Trends in Ransomware Attacks: Infiltration and Encryption Mechanisms of LockBit, Hive, and Akira

Donghwoo Cho, Hyunjun Kim, Soojin Kang, Giyoon Kim, Jongsung Kim

Kookmin University, Seoul, Republic of Korea

Received: September 27, 2025; Revised: November 24, 2025; Accepted: December 22, 2025; Published: December 26, 2025

Abstract

In 2024, approximately 65% of financial institutions worldwide reported experiencing ransomware attacks. To respond to these attacks, multiple countries engaged in international collaboration. However, the average ransom-ware payment in 2024 increased fivefold compared to the previous year. This indicates that the ransomware threat remains persistent. In particular, the spread of the RaaS (Ransomware-as-a-Service) model and the sophistication of attack techniques have increased the importance of technical ransomware analysis. This paper summarizes existing technical analysis studies on Lock-Bit, Hive, and Akira ransomware and examines the evolution of ransom-ware, focusing on technical changes. Specifically, we distinguish between in-filtration and encryption methods to derive generalized evolution patterns and discuss directions for future work.

Keywords: Ransomware Trend, Infiltration Evolution, Encryption Evolution.

1 Introduction

Ransomware is a type of malware that encrypts files on a victim's system and demands payment in exchange for file decryption. Since 2021, the number of financial institutions targeted by ransomware has steadily increased. In 2024, approximately 65% of financial institutions worldwide reported experiencing ransomware attacks [1]. To counter these threats, multiple countries cooperated to conduct international joint operations, such as Operation Cronos [2]. As a result, the total amount of ransomware payments in 2024 decreased by approximately 35% compared to previous year [3]. However, the average ransomware payment in 2024 increased fivefold compared to the previous year [4]. This indicates that the ransomware threat remains persistent. In particular, the spread of the RaaS (Ransomware-as-a-Service) model has lowered the technical barriers for conducting ransomware attacks [5]. Moreover, attackers continue to refine their infiltration and encryption methods by adopting advanced tactics, techniques, and procedures (TTPs) [6].

Ransomware attack techniques are becoming more sophisticated. As a result, the importance of research on analyzing the latest technologies applied to ransomware and proposing countermeasures has increased. Along with this growing importance, trend studies focusing on ransomware technologies have been continuously published. Existing technical trend studies mainly focus on providing comprehensive overviews, starting from the origins of ransomware and describing its major characteristics. The comprehensive approach is useful for under-standing overall attack patterns. However, it has limitations in deriving concrete trends regarding which technical components have evolved. To address these limitations, we analyze how ransomware has evolved in terms of infiltration and data encryption methods. We focus on globally notorious ransomware, LockBit, Hive, and Akira. Through this analysis, we summarize technical evolution pat-terns of ransomware. Moreover, we propose generalized perspectives for effectively responding to ransomware variants.

The structure of this paper is as follows. Section 2 introduces the major ransomware groups analyzed in this study. Section 3 summarizes prior ransomware trend analysis studies and highlights the motivation for this work. Sections 4 and 5 present a technical analysis of changes in ransomware infiltration and encryption

DOI: https://doi.org/10.64799/rebicte.v11i.220

methods based on the analysis results of major ransomware groups. Finally, Section 6 derives generalized findings from observed ransomware evolution pat-terns and discusses directions for future ransomware defense research.

1.1 Our Contributions

Our contributions to this study are as follows:

- We derive evolution patterns from three globally notorious ransomware groups and present generalized conclusions that are not limited to a specific ransomware variant.
- We analyze changes in ransomware infiltration and encryption methods. These results provide insights that support both proactive prevention and damage mitigation following an attack.
- We summarize not only the attack techniques used by recent ransomware but also their technical evolution compared to the past. This enables more effective responses to evolving ransomware threats.

