Jurnal Publikasi Teknik Informatika (JUPTI)
Vol. 3, No. 1 Januari 2024
E-ISSN: 2808-8972 P-ISSN: 2808-9367, Hal 29-37
DOI: https://doi.org/10.55606/jupti.v3i1.2507

Keamanan Komputer Dalam Novel *Spammer* Karya Ronny Mailindra

I Gede Widiantara
Universitas Teknologi Yogyakarta

Eva Dwi Kurniawan
Universitas Teknologi Yogyakarta

Alamat: Jl. RingRoad Utara, Mlati Krajan, Sumberadi, Kec. Mlati, Kab. Sleman
Korespondensi penulis: eva.dwi.kurniawan@staff.uty.ac.id

Abstract*. The threats related to computer viruses have become a highly significant issue in the era of technology. Data and computer system security are the primary concerns in various sectors, including businesses, government, and individuals. This research aims to examine how computer viruses are spread and how computer security works within the novel Spammer by Ronny Mailindra. The method used is hermeneutics. Based on the analysis and discussion, the findings reveal 1) Spyware for mobile phones, 2) Trojans, 3) Viruses, 4) Digital footprints, 5) Remote SSH. In the novel Spammer it is depicted that computer viruses are commonly disseminated through email spam, and one of the network security protocols that proves challenging to breach is the Secure Shell Protocol (SSH).*

Keywords*: Computer Security; Literature; Hermeneutics.*

Abstrak. Ancaman yang terkait dengan virus komputer menjadi isu yang sangat signifikan dalam era teknologi. Keamanan data dan sistem komputer telah menjadi perhatian utama di berbagai sektor, termasuk bisnis, pemerintahan, dan individu. Penelitian ini bertujuan untuk melihat bagaimana penyebaran virus komputer dan cara kerja keamanan komputer yang terdapat di dalam novel Spammer karya Ronny Mailindra. Metode yang digunakan menggunakan pendekatan hermeneutika. Berdasarkan analisa dan pembahasan ditemukan hasil yaitu 1) Ponsel antisadap, 2) Trojan, 3) Virus, 4) Jejak digital, 5) Remote SSH. Pada novel Spammer ditunjukkan bahwa virus komputer biasa disebarkan melalui email spam dan salah satu protokol keamanan jaringan yang sulit dibobol adalah SSH (Secure Shell Protocol).

Kata kunci: Keamanan Komputer; Sastra; Hermeneutika.

LATAR BELAKANG

Dalam era teknologi yang terus berkembang pesat, keberadaan virus komputer dan keamanan komputer telah menjadi isu yang sangat penting. Oleh karena itu, keamanan komputer menjadi perhatian utama di berbagai bidang. Adanya aset data penting berupa informasi sebuah organisasi yang perlu dilindungi dengan mengikuti pendekatan yang komprehensif dan terstruktur terhadap risiko organisasi yang mungkin dihadapi (Riadi dkk, 2019:854).

Penggunaan media penyimpanan dan distribusi data atau informasi adalah faktor yang menyebabkan kerentanannya, memungkinkan data atau informasi dapat diakses oleh pihak yang tidak bertanggung jawab. Mengeksploitasi kerentanan sebuah sistem komputer, penyerang sebagai aktor ancaman, harus memiliki sebuah akses atau setidaknya terdapat suatu

Revised November 20, 2023; Accepted Desember 20, 2023; Published Januari 30, 2024
* Eva Dwi Kurniawan, eva.dwi.kurniawan@staff.uty.ac.id

alat ataupun teknik yang digunakan untuk dapat mengakses kerentanan sistem tersebut (Mahendra dkk, 2022:2). Selain itu, perlu diperhatikan bahwa evolusi teknologi juga berdampak pada pengembangan metode penyerangan, sehingga perlindungan terhadap media penyimpanan dan distribusi data harus terus disesuaikan dan diperbarui agar dapat menghadapi ancaman yang semakin canggih.

Rumusan masalah penelitian ini berfokus pada permasalahan seputar penyebaran virus komputer dan keamanan data komputer sebagai aspek penting dalam karya sastra. Penelitian akan mengeksplorasi bagaimana karya sastra, khususnya novel "Spammer" karya Ronny Mailindra, menggambarkan permasalahan ini dan bagaimana upaya keamanan komputer dihadapi oleh tokoh-tokoh dalam cerita. Pertanyaan-pertanyaan yang muncul mencakup aspek bagaimana virus komputer direpresentasikan dalam konteks sastra, bagaimana penyebarannya dipaparkan dalam novel, dan bagaimana karakter-karakter dalam cerita merespon serta menghadapi tantangan keamanan data komputer. Melalui metode hermeneutika, penelitian ini akan menjelajahi dan menginterpretasi kedalaman cerita untuk memahami implikasi isu-isu keamanan digital dalam karya sastra tersebut.

