Unveiling the Cybercrime Ecosystem: Impact of Ransomware-as-a-Service (RaaS) in Indonesia

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Luqman Hafiz
Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Taufik Hidayat
Department of Computer Engineering, Universitas Wiralodra, Indramayu, Indonesia

Abstract: This study explores the rise of Ransomware-as-a-Service (RaaS) in Indonesia's cybercrime ecosystem, highlighting its role as a significant digital security threat. RaaS lowers the technical barriers to executing ransomware attacks, enabling individuals with minimal expertise to launch sophisticated cyberattacks. Analyzing data from 2020 to 2024, this study identified Indonesia as a hotspot for RaaS-driven cybercrime in Southeast Asia due to low cybersecurity awareness and weak regulatory frameworks. Key findings reveal that government administration, healthcare, and finance are the most frequently targeted sectors due to their sensitive data and inadequate defense capabilities. Ransomware variants such as Luna Moth and WannaCry, dominate the malware landscape by employing tactics like phishing and exploiting outdated systems. These attacks result in severe socioeconomic consequences, including financial losses, operational disruptions, and reputational damage. This study contributes to our understanding of RaaS by examining its operational, economic, and regulatory dimensions in the Indonesian context. This underscores the urgent need for strengthened cybersecurity policies, public-private sector collaboration, and international cooperation to address transnational cybercrime. By providing actionable insights into attack patterns and mitigation strategies, this study aims to guide efforts to combat ransomware threats and enhance Indonesia's digital resilience.

Keywords: Ransomware-as-a-Service (RaaS), Cybersecurity, Cybercrime, Ransomware.

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia
E-mail: budiwibowo1993@gmail.com

Received December 24, 2024; Revised January 9, 2025; Accepted January 12, 2025; Published March 2, 2025.

Introduction

In today's increasingly complex digital landscape, cybercrime threats continue to evolve in tandem with technological advancements. Among these threats, ransomware has emerged as a significant threat in recent years. Ransomware, a type of malicious software designed to encrypt a victim's data and deny access until a ransom is paid, has transcended its status as a mere technical threat. It has evolved into a business model known as Ransomware-as-a-Service (RaaS), which amplifies its impact and risks on a global scale (Meland et al., 2020). RaaS is a framework where cybercriminals develop ransomware and lease it to affiliates or other parties, typically sharing profits from ransoms collected from victims. This model simplifies the execution of cyberattacks, enabling individuals with minimal technical expertise to launch highly disruptive attacks (Meurs et al., 2024). The concept aligns with the sharing economy trend, which is prevalent in legitimate businesses but operates with malicious intent. Reports from leading cybersecurity organizations, such as Sophos and Cybersecurity Ventures, have revealed that ransomware attacks have grown exponentially year by year (Dib et al., 2024) By 2023, global losses attributed to ransomware were projected to reach trillions of dollars (Gaber et al., 2024). These figures underscore the profound impact on organizations, including data loss, reputational damage, and significant recovery costs. Sectors such as healthcare, government, and education are frequent targets due to their sensitive data repositories and often limited resources to effectively combat such threats (Hirano and Kobayashi, 2025).

The RaaS model has revolutionized cybercrime, making it more organized and systematic. This transformation raises critical questions about how the cybersecurity ecosystem can counteract evolving threats. RaaS exemplifies a shift in cybercrime dynamics, where isolated actors targeting specific victims have been replaced by an industry with structured supply chains, customer support, and marketing strategies that are akin to legitimate businesses (Liu et al., 2020). Despite its growing significance, gaps remain in understanding how organizations can effectively safeguard themselves against RaaS (Berrueta et al., 2022). While previous studies have primarily explored the technical dimensions of ransomware, the operational and business aspects of RaaS remain underexplored, leaving a critical gap in strategies for threat mitigation. In addition, the RaaS model poses unique challenges to international legal frameworks and complicates law enforcement efforts. Many RaaS operators exploit jurisdictions with weak regulations or implicit protections for cybercriminals. This dynamic presents a global dilemma: balancing the need for robust international cybersecurity measures while respecting national sovereignty (Aljabri et al. 2024).