2 Related Work

Identifying trends in ransomware infiltration and encryption methods is essential for developing effective ransomware defense strategies. To obtain information, organizations can refer to technical reports published by industry or technical trend studies such as this paper. Research on ransomware technical trends has been continuously conducted. S Aurangzeb et al. analyzed ransomware that emerged between 2013 and 2016 [7]. They examined 76 malware and ransom-ware samples. They also compared their attack methods, characteristics, and payment mechanisms. HT Nerprash et al. analyzed ransomware attack trends targeting healthcare institutions in the United States from 2016 to 2021[8]. During this period, the number of ransomware attacks more than doubled in healthcare sector, increasing from 43 to 91 cases per year. In addition, approximately 42 million patients' personal health information was exposed. S Razaulla et al. analyzed the overall evolution of ransomware[9]. They classified ransom-ware based on infiltration methods, encryption techniques, and target platforms. A Phipps et al. studied trends in ransomware groups of Conti, LockBit, and BlackCat/ALPHV[10]. They collected fragmented ransomware intelligence and derived common characteristics across the analyzed ransomware groups. As demonstrated by these studies, ransomware trends analysis has been conducted from multiple perspectives, including technical characteristics as well as organizational and operational structures. In particular, research on the latest techno-logical trends is important because technological trend analysis must reflect continuous changes. Therefore, we analyze technical trends in ransomware by focusing on changes in infiltration and encryption methods of three representative ransomware groups up to 2025.

3 Background

This Section introduces the ransomware groups of LockBit, Hive, and Akira analyzed in this study.

3.1 LockBit Ransomware

LockBit ransomware first appeared in September 2019 and was initially known as ABCD ransomware. The name LockBit was first observed in January 2020 [11]. Since 2021, LockBit has adopted a double extortion strategy that encrypts victims' data and exfiltrates it. In 2022, the number of LockBit attacks increased sevenfold compared to the previous year. Moreover, LockBit accounted for 16% of the ransomware attack market, making it the most active ransomware world-wide [12]. LockBit further evolved its extortion strategy by adding DDOS (Dis-tributed Denial of Service) attacks, resulting in a triple extortion model [13]. However, in February 2024, Operation Cronos significantly disrupted LockBit's core infrastructure, leading to a noticeable decline in its attack activity [14]. De-spite this disruption, LockBit resumed operations by releasing a new ransomware variant in September 2025 [15].

3.2 Hive Ransomware

Hive ransomware was first identified in June 2021, following an attack on Altus Group, a Canadian IT company [16]. Hive operates under a typical RaaS model uses a double extortion strategy involving data encryption and data exfiltration. According to investigation results released by the U.S. Department of Justice and the FBI, the Hive ransomware group attacked more than 1,500 organizations across approximately 80 countries between June 2021 and January 2023 [17]. During this period, the total amount of ransomware payments demanded or paid by victim organizations was estimated to exceed 100 million USD. As this threat spread, the FBI issued a warning regarding Hive ransomware around August 25, 2021. Subsequently, in January 2023, the U.S. Department of Justice officially announced the removal of Hive's operational infrastructure through an international law enforcement operation. Nevertheless, subsequent reports suggested that the Hive ransomware group was linked to the Hunters International ransom-ware group [18].

3.3 Akira Ransomware

Akira ransomware emerged in March 2023 and targeted a wide range of organizations across North America, Europe, and Australia. Initially, Akira targeted Win-dows system. However, in April 2023, it released a Linux variant targeting VMware ESXi environment. As of January 1, 2024, Akira had compromised more than 250 organizations and generated approximately 42 million USD in ransom-ware revenue [19]. In the third quarter of 2024, Akira held a 13% of the ransom-ware attack market and became the most impactful ransomware in the United States [20]. In the second quarter of 2025, Akira ranked as the second most active ransomware worldwide, with a global attack market share of 12% [21].

4 Evolution of Ransomware Infiltration Methods

This section describes changes in the infiltration methods of LockBit, Hive, and Akira ransomware.

4.1 LockBit Ransomware

LockBit ransomware attempted initial access early on by exploiting a known vulnerability (CVE-2018-13379) in Fortinet FortiOS and FortiProxy products [22]. CVE-2018-13379 is a vulnerability that allows attackers to access system files of the affected software and steal user credential information. In late 2023, LockBit ransomware exploited a vulnerability (CVE-2023-4966) in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway [23]. This vulnerability triggers a buffer overflow in the affected software, leading to a memory leak and enabling the extraction of user credential information from memory. Although LockBit ransomware has exploited different vulnerabilities over time, a common trend can be observed in which it acquires user credentials to gain access to target systems. No known attack cases have been reported since LockBit ransomware resumed its activities in 2025.