KAJIAN TEORITIS

Pallinggi dan Allolinggi (2020:186) menyatakan bahwa untuk menjamin keamanan internet dari masing-masing pengguna sangat sulit untuk diwujudkan. Hal ini dikarenakan jaringan internet sebagai media komunikasi maupun transaksi masih banyak menggunakan jaringan umum. Dengan peningkatan keterampilan penyerang dan kerumitan teknik yang digunakan, melindungi sistem komputer dari ancaman semacam ini menjadi semakin penting dalam menjaga keamanan data dan informasi sensitif.

Virus komputer merupakan sebuah program atau aplikasi yang dapat menyusup pada sistem komputer yang bertujuan untuk mengubah, merusak, menghapus data, dan mengganti program komputer tersebut (Kurniawan, 2020:2). Dalam konteks keamanan komputer, perlindungan terhadap ancaman virus menjadi suatu keharusan, dan upaya pencegahan melalui penggunaan perangkat lunak antivirus serta praktik keamanan digital yang baik sangat diperlukan. Melibatkan pengguna komputer dalam pemahaman tentang praktik keamanan yang tepat juga menjadi kunci dalam menanggulangi risiko terkait dengan potensi serangan virus komputer.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah pendekatan deskriptif untuk mengumpulkan data kualitatif dari teks yang telah menjalani proses pembacaan dan pencatatan. Objek penelitian ini adalah Virus dan Keamanan Komputer, dengan fokus penelitian pada novel Spammer karya Ronny Mailindra. Novel tersebut diterbitkan oleh PT. Bentang Pustaka dan memiliki ketebalan 316 halaman. Pendekatan metodologis yang digunakan dalam penelitian adalah hermeneutika, yang memungkinkan penafsiran mendalam terhadap elemen-elemen dalam teks dengan mempertimbangkan konteks, makna, dan implikasi yang terkandung di dalamnya.

HASIL DAN PEMBAHASAN

Dalam pembahasan ini, akan dianalisis lebih lanjut bagaimana isu-isu terkait dengan penyebaran virus komputer dan keamanan komputer tercermin dalam novel *Spammer* karya Ronny Mailindra.

Dalam era digital yang semakin kompleks, kekhawatiran akan keamanan dan privasi individu telah menjadi perhatian utama. Semakin banyak data pribadi yang disimpan dan dipertukarkan secara *online*, muncul tantangan baru dalam menjaga informasi pribadi dari ancaman seperti peretasan dan pelanggaran data. Peningkatan kesadaran tentang pentingnya privasi *online* telah mendorong upaya untuk mengembangkan kebijakan dan teknologi yang lebih aman, seperti enkripsi *end-to-end* dan alat pengamanan data. Seiring teknologi terus berkembang, upaya untuk menjaga keamanan dan privasi individu akan tetap menjadi prioritas dalam dunia digital yang terus berubah.

Ponsel Antisadap

Dalam era ketidakpastian keamanan digital dan ancaman penyadapan yang merajalela, kekhawatiran akan privasi individu semakin mendalam. Perkembangan teknologi informasi dan kasus-kasus pengawasan oleh negara-negara besar, seperti Amerika Serikat dan Australia, telah memunculkan inovasi baru dalam bentuk ponsel antisadap. Ponsel ini dirancang sebagai langkah proaktif untuk melindungi privasi individu dari potensi ancaman tersebut.

> *Aven juga menekankan bahwa rakyat pasti akan mendukung proyek ponsel antisadap ini, setelah kasus penyadapan yang dilakukan oleh Amerika Serikat dan Australia terhadap presiden dan para petinggi terbongkar.*
>
> (Mailindra,2016:28)

Dalam teks yang dikutip, ditekankan bahwa ada suatu proyek yang disebut sebagai ponsel antisadap yang dirancang untuk melindungi individu dari penyadapan atau pengawasan yang tidak sah. Klaim tersebut juga menyatakan bahwa rakyat diharapkan akan mendukung proyek ini, terutama setelah terungkapnya kasus penyadapan yang dilakukan oleh Amerika Serikat dan Australia terhadap presiden dan para petinggi. Pernyataan ini mencerminkan kekhawatiran akan keamanan digital dan privasi dalam konteks pengawasan oleh pihak asing, serta upaya untuk menawarkan solusi teknologi untuk masalah tersebut.

