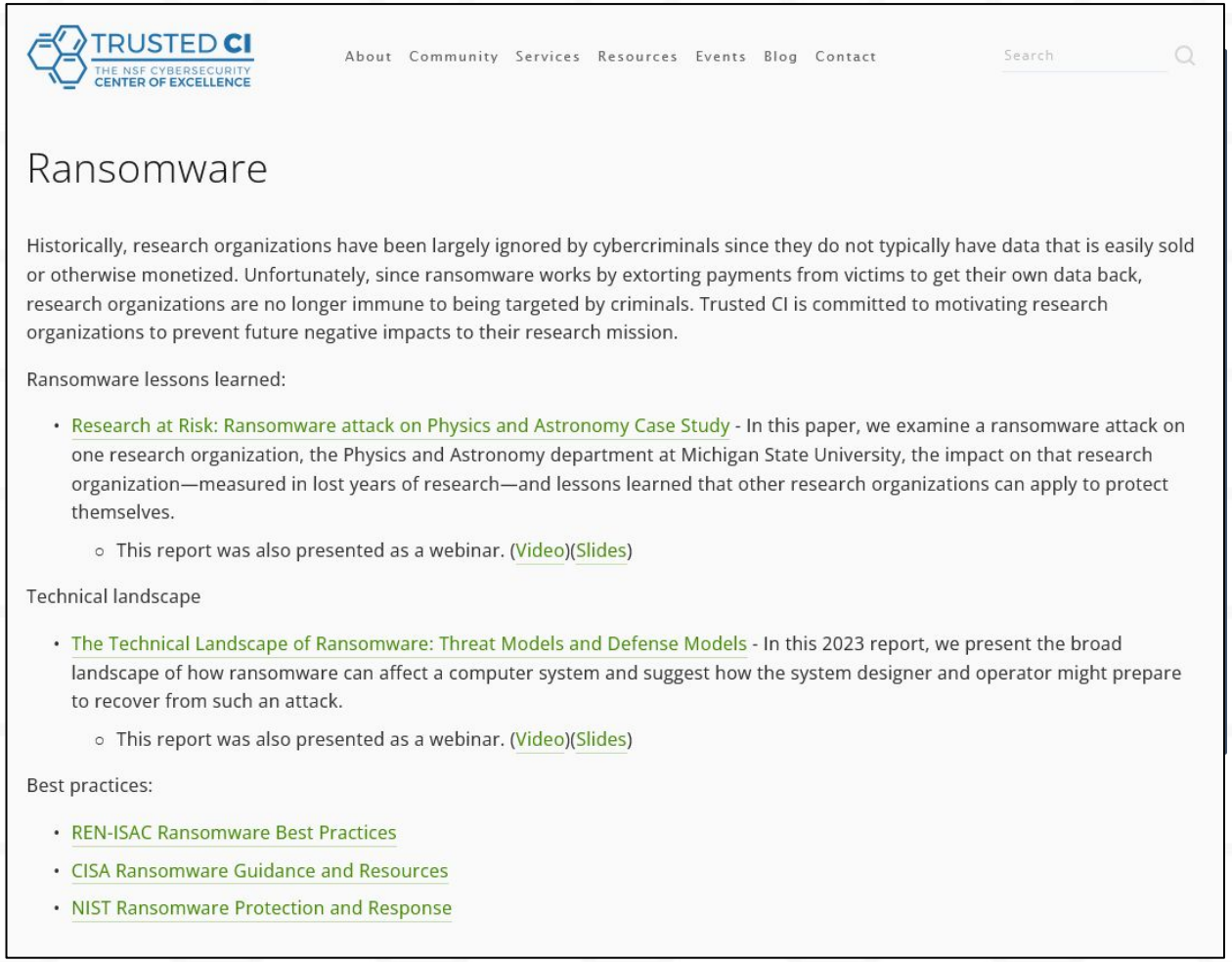
Ransomware has changed the cybercrime landscape, broadly expanding potential victims to include hospitals, schools, cities, and researchers.

Trusted CI is warning researchers to take the risk seriously and be prepared for business continuity and extortion attacks.

We are collecting resources at:

https://www.trustedci.org/ransomware

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE



Traditional Cybercrime: Hack where the money is…

Hack

Steal

Cash, CC#s, SSNs, etc.

Bank, store, etc.