4.2 Hive Ransomware

Hive ransomware primarily attempted infiltration through vulnerable remote access. This is an infiltration method that involves compromising accounts con-figured with single-factor authentication on insecure Remote Desktop Protocol (RDP) services or VPNs [24]. Additionally, some attackers have been using spear phishing techniques to infect users by attaching ransomware to phishing emails. Subsequently, Hive ransomware further sophisticated its initial infiltration meth-ods by exploiting disclosed software vulnerabilities. In 2021, it employed a method of gaining Remote Code Execution (RCE) privileges by exploiting the Microsoft Exchange ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207). As a result, cases of infiltration into internal net-works were reported [25]. Furthermore, Hive ransomware exploited an authentication bypass vulnerability (CVE-2020-12812) in Fortinet SSL VPN devices. In this manner, Hive logged into VPNs without additional authentication steps by targeting weakly configured Multi-factor Authentication (MFA) [26]. This al-lowed Hive ransomware to obtain administrative privileges. Thus, Hive ransom-ware evolved from initially exploiting vulnerable remote access and phishing to increasingly exploiting disclosed vulnerabilities. As a consequence of these changes, the types and scope of attack attempts were observed to continuously expand.

4.3 Akira Ransomware

Akira ransomware primarily attempts initial access by exploiting vulnerabilities in network devices. Early on, it exploited a known vulnerability (CVE-2020-3259) in Cisco VPNs without MFA [27]. Additionally, Akira ransomware used a zero-day vulnerability (CVE-2023-20269) in Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) to gain initial access [28]. In July 2025, attacks by Akira ransomware increased sharply. During this period, the ransomware leveraged a vulnerability in SonicWall SonicOS Management Access and SSL VPN (CVE-2024-40766) to gain initial access [29]. Through this evolution, it is observed that Akira ransomware has continuously exploited new vulnerabilities for initial access.

5 Evolution of Ransomware Encryption Methods

This section describes changes in the encryption processes of LockBit, Hive, and Akira ransomware.

5.1 Key Generation

We summarize changes in key generation methods within the encryption processes of LockBit, Hive, and Akira ransomware.

LockBit Ransomware. LockBit 2.0 ransomware that emerged in mid-2021 used the Windows API to generate secret keys for file encryption. The function used was BCryptGenRandom, which is a secure random number generator that follows the NIST SP 800-90 standard [30]. LockBit ransomware generates the secret key and IV for AES symmetric-key encryption used for file encryption on a per-file basis through this random number generator. The secret keys and IVs used for file encryption are encrypted with the attacker's public key and stored at the end of the encrypted file. From mid-2022, LockBit 3.0 ransomware was used in at-tacks. This variant generates random numbers by leveraging the cpuid and rdrand assembly instructions [31]. In particular, the cpuid instruction can be used to determine whether the execution environment is a virtual machine and is one of the well-known methods for evading analysis [32]. Furthermore, the generated random numbers are validated using an internally generated checksum, which imposes limitations on analysis. At the same time, they are protected using the RtlEncryptMemory function [33], which encrypts specific memory regions to prevent disclosure by analysts. The encrypted random numbers are decrypted using the RtlDecryptMemory function [34] immediately before file encryption. They are then used as the key matrix for the Salsa20 file encryption algorithm.

