Integrity report

Ransomware: a literature study into the operation, propagation and impact.

Anonymous

HUMAN SCORE
88%

READABILITY SCORE
24
/ 100

English · 1,146 words · 10,547 characters

Assessment

Winston has detected the text as 88% human. The content closely matches human linguistic structures and nuances. We are highly confident it was written by a human.

This text has a **readability score of 24/100** and has a **U.S. school College graduate level**, which means it is very difficult to read and is best understood by university graduates.

AI prediction map

Likely AI generated Possibly AI generated Unlikely AI generated

Ransomware: a literature study into the operation, propagation and impact.

Victor Angelier

March 24th, 2026

Introduction

Ransomware is hostage software that is deployed by cyber criminals to earn money. In recent years, this form of cybercrime has become a multi-billion industry that affects countless organisations worldwide. In this essay I present a literature study into ransomware where I analyse the technical operation, propagation methods and impact. I also look at the societal consequences of this type of threat.

Summary of ransomware

Ransomware is a form of malware that encrypts files or complete systems and subsequently a ransom is demanded to restore access (IBM, 2024; Fortinet, n.d.). Attackers make use of symmetric and asymmetric encryption, where the key is managed externally by the attacker, which makes recovery without the decryption-key practically impossible (Trend Micro, 2026; Microsoft, 2025). In many cases the attackers, after payment (often in cryptocurrency), provide the decryption key (Proofpoint, 2025; Microsoft, 2025). This revenue model has developed ransomware into one of the most profitable forms of cybercrime, partly because ransomware-as-a-service (RaaS) models are widely available (Proofpoint, 2025; Censys & Cyentia Institute, 2024; IBM, 2024).

Technical details

IBM describes a typical kill-chain that starts with initial access, followed by post-exploitation, lateral movement, data collection and exfiltration, and finally the complete encryption and extortion (IBM, 2024). In the initial phase attackers often gain entry via phishing emails, malicious digital advertisements or known vulnerabilities (IBM, 2024; CrowdStrike, 2023).

After initial access the attackers often attempt to escalate privileges in order to obtain full system control (IBM, 2024). After that, additional software, such as remote access tools (RATs), are installed to ensure persistent access and to obtain more privileges within the network (CrowdStrike, 2023). This enables attackers to move laterally through the network and compromise multiple systems (IBM, 2024; CrowdStrike, 2023). Through this structured and often automated approach ransomware operations via RaaS models can be executed increasingly faster and broader, with an expected increase of AI-supported phases (Trend Micro, 2026).

Propagation methods

Ransomware makes use of various attack vectors. Industrial reports show that phishing emails and compromised credentials are the most common

attack methodologies (IBM, 2024; Rootshell Security, 2026). Such emails often contain attachments or malicious links that trick the user to execute malware code or to provide credentials (Rootshell Security, 2026). In addition, insufficiently patched systems and publicly exposed vulnerable services are targeted, which is an important factor for many ransomware groups (Censys & Cyentia Institute, 2024). These attack vectors are effective because they exploit both technical vulnerabilities and human errors, which makes detection and prevention extremely complex (CrowdStrike, 2023; Rootshell Security, 2026).

BMA, prevention techniques

BMA (Basic Malware Analysis) plays an important role in identifying and understanding ransomware. Here the focus lies on the analysis of behaviour and source-code of malware during execution, where host-based intrusion detection systems (HIDS) are deployed to detect suspicious behaviour and indicators of ransomware attacks.

Effects after infection

After successful infection and encryption the user loses access to (critical) files or the complete system. Microsoft describes how attackers delete or render unusable local data and even backups, after which the victim is confronted with a ransom demand (Microsoft, 2025). In some cases it concerns "locker" ransomware that blocks systems; in other cases "crypto" ransomware that encrypts specific data, or variants that use data theft and threat of publication ("extortionware") (IBM, 2024; Trend Micro, 2026). This increases the pressure on victims, because recovery without payment is often impossible due to the absence of usable backups (Microsoft, 2025; MacColl et al., 2024).