Pengembangan ponsel antisadap yang disebutkan dalam kutipan sebelumnya merupakan respons terhadap meningkatnya kekhawatiran akan keamanan digital dan privasi, terutama dalam konteks pengawasan oleh pihak asing. Upaya untuk memberikan solusi teknologi dalam hal ini mencerminkan dorongan untuk mengatasi ancaman terhadap privasi individu di era digital yang semakin kompleks.

Trojan

Ketika ketergantungan pada teknologi informasi semakin merajalela, keamanan digital menjadi suatu aspek yang krusial. Ancaman-ancaman seperti virus dan *trojan* tidak hanya merugikan dalam konteks kerusakan data, tetapi juga membuka celah terhadap pelanggaran privasi individu. Seiring kompleksitas dunia digital yang terus berkembang, pemahaman mendalam mengenai keamanan menjadi semakin penting untuk melindungi pengguna dari potensi kerugian yang dapat disebabkan oleh tindakan iseng maupun serangan yang lebih serius.

> *"Biasalah, Pak. Kerjaan orang iseng. Sepertinya virus dan trojan itu mencuri file-file yang ada di laptop Bapak..."*
>
> (Mailindra,2016:57)

Percakapan tersebut mengindikasikan bahwa penggunaan virus atau *trojan* dalam konteks ini mungkin dilakukan oleh seseorang atau kelompok orang yang melakukan tindakan tersebut tanpa maksud yang merugikan. Namun, pernyataan tersebut juga mengungkapkan kekhawatiran bahwa virus dan *trojan* mungkin telah mencuri file-file dari laptop pemilik yang menunjukkan potensi kerugian data pribadi atau informasi sensitif. *Trojan* merupakan salah satu *malware*, dimana masuknya sebuah *malware* ke dalam sistem dapat melalui berbagai macam cara, seperti disisipkan pada sebuah file atau aplikasi tertentu, sehingga korban tidak menyadari bahwa komputernya telah disusupi sebuah *malware* (Siddiq dkk, 2020:161).

Spam

Dalam era ketergantungan pada teknologi informasi, salah satu ancaman yang semakin meresahkan adalah peningkatan kasus spam elektronik atau email spam. Keamanan digital menjadi fokus utama, terutama ketika dihadapkan pada risiko yang diakibatkan oleh serangan virus dan trojan. Fenomena spam elektronik menambah kompleksitas tantangan keamanan, dengan munculnya upaya berbagai pihak untuk mencuri informasi melalui praktik yang merugikan pengguna.

> *". . . Biasanya, virus dan trojan jenis ini cuma mencari alamat email dan menggunakan laptop Bapak untuk mengirimkan spam."*
>
> (Mailindra,2016:57)

Teks di atas menjelaskan bahwa virus dan *trojan* jenis ini biasanya hanya mencari alamat email dan menggunakan laptop seseorang untuk mengirimkan *spam*. Ini mengindikasikan tindakan yang dilakukan oleh jenis *malware* tertentu yang menggunakan alamat email yang ditemukan pada laptop untuk mengirimkan pesan-pesan spam yang tidak diinginkan. Email spam, sering disebut sebagai surat spam, pesan sampah, atau hanya spam, adalah istilah yang digunakan untuk menggambarkan pengiriman besar-besaran pesan iklan yang tidak diinginkan melalui email (Sabry, 2023:1). Pengetahuan tentang risiko keamanan digital dan tindakan pencegahan terhadap malware serta spam menjadi penting dalam upaya melindungi data dan privasi di era teknologi informasi.

Virus

Dalam era digital, penting bagi kita untuk memiliki pemahaman mendalam tentang cara kerja virus komputer. Penerapan langkah-langkah keamanan siber menjadi suatu keharusan agar kita dapat melindungi sistem dan informasi yang kita gunakan setiap hari. Keberhasilan upaya ini akan menentukan keamanan dan integritas data di lingkungan teknologi informasi kita.

