JULIKOM
Jurnal Ilmu Komputer
Doi:
Web: https://journal.penus.or.id/index.php/julikom

Vol. 1, No. 1,
Oktober 2024
Hal. 54-60

E-ISSN: xxxx-xxxx
P-ISSN: xxxx-xxxx

Systematic Literature Review Serangan *Ransomware*: Metode Penyerangan dan Mekanisme Pertahanan

Jaswin[1], Yonky Pernando[2]

[1]Mahasiswa Prodi Teknik Informatika, Universitas Universal
[2]Dosen Prodi Teknik Informatika, Universitas Universal
[1]jaswinftf1@gmail.com , [2]yongkyfernando194@gmail.com

Riwayat Artikel:
Diterima: 23 Okt, 2024
Ditinjau: 25 Okt, 2024
Disetujui: 25 Okt, 2024

Abstrak

Ransomware tetap menjadi ancaman serius di dunia keamanan siber, memanfaatkan teknik canggih untuk membobol dan mengenkripsi data untuk mendapatkan keuntungan finansial. Studi ini menggunakan metodologi *Systematic Literature Review* (SLR) untuk menganalisis pola serangan *ransomware* dan mengevaluasi efektivitas mekanisme pertahanan yang didokumentasikan dalam penelitian terbaru. Tinjauan ini mengidentifikasi vektor serangan umum, termasuk phishing dan eksploitasi kerentanan perangkat lunak, serta mengeksplorasi pendekatan mitigasi seperti strategi cadangan, segmentasi jaringan, dan kesadaran pengguna. Dengan mensintesis temuan dari 30 studi utama, penelitian ini memberikan pemahaman komprehensif tentang siklus hidup serangan *ransomware* dan menyoroti strategi pertahanan praktis bagi organisasi dan individu. Studi ini diakhiri dengan wawasan kunci untuk meningkatkan ketahanan terhadap ancaman siber yang persisten ini.

Kata kunci: *Ransomware, Cybersecurity, Systematic Literature Review*

Abstract

Ransomware continues to pose a critical threat in the realm of cybersecurity, leveraging sophisticated techniques to compromise and encrypt data for monetary gain. This study employs a Systematic Literature Review (SLR) methodology to analyze patterns in ransomware attacks and evaluate the effectiveness of defense mechanisms documented in recent research. The review identifies common attack vectors, including phishing and exploitation of software vulnerabilities, and explores mitigation approaches such as backup strategies, network segmentation, and user awareness. By synthesizing findings from 30 primary studies, this research provides a comprehensive understanding of the lifecycle of ransomware attacks and highlights practical defense strategies for organizations and individuals. The study concludes with key insights to improve resilience against this persistent cyber threat.

Keywords: *Ransomware, Cybersecurity, Systematic Literature Review*

PENDAHULUAN

Ransomware adalah tipe *malware* spesifik yang mengenkripsi data pengguna yang di mana akan menrestriksi akses individual terhadap *filenya* sendiri. *Ransomware* terdiri dari dua kata, *ransom* dan *malware*. *Malware* adalah singkatan dari "*Malicious Software*". *Malware* itu secara spesifik di desain untuk mendapatkan akses atau merusak mesin korban. *Malware* sekarang di ciptakan terutama untuk keuntungan. *Malware* juga digunakan untuk mencuri data seperti *Spyware*, iklan seperti *Ad-ware*, dan mengirim spam email seperti komputer zombi. *Ransomware* adalah topik yang sangat penting di keamanan Teknologi Informasi. Di luar sana banyak sekali metode yang digunakan

untuk melindungi mesin dari serangan *ransomware*. *Ransomware* adalah serangan yang sangat berbahaya, untuk contohnya, kerusakan dari CryptoWall3 di estimasikan melebihi 320 juta US Dolar [1].

