Destiny Hale

CRJS 310

Dr. Akgul

October 27, 2025

Thematic Analysis of Cyberattacks

Introduction

Technological innovations have benefited and transformed the way society performs tasks such as communication, work, and information transfer through various services. These advancements replace traditional and manual methods of interaction and work, providing more effective and efficient processes. However, these technological innovations can also be weaponized for malicious use by hackers and cybercriminals. The rise of cybercrime has introduced significant security implications and ethical considerations about the ways of keeping technological devices and society secure. These crimes come in different forms, such as cyber pornography, cyberattacks, cyberfraud, dark web activity, etc. Recently, cyberattacks have become technically complex and psychologically manipulative.

Between 2023 and 2025, news sources and technology-based publications such as BBC, The Hacker News, Cybernews, CSO, and Security Week reported numerous cyberattacks that led to the exposure of information, public trust, and disruption of systems. These attacks had a profoundly negative impact on individuals and companies. Using thematic analysis, this essay examines several cyberattack articles published by these outlets to identify key patterns, evolving techniques, and emerging trends in these modern cyberattacks. It also explores common themes, such as victim targeting patterns, technological vulnerabilities exploited, methodologies, and

evolving techniques found in these news articles. Collectively, these highlight the current shift of modern cyberattacks.

Victim Targeting Patterns

Before a hacker can attack and gain unauthorized access to any system, they must first identify their victims. This is done through reconnaissance, which involves gathering information about the targets. Hackers use it to determine which vulnerabilities exist and what attack vectors they can use to exploit those weaknesses. Reconnaissance can be either active or passive. Active reconnaissance involves directly targeting systems for system insight (Cycognitio, n.d.). In contrast, passive reconnaissance involves reviewing publicly available information (Cycognitio, n.d.). Both methods provide a map of the digital landscape of their targets, identifying weak access points, valuable assets, and possible entries. It also provides how they are going to attack based on what they have gathered. Cyberattack articles, such as Allianz Life and the Workday CRM platform, reported by Ahmadi (2025) and Schappert (2025), demonstrate this process. Attackers in both cases managed to mimic professionals and business emails by studying internal communications to manipulate individuals and employees into giving their credentials, resulting in full compromise of the systems and accounts.

Reconnaissance is also shaped by motives and intentions. The thought process behind this includes what the hacker wants to get out of the intended target and decides if they want to use it for personal or organizational advantages. Hackers usually seek anything valuable, such as data, personal information, or currency, during this process. The most common targets that hold this type of information are individuals and companies, where this recurring pattern was found in all of the cyberattack articles. At the individual level, for example, the Kido Nurseries

ransomware attack shows how parents who used the platform Famly were targeted by Radiant. From this attack, parents received threatening calls from the attackers, urging them to put pressure on Kido Nurseries to pay a ransom under the threat of exposing their child's information (Tidy, 2025). Arghire (2024) also shows how individuals, such as an employee, were targeted. In the LastPass deepfake attack, an employee received a series of calls and messages from an attacker impersonating a CEO via WhatsApp.

At the company level, attackers target these due to the valuable information they hold within their databases. By compromising these companies, attackers can gain access to customer data, internal communications, and other information. Microsoft, various hotel chains, and infrastructure firms were prime targets due to this case. In Microsoft's cyberattack, Russian hackers targeted users via WhatsApp, Signal, and Microsoft Teams (Lakshmanan, 2025a). For hospitality services such as hotels, Arghire (2025) reported numerous hotels being targeted by a hacker group called RevengeHotels. In the article, Arghire (2025) stated they targeted hotels in countries such as Brazil for this attack and previously targeted other hotels in countries such as Russia, Turkey, Spain, and more. Through a vendor email compromise attack, reported by Hill (2023), infrastructure firms were targeted by attackers through invoice or phishing emails. Collectively, these examples show how attackers target both companies and individuals based on their access privileges to information.

Technology Vulnerabilities Exploited

Once the attacker has identified their targets and created a digital landscape through reconnaissance, they can effectively infiltrate systems by exploiting the vulnerabilities they have discovered. These weaknesses may include outdated software, misconfigurations, or weak

security postures. In every case, cybercriminals have exploited third-party platforms, systems, and authentication-based systems. These are critical digital infrastructures that companies depend on during business operations. Tidy (2025), Ahmadi (2025), and Schappert (2025) demonstrated how weaknesses in third-party platforms created an entry point for attackers. Both employees and individuals in these attacks interact with a compromised platform that allows attackers to gain unauthorized access to the data stored in it.