Hive Ransomware. The initial Hive ransomware generated a single large key table to produce file encryption keys. A Pseudo-random Number Generator (PRNG) was used to generate the key table, and the function employed was Rand. Hive ransomware subsequently generated two keystreams from the key table and used them to derive the file encryption key. Then, the encryption key was extracted by performing an XOR operation based on modular operations on the two key streams. After file encryption was completed, the key table was released from memory. However, on November 30, 2022, a decryption study based on vulnerabilities in Hive ransomware has been released [35]. Because modular operations caused the keystream derived from a fixed key table to be repeatedly reused, correlations emerged between the ciphertexts of different files. As a re-sult, once partial plaintext was obtained, XOR equations could be constructed from the ciphertext, and solving these equations enabled the recovery of up to 95% of the key table. A variant of Hive ransomware emerged just one week after the release of the existing decryption tool [36]. It was reimplemented from the existing Go-based to a Rust-based, and the key management mechanism was comprehensively changed. The variant retained the file encryption operations. However, it changed key table management by encrypting the key table using an authenticated encryption scheme such as XChaCha20-Poly1305 [37]. In this process, the key used to encrypt the key table is generated through ECDH-based public-key operations. Furthermore, the variant of Hive ransomware encrypted and managed the key table using public key–based key derivation and Authenticated Encryption with Associated Data (AEAD). This structure prevented the construction of XOR equations for deriving keystreams from the key table. Consequently, the previous approach was no longer effective for recovering the key table.

Akira Ransomware. Early versions of Akira ransomware used the Windows API to generate the secret keys used for file encryption. The function used was CryptGenRandom, which is a cryptographically secure random number generator [38]. However, the keystream of the stream cipher generated from the initially produced random value was reused identically across all files [39], resulting in a structure that was vulnerable to reused key attacks [40]. Based on this weakness, Avast released a tool on June 29, 2023 to decrypt files infected by Akira ransomware. Shortly thereafter, the Akira ransomware operators distributed a vari-ant that patched the vulnerability within three days. Akira ransomware variant employed the secure PRNG Yarrow, and the seed value for the generator was derived from the return value of a high-resolution timer provided by the operating system. At this stage, the return value of the high-precision timer used as the seed was sufficiently feasible to be searched through brute-force attack based on the file's last modification timestamp. On March 13 2025, Yohanes Nugroho released a tool that decrypts infected files by recovering the encryption key through a GPU-based brute-force attack against the random number generator seed [41]. However, Akira ransomware distributed a new variant that rendered the tool ineffective less than one week after its public release. The new ransom-ware variant continued to use the Yarrow, as in the previous version, and derived the seed value from the return value of a high-precision timer. However, the high-precision timer was invoked dozens of times or more to generate a single random value. This design makes brute-force attacks against the seed value impractical at the current level of computing capability [42].

5.2 File Encryption

This subsection describes changes in file encryption methods within the encryption processes of the LockBit, Hive, and Akira ransomware.

LockBit Ransomware. LockBit 2.0 ransomware employed the symmetric-key encryption algorithm AES for file encryption [43]. The subsequent LockBit 3.0 ransomware adopted the stream cipher algorithm Salsa20 for file encryption in-stead of AES. According to Daniel J. Bernstein's experiments, Salsa20 is a faster algorithm than AES when encrypting data [44]. LockBit 5.0 ransomware, which was released when operations resumed in September 2025, is known to achieve faster encryption speeds than previous versions through code optimization [45].

Hive Ransomware. The early Hive ransomware was implemented in the Go programming language and used XOR operations for file encryption. One characteristic of the ransomware was that it extracted keys from a large keystream and encrypted the original files using XOR operations to increase encryption speed. However, a decryption tool was released for this version of the ransomware. Afterward, Hive ransomware was reimplemented in Rust, while retaining the encryption method that XORs the keystream with the original file [46].

Akira Ransomware. Initial Akira ransomware employed the stream cipher algorithm ChaCha20 for file encryption [43]. However, Akira ransomware modified its file encryption method after a decryption tool for the initial version was re-leased. Specifically, the new version employs the stream cipher algorithms ChaCha20 and KCipher-2 for file encryption [41].

5.3 Partial Encryption

This subsection describes changes in partial encryption methods within the encryption processes of the LockBit, Hive, and Akira ransomware.