Contoh perkembangan paling awal dari *ransomware* muncul 3 dekade yang lalu ketika *compact disks* (CD) dikirimkan kepada tamu konferensi. Kemudian, *ransomware* berevolusi menjadi lebih berfokus pada pengiriman-berbasis-jaringan dan pembayaran *cryptocurrency* [2]. Perkembangan *ransomware* dalam waktu 1 dekade terakhir ini sudah mengalami perkembangan yang eksponensial. Keluarga *ransomware The WannaCry* dan *Petya* membawa perhatian yang baru terhadap serangan *ransomware* pada May 2017. *WannaCry,* untuk contohnya, membuat kekacauan seperti yang telah di laporkan bahwa *ransomware* ini telah menginfeksi 35 000 mesin di 150 negara dalam 3 hari pertama *ransomware* ini di keluarkan [3].

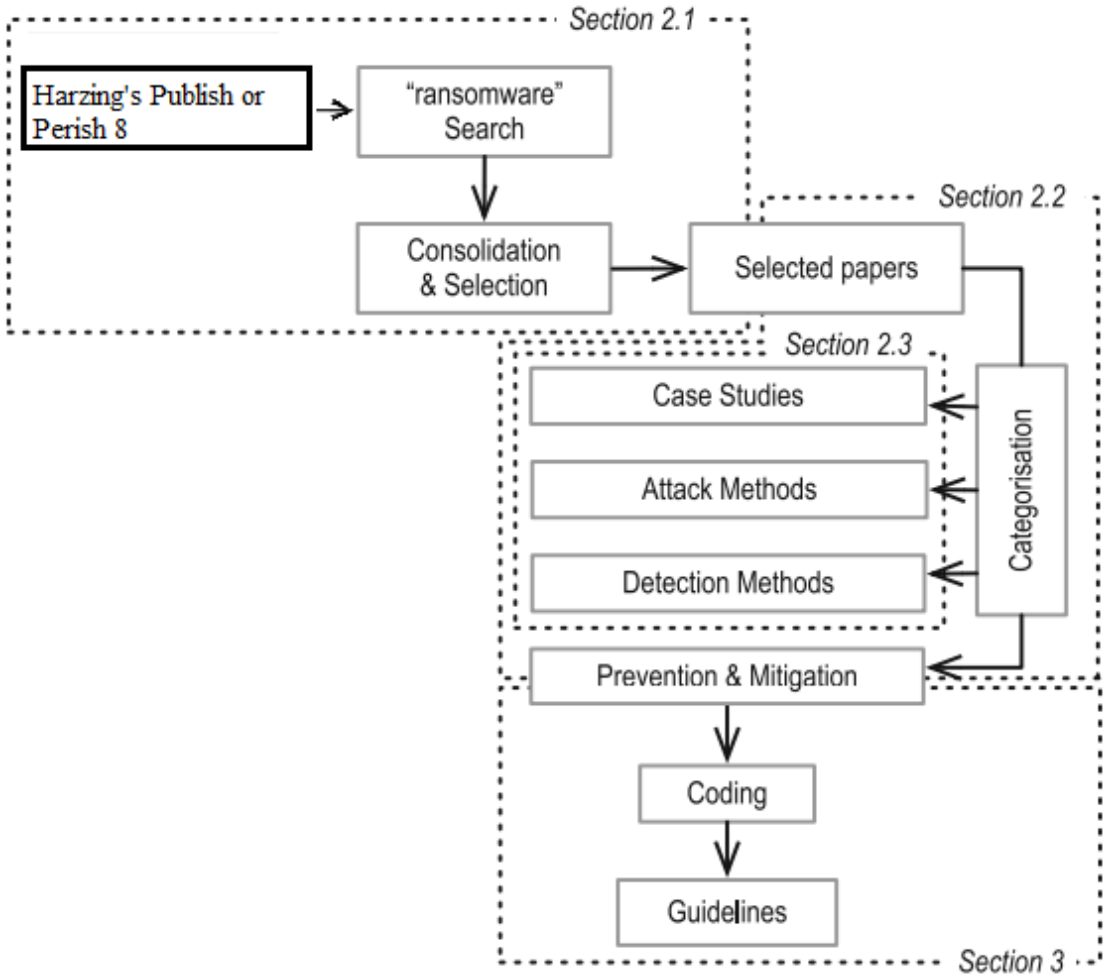
Dalam perkembangan *ransomware* selama ini, *ransomware* dapat dibagi menjadi dua kategori utama yaitu: *crypto* dan *locker ransomware*. Namun, pada akhir-akhir ini ada beberapa tipe yang mendapat popularitas dalam kelompok penyerang[4]. *Crypto Ransomware* merupakan *malware* yang mengunci file yang tersimpan di dalam komputer korban atau perangkat lainnya untuk meminta pembayaran dengan membuat file tersebut tidak dapat diakses oleh user. *Locker Ransomware* adalah *malware* yang mengunci layar sistem atau layar perangkat lainnya, mengrestriksi akses korban terhadap perangkat mereka namun tidak ada data yang di *hack* [5]. *Scareware* merupakan tipe *ransomware* yang menipu pengguna untuk mengunduh atau membeli atau terkadang *software* yang tidak berguna atau jahat, trik ini biasa digunakan menggunakan iklan *pop-up*. *Leakware* yang biasa dikenal dengan *Doxware*, adalah tipe *ransomware* yang baru dan ampuh yang dimana dapat membuat data pengguna menjadi public kecuali telah dibayar [4].