Photo by Nikita Belokhonov: https://www.pexels.com/photo/anonymous-hacker-with-on-laptop-in-white-room-5829726/
Photo by panumas nikhomkhai: https://www.pexels.com/photo/close-up-photo-of-mining-rig-1148820/
Photo by Pixabay: https://www.pexels.com/photo/1-us-bank-note-47344/

Ransomware:
Hack the data, then extort the money…

Hack

Steal and/or Encrypt

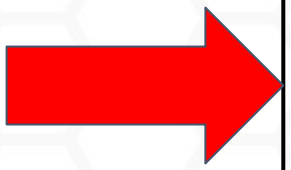
Extort

Photo by Nikita Belokhonov: https://www.pexels.com/photo/anonymous-hacker-with-on-laptop-in-white-room-5829726/
Photo by Christina Morillo: https://www.pexels.com/photo/software-engineer-looking-at-an-ipad-1181335/
Photo by Pixabay: https://www.pexels.com/photo/high-angle-view-of-a-man-256381/
Photo by Markus Spiske: https://www.pexels.com/photo/codes-on-tilt-shift-lens-2004161/

Traditional Cybercrime

Banks
SSNs
CC#s
Medical fraud

Those with fungible data and, in general, enough money to afford strong cybersecurity



Ransomware

K-12
Cities
Universities
etc.

Anyone with data and with money, though perhaps not enough money to afford strong cybersecurity

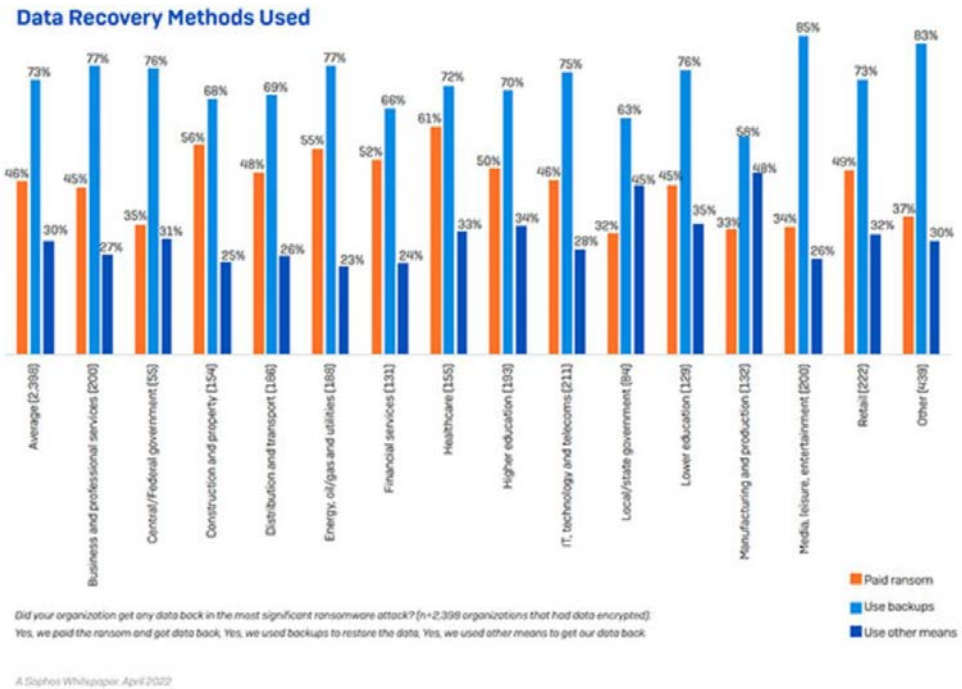
CAMPUS TECHNOLOGY

Cybersecurity Research

Ransomware Hit 64% of Higher Ed Institutions Globally in 2021, Sophos Survey Finds

Higher Ed Was Slowest of all Sectors to Recover, State of Ransomware Report Says

- By Kristal Kuykendall
- 04/27/22



TechRepublic.

Higher education institutions being targeted for ransomware attacks

by **Brian Stone** in **Security**
on May 18, 2022, 2:12 PM PDT

Three colleges have been victims of cyberattacks in the last three months alone.

Image: normalfx/Adobe Stock

While higher education is typically not thought of as a targeted industry for ransomware attacks, a trend may be forming. Three different colleges, North Carolina A&T University, Lincoln College and Austin Peay State University have all been negatively impacted by these types of cyberattacks, with one even leading to the closure of Lincoln College due to the scale of the hack.

INNOVATION

Ransomware Gangs: Who Are They And How To Stop Them

Stu Sjouwerman Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Sep 27, 2021, 09:15am EDT

Stu Sjouwerman is the Founder and CEO of KnowBe4 Inc., the world's largest security awareness training and simulated phishing platform.

GETTY

Cyber-extortion is a thriving trillion-dollar industry run by organized crime syndicates. These ransomware gangs are increasingly becoming more sophisticated, not just in terms of business models but in posturing as corporate entities while simultaneously making extortion demands. These crusaders of crime are trying to gain acceptance as legitimate enterprises, and they're starting to operate as such, coordinating efforts with various partners, offering 24/7 help desks staffed by representatives even branding themselves to hype reputation.

