

Analisa Serangan *Ransomware* “*Lockbit*” Pada Tahun 2022-2023

Azaharia Della Utomo¹, Nadia Anggraini², Tony Setiawan³, Ripki⁴
^{1,2,3,4}Universitas Ibnu Sina, Batam

Corresponding Author: 231055201121@uis.ac.id¹, 231055201050@uis.ac.id², 231055201057@uis.ac.id³,
231055201126@uis.ac.id⁴

Published: July , 2025

ABSTRAK

Ransomware merupakan ancaman yang signifikan dan terus berkembang dalam lanskap keamanan siber, dengan *LockBit* muncul sebagai aktor terkemuka pada tahun 2022 dan 2023. Makalah ini memberikan analisis komprehensif tentang serangan *Ransomware LockBit*, merinci kronologi peristiwa penting, metodologi yang digunakan, dan dampaknya terhadap korban. Operasi *LockBit*, yang dicirikan oleh model *Ransomware-as-a-Service* (RaaS), telah memperluas jangkauan serangan *Ransomware*, menargetkan berbagai sektor termasuk kesehatan dan energi. Studi ini meneliti metode serangan utama seperti phishing, eksploitasi kerentanan, dan taktik pemerasan ganda, yang mengungkapkan kerugian finansial yang substansial, gangguan operasional, dan kerusakan reputasi yang dihadapi oleh organisasi yang terkena dampak. Langkah-langkah pencegahan diusulkan, menekankan pendidikan pengguna, pembaruan perangkat lunak yang tepat waktu, autentikasi multi-faktor, cadangan data secara teratur, dan sistem deteksi dini. Temuan tersebut menekankan perlunya organisasi untuk mengadopsi strategi keamanan siber yang proaktif, berkolaborasi dengan pihak berwenang, dan menghindari pembayaran tebusan. Pada akhirnya, analisis ini menyoroti kebutuhan mendesak akan kebijakan keamanan yang kuat dan mekanisme respons cepat untuk mengurangi risiko yang ditimbulkan oleh ancaman *Ransomware* canggih seperti *LockBit*.

Kata Kunci: *Ransomware*, *LockBit*, Keamanan Siber

ABSTRACT

Ransomware poses a significant and continuously evolving threat within the cybersecurity landscape, with LockBit emerging as a leading actor in 2022 and 2023. This paper presents a comprehensive analysis of LockBit Ransomware attacks, detailing key event chronology, methodologies used, and their impact on victims. LockBit operations, characterized by the Ransomware-as-a-Service (RaaS) model, have expanded the scope of Ransomware attacks, targeting various sectors including healthcare and energy. This study examines primary attack methods such as phishing, vulnerability exploitation, and double extortion tactics, revealing substantial financial losses, operational disruptions, and reputational damage experienced by affected organizations. Proposed prevention measures emphasize user education, timely software updates, multi-factor authentication, regular data backups, and early detection systems. The findings highlight the urgent need for organizations to adopt proactive cybersecurity strategies, collaborate with authorities, and avoid ransom payments. Ultimately, this analysis underscores the critical importance of robust security policies and rapid response mechanisms to mitigate risks posed by advanced Ransomware threats such as LockBit.

Keywords: Ransomware, LokBit, Cybersecurity

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0>

PENDAHULUAN

Dalam era digital yang semakin maju ini, tantangan terhadap keamanan digital semakin meningkat. Salah satu ancaman serius yang telah menjadi perhatian dunia adalah serangan *Ransomware*. *Ransomware* merupakan jenis perangkat lunak berbahaya yang dirancang untuk mengenkripsi atau mengunci akses terhadap data atau sistem komputer korban. Para pelaku *Ransomware* kemudian meminta pembayaran tebusan

dalam bentuk mata uang digital agar data atau sistem dapat dikembalikan kepada pemiliknya. Salah satu kasus yang menggemparkan di Indonesia adalah serangan *Ransomware* yang terjadi pada Bank Syariah Indonesia. Pada saat itu, serangan *Ransomware* berhasil mengeksekusi sistem keamanan bank dan mengenkripsi data sensitif, termasuk data nasabah dan informasi keuangan penting. Hal ini menimbulkan ketidaknyamanan dan kekhawatiran yang signifikan bagi nasabah dan pemilik rekening Bank Syariah Indonesia.