Peneliti dan profesional dalam bidang *cybersecurity* telah membuat berbagai macam usaha untuk melawan *ransomware* sebelum *ransomware* tersebut dapat menyebabkan efek yang negatif terhadap organisasi ataupun pengguna individu. Terdapat banyak penelitian yang menyediakan strategi mitigasi terhadap serangan *ransomware*. Strateginya datang dalam berbagai macam bentuk seperti *software*, panduan, dan *framework*. Beberapa strategi mungkin berkontradiksi satu sama lain dan yang lainnya dapat membantu satu sama lain [3]. Oleh karena itu, penelitian ini bertujuan untuk melakukan *review* terhadap literatur yang telah ada sebelumnya secara sistematik untuk menghasilkan pedoman pencegahan yang telah terkonsolidasi dari sumber-sumber yang relevan. Tujuan dari penelitian ini untuk mempromosikan keberhisan dunia maya untuk memahami pola penyerangan dan pencegahan atau mitigasi *ransomware.*

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah *Systematic Literature Review* yang dimana metode ini digunakan untuk menganalisa literatur yang ada dalam apa metode yang relevan dalam mencari metode penyerangan *ransomware* dan cara untuk mempertahankan komputer pengguna dari *ransomware* [3].

JULIKOM: Jurnal Ilmu Komputer
Vol. 1, No. 1, Oktober 2024, Hal. 54-60
E-ISSN: xxxx-xxxx, P-ISSN: xxxx-xxxx
doi:



Gambar 1. Proses Penelitian [3]

Sumber Literatur Untuk Analisis

Proses SLR dilakukan dengan menggunakan database online untuk mendapatkan litaratur yang telah ada dalam tema *ransomware*. Pencarian dilakukan dengan menggunakan Harzing's Publish or Perish 8 yang di mana *search engine* yang dipakai adalah menggunakan *Google Scholar* yang dapat memberikan literatur yang luas dan dari berbagai sumber yang berkualitas tinggi.

Setiap sumber dicari dengan menggunakan "*ransomware, mitigation, attack pattern*" sebagai keyword pencarian. Pencarian dibatasi untuk jurnal *full-text.* Pencarian jurnal yang dilakukan oleh Harzing dapat memberikan ratusan hasil namun di *filter* kembali dan dalam total adalah 30 buah jurnal yang telah diunduh dan akan di analisis.

Analisis Awal Sumber Literatur

30 jurnal dianalisa untuk memutuskan apa aspek dari *ransomware* yang mereka hadapi. Untuk menghasilkan analisa yang bermutu, saya melakukan limitasi atas kategori yang akan di analisa. Kategori tersebut berada pada table 1. Tujuan dari penelitian ini adalah untuk menemukan pola penyerangan dan juga solusi untuk masalah *ransomware* ini.

Jurnal kemudian dikategorikan untuk berurusan dengan lebih dari satu metode, bisa jadi metode deteksi, metode pencegahan dan mitigasi, dan metode serangan, ataupun studi kasus.

Penemuan Awal

Analisa pada awalnya menemukan tiga kategori dari literatur *ransomware*. Kategori ini adalah metode penyerangan, metode pendeteksian, dan pencegahan dan mitigasi.