As for authentication-based systems, numerous privileges were bypassed. For instance, Russian hackers in the Microsoft attack leveraged to abuse authentication tokens and codes to gain access to other accounts as long as they remained valid (Lakshmanan, 2025a). Similarly, attackers who targeted Amazon Web Services managed to exploit leaked AWS key pairs via misconfigured deployments, public code repositories, compromised developer tools, and forgotten identity and management access (IAM) users (Naprys, 2025). From these weaknesses, they were able to encrypt files to prevent access from users. In contrast, in Microsoft Azure environments, attackers exploited and bypassed multi-factor authentication applications through compromised accounts and employed proxy services (Constantin, 2024). Lastly, for systems, code-signing certificates and user account protection controls were exploited (Aghire, 2025; Lakshmanan, 2025b). In both attacks, hackers used AI-enhanced tools to execute these exploits. Overall, these examples demonstrate how hackers can exploit digital infrastructures across third-party platforms to systems, maintaining unauthorized access and persistence over sensitive data.

Methodologies

After the attacker has established their targeted victims and entry points by exploiting vulnerabilities, their goal is now to maintain unauthorized access and achieve intended outcomes. This is achieved by employing tactics such as malware deployment, social engineering, and privilege escalation. Gathered from every attack, hackers used ransomware, social engineering tactics, and trojan horses to obtain credentials and other information. Most of these methods are credential theft and psychological manipulation-based attacks. For instance, in the Kido Nursery attack, Radiant used ransomware to encrypt the profiles of every child (Tidy, 2025). From this attack, they were able to gather a total of 20 profiles that included the children's birthdate, nursery pictures, and other details from the platform (Tidy, 2025). In another ransomware attack, the campaign was able to encrypt numerous AWS S3 buckets and files from users (Naprys, 2025). According to Naprys (2025), over 158 million AWS key records were leaked, and 1,229 unique credentials were compromised.

As for social engineering attacks, such as phishing and business email compromise, attackers were able to manipulate the human mind and gain information from the user's human error. For instance, in the LastPass attack, attackers used deepfake technology through business email compromise, phishing employees by impersonating a CEO from the company (Arghire, 2024). Although the employees reported the incident, and no credentials were affected, this still shows how attackers can leverage their positions to trick individuals into giving credentials through impersonation of people they know. In another business email compromise attack, attackers used phishing lures, such as malware-embedded linked documents. This allowed employees and senior-level personnel to click on the "view document" link. The results led to hundreds of Microsoft Azure accounts being compromised in the cloud environment (Constantin, 2024). Similarly, in numerous critical infrastructure firms, 15 individuals received phishing

emails from other vendor-compromised email accounts. In each email, there was a fake PDF attachment that included a new payment policy and bank account details (Hill, 2023). It also included professional language that victims might notice in normal communication with their vendors. From these legitimate-looking emails, the attackers were able to maintain their access by bypassing security defenses.

In a phishing campaign, hackers who targeted Allianz Life, an insurance company, were able to gain personal information from 1.4 million customers (Ahmadi, 2025). In another phishing campaign, Russian hackers used fake sign-in pages and productivity apps such as Microsoft Teams to gain trust from users and steal account credentials by using device codes (Lakshmanan, 2025a). In the attack, the attackers sent Microsoft Teams meeting invitations to users via email, which, if clicked, directed users to a message for them to authenticate using one of the generated device codes that the hackers created. From this, the attackers were able to gain access to credentials without the need for a password (Lakshmanan, 2025a). Lastly, in the Workday CRM platform attack, Shiny Hunters pretended to be human resources or IT staff from the company. They were able to gain business contact information such as names, phone numbers, and emails from the CRM platform (Schappert, 2025).

Lastly, trojan horses were used to trick users, infiltrate systems, and gain access to credentials. For example, in global organizations, attackers used trojan horses disguised as legitimate AI tools to trick users into installing them. According to Lakshmanan (2025b), these AI-enhanced tools included a professional interface and valid digital signatures. These tools were able to bypass security tools and go undetected by users. Once installed by users, this allowed the attackers to gain remote access to the infected systems, communicate with them by using control and command, and prepare them to deploy additional payloads. Similarly, RevengeHotels used a remote access trojan and phishing emails to steal credentials (Arghire, 2025). RevengeHotels first started the attack by sending

invoice phishing emails and fake job applications to lure the targeted hotels. Once the victims click the following links, it redirects them to websites embedded with AI-generated malicious scripts. This activated the malware to spread through systems and created an entry point for the attackers to have remote access, exfiltrate files, set up reverse proxies, and bypass user account control protections. These methodologies highlight how attackers use the combination of technical tools with psychological manipulation, exploiting human trust to gain information and bypass security controls.

Evolving Techniques and Trends

The two trends of these modern cyberattacks have shown that hackers are approaching their targets more stealthily, rather than directly executing them with attacks that may alert systems. One trend is the weaponization of AI. In society today, artificial intelligence has been a helpmate to businesses and individuals for generating ideas and regulating data. However, the following cyberattacks have shown how they can be weaponized. For example, in attacks such as LastPass, it was used to create deepfakes of the CEO of the company (Arghire, 2024). The current advancement of artificial intelligence in this attack has made this possible by giving the deepfake videos and calls a realistic feel. In other attacks, such as the hotel and global organizations, both attackers utilized AI to make fake documents or applications seem legitimate and professional to users (Lakshmanan, 2025b; Arghire, 2025). This not only gives the victims the impression that these applications and calls are real, but it also tricks them into installing malware and interacting with compromised systems.

