□□ What Is Ransomware and How to Defend Against It

Maria Cattini | 19/05/2025 | CYBERSECURITY

Ransomware has become one of the most dangerous and widespread cyber threats of our time. These malicious programs are designed to block access to files or entire systems—demanding payment, often in cryptocurrency, to unlock them.

Whether you're an individual or a business, understanding how ransomware works—and how to prevent it—is essential to staying safe in the digital age.

□□ Ransomware: Meaning and Impact

At its core, ransomware is a form of **malware** (malicious software) that encrypts your files or restricts system access, then demands a ransom in exchange for recovery.

These attacks are typically delivered via infected files disguised as legitimate content—like PDFs, ZIP archives, or executable programs. Once opened, the malware silently installs and begins its encryption routine.

Two Main Types of Ransomware

• Crypto-ransomware: Encrypts files and demands a password (available only after ransom payment).
• Locker ransomware: Locks the entire system, making it unusable until payment is made.

□□ How Ransomware Infects Your System

Ransomware spreads primarily through:

□□

Phishing emails

Email di phishing con allegati infetti o link dannosi che possono compromettere i dati sensibili o installare malware sui sistemi aziendali.

□□

Siti web compromessi

Siti web compromessi o annunci online dannosi (malvertising) che possono infettare i dispositivi

degli utenti durante la navigazione.

□□

Vulnerabilità RDP

Vulnerabilità del Remote Desktop Protocol (RDP) che possono essere sfruttate dagli attaccanti per accedere non autorizzato ai sistemi.

□□

Software non aggiornato

Software non aggiornato o impostazioni di sicurezza obsolete che contengono vulnerabilità note che gli attaccanti possono sfruttare.

Cybercriminals often target companies and public services that are more likely to pay large ransoms to avoid business disruption.

□□ A Brief History: From PC Cyborg to CryptoLocker

The first known ransomware, **PC Cyborg**, appeared in 1989, distributed via floppy disks during an AIDS conference. While primitive, it laid the foundation for future attacks.

Fast forward to **2013**, when **CryptoLocker** emerged and revolutionized ransomware by using strong encryption and demanding Bitcoin payments. This virus marked the beginning of a new era in cyber extortion.

□□ Notorious Ransomware Attacks That Shook the World

Two of the most infamous global attacks include:

• WannaCry (2017): Affected over 150 countries, crippling hospitals, telecom companies, and logistics giants. It exploited an NSA-linked vulnerability (EternalBlue) to spread rapidly.
• NotPetya (2017): Originating in Ukraine, this destructive malware also leveraged EternalBlue but aimed more at disruption than profit. It encrypted entire drives and demanded a $300 Bitcoin ransom.

□□ Double Extortion: A Growing Trend

Recent ransomware campaigns have adopted a **double extortion** tactic: they don’t just encrypt

data—they steal it. Victims are forced to pay both for decryption and to prevent public exposure of sensitive files.

Notable example: **Sodinokibi (REvil)** demanded up to $4 million from a French company after both encrypting and exfiltrating their data.

This model, which first gained traction after the **Maze** ransomware campaign in 2019, is now the standard for high-stakes cybercrime.

□□ How Ransomware Operate

Once ransomware is executed:

• It silently scans for files to encrypt.
• It may delay activation to avoid detection.
• It prioritizes less-used files first to buy time.
• Once encryption is complete, a ransom note appears, often with a payment countdown.

□□ Ransom Demands: How They Work

Most attackers demand **cryptocurrency payments**—typically Bitcoin—to make tracking harder. Victims are usually directed to hidden websites on the **Dark Web via the Tor browser**, where payment instructions are provided.

However, **paying doesn’t guarantee file recovery**. In many cases, victims never receive the decryption keys or face additional ransom requests.

Paying also sets a dangerous precedent, making organizations a recurring target.

□□ Is File Recovery Possible?