Studi yang berkonsentrasi pada **metode penyerangan *ransomware*** menekankan mengenai target penyerangan, cara infeksi, aksi jahatnya (enskripsi atau locking) [4]. Pada studi ini juga menjelaskan cara *ransomware* dapat berkomunikasi, dan berdasarkan penelitian [6], metode infeksi yang paling sering digunakan adalah dengan cara *phishing*, platform yang paling sering diserang adalah Windows dan cara ekstorsi adalah dengan BitCoin.

JULIKOM: Jurnal Ilmu Komputer
Vol. 1, No. 1, Oktober 2024, Hal. 54-60
E-ISSN: xxxx-xxxx, P-ISSN: xxxx-xxxx
doi:

Family	First Seen	Infection	Platform	Characteristics						
				C&C Comm.	Encryption	Destruction	Exfiltration	Locking	Del. Shadow	Extortion
PC CYBORG	1989	Phishing	Windows	None	Custom	Overwrite				Cash
GPCode	2008	Drive-by-download	Windows	None	RSA	Overwrite				Prepaid Voucher
Archiveus	2008	Drive-by-download	Windows	None	RSA	Delete				Prepaid Voucher
Randsom.C	2008	Spam	Windows	None	None	None	✓			SMS
Seftad	2008	Spam	Windows	None	MBR	Overwrite		✓		Prepaid Voucher
Krotten	2008	Spam	Windows	None	RSA	Overwrite				Prepaid Voucher
Urausy	2009	Phishing	Windows	None	None	None		✓		Prepaid Voucher
Winlock	2010	Spam	Windows	Hard-coded	None	None	✓		✓	SMS
Reveton	2012	Phishing	OS-Agnostic	None	None	None	✓	✓		Prepaid Voucher
CryptoLocker	2013	Phishing	Windows	Hard-coded	RSA	Overwrite	✓		✓	Bitcoin
CryptoWall	2013	Phishing	Windows	Hard-coded	RSA	Overwrite			✓	Prepaid Voucher
FakeDefender	2013	Malicious App.	Android	None	None	None		✓		Prepaid Vouchers
Lockdroid	2014	Malicious App.	Android	None	None	None		✓		Prepaid Vouchers
SimpLocker	2014	Malicious App.	Android	Hard-coded	AES	Overwrite				Bitcoin
TorrentLocker	2014	Phishing	Windows	Dynamic Domains	AES+RSA	Delete			✓	Prepaid Voucher
TrolDesh	2014	Phishing	Windows	Hard-coded	AES	Delete			✓	Bitcoin
CryptoDefense	2014	Phishing	Windows	None	RSA	Delete			✓	Bitcoin
CTBLocker	2015	Phishing	Windows	None	ECC	Delete			✓	Bitcoin
TeslaCrypt	2015	Exploit kits	Windows	Hard-coded	AES	Delete				Bitcoin
Fusob	2015	Phishing	Mobile	None	None	None		✓		Giftcards
Chimera	2015	Phishing	Windows	Hard-coded	AES	Delete			✓	Bitcoin
LinuxEncoder	2015	Vulnerability	Linux	Hard-coded	AES+RSA	Delete				Bitcoin
Ransom32	2016	Malvertisement	OS-Agnostic	Hard-coded	AES	Overwrite			✓	Bitcoin
Dharma	2016	RDP	Windows	Hard-coded	AES	Delete			✓	Bitcoin
Locky	2016	Phishing	Windows	Dynamic Domains	AES+RSA	Delete			✓	Bitcoin
Cerber	2016	Phishing	Windows	None	AES	Overwrite				Bitcoin
Jigsaw	2016	Phishing	Windows	Hard-coded	AES+RSA	Delete			✓	Bitcoin
KeRanger	2016	Malicious App.	macOS	Hard-coded	AES+RSA	Delete			✓	Bitcoin
Petya	2016	Exploit kits	Windows	Hard-coded	AES	Overwrite		✓		Bitcoin
DMALocker	2016	Exploit kits	OS-Agnostic	Hard-coded	AES	Delete			✓	Bitcoin
Sage	2017	Drive-by-download	Windows	Hard-coded	AES+RSA	Delete				Bitcoin
BadRabbit	2017	Drive-by-download	Windows	Dynamic Domains	AES+RSA	Delete				Bitcoin
WannaCry	2017	Vulnerability	Windows	Hard-coded	AES+RSA	Delete				Bitcoin
GoldenEye	2017	Exploit kits	Windows	Hard-coded	AES	Overwrite			✓	Bitcoin
SamSam	2018	RDP	Windows	Hard-coded	RSA	Delete			✓	Bitcoin
GandCrab	2018	Drive-by-download	OS-Agnostic	Hard-coded	AES	Overwrite			✓	Bitcoin
Sodikonibi	2019	Exploit kits	Windows	Hard-coded	AES+ECC	Overwrite		✓	✓	Bitcoin
Robbinhood	2019	RDP	Windows	Hard-coded	AES+RSA	Delete	✓		✓	Bitcoin
Maze	2019	Exploit kits	OS-Agnostic	Hard-coded	AES+RSA	Overwrite			✓	Bitcoin
Ryuk	2019	RDP	OS-Agnostic	Hard-coded	AES+RSA	Overwrite			✓	Bitcoin
MegaCortex	2019	Exploit-kits	OS-Agnostic	Hard-coded	AES	Overwrite			✓	Bitcoin
LockerGaga	2019	Phishing	Windows	None	AES+RSA	Delete			✓	Bitcoin
Ekans	2019	Vulnerability	ICS	Hard-coded	AES+RSA	Delete			✓	Bitcoin
PureLocker	2020	Vulnerability	PC	Dynamic Domains	AES	Delete			✓	Proton
Tycoon	2020	Vulnerability	Windows	Dynamic Domains	AES	Delete			✓	Proton
CovidLock	2020	Malicious App.	Android	None	None	None		✓		Bitcoin
Corona	2020	Phishing	Windows	None	AES+RSA	Overwrite	✓		✓	Bitcoin

