

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

RANSOMWARE

ND DEPARTMENT OF HEALTH

AUGUST 25, 2021



Beyond the Headlines: What is Ransomware?

Ransomware 101

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Malicious actors then demand ransom in exchange for decryption.



CNA website back up two weeks after insurance giant hit with 'sophisticated ransomware attack'

By ROBERT CHANDLER
CHICAGO TRIBUNE | APR. 25, 2021 AT 11:12 AM



2020 was a great year for ransomware, Palo Alto Networks says

Ransomware suspected in cyberattack that crippled major US newspapers

Source inside Tribune Publishing says printing outage caused by Ryuk ransomware infection.

Infects...Encrypts...Extorts

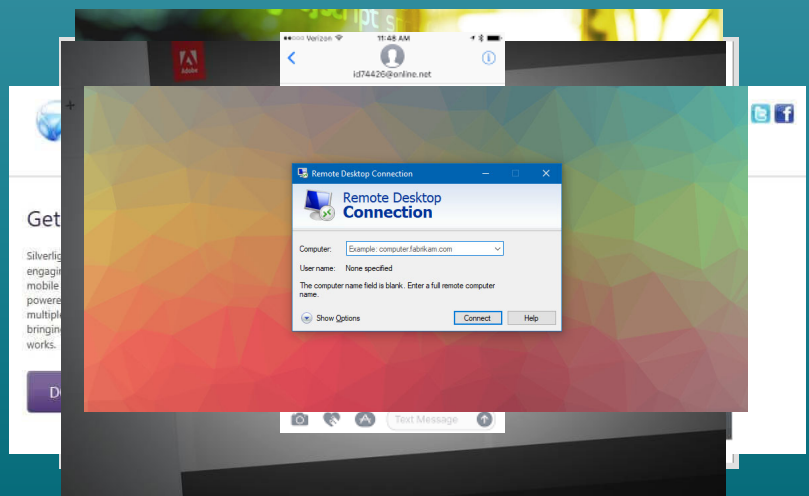
- Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
- Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.
- The monetary value of ransom demands has also increased, with demands for millions of dollars becoming commonplace.
- Ransomware incidents have become more destructive and impactful in nature and scope.



Methods of Infection

The following can all be vectors of infection for ransomware attacks:

- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Messaging Applications (Messenger, Snapchat)
- Brute Force via RDP (Remote Desktop)



Social Engineering

- One of the most prominent tactics used by attackers
- Phishing, i.e. email or malicious websites that solicit personal information by posing as a trustworthy source.
- Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail.
- Technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor.



August 25, 2021

Scenario

- Several members of your staff attend a healthcare workshop and conference in another State and report they made several new connections with vendors and other healthcare providers. They participated in an industry networking session where attendees were sharing contact information on several social media platforms.
- During the vendor show several of your staff picked up flash drives that were laying on a vendors table with product information loaded on them.

Questions

1. What types of attack could your staff vulnerable to?
2. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
 1. What type of threats could there be?
 2. What types of vulnerabilities?
3. Does your organization have a basic cybersecurity program.
 1. Review of organizational acceptable use and IT policies,
 2. Awareness of prominent cyber threats,
 3. Password procedures, and 2 Factor log-ons.
 4. Whom to contact and how to report suspicious activities?

Cyber Threats of Today

Ransomware

- WannaCry
- REvil/Sodinokibi (targeting MSPs)
- Ryuk (targeting medical, education, SLTT)
- Conti, Robinhood, Maze, Fobos, CovidLock, CryptoLocker, Pysa, VoidCrypt...

Malware

- Remote Access Trojans or RATs: **Trickbot**, Emotet, LokiBot, IcedID, BazarLoader
- Wiperware NotPetya
- ICS/OT specific: Triton/hatman malware targets Safety Instrumented Systems (SIS)

Advanced Persistent Threats (APTs)

- Energetic Bear/Berserk Bear (targets U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks)

Threats to External Dependencies

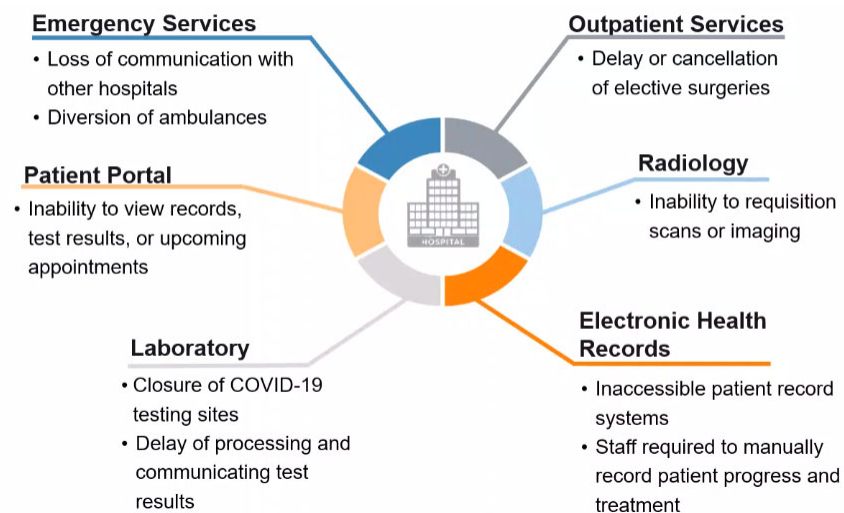
- 3rd party vendors, service providers, infrastructure providers
- Supply chain Compromise



