NEW EDITION

KnowBe4
Human error. Conquered.

# RANSOMWARE
## Hostage Rescue Manual

What You Need to Know to Prepare and Recover from a Ransomware Attack

# Table of Contents

**Introduction** 2
**What is Ransomware?** 2
*Bitcoin and Cryptocurrency* 3
*TOR (Anonymity Network)* 3
*Typical Ransomware Process* 4
**Am I Infected?** 4
**How Most Ransomware Victims Were Exploited** 6
*Social Engineering by Email* 7
*Silent Drive-by-Download* 7
*Unpatched Servers or Services* 7
*Free Software Vector* 7
*Remote Desktop Protocol (RDP)* 8
**I Am Exploited With Ransomware, Now What?** 9
Initial Investigation 9
Declare an Official Ransomware Event 10
Disconnect Network 10
Determine the Scope 11
Limit Initial Damage 13
Gather Team to Share Information 14
Decide on Initial Response 15
Recovery: Repair or Rebuild? 16
*Preserving Evidence* 16
*Rebuilding Supporting Infrastructure* 17
*Back Up Your Encrypted Files (Optional)* 17
*Negotiate and/or Pay the Ransom* 17
*Locate the Payment Method Instructions* 18
*Obtaining Bitcoin* 18
*Installing a TOR Browser (May be optional)* 19
*Paying the Ransom* 19
*Decrypting Your Files* 20
Next Steps: Prevention of Future Cybercriminal Events 21
*Defense in Depth* 21
*Security Awareness Training* 21
*Simulated Phishing Attacks* 22
**Ransomware Attack Response Checklist** 23

# INTRODUCTION

Ransomware is one of the most damaging types of cyber attacks of all time, and the one feared the most by business owners and cybersecurity defenders. This worry is not without reason. In an instant, an organization's critical IT infrastructure can be brought down for weeks to months, completely stopping all business. Some data and systems may be lost forever. Complete recovery may take over a year. Customer impacts may last long past the technical recovery process.

The FBI is investigating about 100 different types of ransomware "gangs" (https://www.reuters.com/technology/fbi-says-it-is-investigating-about-100-types-ransomware-wsj-2021-06-04/) and most are operating in foreign cybercriminal safe havens where the victim's domestic law enforcement agencies cannot stop them. Despite defenders' best efforts, the occurrence of ransomware continues to increase (https://blog.knowbe4.com/ransomware-attacks-in-2021-have-increased-nearly-three-fold-in-the-first-half-of-the-year).

The financial damage caused by ransomware is daunting. Ransomware was successful in exploiting up to 68% of surveyed organizations in one year alone, according to the 2021 Cyberthreat Defense Report (https://info.knowbe4.com/research-2021-cyberthreat-defense-report). Ransomware mitigation vendor Coveware says the average ransom paid in Q3 2021 was $139,739 USD (https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts). Some organizations have paid tens of millions of dollars in ransomware extortion.

Overall, recovery costs are usually many times higher than the ransomware extortion payment. One cybersecurity vendor stated $18 billion was paid globally in ransom in 2020, and total costs were in the hundreds of billions of dollars (https://blog.emsisoft.com/en/38426/the-cost-ofransomware-in-2021-a-country-by-country-analysis/). Another cybersecurity analyst predicted total ransomware costs could hit $250 billion by 2031.

# WHAT IS RANSOMWARE?

Ransomware can take different forms, causing many different types of threats and damage. In its most common form, criminals use it to threaten to prevent access to critical data and systems and/or to release sensitive data unless a ransom has been paid. Here are some of the common impacts of ransomware:

- Encrypts data and systems, causing downtime and recovery costs
- Steals confidential data, exfiltrates it outside the organization, and threatens to release it
- Steals organization, employee and customer login credentials
- Uses compromised victims' systems and earned trust to compromise customers and business partners
- Publicly shames victim, causing reputational damage

The general media has coined the term "double extortion" to describe the threats and damage that ransomware groups promise and/or accomplish along with the traditional encryption of data. All-in-all, the damage that the average ransomware attack causes to a victim organization is often quite extensive.

*Today, over 80% of all ransomware attacks involve "double extortion," data and credential exfiltration.*

The ransomware hackers primarily use the following vectors to infect a machine: phishing emails, unpatched programs, password guessing/theft, compromised vendors, poisoned online advertising, and compromised software downloads.

If the ransomware attack is successful, once the files are encrypted and/or stolen, the hackers will display some sort of screen or webpage explaining how to pay to unlock the data or prevent the unauthorized release of data and credentials. Ransomware often has a less than one-week deadline, which if passed, causes the payment to automatically increase or the encryption may be left in place permanently and the stolen data released publicly or to other cybercriminals.

## Bitcoin and Cryptocurrency

Paying the ransom invariably involves paying with some form of cryptocurrency, such as Bitcoin (abbreviated BTC). Bitcoin is currently the most popular form of cryptocurrency and the most popular type required to pay ransomware extortions. But there are other popular cryptocurrencies including Ethereum, Litecoin, Ripple, Tether, XPR, Dogecoin, Monero and many more.

Some ransomware groups use other types of payments, such as gift cards or money-wiring services, but Bitcoin and cryptocurrencies remain the number one payment method by a large margin because of their nearly guaranteed anonymity. Cryptocurrencies can be transferred anywhere in the world via the Internet. Observers can see the associated "digital wallets" involved in any cryptocurrency transaction, but unless the involved parties go out of their way to identify themselves, who sends or receives the payment is usually unknown. This makes cryptocurrency the ideal payment method for ransomware groups.

## TOR (Anonymity Network)

Ransomware groups will often require that all communications between the victim and themselves happen across TOR ("The Onion Router"). TOR is a virtual network and related browser developed to attempt to anonymize Internet traffic. It uses a special browser (the TOR browser) that is configured to use an ever-changing worldwide volunteer network of network traffic relays. All traffic is encrypted at the origination point and then sent across an anonymized set of randomly selected "TOR nodes," until it reaches its intended destination. The TOR network was designed from the ground up to anonymize and hide the originating and ending destination of the traffic from other observers.

Cybercriminals and other people who wish to anonymize their traffic can use this TOR network to communicate or host websites that cannot be easily tracked by law enforcement or government officials. In this way, it can be a tool for circumventing censorship, but also a tool for more nefarious use of anonymous traffic. Since TOR (and cryptocurrencies) are so well crafted for anonymizing activity, ransomware groups can use it to interact with their victims without much fear of retaliation or discovery.

**A few facts about TOR:**

- Instead of using .com or .net domains, onion web addresses end in .onion
- You cannot browse TOR sites using a regular Internet browser
- TOR was originally developed by the U.S. Naval Research Laboratory and Defense Advanced Research Projects Agency (DARPA)