Tabel 1. Ringkasan Keluarga *Ransomware* Terkemuka dari Tahun 1989-2020[6]

Metode pendeteksian memberikan sinyal peringatan sebelum serangan dimulai yang dimana berguna agar pengguna dapat beraksi dengan cepat. Metode ini bergantung pada serangan *ransomware* yang memperlihatkan perilaku dari penyerangan terhadap sistem komputer [7]. Vehabovic et al. [8] mengusulkan sistem bernama UNVEIL, yang menggunakan analisis dinamis dengan sandbox Cuckoo untuk mendeteksi aktivitas *ransomware*. Dengan memantau modifikasi sistem file, panggilan API, dan pola enkripsi, sistem ini berhasil mengidentifikasi perilaku *ransomware* pada dataset yang terdiri dari lebih dari 148.000 sampel malware. Pendekatan mereka mencapai tingkat deteksi positif sebesar 96,3% untuk jenis-jenis *ransomware* [8].

Pencegahan dan strategi mitigasi memberikan cara-cara pencegahan serangan *ransomware* dan cara mitigasi dari serangan apabila telah terjadi. Chesti et al. [5] mengusulkan *framework* untuk mitigasi ancaman *ransomware* dengan menitikberatkan pada edukasi pengguna dan kebijakan organisasi. Mereka menyoroti langkah-langkah pencegahan seperti melakukan *back-up* secara teratur, menggunakan filter keamanan email, dan menerapkan praktik pengunduhan yang aman. Selain itu, mereka merekomendasikan penggunaan VPN saat menggunakan *Wi-Fi* public dan menginsatal perangkat lunak keamanan untuk membatasi infiltrasi *ransomware*[5].

Ketiga kategori ini akan menjadi focus dari jurnal ini, jadi penjelasan dan analisis lebih lanjut akan di deskripsikan pada bagian selanjutnya.

HASIL DAN PEMBAHASAN

Analisis Metode Serangan Ransomware

Literatur yang ditinjau mengidentifikasi pola umum dan strategi dalam serangan *ransomware*, memberikan pandangan komprehensif tentang metode yang digunakan. Metode serangan ini menunjukkan peningkatan kompleksitas *ransomware* sebagai ancaman utama dalam keamanan siber.