LockBit Ransomware. LockBit 2.0 ransomware encrypts at most 4 KB per file during file encryption. [47]. In subsequent LockBit 3.0 and LockBit 4.0 ransom-ware variants, the partial encryption strategy has become more fine-grained [48]. According to EQST's analysis, LockBit 3.0 ransomware performs full encryption on files with a size of 1 MiB or smaller. For files larger than 1 MiB and up to 5 MiB in size, only the first 1 MiB is encrypted. Finally, for files larger than 5 MiB, the encryption scope depends on whether the '-size' command line argument is used. When the '-size' argument is used, the file is divided into ten equal-sized blocks, and only the odd-numbered blocks are encrypted. In the absence of the '-size' argument, encryption is applied to the beginning, middle, and end portions of the file, each according to attacker defined parameters. LockBit 4.0 ransom-ware encrypts the entire file when the file size is 1 MiB or smaller, consistent with LockBit 3.0 ransomware. Otherwise, encryption is applied to the beginning, middle, and end portions of the file, with each portion accounting for 9% of the file size. Overall, LockBit ransomware has exhibited a shift in the partial encryp-tion region from a fixed size to a relative size determined by the file size.

Hive Ransomware. Hive ransomware encrypts files by applying XOR operations between the file encryption key and data blocks of size 0x1000-byte. During file encryption, the first block is encrypted, while subsequent blocks are left unencrypted at regular intervals. Subsequently, another block is encrypted, and this pattern is repeated throughout the file encryption process. When the file size is smaller than 0x1000- byte, the entire file is encrypted. In Hive ransomware vari-ants, encryption is also performed using the same approach. However, the block size was increased to 0x100000-byte. In addition, during file encryption the '-min-size' command line argument is available to specify the minimum file size to be encrypted [37].

Akira Ransomware. Early Akira ransomware encrypted the first 50% of a file when the target file size was 2 MB or smaller. When the file size exceeded 2 MB, it encrypted 10% of the file from each of four offsets calculated based on the file size [49]. In subsequent Akira ransomware variants, the ransomware additionally checks file extensions and encrypts the entire file when the extension corresponds to a database file targeted for encryption [50].

6 Conclusion

In this paper, we examined the evolutionary trends of ransomware through the globally notorious major ransomware LockBit, Hive, and Akira. The evolutionary trends of infiltration methods observed through major ransomware has been to use newly disclosed vulnerabilities as an initial access. The Table 1 shows a summary of the changes in infiltration methods by ransomware.

Table 1. Summary of Ransomware Infiltration Evolution

Ransomware	Initial Infiltration	Evolved Infiltration
LockBit	Fortinet FortiOS/FortiProxy information disclosure (CVE 2018-13379)	Citrix NetScaler memory leak (CVE-2023-4966)
Hive	Fortinet SSL VPN authentication bypass (CVE-2020-12812)	Microsoft Exchange ProxyShell RCE (CVE-2021-31207, CVE-2021-34473, CVE-2021-34523)
Akira	Cisco VPN authentication bypass (CVE-2020-3259)	Cisco ASA/FTD zero-day RCE (CVE-2023-20269) and SonicWall SonicOS access control/SSL VPN vulnerability (CVE-2024-40766)

An analysis of the evolutionary trends in infiltration methods observed across major ransomware that the major of vulnerabilities exploited for initial access are classified as the "Exploit Public-Facing Application" (T1190) technique defined in the MITRE ATT&CK framework [51]. According to Mandiant's analysis, software vulnerabilities were the most commonly used attack vector for initial access recently [52]. There is a platform that provides information on vulnerabilities exploited by malware, such as CISA's Known Exploited Vulnerabilities (KEV) catalog, to combat known vulnerabilities [53]. However, ransomware attackers also monitor disclosed vulnerabilities and continuously exploit newly identified ones. Therefore, research is needed on reliable cyber threat intelligence (CTI) platforms where attacker access is restricted.

A common evolutionary trends were also confirmed in the encryption method of major ransomware. The Table 2 gives a summary of the changes in encryption methods by ransomware.

