Indian Health Service

Pay Up!

$300 in Bitcoin May Get Your Data Back

SUSAN COPELAND WILSON, PH.D.

DISASTER RECOVERY /
CONTINGENCY PLANNING ANALYST

AUGUST 23, 2023 11:00 A.M.

Ransomware – A Working Definition

Malware designed to deny victim access to files on their computer(s) or system(s).

- Encrypts files
- Demands a ransom payment for the decryption key
- Paying the ransom is the easiest and cheapest way to regain access to their files

Lots of variants but they work similarly.

Analogy: a person who is behind on tetanus shots steps on a rusty nail.

- The cut becomes infected
- Gangrene develops
- Each system becomes septic and shuts down

Why Are We Here?

Because ransomware happens.

In 2022:

- 236 ransomware attacks worldwide (January – June)
- 71% of U.S. companies affected
- 62.3% of victims paid the ransom
- Per CISA, 14 of 16 of US critical infrastructure sectors were attacked
- $456.8 million extorted; most ransoms are small amounts (a few hundred dollars)

Noteworthy attacks that shut down operations

- Baltimore, MD
- Greenville, SC
- Colonial Pipeline

2024 estimate of ransom demands: $42 billion

Impacts to the Healthcare Industry

Healthcare industry is particularly targeted

- Faster ransomware response
- Overwhelmed resources
- Outdated equipment
- Resistance to cloud technology
- Interest in data mining
- Double extortion attacks increased 643% between 2020 – 2021

Unique impacts

- Life endangerment
- Financial implications
- Patient confidentiality

Pathology of an Attack

Pathology – Infection

Phishing attacks account for 91% of all malware attacks

Step 1: Infection

- Someone opens an attachment or clicks a link that introduces the ransomware payload into the network.
- Through Remote Desktop Protocol (RPD) or similar, attacker steals or guesses a user’s ID and password and unleashes ransomware.

Step 2: Ransomware encrypts files

- Infects every segment the user can access
- Infects every additional segment that other users can access
- Infects servers, communications infrastructure, workstations, backups, websites

Step 3: Ransom demanded for decryption key

- No guarantee the key will be sent
- Attackers may still exfiltrate data

Technical Impacts

IT systems: infected and inaccessible

Data and backups: infected and destroyed

Administrative access to systems: infected and inaccessible

Building security: infected and inaccessible

Building environmentals: infected and inhospitable

Critical storage (refrigerators, vaults, imaging): infected and destroyed

Internet and telephonic communications: infected and unavailable

Facility Impacts

Patient Records: unavailable

Patient Visits: paper charts, reschedule, or refer

Administrative tasks:

- Cannot make referrals or request pre-approvals for treatment
- Cannot file claims or manage billing

Patients:

- Might not receive critical care
- Might have to reschedule time and transportation, pay for child care

Operations: no way to know when operations can be restored safely

Treatment

Don’t pay the ransom!

Notify CSIRT and FBI, and follow their guidance.

Warn ALL users, vendors, dependencies, clients, etc.

Identify, find, and remove all trigger files from every device and segment

Determine the attack style: screen-lock or encryption-lock

Disconnect all devices to limit spread. This means **ALL** devices.

Treatment (continued)

Determine what can be recovered

- Perhaps from web-based software, decoded from decryption software, etc.

Determine whether backups are safe to restore

- Ransomware may last for months; backups may be infected

If you can restore:

- Apply malware packages on ALL system segments
- Systematically restore system segments
- Account for what you can’t restore

Don’t hesitate to ask for help!

Lesson Learned

Reinforce user awareness

Apply principle of least privilege

Deploy immutable backups

Upgrade and enforce strong security measures

Upgrade and enforce off-line, encrypted backups and test them

Risks to Recovery

Rise of two-stage ransoms:

- Pay to get your system back
- Pay more to avert exfiltration of your data

Recovery is really, really expensive

- Cost of recovery services (up to $5,000 per assessment)
- Number of encrypted systems
- Ransom risks
  - Attacker does not provide a valid decryption key
  - Attacker increases ransom
  - Decrypted files are corrupted
- Ransomware variant
- Speed to recover

Ransomware at IHS

Ransomware Can’t Happen to Us

YES, it can.

