The Evolution of Ransomware: An Analytical Exploration

Ronny Richardson and Max M. North
Management & Entrepreneurship Department
Information Systems & Security Department
Coles College of Business
Kennesaw State University, GA USA

Sarah M. North
Computer Science Department
College of Computing and Software Engineering
Kennesaw State University, GA USA

[Abstract] An overview of the evolution of ransomware is provided by tracing its 35-year development from the 1989 AIDS Trojan to modern, AI-assisted, multi-extortion cyberattacks. It explores key developments in encryption, payment systems, and organizational targeting, emphasizing the rise of ransomware-as-a-service and law-enforcement countermeasures. The study highlights emerging global trends, regulatory challenges, and the continuing sophistication of cyber extortion tactics.

[Keywords] ransomware, cyber extortion, encryption, cybersecurity countermeasures

Introduction

Ransomware, a form of malicious software designed to block access to computer systems or data until a ransom is paid, has become one of the most damaging and profitable tools in modern cybercrime. Emerging from the primitive 1989 AIDS Trojan, ransomware has evolved over more than three decades into a sophisticated global threat driven by advanced encryption, cryptocurrency transactions, and organized criminal networks. This paper explores that transformation—from early experimental attacks to today's AI-enhanced multi-extortion operations that target entire enterprises and critical infrastructure. By examining its historical development, payment mechanisms, and countermeasures, this study provides a framework for understanding ransomware's persistence and the ongoing challenges it presents to cybersecurity professionals worldwide

The Early Years of Ransomware

The first ransomware attack occurred in December 1989 using 5.25-inch floppy disks developed by Joseph Popp. He sent 20,000 floppy disks to attendees of the World Health Organization's AIDS conference. (Kostka, 2022) Those discs contained ransomware code (although the term

"ransomware" did not yet currently exist) that claimed to assist with AIDS risk assessment. This code would later become known as the AIDS Trojan.[1],[2]

After 90 reboots, the AIDS Trojan would hide the directories, encrypt file names and demand payment (not yet called a ransom) by cashier's check for $189 to a post office box in Panama to restore access. (Knowbe4, n.d.) The need to physically distribute the floppy discs and to collect the payments in a world before the Internet doomed the AIDS Trojan to failure.

Emergence of Criminal Ransomware

Ransomware took a nearly 15-year break after the AIDS Trojan. The first form of criminal ransomware was GPCode (also known as GPCoder), which emerged in December 2004. It targeted Russian users and was distributed as an email attachment claiming to be a job application. Early versions of GPCode had two fundamental flaws: poor encryption and difficulties with payment collection (Emm, 2008).

Those early versions used basic encryption that IT professionals could easily crack. Additionally, it encrypted data into a new file and then deleted the existing files. That meant that file recovery utilities could recover the original versions (Knowbe4, n.d.). Later versions switched to more sophisticated public/private-key encryption methods (660-bit RSA public key encryption) that were difficult or impossible to crack.

Ransomware gangs quickly learned the importance of strong encryption. In 2006, the ransomware Archiveus was the first strain to use 1,024-bit RSA encryption. However, the gang made a serious blunder by using the same password on all attacks (Shea, 2025).

Pre-cryptocurrency, payment collection was a major obstacle for the attackers. Attackers experimented with online pharmacy purchases and premium rate phone numbers as payment methods. Additional experiments were also conducted using virtual currency and gold trading platforms; however, these were eventually shut down by authorities.

Arrival of Cryptocurrency

The arrival of Bitcoin and other cryptocurrencies in the early 2010s (Shea, 2025) provided the first truly anonymous payment system capable of handling large-sized ransoms. This had two major implications. First, higher payments caused ransomware criminals to shift away from individuals and small payments toward organizations and much larger sums (Sakellariadis, 2022).

Second, ransomware criminals became more professional, going as far as to employ specialists who handled different aspects of the attack. Additionally, ransomware-as-a-service (RaaS) has expanded and attackers are even hiring third parties to negotiate payments. A few attackers even have 24/7 help desks (Schissel, 2022).