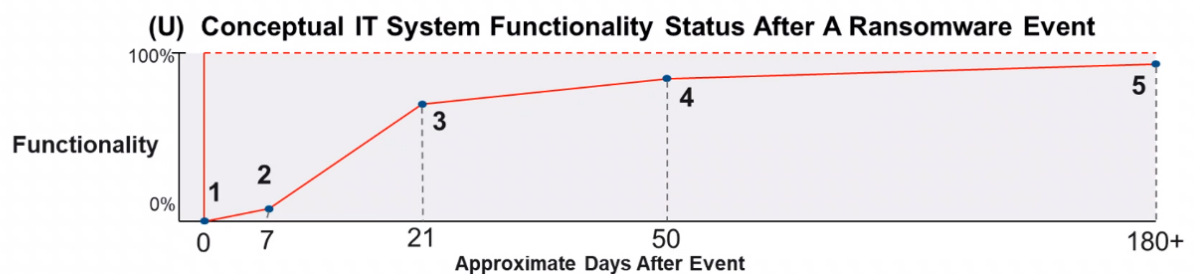
The Threat to Critical Infrastructure



(U) Ransomware: Potential Effects on Hospital Systems



(U) Ransomware and Hospital IT Operations Over Time



1. Immediately after the event, the entire IT network is down, no access to online systems.
2. Available offline back-ups of the system are accessible, restoring access to some.
3. Experts begin returning network functionality to systems after clearing hardware.
4. Majority of hardware has restored access. However, some tools remain offline for cleaning/repair.
5. All hardware has access restored. Some tools may remain out of service or require more cleaning.

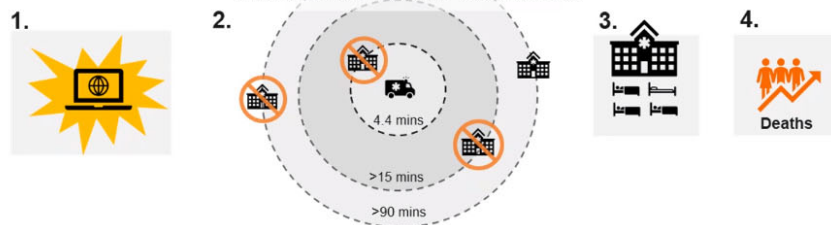


(U) Ransomware and Effects on Health Outcomes

Cyber attacks lead to

- 1) **IT network failure** and disrupt the ability of healthcare systems to access electronic health records (EHRs) and may close hospitals with IT network-based services—such as cardiac technology—and increase hospital strain (i.e., reduced capacity to take in new patients diverting critical care patients to further hospitals).
- 2) **Ambulance diversion**, which is an important system-level interruption that causes delays in treatment and effecting time tolerance, lowering quality of care. In the long term, hospitals that experience cyber events are more likely to experience
- 3) **hospital strain** (measured by ICU bed utilization), worsening health outcomes and contribute to
- 4) **increased mortality**.

(U) Conceptual Model of the Effects of Cyber Attacks on Health Outcomes



(U) This graphic is UNCLASSIFIED

April 28, 2021

9

Scenario Continued

- Shortly after the conference your IT staff notes an increase in suspicious emails.
- Several days after this a member of your purchasing staff wants to review the information about products and inserts the flash drive from the vendor.
- 3 days later all the computers in your facility are not working and display the following
- **“Deposit 5 million in Bitcoin in the following account or you will never see your Data again.”**