Several attacks over the past two years

- None on Federal networks
- All on Tribal entities

A worse-case example at IHS:

- An entire tribal government, school, and clinic were impacted
- Required an entire segmented domain rebuild
- Emergency IT resources were provided from the local Federal hospital to get the clinical back up and running at a minimal capacity
- The site was not reconnected back to IHS for 9 months

Common downtime is anywhere between a month to a year

Why Are We Really Here?

We need an exercise.

Let’s work through a table-top exercise (TTX) together.

Attack at
Sandy’s Dental Clinic

About Sandy’s Dental Clinic

Services

- Primary dental care
- Open 0830-1630, Monday through Friday
- Refers to Crazy Bull Hospital for emergencies, after hours care, critical care, periodontal care, and advanced orthodontics
- Education outreach at schools, community centers

Sees 250 clients per week

- Primarily low income children, adults, seniors
- 2 full time dentists, 2 technicians, 2 administrative staffers, 1 part-time IT person

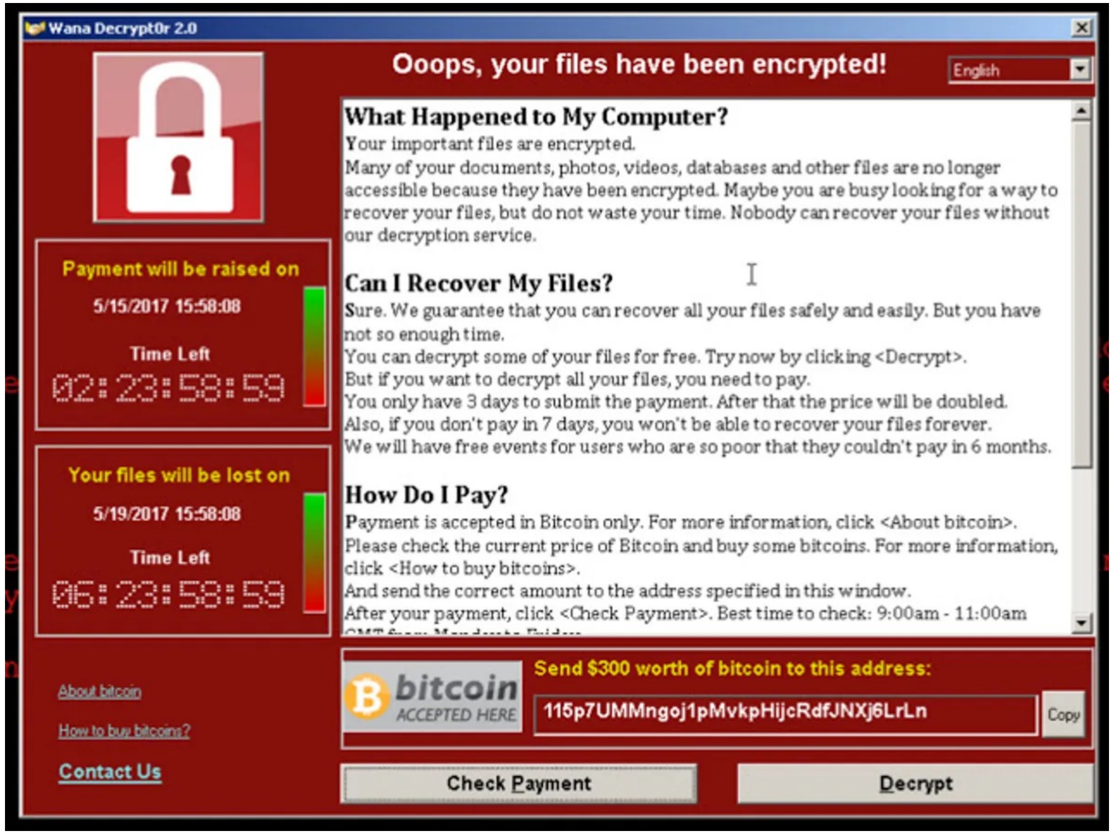
Infrastructure

- EDR, billing and claims processing software, business applications, telecommunications
- Tape backups from internet-connected server; store at Central Bank
- Test restore every two years; backup software encrypts
- Patches applied when possible but are not all current
- Periodic power outages; generators react within five minutes of detected outages