Impact of ransomware

Impact on individuals

Ransomware brings for individuals not only significant financial damage, but also serious psychological and physical consequences (MacColl et al., 2024). Research into victims and incident responders shows that ransomware can also lead to unemployment, feelings of shame and self-blame, disruption of private and family life and serious health problems (MacColl et al., 2024). In particular employees who unknowingly clicked on a phishing link often experience long-term stress, especially when the attack has heavily affected their organisation (MacColl et al., 2024).

Impact on organisations

Ransomware causes operational downtime and thus loss of revenue. It also leads to significant direct financial costs, such as incident response and forensic investigation (IBM, 2024; Microsoft, 2025). Some organisations pay the ransom, but research shows that payment offers no guarantee for full data recovery. Payment also increases the risk of follow-up attacks because the attack is considered successful (Trend Micro, 2026). Additionally, regulators may impose sanctions in case of violation of privacy and security obligations, particularly under regulation such as the AVG (GDPR) (Fortinet, n.d.). Reputational damage can lead to loss of trust among customers and stakeholders, which can have long-term financial consequences (MacColl et al., 2024).

Impact on society

At societal level ransomware, according to various studies, forms one of the most important threats at this moment (MacColl et al., 2024). This is reinforced by the increasing use of AI, which makes attacks more advanced and harder to detect (Microsoft, 2025; Trend Micro, 2026). At macro level ransomware increases the necessity for investments in cyber security, international law enforcement and regulation regarding for example reporting obligations and ransom payments (Bhavsar et al., 2022). At the same time it stimulates innovation in detection and prevention techniques, which in the literature is seen as an important research direction (Bhavsar et al., 2022). Existing RaaS models are continuously improved, and AI will further increase the pressure (Trend Micro, 2026).

Conclusion

The literature shows that ransomware has strongly evolved from simple locker variants to advanced attacks with double and even multiple extortion phases. The most advanced attacks make use of a professional cybercriminal economy, particularly via ransomware-as-a-service (RaaS) models (IBM, 2024; Microsoft, 2025). This technical refinement, including strong encryption, external key management, data theft, is accompanied by broad individual, organisational and societal damage, ranging from financial losses to long-term psychological and social consequences (MacColl et al., 2024). This underlines that ransomware is also a societal challenge, where effective mitigation requires a combination of technical measures, policy development and international cooperation (Bhavsar et al., 2022).

References

Bhavsar, K.C., Patel, N.P. and Vasoya, S. (2022) A systematic literature review on ransomware attacks. arXiv preprint arXiv:2212.04063. Available at: https://arxiv.org/abs/2212.04063.

Censys and Cyentia Institute (2024) Ransomware Information Risks Insights Study. Available at: https://censys.com/blog/top-ransomware-attack-vectors/.

CrowdStrike (2023) How Ransomware Spreads: Top 10 Infection Methods. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/how-ransomware-spreads/.

Fortinet (n.d.) Ransomware. Available at: https://www.fortinet.com/resources/cyberglossary/ransomware.

IBM (2024) Types of Ransomware. Available at: https://www.ibm.com/think/topics/ransomware.

MacColl, J. et al. (2024) The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society. RUSI Occasional Paper. London: Royal United Services Institute. Available at: https://www.rusi.org/explore-our-research/publications/occasional-papers/ransomware-victim-insights-harms-individuals-organisations-and-society.

Microsoft (2025) Ransomware explained: How it works and how to remove it. Available at: https://learn.microsoft.com/en-us/security/ransomware/.

Proofpoint (2025) What is Ransomware? Definition & Prevention. Available at: https://www.proofpoint.com/us/threat-reference/ransomware.

Rootshell Security (2026) Common Ransomware Attack Vectors Explained. Available at: https://www.rootshellsecurity.net/common-ransomware-attack-vectors-explained/.

Trend Micro (2026) What is Ransomware?. Available at: https://www.trendmicro.com/en_us/what-is/ransomware.html.

Fact checker

Ransomware: a literature study into the operation, propagation and impact. Victor Angelier March 24th, 2026 Introduction Ransomware is hostage software that is deployed by cyber criminals to earn money.

No fact-checked statements found

In recent years, this form of cybercrime has become a multi-billion industry that affects countless organisations worldwide.