Questions

1. What is your initial response?
2. What system would be effected?
3. Who would you notify?

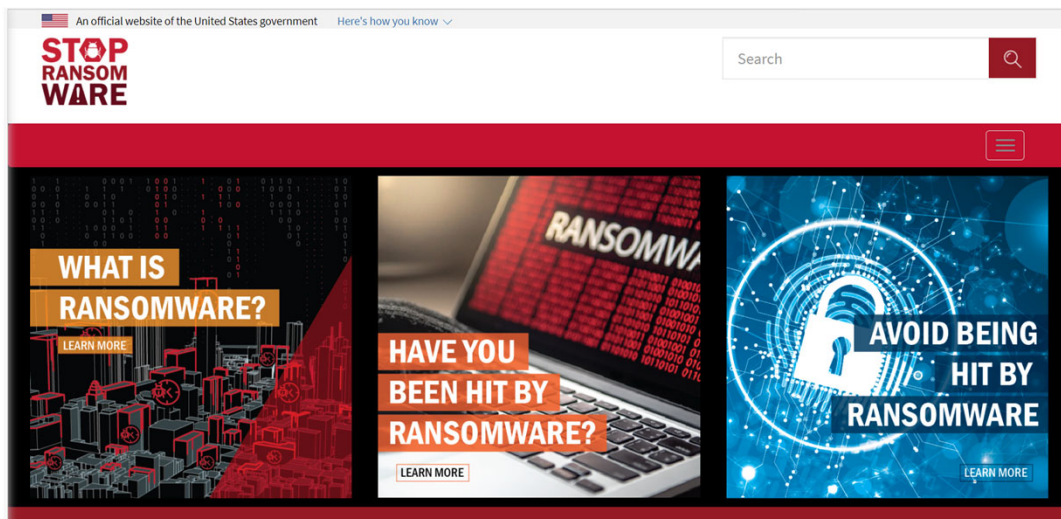
Ransomware Campaign Overview



Ransomware Campaign Key Messages



Federal Ransomware Website



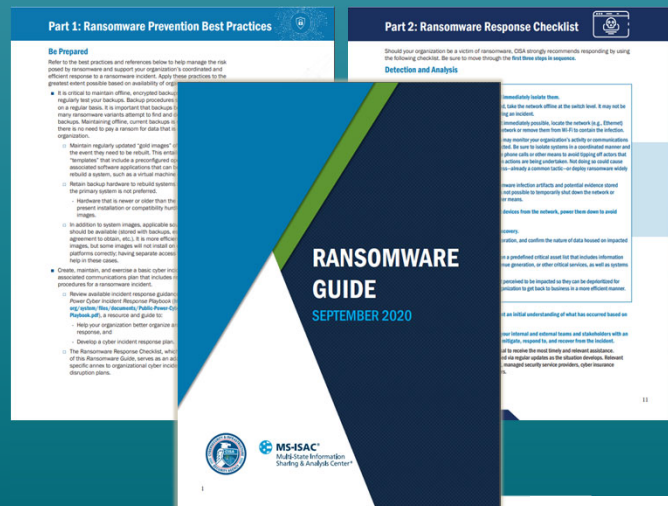
Visit [StopRansomware.gov](https://stopransomware.gov) today!

Ransomware Guide



Joint CISA and MS-ISAC Ransomware Guide

This Ransomware Guide includes recommendations, best practices, recommended incident response policies and procedures, cyber hygiene services, and several checklists that organizations can use to help protect against or response to ransomware attacks.



Ransomware Guide: Select Best Practices



Maintain offline, encrypted backups of data and regularly test your backups.



Create, maintain, and exercise a basic cyber incident response plan and associated communications plan.



Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.



CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: cisa.gov/cyber-resource-hub.



These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

Ransomware Guide: Select Best Practices



Implement a cybersecurity user awareness and training program that includes guidance on identifying and reporting suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness.



Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions.