Dampak dari serangan *Ransomware* pada Bank Syariah Indonesia sangat serius, karena tidak hanya mengganggu operasional internal bank, tetapi juga mengancam kepercayaan masyarakat terhadap sistem perbankan dan keamanan data mereka. Kehilangan data yang berharga dan informasi keuangan dapat menyebabkan kerugian finansial yang signifikan bagi nasabah dan merusak reputasi bank. Kasus Bank Syariah Indonesia menjadi cerminan nyata akan perlunya upaya yang serius dalam melawan serangan *Ransomware*. Keamanan digital harus menjadi prioritas utama bagi lembaga keuangan dan organisasi lainnya untuk melindungi data dan sistem mereka dari serangan yang merusak dan merugikan.

Ransomware telah menjadi ancaman serius dalam dunia digital saat ini. Serangan perangkat lunak berbahaya ini telah menyebabkan kerugian besar pada berbagai sektor, terutama perbankan online. Keamanan online bergantung pada tiga aspek penting: perlindungan data, tindakan pencegahan, dan solusi keamanan yang efektif. Dalam beberapa tahun terakhir, serangan *Ransomware* semakin meluas dan mengancam keamanan data di berbagai negara. India menjadi salah satu negara yang terkena dampak serangan *Ransomware* dengan kerugian mencapai jutaan dolar setelah tiga bank terinfeksi. Negara lain seperti Rusia dan Turki juga menjadi sasaran utama serangan di sektor perbankan.

Serangan *Ransomware* tidak hanya terbatas pada perbankan online, tetapi juga menargetkan sektor lainnya, termasuk perangkat *Internet of Things* (IoT). Hal ini menimbulkan tantangan baru dalam menjaga keamanan sistem secara menyeluruh. Solusi keamanan yang tepat dan upaya perlindungan data yang kuat menjadi penting untuk menghadapi ancaman ini.

Terdapat juga keterkaitan antara *Ransomware* dengan kegiatan pencucian uang. Keuntungan yang diperoleh dari serangan *Ransomware* sering kali dicuci melalui metode tertentu, yang melibatkan pemalsuan identitas dan penggunaan sistem keuangan yang terinfeksi. Upaya untuk mengatasi kegiatan pencucian uang dari hasil *Ransomware* menjadi bagian penting dari perlindungan keamanan sistem secara keseluruhan.

Selain itu, pemahaman sosial terhadap *Ransomware* juga menjadi faktor kunci dalam melawan ancaman ini. *Ransomware* sering dikaitkan dengan kelompok kejahatan tertentu yang mencari keuntungan dari tindakan kriminal mereka. Oleh karena itu,

penelitian dalam bidang ilmu sosial menjadi penting untuk memahami dinamika, teknologi, keamanan, dan implikasi sosial dari *Ransomware*. Melalui pemahaman yang mendalam tentang *Ransomware* dan upaya kolaboratif antara lembaga keamanan, peneliti, dan pengguna, dapat diambil langkah-langkah pencegahan yang efektif. Langkah-langkah tersebut mencakup pembaruan perangkat lunak secara teratur, kesadaran pengguna terhadap taktik phishing dan tindakan keamanan yang bijaksana, serta pencadangan data yang teratur.

Dalam tulisan ini, akan dikaji lebih dalam tentang isu *Ransomware*, termasuk metode serangan, akibat yang ditimbulkan, dan langkah-langkah yang dapat diambil untuk mencegah dan mengatasi serangan *Ransomware*. Dengan pemahaman yang lebih baik tentang *Ransomware* dan upaya yang tepat dalam menerapkan kebijakan keamanan yang kuat, melindungi diri dan organisasi dari ancaman yang mungkin terjadi di dunia digital yang terus berkembang pesat ini.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi literatur. Data dikumpulkan dari berbagai sumber sekunder, termasuk laporan resmi dari lembaga keamanan siber internasional, jurnal ilmiah, serta publikasi vendor keamanan. Tujuan dari penelitian ini adalah untuk mendeskripsikan secara sistematis kronologi, metode serangan, serta dampak yang ditimbulkan oleh *Ransomware LockBit* selama tahun 2022–2023. Selain itu, penelitian ini juga bertujuan untuk merumuskan langkah-langkah pencegahan yang relevan dalam menghadapi ancaman serangan serupa di masa depan.