No fact-checked statements found

In this essay I present a literature study into ransomware where I analyse the technical operation, propagation methods and impact.

No fact-checked statements found

I also look at the societal consequences of this type of threat. Summary of ransomware Ransomware is a form of malware that encrypts files or complete systems and subsequently a ransom is demanded to restore access (IBM, 2024; Fortinet, n.d.). Attackers make use of symmetric and asymmetric encryption, where the key is managed externally by the attacker, which makes recovery without the decryption-key practically impossible (Trend Micro, 2026; Microsoft, 2025).

No fact-checked statements found

In many cases the attackers, after payment (often in cryptocurrency), provide the decryption key (Proofpoint, 2025; Microsoft, 2025).

No fact-checked statements found

This revenue model has developed ransomware into one of the most profitable forms of cybercrime, partly because ransomware-as-a-service (RaaS) models are widely available (Proofpoint, 2025; Censys & Cyentia Institute, 2024; IBM, 2024).

No fact-checked statements found

Technical details IBM describes a typical kill-chain that starts with initial access, followed by post-exploitation, lateral movement, data collection and exfiltration, and finally the complete encryption and extortion (IBM, 2024).

No fact-checked statements found

In the initial phase attackers often gain entry via phishing emails, malicious digital advertisements or known vulnerabilities (IBM, 2024; CrowdStrike, 2023).

No fact-checked statements found

After initial access the attackers often attempt to escalate privileges in order to obtain full system control (IBM, 2024).

No fact-checked statements found

After that, additional software, such as remote access tools (RATs), are installed to ensure persistent access and to obtain more privileges within the network (CrowdStrike, 2023).

No fact-checked statements found

This enables attackers to move laterally through the network and compromise multiple systems (IBM, 2024; CrowdStrike, 2023).

No fact-checked statements found

Through this structured and often automated approach ransomware operations via RaaS models can be executed increasingly faster and broader, with an expected increase of AI-supported phases (Trend Micro, 2026).

No fact-checked statements found

Propagation methods Ransomware makes use of various attack vectors. Industrial reports show that phishing emails and compromised credentials are the most common attack methodologies (IBM, 2024; Rootshell Security, 2026).

No fact-checked statements found

Such emails often contain attachments or malicious links that trick the user to execute malware code or to provide credentials (Rootshell Security, 2026).

No fact-checked statements found

In addition, insufficiently patched systems and publicly exposed vulnerable services are targeted, which is an important factor for many ransomware groups (Censys & Cyentia Institute, 2024).

No fact-checked statements found

These attack vectors are effective because they exploit both technical vulnerabilities and human errors, which makes detection and prevention extremely complex (CrowdStrike, 2023; Rootshell Security, 2026).

No fact-checked statements found

BMA, prevention techniques BMA (Basic Malware Analysis) plays an important role in identifying and understanding ransomware.

No fact-checked statements found

Here the focus lies on the analysis of behaviour and source-code of malware during execution, where host-based intrusion detection systems (HIDS) are deployed to detect suspicious behaviour and indicators of ransomware attacks.

No fact-checked statements found

Effects after infection After successful infection and encryption the user loses access to (critical) files or the complete system.

No fact-checked statements found

Microsoft describes how attackers delete or render unusable local data and even backups, after which the victim is confronted with a ransom demand (Microsoft, 2025).

No fact-checked statements found

In some cases it concerns "locker" ransomware that blocks systems; in other cases "crypto" ransomware that encrypts specific data, or variants that use data theft and threat of publication ("extortionware") (IBM, 2024; Trend Micro, 2026).

No fact-checked statements found

This increases the pressure on victims, because recovery without payment is often impossible due to the absence of usable backups (Microsoft, 2025; MacColl et al., 2024).

No fact-checked statements found

Impact of ransomware Impact on individuals Ransomware brings for individuals not only significant financial damage, but also serious psychological and physical consequences (MacColl et al., 2024).

No fact-checked statements found

Research into victims and incident responders shows that ransomware can also lead to unemployment, feelings of shame and self-blame, disruption of private and family life and serious health problems (MacColl et al., 2024).

No fact-checked statements found

In particular employees who unknowingly clicked on a phishing link often experience long-term stress, especially when the attack has heavily affected their organisation (MacColl et al., 2024).