> *Selain rawan penyalahgunaan, dokumen-dokumen digital tersebut rentan terinfeksi virus. Jika sudah tertular, lalu dibawa ke komputer lain, komputer lain tersebut juga akan ikut tertular.*
>
> (Mailindra,2016:107)

Dari kalimat tersebut, ditekankan bahwa dokumen-dokumen digital memiliki kerentanan terhadap infeksi virus, yang dapat merusak sistem komputer. Pernyataan ini juga menggambarkan konsekuensi dari penyebaran virus melalui dokumen digital yang sudah

terinfeksi, di mana komputer lain yang menerima dokumen tersebut juga dapat terinfeksi. Ini menggarisbawahi pentingnya pemahaman dan praktik keamanan digital yang efektif untuk mencegah infeksi virus dan menjaga integritas data digital. Kesadaran tentang risiko dan upaya perlindungan data digital menjadi esensial dalam upaya melindungi sistem dan perangkat dari ancaman virus yang dapat merusak atau mencuri informasi. Salah satu upaya yang bisa dilakukan adalah pastikan untuk memverifikasi sumber email terlebih dahulu dan hindari membuka lampiran yang mencurigakan dalam email yang tidak dikenal atau tidak diharapkan (Hartono, 2023:59).

Jejak Digital

Setiap klik, pencarian, atau unggahan memberikan jejak yang membentuk gambaran digital dari kehidupan dan preferensi seseorang. Dalam era di mana teknologi dan konektivitas melibatkan kita dalam berbagai platform, jejak digital menjadi semacam warisan digital yang mencatat perjalanan kita di dunia virtual. Meskipun memberikan kemudahan dan aksesibilitas, jejak digital juga membawa implikasi terhadap privasi dan keamanan data.

> *Ini ajaib. Jika seseorang pernah online dan meninggalkan jejak di internet, situs-situs itu pasti ingat.*
>
> (Mailindra,2016:109)

Kutipan ini menggambarkan realitas bahwa setiap tindakan *online* yang kita lakukan meninggalkan jejak digital yang dapat diingat oleh situs-situs web dan platform *online*. Jejak digital ini mencakup informasi, aktivitas, dan interaksi yang tersimpan dalam berbagai bentuk, seperti data pencarian, riwayat penjelajahan web, dan aktivitas media sosial. Jejak digital, yang juga dikenal sebagai digital footprint, merujuk pada data-data yang tersisa setelah melakukan aktivitas di internet. Ini adalah cara di mana platform media sosial memungkinkan pengguna untuk dengan mudah mengakses berbagai fitur dan layanan. Bahkan tindakan sehari-hari seperti mengirim email, menjelajahi situs web, atau berbagi konten di media sosial dapat menciptakan jejak digital yang bersifat permanen (Setiawan dkk, 2022:125).

Fenomena ini menggarisbawahi pentingnya kesadaran akan privasi dan pengelolaan informasi pribadi di era digital, karena informasi yang kita tinggalkan di internet dapat memiliki implikasi jangka panjang dan dapat diakses oleh berbagai pihak. Selain itu, pernyataan ini mengingatkan kita tentang kompleksitas dunia *online* yang terus berkembang, yang membutuhkan pemahaman dan pengelolaan yang cermat terhadap jejak digital yang kita tinggalkan.

Remote SSH

Remote SSH telah menjadi elemen krusial dalam lingkup kerja jarak jauh dan pengelolaan sistem. Sebagai protokol koneksi yang aman, Remote SSH memfasilitasi akses ke perangkat atau server dari lokasi yang berjauhan. Dengan keamanan terenkripsi yang diberikan, Remote SSH memberikan kenyamanan dan fleksibilitas bagi pengguna untuk mengelola infrastruktur teknologi dari mana saja di dunia.

> *Vergis lalu menyalakan remote SSH-sebuah aplikasi komputer untuk berkomunikasi secara aman dengan mesin lain melalui jaringan dan internet.*
>
> (Mailindra,2016:116)

Dalam kutipan ini, disebutkan bahwa "Vergis" mengaktifkan *Remote SSH*, sebuah aplikasi komputer yang digunakan untuk berkomunikasi dengan mesin lain melalui jaringan dan internet secara aman. *Secure Socket Shell* (SSH) adalah sebuah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan (Desmira dan Wiryadinata, 2022:29). *Remote SSH*, yang merujuk pada protokol keamanan *Secure Shell*, memungkinkan pengguna untuk mengakses dan mengelola mesin jarak jauh dengan keamanan tinggi. Penggunaan *Remote SSH* adalah solusi yang umum digunakan untuk mengamankan akses dan komunikasi dengan mesin atau server di lingkungan digital.

Firewall

Firewall berperan dalam mencegah akses yang tidak sah, serangan malware, dan aktivitas berbahaya lainnya dengan menerapkan aturan dan kebijakan tertentu. Di tengah meningkatnya konektivitas digital, firewall menjadi elemen esensial dalam strategi keamanan siber, berkontribusi secara signifikan dalam menjaga integritas jaringan. Perlindungan informasi sensitif menjadi fokus utama firewall dalam menghadapi ancaman keamanan yang terus berkembang di lingkungan online.