The Move to Targeted Enterprise Attacks

In 2016, a new ransomware version called SamSam (also known as MSIL/Samas.A.) was introduced. Rather than depending on mass distribution, it targeted specific organizations. It

[1] A Trojan Horse (also known simply as a Trojan) is a type of malware that is disguised as a legitimate program. It is typically distributed as an email attachment or downloadable file on the Internet. The term come from the *Aeneid* by Virgil and the *Odyssey* by Homer. In these stories, enemy soldiers were able to infiltrate Troy hidden inside a large wooden horse (Fortinet, n.d.) (McAfee, n.d.). Trojans are not able to self-replicate. That is, they must be manually copied/installed on each system they infect (McGowan, 2025).
[2] It was also known as the PC Cyborg virus (Knowbe4, n.d.).

targeted specific organizations, focusing on entire networks rather than individual computers. (Cybersecurity & Infrastructure Security Agency, 2018) The primary targets of SamSam were hospitals and educational institutions (Nomios, n.d.). Other variants that emerged during this period included WannaCry and NotPetya.[3]

Adding Platforms and Changing Targets

Early ransomware primarily targeted Windows PCs due to their large user base. In the mid-2010s, ransomware gangs began targeting Apple and Linux computers as well as mobile devices (Shea, 2025). As ransomware has grown, industries have responded differently to the threats. Banks and other financial firms have responded the strongest because cybersecurity is at the core of their business. If they fail at cybersecurity, firms and individuals will move their money to more secure institutions. Other industries have done little or nothing to address their weak cybersecurity. Some of these industries include pipelines, electrical generating plants, and water works (Kaplan, 2021).

Double, Triple, and Quadruple Extortion

In 2019, ransomware evolved to include double extortion tactics. That is, the ransomware not only encrypted data, but it also sent a copy of the data back to the criminals. The criminals could then threaten to release the data if the ransom was not paid. That eliminated reliable backups as an effective protection against ransomware (Cybermagazine, 2024). The first ransomware to tuse this approach was from the Maze ransomware group (Shea, 2025).

Exfiltration of data is growing increasingly popular among cybercriminals. One 2025 report estimated that 80 percent of the attacks in 2024 focused solely on data exfiltration (Muncaster, 2025). This same report stated that exfiltration-only ransomware attacks are 34 percent faster than encryption-based attacks.

Exfiltration attacks do have a major drawback. For criminals, hosting and distributing terabytes of data is expensive, and this expense must be paid regardless of whether they receive a ransom or not. It is also logistically more difficult to steal the data (Channel E2E Staff, 2025).

In 2021, triple extortion was added to the ransomware playbook. Triple extortion includes a distributed denial-of-service (DDoS) attack. The ransom may demand payment either to prevent a DDoS attack from starting or to stop an ongoing attack (Check Point, n.d.). One of the first examples of triple extortion ransomware was the BlackCat ransomware (Shea, 2025).

A more recent development in response to improved security measures is quadruple extortions. This is where a victim's clients are contacted to pressure on the victim into paying the ransom (O'Flaherty, 2025). It is not just the clients; regulatory agencies are also being involved. One survey reported that 47 percent of attacked organizations had the attackers threaten to file a regulatory complaint if a ransom was not paid or if the organization failed to disclose the incident (Israeld Defense, 2025).

For example, a 2021 attack on the District of Columbia's Metropolitan Police Department (MPD) resulted in the criminals gaining access to police psychological evaluations (Goodin, 2021) and gang informants information (Goodin, Ransomware crooks threaten to ID informants if cops, 2021) when a ransom was not paid.

[3] NotPetya appears to the victim as ransomware but, in actuality, destroys data permanently rather than encrypting it. (Cybermagazine, 2024)

In 2023, a ransomware gang called Ransomed.vc claimed to have infected Sony's systems. Ransomed.vc approached extortion by leveraging the threat of the European Union's General Data Protection Regulation (GDPR). Releasing Sony's data would have exposed the company to massive GDRP fines (Geigner, 2023). In other words, the ransomware gang effectively acted as an enforcement arm of the GDPR.

Ransomware Timeline by Key Features

The ransomware timeline traces its evolution from the 1989 AIDS Trojan to today's sophisticated, AI-driven attacks, highlighting major breakthroughs in encryption, payment systems, and global cybercriminal tactics shaping modern digital extortion. The following is a brief timeline list.

