

Malware & Ransomware

AnnexVault LLC
Groundhog Research Group™

Original publication: April 2025
Revised: 26 October 2026

Summary

Why this matters to AnnexVault

This report connects technical evidence with operational impact. Malware and ransomware are not only code problems, they affect decisions about continuity, recovery, and risk.

Cyber threats like malware and ransomware have become pervasive, targeting individuals, businesses, and governments. Understanding the nature of these attacks and the role of cyber threat intelligence (CTI) is essential for mitigating risks. Malware refers to malicious software designed to harm or exploit systems, while ransomware specifically targets a victim's data by encrypting it and demanding ransom.

Types of Malware

Malware includes several different categories:

- **Viruses:** Infect programs and replicate when those programs are run.
- **Worms:** Self-replicating malware that spreads across networks without user intervention.
- **Trojans:** Disguise themselves as legitimate software, delivering hidden malicious payloads.
- **Spyware/Adware:** Collects information without user consent or displays unwanted ads.

Ransomware

Ransomware is a specific type of malware designed to encrypt files and demand a ransom for their release. In many cases, the threat actors may also threaten to expose sensitive data unless the ransom is paid, a tactic known as double extortion.

Common Attack Vectors:[1]

- **Phishing Emails:** Attachments or links in emails are used to deploy ransomware.
- **Exploiting Software Vulnerabilities:** Outdated or unpatched systems are common entry points.
- **Remote Desktop Protocol (RDP):** Poorly configured RDP settings allow attackers to gain access to systems.

Key Example:

- **WannaCry (2017):** Used an exploit in Windows to infect thousands of computers globally, including healthcare systems.[2]

Historical Ransomware Cost Estimates[3]

Cybersecurity Ventures projected global ransomware damage costs of \$5 billion in 2017 and \$20 billion in 2021. These were forecasts of total damages, including ransom payouts, downtime, recovery and other costs, not measured ransom payments. [3]

Role of Cyber Threat Intelligence (CTI)

CTI is essential for detecting, analyzing, and mitigating malware and ransomware threats. CTI focuses on:

- **Indicators of Compromise (IOCs):** Data like malicious file hashes and IP addresses.
- **Tactics, Techniques, and Procedures (TTPs):** Understanding the specific actions attackers take.
- **Threat Actor Profiles:** Understanding the groups behind the attacks (e.g., cybercrime syndicates).

Malware and ransomware are significant threats in the cybersecurity landscape, and a strong understanding of these threats, combined with effective CTI, can help organizations minimize the risk of an attack. Regular backups, patch management, and strong detection mechanisms are crucial for defense.

Psychological & Behavioral Analysis of Malware and Ransomware Attacks

Malware and ransomware attacks are not just technical issues; they also involve complex psychological and behavioral components. Understanding the psychological drivers behind these attacks, both from the attacker and victim perspective, can provide valuable insights for cyber defense strategies and enhance awareness in handling such threats.

Psychology of Attackers

Attackers use malware and ransomware for various reasons, employing psychological tactics to manipulate victims. Key factors influencing their behavior include:

- **Financial Motivation (Greed):**

Ransomware attackers are often driven by the potential for large financial gains. Attackers can demand cryptocurrency payments, but Bitcoin transactions are recorded on a public ledger and can be traced; they should not be described as reliably anonymous.[4]

- **Power and Control:**

Encrypting files and disrupting systems gives attackers leverage over victims.[1]

- **Psychological Manipulation (Social Engineering):**

Attackers often exploit human emotions like fear or urgency through phishing emails to trick victims into downloading malware or providing sensitive information.

Challenge and Peer Recognition

A 2017 UK National Crime Agency assessment identified challenge, accomplishment and peer recognition as motivations in its small sample of cyber-offender debriefs. This supports considering status and social context alongside financial motives; it does not establish a universal age profile or a ransomware-specific explanation.[5]

Psychological Impact on Victims

Ransomware incidents can have psychological effects that influence decisions. Interview-based research documents varied, context-dependent experiences; the following are possible responses, not a profile of every victim:[6]

- **Fear and Panic:**

Fear of losing important data can put decision-makers under pressure.[6]

- **Urgency:**

Ransom deadlines can create pressure, but victims may still have recovery and response options.[6]

- **Shame and Guilt:**

Some victims report shame or guilt; organisational blame can aggravate the harm of an incident.[6]

- **Helplessness:**

Some victims may feel powerless, particularly when recovery options are uncertain.[6]

- **Post-Attack Trauma:[6]**

The psychological toll of these attacks can last long after the event, leading to stress, anxiety, and fear of future attacks.