Indonesia is the largest digital economy in Southeast Asia, has experienced significant growth in internet adoption and technological advancement. While these developments have propelled socioeconomic progress, they have also exposed the country to increasing cybercrime activities. Among these threats, ransomware has become a particularly prominent threat. Once limited to highly skilled attackers, ransomware has evolved into an accessible and scalable model known as Ransomware-as-a-Service (RaaS). This shift has transformed ransomware attacks into a structured and organized industry, posing severe challenges to Indonesia's digital security landscape (Luuk et al., 2023).

Several factors contribute to the unique cybercrime ecosystem in Indonesia, including rapid digital transformation, low awareness of cybersecurity among businesses and individuals, and challenges in enforcing cybersecurity regulations. The RaaS model intensifies these vulnerabilities by enabling individuals with minimal technical expertise to execute sophisticated cyberattacks (Arabo et al., 2020). Through RaaS platforms, attackers gain access to ransomware tools, comprehensive support systems, and revenue-sharing models, effectively lowering the barriers to entry. This has led to a surge in ransomware incidents, particularly targeting critical sectors, such as healthcare, education, and small-to-medium enterprises (SMEs), which are often more vulnerable due to limited cybersecurity resources and outdated infrastructure. In healthcare, reliance on legacy systems and the critical need for rapid access to patient data often forces organizations to make compromises on security. Similarly, educational institutions typically have large, diverse networks with less robust cybersecurity protocols, making them easy targets for ransomware. SMEs, which frequently lack dedicated IT security teams, are also especially at risk because they often cannot afford the advanced cybersecurity measures required to counter increasingly sophisticated attacks. Addressing the RaaS phenomenon in Indonesia is of critical importance. While global studies have explored the technical aspects of ransomware, such as encryption methods and attack vectors, they often overlook the socio-economic and operational implications of the RaaS business model, particularly in localized contexts like Indonesia. Research conducted by organizations such as Symantec and Kaspersky highlighted the global prevalence of RaaS, yet Indonesia-specific studies remain limited. Furthermore, while international collaborative efforts to combat RaaS have yielded positive outcomes, Indonesia’s unique socio-political and economic environment demands customized strategies (Hirano et al., 2022).

A significant knowledge gap exists in terms of terms of understanding the intersection between RaaS operations and Indonesia's broader cybercrime landscape. Although individual ransomware attacks have been well-documented, there is insufficient research on the socioeconomic and infrastructural conditions that enable the growth of RaaS in the country

(Berardi et al., 2023). This includes the role of dark web marketplaces, cryptocurrency as a medium for anonymous transactions, and Indonesian organizations' limited cybersecurity readiness. The transnational nature of RaaS operations complicates Indonesian law enforcement, which is often constrained by jurisdictional limitations and the lack of international cooperation agreements. From a regulatory perspective, Indonesia faces substantial challenges in addressing RaaS threats (Wibowo, 2024). While the National Cyber and Encryption Agency (BSSN) has tried to combat cybercrime, its resources remain inadequate given the scale of the threat (Wibowo & Hidayat, 2024). Similarly, the delayed implementation of the 2019 Personal Data Protection Bill has created legal gaps that cybercriminals readily exploit. Many SMEs, which are major targets of RaaS attacks, lack the resources and expertise to implement robust cybersecurity measures, further compounding the risk (Tariq, 2024). This study aims to address these gaps by examining the operational, economic, and regulatory dimensions of RaaS in Indonesia's cybercrime ecosystem (Yuswanto et al., 2024). Unlike prior research that predominantly focuses on technical analyses, this study takes a multidimensional approach, exploring how RaaS actors exploit Indonesia's vulnerabilities, the socioeconomic impact on critical sectors, and the effectiveness of existing policy frameworks.

The objectives of this research are threefold:

1. To analyze how RaaS platforms operate and proliferate within Indonesia's digital ecosystem.
2. To evaluate the socioeconomic impacts of RaaS on key sectors such as SMEs, healthcare, and education.
3. To assess the effectiveness of Indonesia's cybersecurity policies and propose strategies to enhance resilience against RaaS threats.