AIDS Trojan / PC Cyborg

- **Year**: 1989
- **Payment**: Postal mail
- **Significance**: First known case of ransomware but otherwise insignificant (Wagner, 2021).

GPCoder

- **Year**: 2005
- **Payment**: e-gold and Liberty Reserve. Early versions also requested payment via Western Union or premium text messages.
- **Significance**: Early ransomware that encrypted files. Also, marked a shift to more sophisticated encryption (Knowbe4, n.d.) (O'Kane, 2018).

WinLock & Reveton

- **Year**: 2011
- **What happened**: Locked computer screens and pretended they were locked by law enforcement. Did not encrypt the data.
- **Payment**: $10 payment via text message
- **Significance**: First use of "screen locker" ransomware, early use of scare tactics (Shea, 2025).

CryptoLocker

- **Year**: 2013
- **What happened**: Spread via malicious email attachments and used strong RSA encryption. Hosted on the Tor networks.
- **Payment**: Bitcoin
- **Significance**: First ransomware to have a large-scale impact (Shea, 2025) (O'Kane, 2018).

Ransomware Expands and Diversifies

- **Years**: 2014-2015
- **Examples**: CryptoWall, CTB-Locker, TeslaCrypt, Simplelocker
- **Targets beyond Windows**: Android, Linux
- **Significance**: More targets and more advanced encryption techniques (O'Kane, 2018).

Ransomware-as-a-Service (RasS) Begins

- **Year**: 2016
- **Examples**: Cerber, Jigsaw
- **Significance**: For the first time, criminals without technical knowhow can launch ransomware attacks. Used affiliate programs (Goud, 2025).

First JavaScript Ransomware

- **Year**: 2016
- **Example**: Ransom32
- **Targets**: Based entirely on JavaScript, it allowed the ransomware to function on all operating systems.
- **Significance**: It was about to cast a much wider net than prior ransomware attacks

WannaCry and NotPetya

- **Year**: 2017
- **What happened**: Used NSA's EternalBlue exploit to spread globally[4]. Additionally, it overwrote the master boot record and encrypted the master file table. This locked the entire hard drive and was much faster than encrypting individual files.
- **Targets**: Hospitals, transportation infrastructure, banks
- **Significance**: Massive real-world impact; disrupted critical infrastructure (Shea, 2025).

Double Extortion Emerges

- **Year**: 2019
- **Example**: Maze ransomware group (see above)
- **Tactic**: Encrypt + exfiltrate data and threaten to leak it if ransom unpaid
- **Significance**: Backup strategies no longer adequate; increases victim pressure (Goud, 2025).

Ransomware-as-a-Service Matures

- **Years**: 2020-2021
- **Examples**: REvil, DarkSide
- **Tactics**: Targeting large enterprises, RaaS marketplaces
- **Significance**: Industrial-scale operations with millions in ransoms (Goud, 2025).

New Models and Law Enforcement Pushback

- **Years**: 2022-2023
- **Trends**: Leak sites, extortion-only attacks (no encryption), crypto laundering
- **Example**: LockBit
- **Significance**: Law enforcement begins to disrupt operations. One example of this is the Hive takedown (The Ransomware Task Force, 2024).

[4] EternalBlue is a Windows exploit tool. It was developed by the U.S. National Security Agency. It takes advantage of a critical vulnerability in the Server Message Block version 1 network protocol. In 2017, a hacking group called Shadow Brokers stole it from the NSA and leaked it online. (Multi-State Information Sharing & Analysis Center, 2019)

- **Example**: Akira ransomware gang (RaaS) had extorted over $42M by 2024
- **Trends**: Data-only extortion, better operational security, focus on large enterprises, more stealth
- **Significance**: Professionalized operations, more targeted attacks, increasing resilience against law enforcement (Wikipedia, n.d.).

Evolution of Payment Methods

The evolution of ransomware payments reflects the shift from traceable methods like cashier's checks and prepaid cards to anonymous digital currencies. Each stage improved criminal efficiency, with Bitcoin ultimately revolutionizing how cybercriminals demand and collect ransoms in today's digital economy. A concise list is presented below.