Table 2. Summary of Ransomware Encryption Evolution

Ransomware	Initial Encryption			Evolved Encryption		
	Key Generator	File Encryption	Partial Encryption Method (strategy)	Key Generator	File Encryption	Partial Encryption Method (strategy)
LockBit	BCryptGenRandom	AES	Fixed-size	cupid and rdrand	Salsa20	File size
Hive	Rand	XOR	Block	Rand and ECDH-derived key	XOR	Block
Akira	CryptGenRandom	Chacha20	File size	Yarrow	Chacha20 KCipher-2	File size and file type

We were able to conclude that there are two trends in the evolution of encryption methods, observed through major ransomware. First, as soon as a tool for decrypt ransomware-infected files is released, ransomware attackers quickly removed the decryption component to disable the tool. To prepare for this, it is necessary to analyze the opportunity cost according to whether or not to disclose, based on past decryption tool disclosure cases. Second, partial encryption strategies have become increasingly sophisticated. Previously, partial encryption considered only file size or set the encryption region to a fixed size. However, it has evolved to consider data importance, such as file extensions, or to set the encryption region to a relative size based on file size rather than a fixed size. This makes file recovery difficult for unencrypted regions. Therefore, research on file recovery for unencrypted regions should be conducted.

This study analyzed technical changes in major ransomware and summarized evolutionary trends in ransomware. Ransomware has continued to undergo technical changes. To respond these changes, it is necessary to continuously analyze technical changes in ransomware and develop corresponding countermeasures. Based on the analysis results, future research directions were proposed. This paper is expected to contribute to research on countermeasures against new ransomware variants.

References

[1] statista, https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global, last accessed 2025/12/18.

[2] EUROPOL, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation, last accessed 2025/12/18.

[3] Chainalysis, https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025, last accessed 2025/12/18.

[4] SOPHOS, https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024, last accessed 2025/12/18.

[5] IBM, https://www.ibm.com/think/insights/the-rise-of-raas, last accessed 2025/12/18.

[6] DRAGOS, https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2025, last accessed 2025/12/18.

[7] Aurangzeb, Sana, et al. “Ransomware: a survey and trends.” J. Inf. Assur. Secur 6.2 (2017): 48-58.

[8] Neprash, Hannah T., et al. “Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021.” JAMA Health Forum. Vol. 3. No. 12. American Medical Association, 2022.

[9] Razaulla, Salwa, et al. “The age of ransomware: A survey on the evolution, taxonomy, and research directions.” IEEE Access 11 (2023): 40698-40723.

[10] Phipps, Andrew, and Jason RC Nurse. “Inside ransomware groups: An analysis of their origins, structures, and dynamics.” Computers & Security (2025): 104705.

[11] CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a, last accessed 2025/12/18.

[12] BLACKFOG, https://www.blackfog.com/2022-ransomware-attack-report/, last accessed 2025/12/18.

[13] BLEEPINGCOMPUTER, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/, last accessed 2025/12/18.

[14] Trend Micro, https://www.trendmicro.com/en/research/24/d/operation-cronos-aftermath.html, last accessed 2025/12/18.

[15] Trend Micro, https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html, last accessed 2025/12/18.

[16] BLEEPINGCOMPUTER, https://www.bleepingcomputer.com/news/security/hive-ransomware-enters-big-league-with-hundreds-breached-in-four-months/, last accessed 2025/12/18.

[17] U.S. Department of Justice, https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant, last accessed 2025/12/18.

[18] Infosecurity Magazine, https://www.infosecurity-magazine.com/news/ransomware-hunters-international/, last accessed 2025/12/18.

[19] CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a, last accessed 2025/8/6.

[20] Statista, https://www.statista.com/statistics/1411163/ransomware-variants-detected-usby-market-share/, last accessed 2025/12/18.

[21] DRAGOS, https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q2-2025#ransomware-groups-trends-patterns-and-observations-second-quarter-of-2025, last accessed 2025/12/18.

[22] Australian Signals Directorate, https://www.cyber.gov.au/about-us/advisories/2021-006-asdacsc-ransomware-profile-lockbit-20, last accessed 2025/12/18.

[23] CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a, last accessed 2025/12/18.

[24] Picus Security, https://www.picussecurity.com/resource/blog/cisa-alert-aa22-321a-hive-ransomware-analysis-simulation-ttps-iocs, last accessed 2025/12/18

[25] Varonis, https://www.varonis.com/blog/hive-ransomware-analysis, last accessed 2025/12/18.

[26] SentinelOne, https://www.sentinelone.com/anthology/hive/, last accessed 2025/12/18.

[27] TRUESEC, https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259, last accessed 2025/12/18.