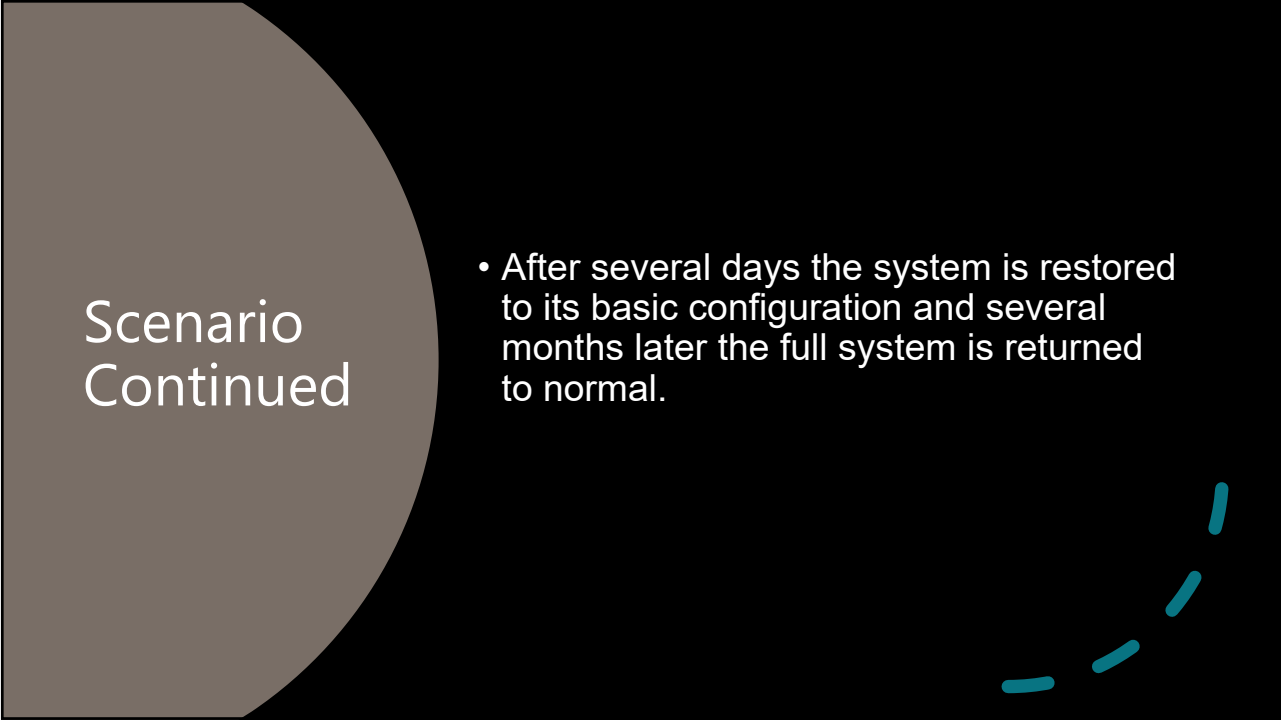


Consider risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on.



Retain and secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.





Scenario Continued

- After several days the system is restored to its basic configuration and several months later the full system is returned to normal.

Questions

1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
2. When does your organization determine a cyber incident is closed?
3. What would you change at your facilities after this attack?
4. Would you pay the ransom?

How to Prepare for, Mitigate Against



Preparation phase: How are staff trained and prepared? What tools and resources are they armed with to respond to ransomware incidents? Consider awareness and education for users here



Identification phase: How do you recognize and detect a ransomware incident? How do you go about understanding the strain of ransomware, attack vector, and attack group through gathering data and performing initial analysis?



Containment phase: For ransomware incidents, it is imperative that infected systems are quickly contained to limit the damage. How will you contain the incident from spreading to network shares and other connected devices?



How to Respond to, and Recover From



Eradication phase: How will you perform a forensic analysis of data to determine the cause of the incident, remove the ransomware from infected devices, patch vulnerabilities and update protection?



Recovery phase: How will you return to normal operation? Re-imaging or restoring from backup may not work if the ransomware lay dormant during the last image or backup cycle, or if part of the ransomware attack was to seek and destroy back-ups.



Post-Incident phase: After the incident is resolved, what can you learn to prevent it from happening again in the future? How will you document the incident? Detail improvements to IR plans, additional security controls, preventative measures or new security initiatives?



Consideration: Zero Trust Strategy Model

Old Model, New Mindset

- Require real-time authentication tests of users
- Automatically block suspicious activities
- Prevent adversaries from privilege escalation demonstrated in SolarWinds incident

SolarWinds Example

- Victim organizations' emphasis on network perimeter security, **lack internal detection** methods for intruders already present in network
- Decades' old reliance on detector mechanisms deployed at **network perimeter** fed by intel only on known threats/actors
- Need **balance between internal/external detection methods** for effective implementation

Zero Trust Guiding Principles



- Never trust, always verify and explicitly authorize to least privilege required
- Assume breach; assume adversary already is present in environment
- Deny by default and heavily scrutinize all users, data flows, requests
- Explicitly verify all access to resources using multiple attributes (dynamic and static)

Zero Trust vs. Ransomware: Perimeter



Develop both perimeter and internal detection and security network strategies with coordinated and aggressive detection systems.



Deny access privilege by default, and heavily scrutinize every user and request.



Continually and explicitly verify all access using continual, dynamic and static authentication protocols.



Limit access privileges to minimal level to do job.



Study and learn ransomware attackers' tactics and use them to develop internal alerts.

- Threat actors use the same commands, sell them to other threat actors.
- Threat actors tend to copy and run the same scripts, over and over again.



Zero Trust vs. Ransomware: Internal



Assume malicious intruders are already present in network.



Create “honey files” and seed them throughout the network.

- Fake files given specific titles to lure attackers (e.g., “passwords.xlsx” or “strategic plan”).
- Attempts to access honey files alert of possible malicious activity, including that a ransomware attack may be underway.



Set up dynamic alerts, protocols and stored procedures that:

- Shut down network and/or compartmentalize network sectors where large exfiltration of files is detected;
- Shut down network access if any privilege access anomaly is determined; and
- Develop “hands on keyboard” alerts: notice actors have accessed network, anomalous activity.



Pull the plug!

If You Are The Victim of An Attack

Victims of ransomware should report it immediately to:



CISA at us-cert.cisa.gov/report;



Local FBI Field Office; or



Local Law Enforcement.