- **Cashier's check:** It is only used by AIDS Trojan and not viable for large-scale attacks.
- **Short message service to premium rate numbers:** This is a favorite mobile phone lockers.
- **Gift vouchers:** These can be resold on eBay to collect cash.
- **Payment Services:** YandexMoney (Russian website similar to PayPal) was among the first online payment service. Other popular services included payment to a Liberty Reserve account (Costa Rica) and the now failed E-Gold account (Canada). Criminals would later switch to Western Union and PayPal. These are not ideal solutions as they are tied to bank accounts and can be traced.
- **Prepaid services:** These were once e predominant ransom payment method. They used online payment systems such as Ukash, Paysafecard and Moneypak. Criminals would resell the prepaid vouchers.
- **Digital currency:** Bitcoin is hard/impossible to trace and has been adopted by most criminals (O'Kane, 2018).

Brief Summary of Key Trends

Recent ransomware trends show a shift from simple encryption to full-scale data extortion, fueled by ransomware-as-a-service models and cryptocurrency payments. Despite growing law enforcement efforts, attacks are expanding in scale, targeting governments, healthcare, and critical infrastructure worldwide. A short synopsis is outlined below.

- **Encryption to extortion**: Modern attacks often involve stealing data before encryption or skipping encryption entirely.
- **Rise of RaaS**: Affiliate-based business model allows scalability.
- **Increased ransoms**: From individuals to hospitals, pipelines, governments, and other large enterprises.
- **Cryptocurrency reliance**: Payments are harder to trace, especially with Monero and mixers.
- **Law enforcement**: Seizures, arrests, and infrastructure takedowns, though with limited long-term impact.

The Future of Ransomware

While ransomware is not going away, overall payments declined in 2024, especially in the second half of the year. Additionally, profits dropped from $1.25 billion in 2023 to $818 million in 2024 (bankinfosecurity.com, 2025). Analysts attribute the decline to law enforcement takedowns. In late

2023, the FBI distributed the decryption keys to victims of the ransomware group BlackCat (also known as AlphV) and took down its dark web presence. In early 2024, the UK's National Crime Agency hijacked the infrastructure of the ransomware group Lockbit; seizing its cryptocurrency wallets, taking down its dark web sites, and even obtaining lists of its members (Ars Technica, 2025).

In early May 2025, law enforcement officials dismantled approximately 300 servers and neutralized 650 malicious domains worldwide. They also seized a total of EUR 21.2 million in cryptocurrency (Gbhackers, 2025). While ransomware attacks and their associated payments are in decline, the 2025 Cyberthreat Defense Report estimates that only about half of the organizations that pay the ransom actually recover their data (Morningstar.com, n.d.).

Rising Trends in Ransomware

Ransomware is rapidly advancing as technology and criminal tactics evolve. Once simple, it has become a global enterprise driven by AI and complex networks. With new targets like medical devices and infrastructure, it remains a major global cybersecurity threat.

Several trends are likely to continue:

- **The rise of AI:** AI allows criminals to write better code, craft more naturally sounding messages, and use LinkedIn, corporate directories, and other social networking services to develop more realistic spear-fishing attacks.
- **More attacks on medical devices:** The healthcare industry is already a prime target for ransomware. Imagine attacks on pacemakers, defibrillators, and insulin pumps. One of the authors has a pacemaker and it can be accessed over Wi-Fi.
- **More publicity:** Ransomware gangs are known to publicize their exploits. They understand that headlines generate fear and attract affiliates to join their schemes, which in turn gives them more opportunities to infiltrate target organizations.
- **Lower barriers to entry:** As discussed, AI and ransomware-as-a-service make it easier than ever to carry out a ransomware attack with little or no skills. Additionally, modern gangs are compartmentalized, allowing individuals to start in a low-skill roles and work their way up within the organization (Pearson, 2024).
- **Global attacks on ransomware groups:** Australia has developed a playbook on ransom payments, and it appears the UK will follow. Florida and North Caroline have banned public entities from paying ransoms, and more states are likely to follow suit. Countries are joining forces to disrupt the ransomware infrastructure (builtin.com, n.d.). The top five countries for cyberattacks, in order, were Russia, Ukraine, China, Nigeria, and Romania (The United States was fourth). Given this mix, it is clear that law enforcement remains challenging (SciencesPo, 2024).
- **Payment bans:** The UK is currently planning implement a ban on ransom payments for critical sectors and public sector bodies (O'Flaherty, 2025). There are three factors underlying the growth of ransomware: (I) a large pool of security-poor organizations, (II) the availability of difficult-to-trace or unregulated payment methods, and (III) the ability of ransomware gangs to exploit jurisdictional boundaries. All three of these ensure that payment bans will not be effective (Sakellariadis, 2022).