By integrating theoretical and practical perspectives, this research aims to provide a comprehensive understanding of RaaS in Indonesia. The findings aim to guide policymakers, cybersecurity practitioners, and researchers in developing effective measures to mitigate the rising threats of RaaS and foster a more secure digital environment.

Research Method

This study adopts an ethnographic approach to explore Indonesia's cybercrime ecosystem, focusing on the role of Ransomware-as-a-Service (RaaS) in digital security threats. By adapting ethnographic methods to online communities, ethnography provides an effective framework for understanding the operations of RaaS platforms within Indonesia's digital landscape. The study utilized secure hardware, including a Linux-based laptop with Virtual

Private Network (VPN) and Tor Browser for anonymous access to dark web platforms, along with tools such as Maltego (for network mapping), Shodan (for identifying vulnerable devices), and Chainalysis (for cryptocurrency transaction tracing). Secondary data were gathered from global cybersecurity reports, such as those from Kaspersky and Symantec, as well as interviews with cybersecurity experts and law enforcement officials in Indonesia. Data collection involved identifying relevant dark web forums and RaaS marketplaces through keyword analysis, observing transaction patterns, affiliate recruitment, and customer interactions over three months, and compiling ransomware attack reports targeting various sectors in Indonesia. The analysis focused on thematic identification of operational structures, such as revenue-sharing models and service features offered by RaaS platforms, and quantitative evaluation of attack frequencies and their economic impacts on sectors like healthcare, education, and SMEs. A comparative analysis with global data was also conducted to highlight Indonesia's unique vulnerabilities. Ethical considerations were prioritized by ensuring that access to dark web platforms was purely for observational purposes without active engagement and applying data anonymization techniques to protect sensitive information. The results revealed that RaaS platforms exploit low cybersecurity awareness and weak enforcement frameworks in Indonesia, with high attack prevalence in resource-constrained sectors, significant reliance on cryptocurrencies for anonymous transactions, and notable gaps in regulatory enforcement. This study contributes by offering a replicable methodology and providing actionable insights for policymakers and cybersecurity practitioners, aimed at developing strategies to combat RaaS operations and address both technical and socio-economic vulnerabilities.

Results and Discussion

This illustration depicts global trends in cyber incidents from 2004 to 2023 based on data from the International Monetary Fund (2024). The graph classifies cyberattacks into several categories, such as phishing, spoofing, social engineering, network or website disruptions, cyber extortion, and data breaches, both intentional and unintentional. The red line on the graph represents the total number of cyberattacks, as measured by the Cybersecurity Incident Severity Metrics (CISSM), plotted on the right-hand axis. Ransomware, which is categorized under cyber extortion, has shown a sharp increase since 2015. This trend is evident in the steadily growing purple bars, particularly during the 2017–2021 period, with a peak in 2021. This surge reflects the expansion of the Ransomware-as-a-Service (RaaS) model, in which threat actors offer ransomware software for rent or sale to third parties, accelerating the global spread of ransomware attacks.

Figure 1 Global Number of Cyber Incidents (Source: International Monetary Fund 2024)

However, since 2021, this graph indicates a slight decline in ransomware incidents through 2023. This decline is likely influenced by enhanced global cybersecurity efforts, such as stricter regulations on cryptocurrency transactions—commonly used for ransom payments—and increased awareness of ransomware threats. Nevertheless, ransomware remains one of the most destructive forms of cyberattacks because of its substantial financial and operational impacts on organizations.

Most Commonly Detected Ransomware in Indonesia

Based on monitoring anomalous traffic in Indonesia's cyberspace, five ransomware variants were identified as the most frequently detected threats, as illustrated in Figure 1. These ransomware variants include Luna Moth, WannaCry, Locky, LockBit, and GandCrab. Figure 2 shows that Luna Moth is the most dominant ransomware variant, with over 400,000 activities recorded. This number significantly exceeds the number of other variants, making Luna Moth the leading ransomware threat in Indonesia. WannaCry ranks second with approximately 100,000 activities, followed by Locky, LockBit, and GandCrab, which recorded between 50,000 and 70,000 activities each. The prevalence of Luna Moth reflects the sophistication of modern ransomware attacks. This variant frequently employs social engineering tactics, such as phishing, to gain unauthorized access to victims' systems, followed

by data encryption and ransom demands. Wannacry although its activity has declined since its peak in 2017, remains a significant threat in Indonesia, especially in organizations with outdated security systems.

