Ransomware Attacks

Preparing for a Cyber Security Incident

Neenah Joint School District Team

Rocco Marchionda, Director of Instructional Technology

Thad Kraus, Systems Deployment Manager

Agenda

- Introduction
- The Attack - January 10, 2022
- CRT (800) 943-0003 x2
- Recommendations
- Questions?

Overview

- 3:00 a.m. and all is well….6:00 a.m. not so much!
- Phones - Internet Access - Security system - Message from "Threat Actors"
- Superintendent Role - Trust your Tech Team!

Wisconsin Cyber Response Team

800-943-0003 x2

Anatomy of an Attack

- Preparation
- The Event
- Response
- DeBrief

Preparation

- Incident Response Conversations
- Digital Disaster Recovery Plan
- Cyber Incident Response Plan
- Plan for Cyber Insurance

The Event

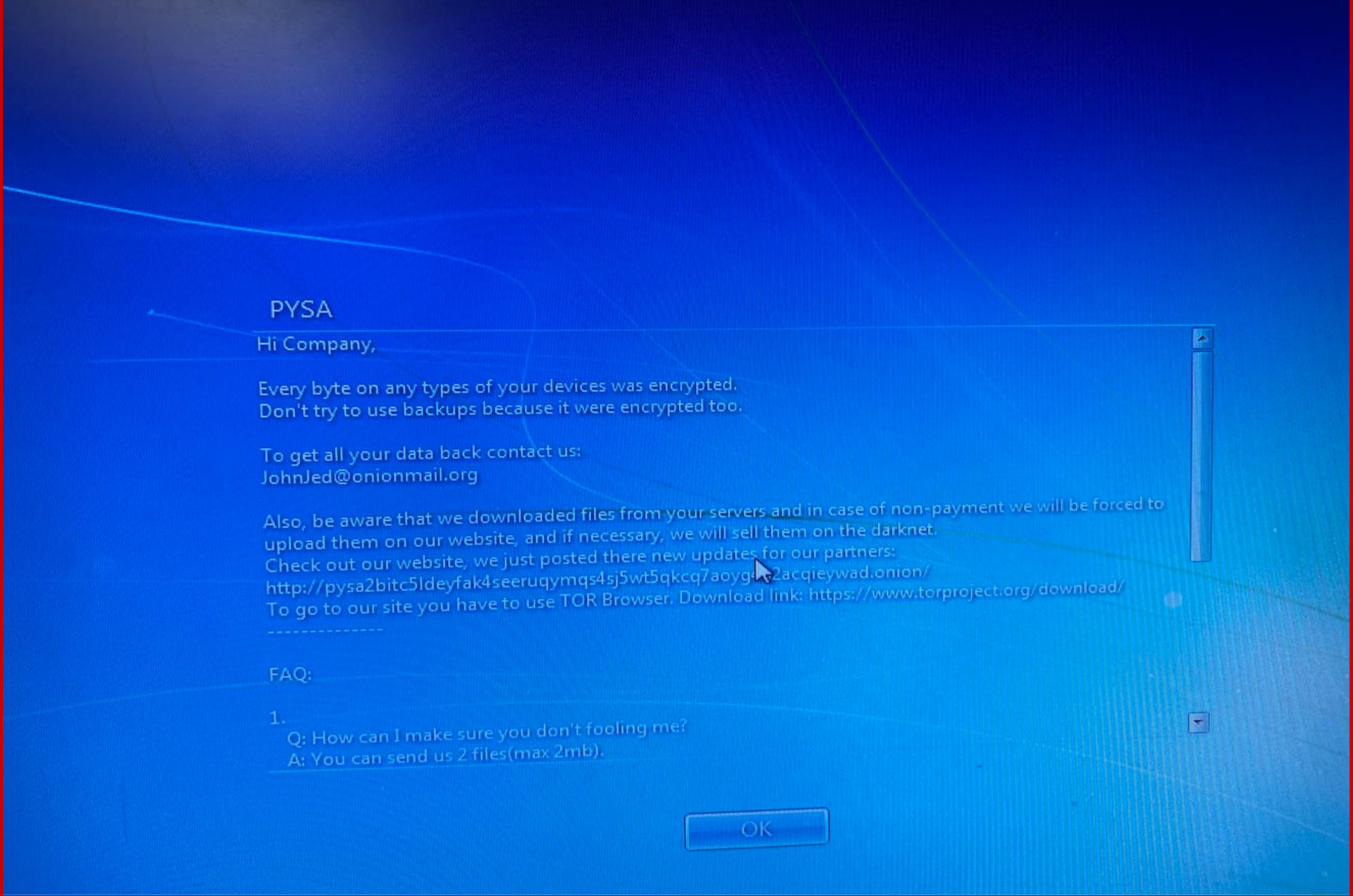
Monday Morning January 10, 2022

- Suspicious Activity Reported by Users

- Anomalies on District Equipment

- The Note

- No Access



PYSA

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
JohnJed@onionmail.org

Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet.
Check out our website, we just posted there new updates for our partners:
http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4[illegible]2acqieywad.onion/
To go to our site you have to use TOR Browser. Download link: https://www.torproject.org/download/