The Incident

Monday, 0800h

- Technicians turn on workstations
- Message on screen
  - $300
  - Accepts bitcoin only
- All systems locked
  - All laptops, servers, applications
  - Telecommunications shut down
  - No internet access
  - Building access management and environmentals
  - Repositories that hold temperature-sensitive medications



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Situation at the Clinic

Cannot see patients

Cannot notify patients

Clients need to be referred to Crazy Bull Hospital

Electronic building accesses is shutdown; only keyed backdoor is accessible

Internet, telephone, and online communications dead

Staff is intimidated by Bitcoin

Data is hosed

Backups are infected and corrupted; they had not been checked

Temperature-sensitive medications will be damaged or destroyed

Estimated cost to restore: $1 million

System Team Response

Who is involved?

- Suppose key responder or leadership is not available or can’t be reached?

What plans do we have for guidance?

- Suppose we have an ISCP for EDR (but it’s 3 years out of date) but none for the patient scheduling or records systems?

What do we do?

- Check backups for infection? How?
- Contact CSIRT? How?
- Contact FBI? How?

How do we determine impacts?

- Outage assessment?

Restoration Tasks

Plan Activation

- Continuity of Operations plan
- Incident response plan
- Disaster recovery plan
- Information system contingency plans

Systems

- System rebuild and sanitize (run anti-malware software on all backups)
- Technical support for telecommunications
- Change all passwords
- Rebuild / recover patient records

Financials

- Billing and claims
- Operations costs
- Insurance

Communications

- Community outreach
- Client outreach

Lessons Learned

What we learned

- Ransomware shutdown all systems and telecommunications before we identified it
- Online backups left us vulnerable
- The Incident Response Plan is obsolete and untested; doesn’t address ransomware
- Malware detection software was obsolete and unpatched
- We don’t have:
  - A segmentation policy (identify every communication so anomalies are detectable)
  - Deception tools (e.g., lures, honeypots)
  - Adequate IT staff or budget

Lessons Learned (Continued)

What we did

- Need off-line backups and backup protection software
- Need outage assessment
- Check backups for infection
- Ransomware detection and protection software

After-Action Report

Who writes this?

Outcomes

- Update plans
- Update backup protocols
- Communicate with clients that their data may have been released
- What else?

Best Practices

Planning

Risk Assessment (https://www.alertmedia.com/blog/business-threat-assessment/)

- External (e.g., weather, transportation, communications, violent acts)
- Internal (e.g., IT, supply change, utilities, hazardous wastes, accidents)

Business Impact Analysis (BIA)

Planning

- Continuity of Operations Plan (COOP)
- Disaster Recovery Plan (DRP)
- Incident Response Plan (IRP)
- Information System Contingency Plan (ISCP)

Vigilance

Preventing Attacks

Prevention beats response.

Keep operating systems, software, and applications current

- Patching, cyber-hygiene
- Configuration baseline
- Trusted software

Tighten access control

- Least privilege access
- Hardening access points
- Network segmentation

Set anti-virus and anti-malware solutions to automatically update and run regular scans

Require training, exercises, reviews for tech staff and users

Preventing Attacks (continued)

Back up data regularly and double-check that those backups were completed.

- FISMA and HIPAA requirement
- Use backup protection software that encrypts

Secure backups

- Off-site or at least off-network storage
- Make sure they are not connected to the computers and networks they are backing up.

Create a facility-specific COOP plan, incident response plan (IRP), and disaster recovery plan (DRP) in case your facility is the victim of a ransomware attack.

Response to Attacks

Typical response to cybersecurity events:

- Report to CSIRT (incident@ihs.gov)
- File with a cybersecurity insurance provider
- Engage cybersecurity expertise for cleanup, root cause analysis, and mitigation
- Do not pay ransom!

IHS follows FBI recommendations

For tribal networks, engage the FBI directly while CSIRT reports it and requests assistance from its chain of reporting:

- FBI Field Offices: https://www.fbi.gov/contact-us/field-offices
- FBI Tip Line: https://tips.fbi.gov/home
- FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/

Wrap Up

Questions?

Comments?

Experiences?

INDIAN HEALTH SERVICE · PHS · 1955