- **Global attacks:** Ransomware gangs have begun testing their latest exploits on firms in Africa, Asia, and South America; regions with much less advanced cybersecurity. They do this to test and refine their techniques before moving to high-value targets in Europe and North America, where cybersecurity measures are more advanced (Kissin, 2024).
- **Targeting critical infrastructure:** Following the success of the attack on Colonial Pipeline and its massive impact, ransomware gangs will likely continue to target critical infrastructure (Goud, 2025).
- **Violence:** While no direct ransomware-related violence has yet occured, there have been threats. Given the money involved, it is not unlikely that a victimized firm might have its CEO threatened. However, researchers estimate that ransomware attacks killed between 42 and 67 Medicare patients between 2016 and 2021 due to delays in life-savings treatments (Pearson, 2024).
- **More collaboration:** As the threat of ransomware continues to grow, especially with state actors involved, governments will likely continue to increase their cybersecurity efforts. International cooperation will likely grow as well (Goud, 2025).

Key Technical and Tactical Shifts

Ransomware has advanced through major technical and tactical shifts, evolving from basic encryption and email-based attacks to sophisticated, multi-layered operations. The rise of RaaS, cryptocurrency payments, and large-scale targeting has transformed cybercrime into a global, organized, and highly profitable enterprise. A brief list is provided below:

- **Encryption methods:** Ransomware has moved from simple symmetric only encryption to strong public/private encryption.
- **Changes in distribution methods:** Early ransomware attacks depended on users opening email attachments (social engineering.) Later versions exploited software vulnerabilities, used worm-like spreading methods (WannaCry), and employed chain attacks.
- **RaaS:** Thios allows gangs and individual users with lower technical skills to carry out attacks.
- **Double, triple, and quadruple attacks:** Gangs now steal data, threaten its release unless the ransom is paid, and even contact the victim's clients.
- **Payment method:** The move to cryptocurrency allows the gangs to remain anonymous.
- **Scale:** Early ransomware attacks targeted individuals and small businesses with limited ability to pay. Modern attacks target infrastructure, healthcare, and small to medium-sized governments that have the ability to pay larger ransoms.

Concise Concluding Inferences

Ransomware has evolved from simple, opportunistic attacks into a complex and highly organized global enterprise, reflecting the growing sophistication of cybercriminal strategies and the expanding digital ecosystem they exploit. Its progression from the early AIDS Trojan to modern, AI-driven, multi-extortion models demonstrates how innovation and exploitation often advance side by side in the digital age, where technology's benefits can quickly become its vulnerabilities. Although defensive technologies, public awareness, and international law enforcement coordination have improved, ransomware's adaptability and constant reinvention ensure it remains

a persistent and evolving threat. Understanding its historical trajectory not only highlights the urgency of continued vigilance but also underscores the importance of proactive, integrated approaches that combine technology, policy, education, and cross-border cooperation to mitigate future risks in our increasingly connected and data-dependent world.

From a management perspective, the evolution of ransomware described in this article, underscores that cyber risk is no longer merely a technical issue, but a strategic, board-level concern shaped by geopolitical realities. As ransomware gangs exploit jurisdictional boundaries, leverage cryptocurrency anonymity, and operate through ransomware-as-a-service networks, they effectively function as transnational enterprises that outpaced traditional law enforcement structures. This creates a fragmented enforcement landscape in which firms must manage not only cybersecurity defenses but also regulatory exposure, reputational risk, and cross-border legal complexities. The use of tactics such as threatening GDPR violations or contacting regulators and clients illustrates how cybercriminal groups weaponize international compliance frameworks to increase pressure on victims. For global organizations, this demands an integrated management approach—combining technical resilience, legal preparedness, crisis communication, and international coordination, while recognizing that geopolitical tensions, uneven cyber laws, and varying state responses create asymmetries that ransomware gangs deliberately exploit.