The impact of these ransomware variants has been substantial, and businesses, healthcare institutions, educational organizations, and government agencies being particularly hard-hit. Many entities have faced severe operational disruptions, financial losses, and compromised sensitive data, leading to a decline in customer trust. Critical sectors such as healthcare have been especially vulnerable, with ransomware attacks causing delays in medical procedures and disruptions in patient care. Some organizations have been forced to pay the ransom, while others have suffered from prolonged downtime and high recovery costs.

In response, both public and private entities have taken several steps to mitigate the impact. The Indonesian government has issued cybersecurity advisories and increased efforts to monitor and analyze cyber threats. Cybersecurity firms and law enforcement agencies have also increased their efforts to identify and dismantle ransomware operators and their infrastructure. At the organizational level, affected businesses have strengthened their cybersecurity measures, including improving their firewall protections, adopting multi-factor authentication (MFA), and conducting regular employee training on phishing threats. However, many organizations still face challenges in effectively addressing these threats due to resource constraints and the evolving sophistication of ransomware tactics.

These findings highlight ransomware as a critical threat to Indonesia's cybersecurity landscape. Variants like Luna Moth demonstrate a growing reliance on the Ransomware-as-a-Service (RaaS) model, where ransomware software is rented or sold to less technically skilled threat actors. This model facilitates the widespread dissemination of ransomware attacks and amplifies their impact. To address the surge in ransomware activity, a multi-pronged mitigation approach is required. This includes raising cybersecurity awareness, strengthening digital security infrastructures, fostering collaboration between the public and private sectors to improve detection and prevention efforts, and increasing support for small businesses that may lack the resources to implement robust defenses. In addition, regular software updates and the implementation of robust data backup systems are essential to minimize the impact of ransomware attacks.

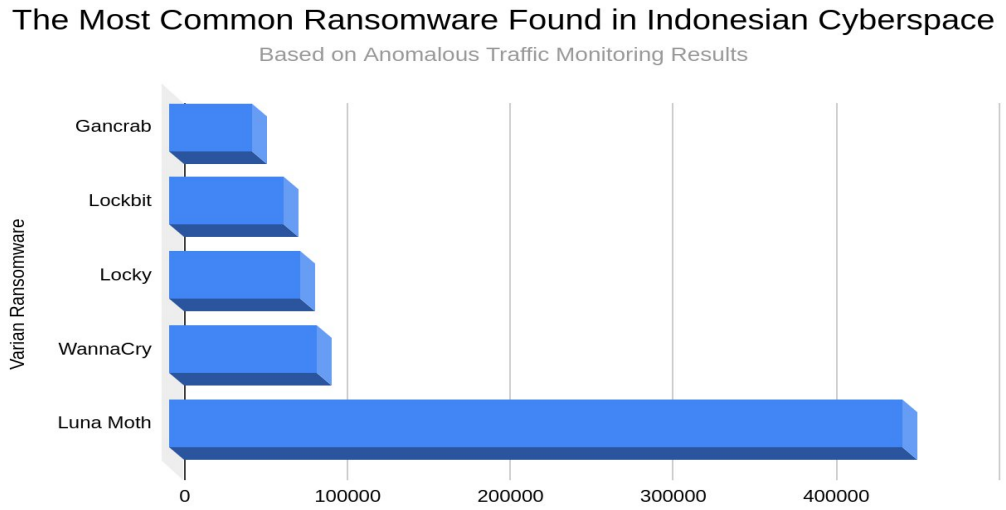

Figure 2 Most detected ransomware in Indonesia's cyberspace based on anomalous traffic monitoring (source: BSSN Report 2023)