1. Vektor Infeksi

Ransomware sering memulai serangannya melalui vektor infeksi yang memanfaatkan kerentanan manusia dan teknis. *Email phishing* tetap menjadi mekanisme penyebaran paling umum, di mana penyerang menyisipkan tautan atau lampiran berbahaya yang akan mengeksekusi *ransomware* ketika diakses. Unduhan *drive-by* dari situs web yang berbahaya juga merupakan titik masuk lainnya, Kerentanan *software* yang sudah usang, seperti yang dieksploitasi *WannaCry* melalui protocol SMB, juga berperan penting dalam infeksi *ransomware* [9] Taktik rekayasa social (*social engineering*) semakin memperbesar ancaman ini dengan menipu pengguna agar melakukan tindakan berbahaya, seperti memberikan informasi pribadi, atau menjalankan file yang terinfeksi [10].

2. Varian Serangan

   Ransomware telah berkembang menjadi berbagai varian, masing-masing dengan metode operasinya sendiri. *Screen lockers* melumpuhkan pengguna dengan membekukan antarmuka sistem, memaksa mereka membayar untuk mendapatkan kembali akses. *Crypto-ransomware* mengenkripsi file menggunakan algoritma canggih seperti AES-256, menyandera data pengguna hingga tebusan dibayar. *Ransomware* dengan eksfiltrasi data memperluas model ini dengan mengancam akan membocorkan informasi sensitif jika tuntutan tidak dipenuhi, bahkan menargetkan sistem dengan solusi pencadangan yang kuat. *Ransomware* tanpa file menghindari deteksi dengan beroperasi sepenuhnya di memori, tanpa memerlukan file yang dapat dieksekusi [10].

3. Tahapan Eksekusi

   Siklus hidup serangan *ransomware* melalui tahapan yang terdefinisi dengan baik. Pada tahap Infeksi, korban sering kali menjadi target dengan email spam yang berisi lampiran berbahaya, seperti file ZIP atau tautan ke situs web yang dikompromikan. Selama Instalasi, *ransomware* menyisipkan kode ke dalam proses sistem seperti *svchost.exe*, memodifikasi *registry* untuk memastikan persistensi, dan menghapus salinan cadangan untuk mencegah pemulihan. Fase Komunikasi melibatkan koneksi ke server command-and-control menggunakan protokol terenkripsi seperti HTTPS, sering kali menggunakan SSL untuk mengenkripsi lalu lintas data[10]. Dalam fase Eksekusi, *ransomware* mengidentifikasi file yang akan dienkripsi, menggunakan kunci AES yang dihasilkan untuk mengenkripsi data, dan mengunggah kunci enkripsi ke *server* command-and-control[9]. Pada fase Pemerasan, catatan tebusan ditampilkan dengan permintaan pembayaran, biasanya menggunakan cryptocurrency. Terakhir, dalam fase Pelepasan, beberapa korban menerima kunci dekripsi, meskipun ini tidak selalu dijamin[10].

4. Teknik Penghindaran

   Untuk menghindari deteksi, ransomware menggunakan berbagai teknik. Obfuscation menyamarkan kodenya, sehingga sulit dideteksi oleh perangkat lunak antivirus [9]. Perilaku polimorfik memungkinkan *ransomware* mengubah kodenya secara dinamis, menyulitkan metode deteksi berbasis tanda tangan. *Ransomware* tanpa file semakin menantang pertahanan tradisionral dengan menghindari penggunaan file yang dapat dieksekusi dan hanya beroperasi di memori sistem. Protokol komunikasi terdesentralisasi, seperti penggunaan jaringan *Tor*, membuat aktivitas *ransomware* sulit dilacak dan operasinya sulit dinonaktifkan [10].

Analisis Pencegahan Dan Mitigasi Ransomware

Literatur yang ditinjau menyajikan kesamaan antara pedoman tersebut. Hasilnya, daftar pedoman gabungan untuk pencegahan dan mitigasi *ransomware* dihasilkan dari jurnal yang ditinjau. Meskipun bukan solusi absolut, penerapan pedoman ini dapat membantu mencegah dan memitigasi *ransomware* serangan. Pedoman ini dapat dipertimbangkan oleh semua pengguna komputer, tetapi ada juga yang mempertimbangkan apa yang perlu diterapkan oleh pengguna bisnis.