[28] Picus Security, https://www.picussecurity.com/resource/blog/cve-2023-20269-akira-ransomware-exploits-cisco-asa-vulnerability, last accessed 2025/12/18.

[29] Help Net Security, https://www.helpnetsecurity.com/2025/09/29/akira-ransomware-sonicwall-vpn, last accessed 2025/12/18.

[30] Microsoft Learn, https://learn.microsoft.com/en-us/windows/win32/api/bcrypt/nf-bcrypt-bcryptgenrandom, last accessed 2025/12/18.

[31] SOMANSA, https://www.somansa.com/wp-content/uploads/2023/01/lockbit30_202212.pdf, last accessed 2025/12/18.

[32] Deep Instinct, https://www.deepinstinct.com/blog/malware-evasion-techniques-part-2-anti-vm-blog, last accessed 2025/12/18.

[33] Microsoft Learn, https://learn.microsoft.com/en/windows/win32/api/ntsecapi/nf-ntsecapi-rtlencryptmemory, last accessed 2025/12/18.

[34] Microsoft Learn, https://learn.microsoft.com/en-us/windows/win32/api/ntsecapi/nf-ntsecapi-rtldecryptmemory, last accessed 2025/12/18.

[35] Kim, Giyoon, et al. “A method for decrypting data infected with hive ransomware.” Journal of Information Security and Applications 71 (2022): 103387.

[36] Bitdefender, https://www.bitdefender.com/en-us/blog/hotforsecurity/hive-ransomware-switches-to-rust-to-increase-encryption-complexity, last accessed 2025/12/18.

[37] Microsoft Security, https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust/, last accessed 2025/12/18upgrades-in-rust/, last accessed 2025/12/18.

[38] Wikipedia, https://en.wikipedia.org/wiki/CryptGenRandom, last accessed 2025/12/18.

[39] CyberCX, https://cybercx.com.au/blog/akira-ransomware/, last accessed 2025/12/18.

[40] Wikipedia, https://en.wikipedia.org/wiki/Stream_cipher_attacks, last accessed 2025/12/18.

[41] Tinyhack, https://tinyhack.com/2025/03/13/decrypting-encrypted-files-from-akira-ransomware-linux-esxi-variant-2024-using-a-bunch-of-gpus/, last accessed 2025/12/18.

[42] PORTHAS INC, https://www.porthas.com/blog/akira-ransomware-in-depth-technical-analysis, last accessed 2025/12/18.

[43] Gen, https://www.gendigital.com/blog/insights/research/decrypted-akira-ransomware, last accessed 2025/12/18.

[44] Bernstein, D.J.: The Salsa20 family of stream ciphers. In: Robshaw, M., Billet, O. (eds.) New Stream Cipher Designs, LNCS, vol. 4986, pp. 84–97. Springer, Berlin, Heidelberg (2008).

[45] Itiatechnology group, https://www.altiatech.com/lockbit-5-0-the-evolution-of-ransomware-s-most-persistent-threat, last accessed 2025/12/18.

[46] Microsoft, https://www.microsoft.com/en-us/security/blog/2022/07/05/hive-ransomware-gets-upgrades-in-rust, last accessed 2025/12/18.

[47] CYBOTS, https://cybotsai.com/lockbit2-0-accenture, last accessed 2025/12/18.

[48] EQST, https://lms.eqst.co.kr/home/brd/bbs/viewAtclMain?atclSn=1128&bbsCd=INSIGHT&langCd=en&mcd=MC00000081, last accessed 2025/12/18.

[49] Avast, https://www.nomoreransom.org/uploads/User%20Manual%20-%20Akira_Decryptor.pdf, last accessed 2025/12/18.

[50] SK Shieldus: KARA Ransomware Trend Report 2024 Q4. Technical Report, SK Shieldus, Republic of Korea (2024).

[51] MITRE, https://attack.mitre.org/techniques/T1190, last accessed 2025/12/18.

[52] Mandiant: M-Trends 2025. Threat Intelligence Report, Google Cloud, United States (2025).

[53] CISA, https://www.cisa.gov/known-exploited-vulnerabilities-catalog, last accessed 2025/12/18.