An analysis of 83 cyber incidents detected and assisted in 2023 revealed three major types of attacks with the highest occurrence: web defacement, ransomware, and data breaches. As shown in Figure 2, web defacement was the highest with 30 incidents, followed by ransomware with 20 incidents, and data breaches with 12 incidents. Other incidents, such as illegal access (11 incidents), traffic anomalies, DDoS attacks, phishing, email hijacking, and malware activities, recorded lower numbers. The accompanying table highlights the distribution of affected sectors, with government administrations accounting for 59 incidents. This was followed by the energy and mineral resources (ESDM) sector with 6 incidents, and both the healthcare and financial sectors recording 5 incidents each. Other sectors, such as transportation, information, and communication technology (ICT), experienced fewer incidents. These results indicate that web defacement and ransomware are the greatest threats in Indonesia's cybersecurity landscape, especially targeting government administration. Web defacement is often utilized to damage the reputation of organizations, particularly governmental institutions, by replacing website content with provocative messages or symbols. This underscores the urgent need to enhance the web security of government websites. At the same time, ransomware, which has been reported in 20 incidents, highlights an escalating threat to sectors managing sensitive data. The government and strategic sectors are primary targets because of the high value of their data, making them vulnerable to extortion.

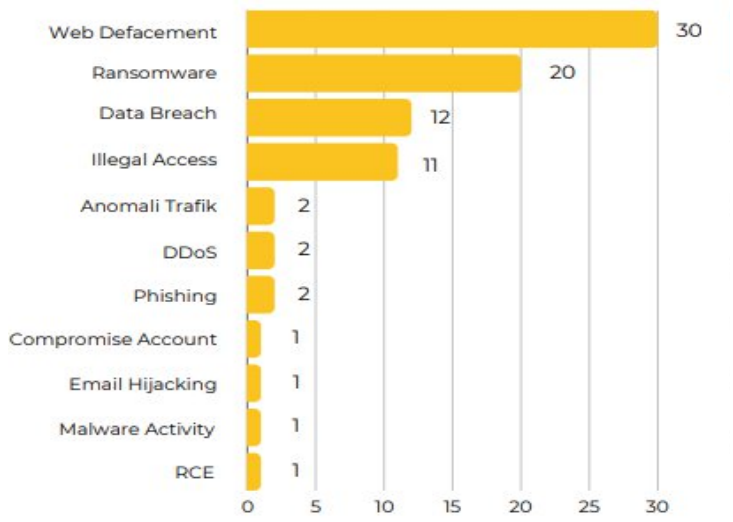

Figure 3 Classification of incidents and sectors undertaken Cyber Incident Response Assistance Service (source: BSSN Report 2023)

In addition, data breaches remain a significant concern due to the exposure of sensitive information, which can be exploited for further attacks or identity theft. The heavy targeting of the government administration sector indicates that cyber threats impact not only commercial entities and public services. Disruptions in these services could have far-reaching consequences on national operations. Thus, stronger mitigation measures, such as implementing standardized cybersecurity frameworks and educational programs to increase risk awareness in government sectors, are urgently required.

Conclusions

This study comprehensively examines the cybercrime ecosystem in Indonesia, with a particular focus on the growing threat posed by Ransomware-as-a-Service (RaaS). The findings revealed that RaaS has significantly contributed to the escalation of ransomware incidents in Indonesia, making it a hotspot for cybercriminal activities in Southeast Asia. By targeting high-value sectors, such as government administration, financial institutions, and healthcare providers, RaaS operations exploit systemic vulnerabilities and pressure victims into compliance, causing substantial financial and operational damage. This study highlights the adaptability of threat actors using RaaS models and underscores the critical need for proactive and integrated cybersecurity measures to mitigate such threats. The study contributes to scientific discourse by deepening the understanding of the RaaS ecosystem and its implications for digital security in developing nations. It provides actionable insights into attack patterns, targeted sectors, and economic impacts, which can inform the design of more effective cybersecurity strategies. Moreover, this research emphasizes the importance of

regulatory frameworks and international cooperation to address the broader challenges posed by cybercrime in interconnected digital landscapes. By bridging the gap between technical vulnerabilities and policy-level responses, this study makes valuable contributions to both academic research and practical efforts in combating ransomware threats.