Acknowledgments and AI Disclaimer

The lead author of this article is Ronny Richardson, a professor and researcher in the Department of Management & Entrepreneurship at the Coles College of Business, Kennesaw State University. Coauthors include Max North, a professor/researcher in the Department of Information Systems & Security at the Coles College of Business, and Sarah North, a principal lecturer/researcher in the Department of Computer Science at the College of Computing and Software Engineering. They are researchers and leaders in the Immersive Visualization Environments Research & Metaverse Supercluster.

AI Disclaimer: *This paper was created with the assistance of AI-based tools (such as ChatGPT) for tasks including drafting, editing, grammar correction, and idea refinement. However, all intellectual direction, critical analysis, final content decisions, and academic integrity of the work are the sole responsibility of the authors. The use of AI was supplementary and did not substitute for human judgment, originality, or authorship. The content of this article does not reflect the opinions, positions, or policies of the Department of Management & Entrepreneurship, the Department of Information Systems & Security, the Coles College of Business, or the Department of Computer Science in the College of Computing and Software Engineering.*

References

Ars Technica. (2025, February 6). *Ransomware payments declined in 2024 despite massive. well-known hacks*. Retrieved from Arstechnica.com: https://arstechnica.com/security/2025/02/ransomware-payments-declined-in-2024-despite-well-known-massive-hacks/

bankinfosecurity.com. (2025, April 7). *Ransomware Underground Faces Declining Relevance*. Retrieved from bankinfosecurity.com:

https://www.bankinfosecurity.com/blogs/ransomware-underground-faces-declining-relevance-p-3850

builtin.com. (n.d.). *5 Ways Ransomware Will Change in 2025*. Retrieved from https://builtin.com/articles/future-ansomware-trends

Channel E2E Staff. (2025, July 21). *The State of Ransomware in 2025: Extortion-Only Strugglesand New Tactics*. Retrieved from channele2e.com: https://www.channele2e.com/native/the-state-of-ransomware-in-2025-extortion-only-struggles-and-new-tactics

Check Point. (n.d.). *What is Triple Extortion Ransomware?* Retrieved from checkpoint.com: https://www.checkpoint.com/cyber-hub/ransomware/what-is-triple-extortion-ransomware/

Cybermagazine. (2024, December 12). *Cisco Talos: Tracking Ransomware's 35 Year Evolution*. Retrieved from cybermagazine.com: https://cybermagazine.com/articles/cisco-talos-tracking-ransomwares-35-year-evolution

Cybersecurity & Infrastructure Security Agency. (2018, December 3). *SamSam Ransomware*. Retrieved from cisa.gov: https://www.cisa.gov/news-events/cybersecurity-advisories/aa18-337a

Emm, D. (2008, September). Cracking the code: The history of Gpcode. *Computer Fraud & Security*(9), 15-17.

Fortinet. (n.d.). *Trojan Horse Virus*. Retrieved from Fortinet.com: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

Gbhackers. (2025, May 28). *Worldwide Operation Shuts Down Hundreds of RansomwareServers and Domains, Ending Key Attack Infrastructure*. Retrieved from gbhackers.com: https://gbhackers.com/operation-shuts-down-hundreds-of-ransomware-servers/

Geigner, T. (2023, September 28). *Techdirt*. Retrieved from The Group Claiming To Have Hacked Sony Is Using GDPR AsA Weapon For Demanding Ransoms: https://www.techdirt.com/2023/09/28/the-group-claiming-to-have-hacked-sony-is-using-gdpr-as-a-weapon-for-demanding-ransoms/

Goodin, D. (2021, May). *Ars Technica*. Retrieved from Ransomware crooks post cops' psych evaluations after talks with: https://arstechnica.com/gadgets/2021/05/ransomware-crooks-post-cops-psych-evaluations-after-talks-with-dc-police-stall/

Goodin, D. (2021, April https://arstechnica.com/information-technology/2021/04/ransomware-attack-on-dc-police-threatens-safety-of-cops-and-informants/). *Ransomware crooks threaten to ID informants if cops*. Retrieved from Ars Technica.