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

PYSA

Hi Company

Every byte on any types of your devices was encrypted.

Don’t try to use backups because it were encrypted too

To get all your data back contact us: http:\\xxxxxxxxxx

Also be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet. Check out your website, we just posted there new updates for our partners To go to our site you have to use TOR Browser.

Our Response

- Unplug EVERYTHING
- Call the CRT 800-943-0003 **x2**
- Call our Networking Engineering Company
- Call Insurance Company
- Launch the Plan
- **Take Notes**

Our Response

- Prioritize Services
- Engage Stakeholders that are needed for decisions
- Documentation

Our Response

- Divide and Conquer
    - Forensics
    - Infrastructure
    - Essential Services

Our Response

Monday January 10, 2022

- Establish Temporary Internet
- Timeline of Recovering Backups

Tuesday January 11, 2022

- Recover and Secure Critical District Services
- Recover Core Networking Services

Wednesday January 12, 2022

- Begin Restoring Staff Access to Devices and Services

Our Response

Thursday January 13, 2022

- Complete changing staff passwords
- Complete securing staff devices
- **Students return to school**

Friday January 14, 2022

- Reset student passwords
- Restore 9-12 student access to digital services

Monday January 17, 2022

- Restore K-8 student access to digital services

Debrief

- CRT: 800-943-0003 x2
- Cyber Insurance (Check YOUR Policy)
- BEGIN Cyber Response Planning - “Conversations”
- Schedule Staff Training

Debrief

- Two/Multi Factor Authentication / Endpoint Protection
- Documentation
- Breaks & Food
- Use ***YOUR*** Resources

Cyber Response Team (CRT)

- **Mission:** To provide support for critical infrastructure in the state of Wisconsin in order to prevent, mitigate and respond to cyber incidents, through training, assessment, and incident response.
- **Vision:** Coordinated response effort from the state volunteer Cyber Response Team (CRT) and National Guard, assisting in both preventing and responding effectively in the event of an emergency.

Cyber Response Team (CRT)

- Nested in DHS Strategic Plan, WI Homeland Security Strategy
- Initiated in 2015
- DMA led in collaboration with DET, WEM, and WSIC
- US Department of Homeland Security Grant Funding
- 144 members (121 public / 23 private)
- 28 facilitators (WSIC, National Guard, Coast Guard, WEM, DET, DPI, CISA, DHS)
- All volunteer

Cyber Response Team (CRT)

Support covers all 16 Critical Infrastructure Sectors

- Agriculture and Food
- Financial Services
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities (elections, education)
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water and Wastewater Systems

Cyber Response Team (CRT)

- 6 of 464 school districts are represented (as of 8 March 2022)
- Resources Available
  - Training: Quarterly Training Program / SANS Training
  - Assessments: 11 requested for Cyber Resilience Review
  - Response: CRT / National Guard

Cyber Response Team (CRT)

Action Steps

- Encourage your staff to join the CRT
- Request an assessment: CISA, CRT, National Guard
- Incident Response Plan
  - Write/Review/Update your plan
  - Have a printed copy
  - Cyber Insurance / Infrastructure Support / CRT
- Start a cyber club: Cyber Patriot / Go CyberStart / National Cyber Cup

Communication

- Insurance Company
- Internal Tech Team
- Attorneys - NJSD & Insurance Company
- Threat Actors
- Staff
- Retirees
- Media

Wisconsin Cyber Response Team

800-943-0003 x2

QUESTIONS?

Dr. Mary Pfeiffer, District Administrator
mpfeiffer@neenah.k12.wi.us

Matt Anderson, Director of Instructional Technology
manderson@neenah.k12.wi.us

LTC Sarah Frater, WI Cyber Response Team, WI National Guard
sarah.r.frater.mil@army.mil

Thad Kraus, Systems Deployment Manager
thad.kraus@neenah.k12.wi.us