Recovering encrypted files is often difficult without the decryption key. Modern ransomware uses robust algorithms like **AES** and **RSA**, making brute-force decryption virtually impossible.

In rare cases:

• Authorities have seized Command & Control servers containing keys.
• Flaws in the malware have allowed decryption tools to be developed.
• Data recovery software may help in limited situations—but success rates are low.

□□ How to Protect Against Ransomware Attacks

Prevention is your best defense. Here’s how to reduce your exposure:

Essential Cybersecurity Practices

□□

Automated Backups

Back up your data regularly and keep at least one copy offline.

□□

Install Security Software

Use a reputable antivirus and enable anti-ransomware features.

□□

Keep Systems Updated

Patch operating systems, browsers, and software to close vulnerabilities.

□□

Educate Your Team

Train employees to recognize phishing attempts and suspicious links.

□□

Strengthen Access Control

Use strong passwords, 2FA, and restrict administrative privileges.

□□

Use a Firewall and VPN

These tools can help prevent unauthorized access, especially on public networks.

Healthcare: The Most Targeted Sector

According to the **Clusit 2024 report**, the **healthcare sector** saw a 30% increase in ransomware attacks in 2023. Notable cases in Italy include:

• Modena Hospitals: Affected in November 2023, disrupting services for patients and staff.
• Vanvitelli Hospital, Naples: Attacked in July 2023, requiring national cybersecurity assistance.
• ASL 1 Abruzzo: Hit in May 2023 by the Monti ransomware gang, which exfiltrated over 500 GB of data and leaked part of it online.

Final Thoughts

Ransomware is not going away anytime soon. These attacks are evolving—becoming more targeted, more destructive, and harder to detect.

Companies must **prioritize cybersecurity training**, invest in robust backup strategies, and treat cyber hygiene as an ongoing mission, not a one-time fix.

Stay Informed. Stay Prepared.

Want to learn more about ransomware and digital threats?

Explore OSINT resources
Join our security updates on Telegram
Download our free guide: "Cybersecurity Basics for Everyone"
Ransomware has become one of the most dangerous and widespread cyber threats of our time. These malicious programs are designed to block access to files or entire systems—demanding payment, often in cryptocurrency, to unlock them.

Whether you're an individual or a business, understanding how ransomware works—and how to prevent it—is essential to staying safe in the digital age.

Ransomware: Meaning and Impact

At its core, ransomware is a form of **malware** (malicious software) that encrypts your files or restricts system access, then demands a ransom in exchange for recovery.

These attacks are typically delivered via infected files disguised as legitimate content—like PDFs, ZIP archives, or executable programs. Once opened, the malware silently installs and begins its encryption routine.

Two Main Types of Ransomware

• Crypto-ransomware: Encrypts files and demands a password (available only after ransom payment).
• Locker ransomware: Locks the entire system, making it unusable until payment is made.

How Ransomware Infects Your System

Ransomware spreads primarily through:

□□

Phishing emails

Email di phishing con allegati infetti o link dannosi che possono compromettere i dati sensibili o installare malware sui sistemi aziendali.

□□

Siti web compromessi

Siti web compromessi o annunci online dannosi (malvertising) che possono infettare i dispositivi degli utenti durante la navigazione.

□□

Vulnerabilità RDP

Vulnerabilità del Remote Desktop Protocol (RDP) che possono essere sfruttate dagli attaccanti per accedere non autorizzato ai sistemi.

□□

Software non aggiornato

Software non aggiornato o impostazioni di sicurezza obsolete che contengono vulnerabilità note che gli attaccanti possono sfruttare.

Cybercriminals often target companies and public services that are more likely to pay large ransoms to avoid business disruption.

□□ A Brief History: From PC Cyborg to CryptoLocker

The first known ransomware, **PC Cyborg**, appeared in 1989, distributed via floppy disks during an AIDS conference. While primitive, it laid the foundation for future attacks.