Behavioral Aspects in Defense

Understanding how people behave in response to malware and ransomware attacks can improve defense strategies:

- **Security Awareness Training:**

Training employees to recognize the psychological tricks (e.g., urgency, fear) that attackers use can reduce the chances of falling victim to phishing or social engineering.

- **Incident Response Planning:**

A clear, practised response plan can reduce uncertainty about responsibilities and recovery steps.[6]

- **Behavioral Monitoring:**

Monitoring for unusual behaviors, such as accessing unfamiliar files or running unknown processes, can help detect malware early.

Psychological Models in Cyber Threat Intelligence (CTI)

Incorporating psychological and behavioral models into CTI can improve the effectiveness of cybersecurity:

- **Motivational Models:**

Understanding possible attacker motivations can inform assessments of targeting, without reliably predicting the next victim.[1]

- **Risk Perception Models:**

These models assess how different individuals and organizations perceive the risk of cyberattacks. Some underestimate the risk, while others overreact, leading to unnecessary stress.

- **Trust and Deception Models:**

These models examine how attackers build fake trust, for example through phishing emails. Understanding these patterns helps build better security defenses.

Malware and ransomware attacks rely heavily on psychological manipulation, both from the attacker's side (to exploit human vulnerabilities) and the victim's side (leading to decisions like paying the ransom). Recognizing these psychological and behavioral factors can help organizations better prepare for, respond to, and prevent these attacks.

Geopolitical and Cultural Insights into Malware and Ransomware Attacks

Malware and ransomware attacks are deeply influenced by geopolitical and cultural factors. Different regions and countries contribute to the development and spread of these cyber threats, driven by various economic, political, and cultural motives. Understanding these influences can help organizations and governments better anticipate, prevent, and respond to cyberattacks.

- **Nation-State Sponsored Cyberattacks:**

Many ransomware and malware attacks are linked to nation-states. Countries like Russia, China, and North Korea are often implicated in cyberattacks for espionage, sabotage, or financial gain.

Example: In 2018, the U.S. Department of Justice charged a North Korean programmer and alleged that the Lazarus-linked conspiracy created the malware used in WannaCry and stole funds from Bangladesh Bank.[7]

Cultural Factors in Malware and Ransomware Attacks

- **Localized Targeting:**

Cybercriminals often exploit regional knowledge and cultural norms to improve their chances of success. For example, a 2021 CISA/FBI advisory warned that U.S. holidays and weekends can offer attackers an opportunity when offices are closed. Phishing messages can also be tailored to a target's language and working context.[8] [9]

Risk Simulation in Malware and Ransomware Attacks

Risk simulation helps organizations understand how malware and ransomware could impact them. Key aspects include:

- **Attack Surface Simulation:**

Identifies vulnerable points in the network, such as unpatched software or phishing entry points.

- **Business Impact Analysis:**

Simulates the potential financial and operational impact, allowing organizations to estimate costs related to downtime, ransom payments, and reputational damage.

- **Recovery Time Simulation:**

Estimates recovery time under stated assumptions, helping organisations prepare for possible operational disruptions.[1]

References

[1] CISA, StopRansomware Guide (retrieved 26 October 2026)

[2] UK National Audit Office, Investigation: WannaCry cyber attack and the NHS (2017-10-27)

[3] Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031 (2021)

[4] DOJ, Seizure of Cryptocurrency Paid to DarkSide (2021-06-07)

[5] UK National Crime Agency, Pathways Into Cyber Crime (2017-01-13; small qualitative UK offender sample)

[6] Hüscher et al., Your Data is Stolen and Encrypted: The Ransomware Victim Experience, RUSI (2024-07-02; qualitative interviews, not universal prevalence)

[7] DOJ, North Korean Regime-Backed Programmer Charged (2018-09-06; allegations)

[8] CISA/FBI, Ransomware Awareness for Holidays and Weekends (2021-08-31)

[9] CISA/NSA/FBI/MS-ISAC, Phishing Guidance: Stopping the Attack Cycle at Phase One (2023; retrieved 2026-10-26)