HASIL DAN PEMBAHASAN

Ransomware: LockBit

Pada tahun 2022, *LockBit* merupakan varian *Ransomware* yang paling banyak digunakan di seluruh dunia dan terus berkembang pesat pada tahun 2023. Sejak Januari 2020, afiliasi yang menggunakan *LockBit* telah menyerang berbagai organisasi dengan berbagai ukuran di berbagai sektor infrastruktur penting, termasuk layanan keuangan, pangan dan pertanian, pendidikan, energi, pemerintah dan layanan darurat, perawatan kesehatan, manufaktur, dan transportasi. Operasi *Ransomware LockBit* berfungsi sebagai model *Ransomware-as-a-Service* (RaaS) di mana afiliasi direkrut untuk melakukan serangan *Ransomware* menggunakan alat dan infrastruktur *Ransomware LockBit*. Karena banyaknya afiliasi yang tidak terhubung dalam operasi tersebut, serangan *Ransomware LockBit* sangat bervariasi dalam taktik, teknik, dan prosedur (TTP) yang diamati. Varians dalam TTP *Ransomware* yang diamati ini menghadirkan tantangan penting bagi

organisasi yang berupaya menjaga keamanan jaringan dan melindungi dari ancaman *Ransomware*.

Badan Keamanan Siber dan Infrastruktur (CISA), Biro Investigasi Federal (FBI), Pusat Analisis dan Pembagian Informasi Multi-Negara (MS-ISAC), dan mitra internasional berikut, yang selanjutnya disebut sebagai "organisasi penyusun," merilis Pemberitahuan Keamanan Siber (CSA) ini yang merinci aktivitas yang diamati dalam insiden *Ransomware LockBit* dan memberikan mitigasi yang direkomendasikan untuk memungkinkan pembela jaringan secara proaktif meningkatkan pertahanan organisasi mereka terhadap operasi *Ransomware* ini.

Kronologi Kejadian: Serangan *Ransomware LockBit* (2022-2023)

Serangan *Ransomware LockBit* telah menyebabkan gangguan besar pada berbagai sektor, termasuk lembaga pemerintah, rumah sakit, dan perusahaan besar. Berikut adalah beberapa contoh kronologi serangan yang signifikan yang terjadi dalam rentang waktu 2022-2023:

1. Serangan terhadap Rumah Sakit dan Layanan Kesehatan

Pada Mei 2022, grup peretas *LockBit* menyerang sistem IT di sebuah rumah sakit besar di Eropa. Dalam serangan ini, peretas berhasil mengenkripsi data pasien dan merusak sistem manajemen rumah sakit. Akibat serangan tersebut, rumah sakit terpaksa menangguhkan layanan medis mereka untuk sementara waktu, mempengaruhi ribuan pasien. *LockBit* juga mengancam akan merilis data pribadi pasien jika tebusan tidak dibayar.

2. Serangan terhadap Perusahaan Energi

Pada Februari 2023, serangan besar lainnya terjadi pada sebuah perusahaan energi besar di Eropa yang memanfaatkan *LockBit* untuk mengenkripsi data sensitif dan mengancam untuk merusak sistem SCADA (*Supervisory Control and Data Acquisition*) mereka. Serangan ini berpotensi mengganggu distribusi energi secara besar-besaran, menyebabkan kerugian finansial yang signifikan dan merusak reputasi perusahaan. Keamanan data yang terlibat dalam sektor energi membuat serangan ini sangat berisiko dan berdampak luas.

3. Penyebaran Melalui *Ransomware-as-a-Service* (RaaS)

Pada 2023, *LockBit* mulai mengembangkan model *Ransomware-as-a-service* (RaaS), yang memungkinkan afiliasi untuk menyewa perangkat lunak *Ransomware* mereka untuk menyerang organisasi lain. Ini memperluas jangkauan serangan mereka dan meningkatkan jumlah korban yang terdampak. Afiliasi yang menggunakan *LockBit* mengincar berbagai industri, dari manufaktur hingga lembaga pemerintahan, dengan hasil yang bervariasi tergantung pada kecanggihan afiliasi tersebut.