No fact-checked statements found

Impact on organisations Ransomware causes operational downtime and thus loss of revenue. It also leads to significant direct financial costs, such as incident response and forensic investigation (IBM, 2024; Microsoft, 2025).

No fact-checked statements found

Some organisations pay the ransom, but research shows that payment offers no guarantee for full data recovery.

No fact-checked statements found

Payment also increases the risk of follow-up attacks because the attack is considered successful (Trend Micro, 2026).

No fact-checked statements found

Additionally, regulators may impose sanctions in case of violation of privacy and security obligations, particularly under regulation such as the AVG (GDPR) (Fortinet, n.d.). Reputational damage can lead to loss of trust among customers and stakeholders, which can have long-term financial consequences (MacColl et al., 2024).

No fact-checked statements found

Impact on society At societal level ransomware, according to various studies, forms one of the most important threats at this moment (MacColl et al., 2024).

No fact-checked statements found

This is reinforced by the increasing use of AI, which makes attacks more advanced and harder to detect (Microsoft, 2025; Trend Micro, 2026).

No fact-checked statements found

At macro level ransomware increases the necessity for investments in cyber security, international law enforcement and regulation regarding for example reporting obligations and ransom payments (Bhavsar et al., 2022).

No fact-checked statements found

At the same time it stimulates innovation in detection and prevention techniques, which in the literature is seen as an important research direction (Bhavsar et al., 2022).

No fact-checked statements found

Existing RaaS models are continuously improved, and AI will further increase the pressure (Trend Micro, 2026).

No fact-checked statements found

Conclusion The literature shows that ransomware has strongly evolved from simple locker variants to advanced attacks with double and even multiple extortion phases.

No fact-checked statements found

The most advanced attacks make use of a professional cybercriminal economy, particularly via ransomware-as-a-service (RaaS) models (IBM, 2024; Microsoft, 2025).

No fact-checked statements found

This technical refinement, including strong encryption, external key management, data theft, is accompanied by broad individual, organisational and societal damage, ranging from financial losses to long-term psychological and social consequences (MacColl et al., 2024).

No fact-checked statements found

This underlines that ransomware is also a societal challenge, where effective mitigation requires a combination of technical measures, policy development and international cooperation (Bhavsar et al., 2022).

No fact-checked statements found

References Bhavsar, K.C., Patel, N.P. and Vasoya, S. (2022) A systematic literature review on ransomware attacks.

No fact-checked statements found

arXiv preprint arXiv:2212.04063. Available at: https://arxiv.org/abs/2212.04063. Censys and Cyentia Institute (2024) Ransomware Information Risks Insights Study.

No fact-checked statements found

Available at: https://censys.com/blog/top-ransomware-attack-vectors/. CrowdStrike (2023) How Ransomware Spreads: Top 10 Infection Methods.

No fact-checked statements found

Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/how-ransomware-spreads/. Fortinet (n.d.) Ransomware. Available at: https://www.

No fact-checked statements found

fortinet.com/resources/cyberglossary/ransomware. IBM (2024) Types of Ransomware. Available at: https://www.ibm.

No fact-checked statements found

com/think/topics/ransomware. MacColl, J. et al. (2024) The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society.

No fact-checked statements found

RUSI Occasional Paper. London: Royal United Services Institute. Available at: https://www.rusi.org/explore-our-research/publications/occasional-papers/ransomware-victim-insights-harms-individuals-organisations-and-society.

No fact-checked statements found

Microsoft (2025) Ransomware explained: How it works and how to remove it. Available at: https://learn.

No fact-checked statements found

microsoft.com/en-us/security/ransomware/. Proofpoint (2025) What is Ransomware? Definition & Prevention. Available at: https://www.

No fact-checked statements found

proofpoint.com/us/threat-reference/ransomware. Rootshell Security (2026) Common Ransomware Attack Vectors Explained. Available at: https://www.

No fact-checked statements found

rootshellsecurity.net/common-ransomware-attack-vectors-explained/. Trend Micro (2026) What is Ransomware?. Available at: https://www.trendmicro.com/en_us/what-is/ransomware.html.

No fact-checked statements found