References

Aljabri, M., Alhaidari, F., Albuainain, A., Alrashidi, S., Alansari, J., Alqahtani, W., & Alshaya, J. (2024). Ransomware detection based on machine learning using memory features. *Egyptian Informatics Journal*, *25*(July 2023), 100445. https://doi.org/10.1016/j.eij.2024.100445

Arabo, A., Dijoux, R., Poulain, T., & Chevalier, G. (2020). Detecting ransomware using process behavior analysis. *Procedia Computer Science*, *168*(2019), 289–296. https://doi.org/10.1016/j.procs.2020.02.249

Berardi, D., Giallorenzo, S., Melis, A., Melloni, S., Onori, L., & Prandini, M. (2023). Data Flooding against Ransomware: Concepts and Implementations. *Computers and Security*, *131*. https://doi.org/10.1016/j.cose.2023.103295

Berrueta, E., Morato, D., Magaña, E., & Izal, M. (2022). Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic. *Expert Systems with Applications*, *209*(July), 118299. https://doi.org/10.1016/j.eswa.2022.118299

B. Wibowo and M. Alaydrus, "Smart Home Security Analysis Using Arduino Based Virtual Private Network," 2019 Fourth International Conference on Informatics and International Journal of Science Education and Cultural Studies International Journal of Science Education and Cultural Studies, ISSN 2964-2604, Volume 3 Number 2 September 2024 https://doi.org/10.58291/ijsecs.v3i2.306 65 Computing (ICIC), Semarang,

Dib, O., Nan, Z., & Liu, J. (2024). Machine learning-based ransomware classification of Bitcoin transactions. *Journal of King Saud University - Computer and Information Sciences*, *36*(1), 101925. https://doi.org/10.1016/j.jksuci.2024.101925

Gaber, M., Ahmed, M., & Janicke, H. (2024). Zero Day Ransomware Detection with Pulse: Function Classification with Transformer Models and Assembly Language. *Computers & Security*, *148*(September 2024), 104167. https://doi.org/10.1016/j.cose.2024.104167

Hirano, M., Hodota, R., & Kobayashi, R. (2022). RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*, *40*, 301314.

https://doi.org/10.1016/j.fsidi.2021.301314

Hirano, M., & Kobayashi, R. (2025). RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep learning based ransomware detectors. *Computers and Security*, *150*(June 2024), 104202. https://doi.org/10.1016/j.cose.2024.104202

Liu, T. M., Kao, D. Y., & Chen, Y. Y. (2020). Loocipher ransomware detection using lightweight packet characteristics. *Procedia Computer Science*, *176*, 1677–1683. https://doi.org/10.1016/j.procs.2020.09.192

Luuk, B., (Maria) Susanne, V. H. de G., Ellen, M. ter H., Ynze, V. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers and Security*, *127*, 103099. https://doi.org/10.1016/j.cose.2023.103099

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers and Security*, *92*(7034). https://doi.org/10.1016/j.cose.2020.101762

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. *Computers and Security*, *138*(July 2023), 103670. https://doi.org/10.1016/j.cose.2023.103670

Tariq, U. (2024). Combatting ransomware in ZephyrOS-activated industrial IoT environments. *Heliyon*, *10*(9), e29917. https://doi.org/10.1016/j.heliyon.2024.e29917

Wibowo, B. (2024). *Social Engineering as a Major Cybersecurity Threat : Analysis of Challenges and Solutions for Organizations*. 57–65.

Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, *2*(1), 1–9. https://doi.org/10.58291/abdisultan.v2i1.294

Yuswanto, A., Wibowo, B., & Hafiz, L. (2024). A Review Method for Analysis of the Causes of Data Breach in the Pasca Pandemic. *Jurnal Komputer Dan Elektro Sains*, *3*(1), 1–5. https://doi.org/10.58291/komets.v3i1.205