Metode Yang Digunakan Oleh Pelaku

LockBit menggunakan berbagai teknik untuk menyebarkan malware dan mengenkripsi data korban. Beberapa metode yang umum digunakan antara lain:

1. Phishing dan Social Engineering

Salah satu cara utama peretas mengakses jaringan korban adalah melalui phishing. Email phishing yang menyamar sebagai pesan sah dari bank, pemerintah, atau rekan bisnis biasanya mengandung lampiran berbahaya atau tautan yang mengarah ke situs web berbahaya. Ketika korban membuka lampiran atau mengklik tautan, malware *LockBit* akan diunduh dan diinstal di sistem korban.

2. Eksploitasi Kerentanannya (Exploitation)

LockBit juga memanfaatkan kerentanannya dalam perangkat lunak yang belum diperbarui atau yang memiliki celah keamanan. Salah satu contoh eksploitasi yang digunakan oleh *LockBit* adalah melalui RDP (Remote Desktop Protocol), yang memungkinkan peretas untuk mengakses dan mengendalikan komputer korban dari jarak jauh. Selain itu, *LockBit* juga sering memanfaatkan vulnerabilities di aplikasi-aplikasi seperti Microsoft Exchange, yang memungkinkan mereka untuk menembus sistem dengan cepat.

3. Penggunaan *Ransomware-as-a-Service* (RaaS)

Grup peretas *LockBit* mengoperasikan model *Ransomware-as-a-Service* (RaaS), yang memungkinkan afiliasi pihak ketiga untuk menyewa perangkat lunak *Ransomware* mereka untuk meluncurkan serangan terhadap target yang mereka pilih. RaaS mengurangi hambatan teknis bagi peretas yang tidak memiliki keterampilan untuk membuat *Ransomware* mereka sendiri dan memperluas cakupan serangan *LockBit* secara signifikan.

4. Teknik Double Extortion

Salah satu ciri khas dari serangan *LockBit* adalah penggunaan *Double Extortion*. Setelah mengenkripsi data korban, peretas tidak hanya menuntut tebusan untuk mendekripsi data, tetapi juga mengancam akan merilis data yang dicuri di dark web jika pembayaran tidak dilakukan. Teknik ini meningkatkan tekanan terhadap korban untuk membayar, karena selain kehilangan akses ke data, mereka juga menghadapi risiko kebocoran informasi sensitif.

Dampak Serangan *LockBit* Terhadap Korban

Dampak serangan *LockBit* sangat bervariasi tergantung pada jenis organisasi yang menjadi korban dan seberapa cepat mereka dapat merespons serangan. Beberapa dampak utama yang dialami oleh korban adalah:

1. Kerugian Finansial

Salah satu dampak terbesar dari serangan *LockBit* adalah kerugian finansial yang sangat besar. Organisasi yang diserang harus mengeluarkan biaya besar untuk pemulihan data, pembaruan sistem keamanan, dan untuk menangani potensi litigasi atau denda yang timbul dari kebocoran data. Dalam beberapa kasus, organisasi memilih untuk membayar tebusan untuk mendapatkan kunci dekripsi, yang sering kali mencakup jumlah yang sangat besar. Sebagai contoh, pada serangan terhadap perusahaan energi pada 2023, perusahaan diperkirakan menghabiskan lebih dari \$50 juta untuk pemulihan.

2. Gangguan Operasional

Serangan *Ransomware* seperti *LockBit* menyebabkan gangguan besar pada operasi bisnis. Di sektor kesehatan, serangan ini dapat mengakibatkan penundaan prosedur medis penting, mempengaruhi pasien, dan memperburuk beban rumah sakit yang sudah penuh. Di sektor energi, gangguan pada sistem SCADA dapat mengancam keselamatan publik dan mengganggu distribusi energi secara luas.

3. Kerusakan Reputasi

Selain kerugian finansial, organisasi yang terkena serangan *Ransomware* sering kali mengalami kerusakan reputasi yang signifikan. Kebocoran data sensitif atau gangguan layanan dapat merusak kepercayaan pelanggan dan mitra bisnis, yang mempengaruhi hubungan jangka panjang dan dapat mengakibatkan hilangnya pelanggan.