Sophisticated Attackers

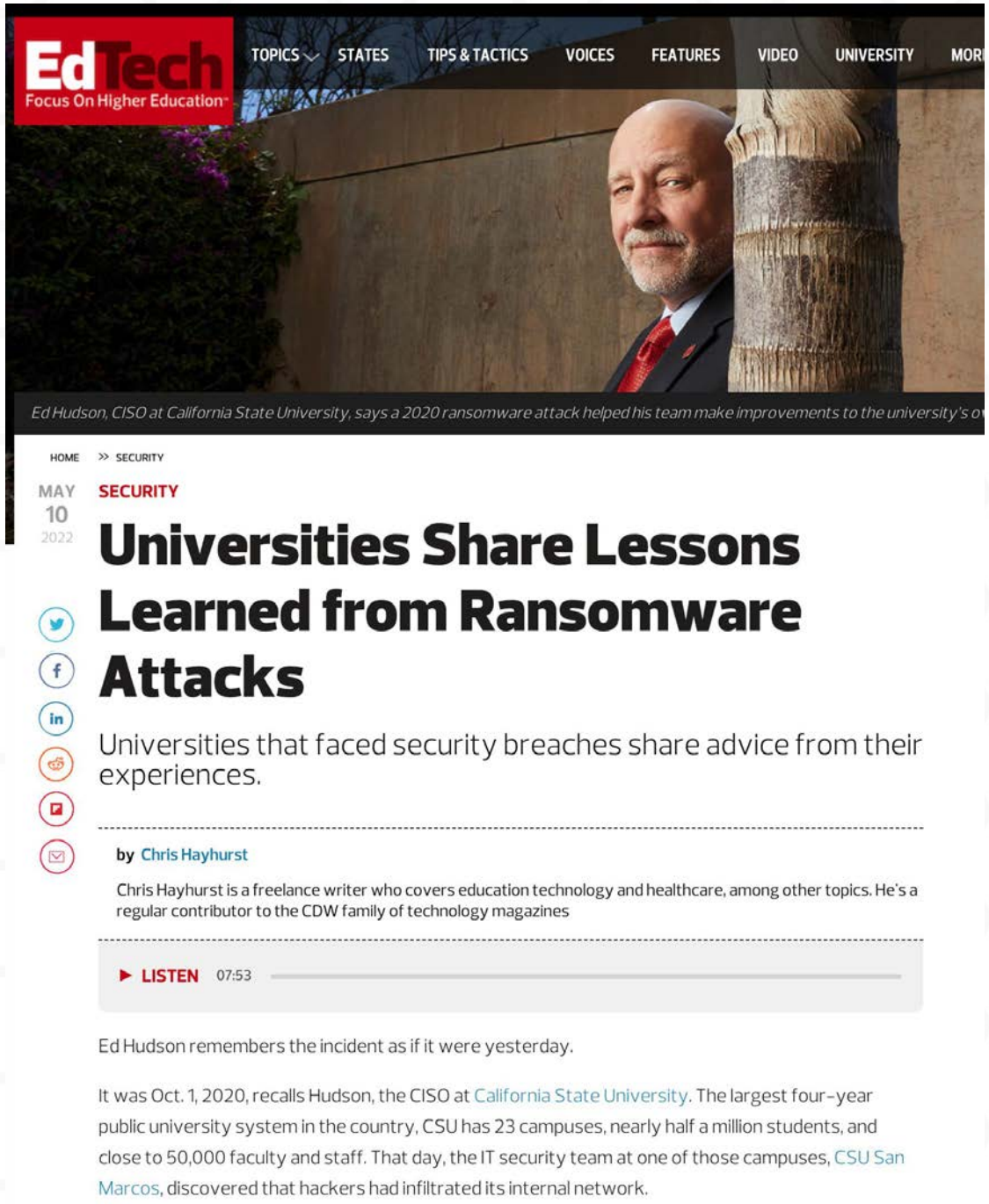
"These crusaders of crime are trying to gain acceptance as legitimate enterprises, and they're starting to operate as such, coordinating efforts with various partners, offering 24/7 help desks staffed by representatives even branding themselves to hype reputation."

Most of us are…

A large, relatively open attack surface.

Smaller information security teams than the criminal gangs.

Slower - defense is harder than offense.



"Build a collaborative network. [California State University] maintains close relationships with state and federal threat intelligence agencies, and with higher ed-focused cybersecurity organizations like EDUCAUSE and REN-ISAC."

Let's work together…

We can share intelligence and practices.

REN-ISAC: Research & Education Networks Information Sharing & Analysis Center

https://www.ren-isac.net/public-resources/Ransomware_Best_Practices.html

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

REN-ISAC

Let's Discuss

For more info:
https://www.trustedci.org/ransomware

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, 1920430, 2241313. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.