1. Implementasi Strategi Back-up

   Backup yang dilakukan secara berkala sangat penting untuk memitigasi dampak dari serangan *ransomware*. Proses *backup* direkomendasikan disimpan secara *offline* yang terlepas dari jaringan untuk mencegah *ransomware* untuk mengakses atau mengunci file-file yang penting. Alat seperti *cloud storage* atau media penyimpanan eksternal (contoh: *Harddisk*) dapat juga diutilisasi. *Backup* harus dilakukan secara teratur, dengan setidaknya dilakukan harian, untuk memastikan bahwa data dapat di pulihkan [5]. Terlebih lagi, melakukan percobaan secara periodik terhadap proses pemulihan *backup* sangatlah penting untuk memastikan integritas data dan aksesibilitas dalam keadaan darurat [6].

2. Install dan Update Perangkat Lunak Proteksi

   Instalasi dan pembaruan rutin perangkat lunak *antimalware* adalah langkah dasar dalam pencegahan *ransomware*. Perbarui sistem operasi, aplikasi, dan *firmware* secara teratur untuk menutup celah keamanan yang dapat dieksploitasi oleh *ransomware* [11].

3. Edukasi dan Kesadaran Keamanan Siber
   Kesalahan manusia sering menjadi masalah utama bagi serangan *ransomware*, terutama melalui *phising*. Program pelatihan untuk meningkatkan kesadaran karyawan tentang email berbahaya, tautan mencurigakan, dan praktik penggunaan internet yang aman sangat penting [5]. Pelatihan juga harus mencakup cara mengenali rekayasa sosial yang sering digunakan oleh penyerang untuk mendapatkan akses ke sistem [7].
4. Segmentasi dan Pemantuan Jaringan
   Segmentasi jaringan memungkinkan isolasi sistem penting untuk mencegah penyebaran *ransomware* di seluruh infrastruktur organisasi. Memisahkan data sensitif dan lingkungan operasional ke zona yang berbeda dapat membatasi dampak serangan. Selain itu, pemantuan jaringan untuk mendeteksi aktivitas mencurigakan seperti transfer data tak terotorisasi dapat memberikan peringantan dini terhadap potensi serangan [7].
5. Mematikan Mesin Setelah Infeksi
   Ketika *ransomware* telah menginfeksi komputer yang terhubung ke suatu jaringan, *malware* memiliki kemampuan untuk memperbanyak diri ke komputer lainnya dalam jaringan yang menimbulkan banyak perangkat yang ditahan. Sebuah komputer akan memperlihatkan tanda yang terlihat sebagai tanda infeksi. Tanda ini termasuk ke layar yang terkunci atau file yang terenkripsi. Pada saat itu juga, pengguna diharuskan untuk bertindak cepat dengan memutuskan jaringan dan menonaktifkan semua perangkat secepat mungkin. Teknik mitigasi ini dikenal dengan *drop and roll*. Ini akan mengurangi kerusakan yang ditimbulkan dari serangan dengan menghambat *malware* untuk memperbanyak diri [7].

KESIMPULAN DAN SARAN

Ransomware tetap menjadi ancaman keamanan siber yang selalu berkembang, menggunakan berbagai vektor infeksi, cara penyerangan, dan teknik penghindaran untuk melewati pendeteksian. Pencegahan dan cara mitigasi yang efektif memerlukan pendekatan yang komprehensif, termasuk data *backup*, pembaruan perangkat lunak, edukasi pengguna, segmentasi jaringan, dan tanggapan yang cepat saat terjadi serangan. Namun, tantangan baru terus muncul, sehingga diperlukannya inovasi berkelanjutan untuk memperkuat pertahanan. Hal ini menggarisbawahi perlunya pendekatan yang lebih komprehensif untuk memahami dan mengatasi ancaman *malware*. Oleh karena itu, keterbatasan dalam ruang lingkup dan kedalaman penelitian harus ditingkatkan untuk memperbaiki penelitian kedepannya.