Langkah-Langkah Yang Dilakukan Untuk Mencegah Serangan *LockBit*

1. Pendidikan dan Pelatihan Pengguna

Pencegahan serangan *Ransomware* dimulai dengan pendidikan pengguna. Organisasi harus memberikan pelatihan kepada karyawan untuk mengenali tanda-tanda phishing dan praktik social engineering. Pengguna yang terlatih lebih mampu mengenali email atau pesan mencurigakan yang dapat mengarah pada serangan.

2. Pembaruan Perangkat Lunak Secara Teratur

Perusahaan harus memastikan bahwa semua perangkat lunak dan sistem operasi mereka selalu diperbarui dengan patch terbaru. Pembaruan ini biasanya berisi perbaikan untuk kerentanannya yang dapat dieksploitasi oleh peretas. Pembaruan yang tepat waktu adalah langkah pertama dalam mengurangi risiko serangan *Ransomware*.

3. Penggunaan Multi-Faktor Autentikasi (MFA)

Mengaktifkan Multi-Factor Authentication (MFA) di semua titik akses penting adalah langkah penting dalam mencegah peretas mengakses sistem

organisasi. MFA membuatnya lebih sulit bagi peretas untuk mendapatkan akses ke akun meskipun mereka berhasil mencuri kredensial pengguna.

4. Pencadangan Data yang Teratur

Organisasi harus memiliki kebijakan pencadangan data yang teratur dan memastikan bahwa cadangan tersebut disimpan di lokasi yang terisolasi dari jaringan utama. Cadangan yang aman memungkinkan organisasi untuk memulihkan data mereka tanpa membayar tebusan, bahkan jika data mereka dienkripsi.

1. Deteksi dan Respons Dini

Implementasi sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) yang efektif dapat membantu mendeteksi serangan pada tahap awal. Respons yang cepat terhadap insiden dapat mencegah penyebaran *Ransomware* lebih lanjut dan meminimalkan dampak serangan.

Pembelajaran Yang Dapat Diambil

Serangan *LockBit* selama 2022-2023 menawarkan beberapa pembelajaran penting dalam mengelola ancaman *Ransomware*:

1. Proaktif dalam Keamanan: Organisasi harus mengadopsi pendekatan proaktif terhadap keamanan siber, termasuk penerapan kebijakan keamanan yang ketat dan pelatihan berkelanjutan.
2. Tidak Membayar Tebusan: Meskipun sangat menggoda untuk membayar tebusan, pembayaran tidak menjamin data akan dipulihkan, dan itu hanya akan mendanai lebih banyak serangan. Sebaiknya fokus pada pemulihan data melalui cadangan yang aman.
3. Kolaborasi dengan Pihak Berwenang: Organisasi harus bekerja sama dengan otoritas keamanan siber dan penegak hukum untuk melaporkan serangan dan berbagi informasi tentang metode yang digunakan oleh peretas.

KESIMPULAN

Serangan *Ransomware LockBit* pada 2022 dan 2023 menggambarkan evolusi ancaman siber yang semakin canggih dan terorganisir. Melalui penggunaan teknik seperti phishing, eksploitasi kerentanannya, dan model *Ransomware-as-a-service*, *LockBit* mampu menyerang berbagai organisasi besar dan menyebabkan kerugian yang signifikan. Namun, dengan langkah-langkah pencegahan yang tepat, organisasi dapat memitigasi risiko ini dan memperkuat pertahanan mereka terhadap serangan *Ransomware* yang akan datang. Pembelajaran dari serangan-serangan ini menekankan pentingnya kebijakan keamanan yang komprehensif dan respons yang cepat dalam menghadapi ancaman siber.

DAFTAR PUSTAKA

- Cyberscurity & Infrastruktur Security Agency (2023). *Understanding Ransomware Threat Actors: LockBit*. CISA Cybersecurity Reports.
- Smith, J., & Williams, R. (2023). *An Analysis of Ransomware Attacks: LockBit's Evolving Threat*. Cybersecurity Journal.
- The Indonesian Institute of Science and Technology Research (2023). *Ransomware: Memahami Ancaman Keamanan Digital*. Ransomware Journal
- National Cybersecurity Center (2023). *LockBit: A New Era in Ransomware*. NCC Cyber Reports.
- Kaspersky, A. (2023). *LockBit 3.0: The Rise of Ransomware-as-a-Service*. Kaspersky Labs.