Fast forward to **2013**, when **CryptoLocker** emerged and revolutionized ransomware by using strong encryption and demanding Bitcoin payments. This virus marked the beginning of a new era in cyber extortion.

□□ Notorious Ransomware Attacks That Shook the World

Two of the most infamous global attacks include:

• WannaCry (2017): Affected over 150 countries, crippling hospitals, telecom companies, and logistics giants. It exploited an NSA-linked vulnerability (EternalBlue) to spread rapidly.
• NotPetya (2017): Originating in Ukraine, this destructive malware also leveraged EternalBlue but aimed more at disruption than profit. It encrypted entire drives and demanded a $300 Bitcoin ransom.

□□ Double Extortion: A Growing Trend

Recent ransomware campaigns have adopted a **double extortion** tactic: they don't just encrypt data—they steal it. Victims are forced to pay both for decryption and to prevent public exposure of sensitive files.

Notable example: **Sodinokibi (REvil)** demanded up to $4 million from a French company after both encrypting and exfiltrating their data.

This model, which first gained traction after the **Maze** ransomware campaign in 2019, is now the standard for high-stakes cybercrime.

□□ How Ransomware Operate

Once ransomware is executed:

• It silently scans for files to encrypt.
• It may delay activation to avoid detection.
• It prioritizes less-used files first to buy time.
• Once encryption is complete, a ransom note appears, often with a payment countdown.

□□ Ransom Demands: How They Work

Most attackers demand **cryptocurrency payments**—typically Bitcoin—to make tracking harder. Victims are usually directed to hidden websites on the **Dark Web via the Tor browser**, where payment instructions are provided.

However, **paying doesn't guarantee file recovery**. In many cases, victims never receive the decryption keys or face additional ransom requests.

Paying also sets a dangerous precedent, making organizations a recurring target.

□□ Is File Recovery Possible?

Recovering encrypted files is often difficult without the decryption key. Modern ransomware uses robust algorithms like **AES** and **RSA**, making brute-force decryption virtually impossible.

In rare cases:

• Authorities have seized Command & Control servers containing keys.
• Flaws in the malware have allowed decryption tools to be developed.
• Data recovery software may help in limited situations—but success rates are low.

□□ How to Protect Against Ransomware Attacks

Prevention is your best defense. Here’s how to reduce your exposure:

Essential Cybersecurity Practices

□□

Automated Backups

Back up your data regularly and keep at least one copy offline.

□□

Install Security Software

Use a reputable antivirus and enable anti-ransomware features.

□□

Keep Systems Updated

Patch operating systems, browsers, and software to close vulnerabilities.

□□

Educate Your Team

Train employees to recognize phishing attempts and suspicious links.

□□

Strengthen Access Control

Use strong passwords, 2FA, and restrict administrative privileges.

□□

Use a Firewall and VPN

These tools can help prevent unauthorized access, especially on public networks.

□□ Healthcare: The Most Targeted Sector

According to the **Clusit 2024 report**, the **healthcare sector** saw a 30% increase in ransomware attacks in 2023. Notable cases in Italy include:

• Modena Hospitals: Affected in November 2023, disrupting services for patients and staff.
• Vanvitelli Hospital, Naples: Attacked in July 2023, requiring national cybersecurity assistance.
• ASL 1 Abruzzo: Hit in May 2023 by the Monti ransomware gang, which exfiltrated over 500 GB of data and leaked part of it online.

□□ Final Thoughts

Ransomware is not going away anytime soon. These attacks are evolving—becoming more targeted, more destructive, and harder to detect.

Companies must **prioritize cybersecurity training**, invest in robust backup strategies, and treat cyber hygiene as an ongoing mission, not a one-time fix.

□ Stay Informed. Stay Prepared.

Want to learn more about ransomware and digital threats?

□□Explore OSINT resources
□□Join our security updates on Telegram
□□Download our free guide: "Cybersecurity Basics for Everyone"