Goud, N. (2025, October 11). *The Evolution of Ransomware: From the 1970s to 2024*. Retrieved from cybersecurity-insiders.com: https://www.cybersecurity-insiders.com/the-evolution-of-ransomware-from-the-1970s-to-2024/

Israeld Defense. (2025, August 8). *Semperis 2025 Ransomware Study Highlights Persistence ofCyber Threats and Evolving Tactics*. Retrieved from israeldefense.co.il: https://www.israeldefense.co.il/en/node/65903

Kaplan, F. (2021, July). *The U.S. Takes an Important Cybersecurity Step—Two Decades*. Retrieved from Slate.,com: https://slate.com/news-and-politics/2021/07/dhs-pipeline-cybersecurity-requirements.html

Kissin, E. (2024, April 24). *Hackers are using developing countries for ransomware practice*. Retrieved from arstechnica.com: https://arstechnica.com/security/2024/04/hackers-are-carrying-out-ransomware-experiments-in-developing-countries/

Knowbe4. (n.d.). *AIDS Trojan or PC Cyborg Ransomware*. Retrieved from knowbe4.com: https://www.knowbe4.com/ransomware-knowledgebase/aids-trojan

Knowbe4. (n.d.). *GPcode Ransomware*. Retrieved October 2025, from knowbe4.com.

Kostka, C. (2022, March 17). *The First Ransomware Attack: Lessons Learned from History*. Retrieved from ransomware.org.

McAfee. (n.d.). *What Is a Trojan Horse?* Retrieved from Mcafee.com: https://www.mcafee.com/learn/trojan-horse/

McGowan, E. (2025, June 10). *Trojan viruses explained (plus tips on how to remove them)*. Retrieved from us.norton.com: https://us.norton.com/blog/malware/what-is-a-trojan

Morningstar.com. (n.d.). *Only Half of Ransomware Victims Recover Data After Paying,Finds CyberEdge Group's 2025 Cyberthreat Defense Report*. Retrieved from Morningstar.com: https://www.morningstar.com/news/business-wire/20250415839378/only-half-of-ransomware-victims-recover-data-after-paying-finds-cyberedge-groups-2025-cyberthreat-defense-report

Multi-State Information Sharing & Analysis Center. (2019). *EternalBlue.* Multi-State Information Sharing & Analysis Center.

Muncaster, P. (2025, February 25). *Only a Fifth of Ransomware Attacks Now Encrypt Data*. Retrieved from infosecurity-magazine.com: https://www.infosecurity-magazine.com/news/only-fifth-ransomware-attacks/

Nomios. (n.d.). *How SamSam Ransomware works in a nutshell*. Retrieved March 2024, from normios.com: https://www.nomios.com/resources/what-is-samsam-ransomware/

O'Flaherty, K. (2025, January 22). *Ransomware: Predictions and Actions in 2025*. Retrieved from scmagazineuk.com: https://insight.scmagazineuk.com/ransomware-predictions-and-actions-in-2025

O'Kane, P. S. (2018, September). Evolution of Ransomware. *Special Issue:Privacy, Data Assurance, Security Solutions for Internet of Things, 7*(5), 321-327.

Pearson, J. (2024, June 11). *Ars Technica*. Retrieved from arstechnica.com: https://arstechnica.com/security/2024/06/ransomware-gangs-are-adopting-more-brutal-tactics-amidst-crackdowns/

Sakellariadis, J. (2022, August 2). *Behind the rise of ransomware*. Retrieved from atlanticcouncil.org: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/

Schissel, N. (2022, February 23). *Ransomware Attacks Becoming More "Professional," Report Warns*. Retrieved from mltaikins.com: https://www.mltaikins.com/insights/ransomware-attacks-becoming-more-professional-report-warns/

SciencesPo. (2024, April 18). *Where do cyber threats come from?* Retrieved from sciencespo.fr: https://www.sciencespo.fr/centre-etudes-europeennes/en/news/where-do-cyber-threats-come-from/

Shea, S. (2025, April 18). *The history and evolution of ransomware attacks*. Retrieved from techtarget.com: https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware

The Ransomware Task Force. (2024, September 26). *2023 RTF Global Ransomware Incident Map: Attacks Increase by 73%, Big Game Hunting Appears to Surge*. Retrieved from securityandtechnology.org: https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map/

Wagner, K. A. (2021). *Evolution of Ransomware.* The MITRE Corporation.

Wikipedia. (n.d.). *Akira*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Akira