Saran untuk penelitian selanjutnya:

1. Perluas Cakupan Analisis: Jurnal saat ini terlalu berfokus pada metode dan teknik yang sudah ada sebelumnya. Penelitian kedepannya harus mengeksplorasi tren-tren dalam *ransomware*.
2. Pendalaman Analisis Teknis: Meskipun jurnal membahas mengenai pola serangan dan strategi mitigasi, analisis teknis mendalam tentang algoritma enkripsi, metode penghindaran, atau *ransomware* berbasis memori belum dibahas. Penelitian selanjutnya sebaiknya mengupas aspek ini secara rinci.
3. Validasi Empiris: Temuan dalam jurnal ini terlalu bergantung pada data sekunder dari literatur yang ada. Penelitian selanjutnya dapat menyertakan studi kasus, simulasi, atau pengujian empiris untuk memvalidasi dan memperkuat strategi yang diusulkan.
4. Fokus pada Dampak Sektor Tertentu: Jurnal ini menggeneralisasi ancaman *ransomware* di semua sektor. Penelitian mendatang dapat menganalisis kerentanan spesifik sektor tertentu, seperti kesehatan atau infrastruktur kritis, untuk memberikan pertahanan yang lebih spesifik.

UCAPAN TERIMA KASIH

Kami ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah mendukung dan berkontribusi terhadap penelitian ini. Kami juga ingin mengucapkan terima kasih kepada keluarga dan teman-teman yang telah memberikan dukungan moral selama penelitian ini berlangsung. Semoga penelitian ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan dan menjadi dasar yang kuat untuk untuk meningkatkan keamanan siber dari serangan *ransomware*.

DAFTAR PUSTAKA

[1] A. H. Mohammad, “Ransomware Evolution, Growth and Recommendation for Detection,” *Mod Appl Sci*, vol. 14, no. 3, p. 68, Feb. 2020, doi: 10.5539/mas.v14n3p68.

[2] A. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno, and A. Yayimli, “Ransomware Detection and Classification Strategies,” Apr. 2023, doi: 10.1109/BlackSeaCom54372.2022.9858296.

[3] Z. Manjezi and R. A. Botha, "Preventing and Mitigating Ransomware: A Systematic Literature Review," in *Communications in Computer and Information Science*, Springer Verlag, 2019, pp. 149–162. doi: 10.1007/978-3-030-11407-7_11.

[4] S. Razaulla *et al.*, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access*, vol. 11, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.

[5] I. A. Chesti, M. Humayun, N. U. Sama, and N. Z. Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware," in *2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ICCIS49240.2020.9257708.

[6] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," in *IEEE International Conference on Program Comprehension*, IEEE Computer Society, 2022, pp. 36–47. doi: 10.1145/nnnnnnn.nnnnnnn.

[7] Z. Manjezi and R. A. Botha, "Preventing and Mitigating Ransomware: A Systematic Literature Review," in *Communications in Computer and Information Science*, Springer Verlag, 2019, pp. 149–162. doi: 10.1007/978-3-030-11407-7_11.

[8] A. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno, and A. Yayimli, "Ransomware Detection and Classification Strategies," Apr. 2023, doi: 10.1109/BlackSeaCom54372.2022.9858296.

[9] A. M. Maigida, S. M. Abdulhamid, M. Olalere, J. K. Alhassan, H. Chiroma, and E. G. Dada, "Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms," Jul. 01, 2019, *Springer Science and Business Media Deutschland GmbH*. doi: 10.1007/s40860-019-00080-3.

[10] A. Sainuri Mubarak, M. Nur Insirat, M. Nurul Lutfiya, S. Negeri, U. Muhammadiyah Makassar, and U. Negeri Makassar, "SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention", doi: 10.31284/p.snestik.2024.5588.

[11] S. G. Selvaganapathy, S. Sadasivam, and V. Ravi, "A Review on Android Malware: Attacks, Countermeasures and Challenges Ahead," *Journal of Cyber Security and Mobility*, vol. 10, no. 1, pp. 177–230, 2021, doi: 10.13052/jcsm2245-1439.1017.