The second trend that was discovered through these attacks is that the use of stolen credentials has been a primary key to accessing databases and sensitive information. In some attacks, hackers access databases by either guessing what the potential passwords are that the user might use to log in or by using a list of common passwords. Once the right guess or entries

work, they can access the systems and accounts. However, these attempts may alert systems. Attackers now use manipulative techniques, such as impersonation, to lure their victims into giving their login credentials. Two attack examples demonstrate these techniques.

In the infrastructure firm attack, the attackers impersonated vendors from other companies by using compromised accounts retrieved from those companies. Utilizing these compromised accounts, the attackers were able to create numerous emails that contained grammatical errors and characteristics that made them legitimate (Hill, 2023). These emails made it difficult for the victims and systems to detect. Similarly, Russian hackers impersonated as associates from other companies. In the attack, they have sent victims Microsoft Teams invitation emails to join meetings. Also, within those emails, they provide registration links embedded with a fake page for the user to click on. According to Lakshmanan (2025a), the attacker generates a legitimate code request for the user to enter into the fake sign-in page. This tricks the user into trusting a fake service without notice. Since these emails and messages "represented" a trusted person and service, this allowed the attackers to gain more credentials and gave them a disguise to maintain unauthorized access to systems. Overall, these successful techniques and trends focused on exploiting the trust of users and technologies through systems that rely on trust. This creates new advantages for hackers.

Conclusion

Although technology has benefited us in our day-to-day tasks, these can also be weaponized by hackers due to cybercrime. The thematic analysis shows the current shift of cyberattacks, moving towards psychological manipulation and stealth with the assistance of

technical complexity. Discovered recurring themes and patterns indicate that attackers target victims who have access privileges to information and exploit critical digital infrastructures such as third-party systems, authentication-based systems, and other systems. In order to accomplish these attacks, they use methodologies such as ransomware, social engineering, and Trojan horses to maintain unauthorized access and deceive victims. Two evolving trends show that attackers are most likely to approach their targets stealthily rather than directly. One trend is the weaponization of AI. In the examples, the attackers used it to create deepfakes and malicious tools. In the other trend, stolen credentials are the keys to gaining access to systems and other credentials. The examples show that this is done through impersonation. This analysis highlights the need for robust security postures, strong frameworks for AI, and user awareness to mitigate the current shift. As for future research, this can help examine how public education can avoid psychological manipulation embedded in cyberattacks and how AI can assist in threat detection.

References

Active vs passive reconnaissance: 6 key differences. CyCognito. (n.d.). https://www.cycognito.com/learn/exposure-management/active-vs-passive-reconnaissance.php

Ahmadi, A. A. (2025, July 26). *Allianz Life: Insurance Giant says most US customer data stolen in cyber-attack*. BBC News. https://www.bbc.com/news/articles/cd6nyng861wo

Arghire, I. (2024, April 12). *LastPass Employee Targeted With Deepfake Calls* . Security Week. https://www.securityweek.com/lastpass-employee-targeted-with-deepfake-calls/

Arghire, I. (2025, September 18). *Threat Actor Infests Hotels With New RAT*. Security Week. https://www.securityweek.com/threat-actor-infests-hotels-with-new-rat/

Constantin, L. (2024, February 14). *Attack campaign targeting azure environments compromised hundreds of accounts*. CSO . https://www.csoonline.com/article/1307764/attack-campaign-targeting-azure-environments-compromised-hundreds-of-accounts.html

Hill, M. (2023, July 26). *VEC campaign targets critical infrastructure firms with invoice fraud attack*. CSO . https://www.csoonline.com/article/647040/vec-campaign-targets-critical-infrastructure-firms-with-invoice-fraud-attack.html

Lakshmanan, R. (2025a, February 14). *Microsoft: Russian-Linked Hackers Using "Device Code Phishing" to Hijack Accounts*. The Hacker News. https://thehackernews.com/2025/02/microsoft-russian-linked-hackers-using.html

Lakshmanan, R. (2025b, September 29). *EvilAI malware masquerades as AI tools to infiltrate Global Organizations*. The Hacker News. https://thehackernews.com/2025/09/evilai-malware-masquerades-as-ai-tools.html

Naprys, E. (2025, April 16). *Huge ransomware campaign targets AWS S3 storage: attackers have thousands of keys*. Cybernews . https://cybernews.com/security/aws-cloud-storage-bucket-ransomware-attacks/

Schappert , S. (2025, August 18). *Workday CRM platform hit by hackers, suspected link to Salesforce attackers* . Cybernews . https://cybernews.com/security/workday-hr-platform-cyberattack-shiny-hunters-crm-salesforce/

Tidy, J. (2025, September 26). *Nursery hackers threaten to publish more children's profiles*. BBC News. https://www.bbc.com/news/articles/c07vxv8v89lo