trusted CI webinar series

Title: Lessons from a Real-World Ransomware Attack on Researchers at Michigan State University

Presenters: Andrew Adams, Tom Siu, Von Welch

Host: Jeannette Dopheide

Slides: https://tinyurl.com/yfbc48ds

The meeting will begin shortly.

Participants are muted. Click the chat button to ask a question.

This meeting will be recorded.

The Trusted CI Webinar Series is supported by National Science Foundation grant #1920430.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.
Lessons learned from a real-world ransomware attack on researchers at Michigan State University

Andrew Adams, Trusted CI
Tom Siu, Michigan State University
Von Welch, Trusted CI

Trusted CI Webinar
December 6th, 2021
Introduction

Research at Risk: Ransomware attack on Physics and Astronomy Case Study
Adams, Andrew; Siu, Tom; Songer, Julie; Welch, Von

https://hdl.handle.net/2022/26638

Collaboration between MSU CIO’s Office and Trusted CI
Our Presentation

• The story of the cyberattack at Michigan State University in 2020 - Tom Siu, MSU CISO
• Lessons learned for research to be better prepared for cyberattacks - Andrew Adams
• Q&A
The Attack

During the Pandemic...June 2020

● Netwalker ransomware
  ○ Vector: vulnerable departmental VPN
  ○ Server and client vulnerabilities exploited
● Impacts
  ○ Data exfiltration from file servers- unstructured data
  ○ Malware propagated to 100s of departmental hosts
  ○ Lateral movement within department’s IT infrastructure
● Response
Investigation and Lessons Learned

Worked with MSU’s CIO office to identify and interview those involved in the incident

• Interviewed 10 involved in and/or affected by the incident
  ○ Half from MSU’s centralized-IT, half from Physics & Astronomy
  ○ *Sample questions posed to interviewees in the report*
Investigation, cont.

Divergent views from the two groups:

- Cost to science
  - Centralized-IT measured it in months
  - P&A measured it in years

- P&A’s IT staff’s cybersecurity skill set
  - P&A thought it adequate
  - Centralized-IT thought it inadequate
Investigation, cont.

3 Key Factors:

- We were doing this long before you, so we’re better at it than you.
- No thanks, we’re going to do this alone.
- Condoning a usability/productivity trumping security atmosphere.
Q&A
Thank yous

Michigan State University, especially CISO Tom Siu, CIO Melissa Woo, the staff and leadership of the Physics and Astronomy department, the dean of the MSU College of Natural Science, and everyone we interviewed.

Trusted CI is supported by the National Science Foundation under Grants 1234408, 1547272, and 1920430.

The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.
The Report

Research at Risk: Ransomware attack on Physics and Astronomy Case Study
Adams, Andrew; Siu, Tom; Songer, Julie; Welch, Von
https://hdl.handle.net/2022/26638
Staying Connected with Trusted CI

Trusted CI Webinars
4th Monday of month at 11am ET.
https://trustedci.org/webinars

Follow Us
https://trustedci.org
https://blog.trustedci.org
@TrustedCI

Slack
Email ask@trustedci.org for an invitation.

Email Lists
Announce and Discuss
https://trustedci.org/trustedci-email-lists

Ask Us Anything
No question too big or too small.
info@trustedci.org

Cyberinfrastructure Vulnerabilities
Latest news on security vulnerabilities tailored for cyberinfrastructure community.
https://trustedci.org/vulnerabilities/
About the Trusted CI Webinar series

To view presentations, join the announcements mailing list, or submit requests to present, visit: trustedci.org/webinars or email webinars@trustedci.org

Next Webinar: Trusted CI Webinar: Mon January 24th at 11am Eastern
Topic: EDUCAUSE HECVAT and OSC Engagement
Trusted CI License Statement

This presentation is shared under the Creative Commons Attribution NonCommercial 3.0 Unported (CC BYNC 3.0) license.

The full terms of this license are available at http://creativecommons.org/licenses/bync/3.0/.
Thanks!

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