> *Aktivitas program itu bisa lolos karena komputer yang dipakai buruannya tidak mempunyai firewall-tembok api, benteng pencegah koneksi yang tidak diinginkan.*
>
> (Mailindra,2016:153)

Kutipan teks di atas memberikan gambaran bahwa aktivitas program yang berusaha lolos berhasil karena komputer target yang digunakan tidak memiliki *firewall* yang merupakan komponen kunci dalam keamanan jaringan. Firewall merupakan suatu sistem yang dirancang untuk menjaga jaringan komputer dari serangan yang berasal dari luar jaringan (Ferguson dan Huston, 1998 dalam Setiawan dkk, 2023:214). Ketiadaan *firewall* pada komputer target

membuatnya rentan terhadap aktivitas program yang mencoba masuk tanpa hambatan. Kesadaran tentang pentingnya penggunaan *firewall* dalam melindungi sistem komputer dan jaringan menjadi penting dalam mengurangi risiko ancaman digital dan menjaga keamanan data serta integritas jaringan.

KESIMPULAN DAN SARAN

Dalam era teknologi yang terus berkembang, keamanan komputer dan ancaman virus menjadi fokus utama. Karya sastra "Spammer" karya Ronny Mailindra menggambarkan kompleksitas isu keamanan komputer dan respons terhadap virus komputer. Keberadaan virus komputer tidak hanya mengancam keamanan data dan sistem, tetapi juga menuntut pendekatan komprehensif dalam penanganannya. Penelitian ini menggarisbawahi pentingnya memahami isu-isu keamanan komputer yang tercermin dalam karya sastra, sebagai sarana untuk menyampaikan pesan tentang dampak dan tantangan dalam dunia teknologi.

Meskipun penelitian ini memberikan wawasan yang berharga tentang novel "Spammer" karya Ronny Mailindra, terdapat kekurangan dalam analisis yang dapat ditingkatkan. Rekomendasi untuk peneliti berikutnya yang akan meneliti "Spammer" adalah mempertimbangkan penerapan teori-teori tambahan, selain yang telah digunakan, untuk menggali aspek-aspek yang lebih kompleks terkait keamanan komputer yang mungkin belum tercakup sepenuhnya. Dengan memasukkan perspektif teoritis yang beragam, penelitian dapat menawarkan interpretasi yang lebih kaya dan menyeluruh terhadap isu-isu keamanan komputer yang dihadirkan dalam novel tersebut.

DAFTAR REFERENSI

Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking. Jurnal Ilmu Komputer dan Sistem Informasi, 28-33. https://doi.org/10.55338/jikomsi.v5i1.242

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. Bincang Sains dan Teknologi, 55-62. https://doi.org/10.56741/bst.v2i02.353

Kurniawan, D. (2020). Membasmi Virus Komputer dan Android. Jakarta: PT Elex Media Komputindo.

Mahendra, G. S., Wali, M., Idwan, H., Listartha, I. M., Yuliastuti, G. E., Sasongko, D., Saskara G. A. J., Alfina. (2022). Keamanan Komputer. Jakarta Selatan: PT Galiono Digdaya Kawthar.

Mailindra, R. (2016). Spammer. Yogyakarta: PT Bentang Pustaka.

Palinggi, S., & Allolinggi, L. R. (2020). Analisa Deskriptif Industri Fintech di Indonesia: Regulasi dan Keamanan Jaringan dalam Perspektif Teknologi Digital. Jurnal Ekonomi dan Bisnis, 177-192.

Permana, A. A., Hayati, N., Abdurrasyid, Wijayanti, R. R., Botutihe, M. H., Irmawati, Adhicandra, I., Putra, Y., Rukmana, A. Y., Pomalingo, S., Khadafi, S., Irawan, A. S. Y., Jarwo. (2023). KEAMANAN INFORMASI. Get Press Indonesia.

Riadi, I., Yudhana, A., & W., Y. (2019). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 853-860.

Sabry, F. (2023). Email Spam: Fundamentals and Applications. One Billion Knowledgeable.

Setiawan, I., Rusydi, I., Rahmawati, A., & Hasanah, S. (2022). JEJAK DIGITAL SEBAGAI ALAT BUKTI PETUNJUK MENURUT PASAL 184 KITAB UNDANG UNDANG HUKUM ACARA PIDANA. Jurnal Ilmiah Galuh Justisi, 119-132. http://dx.doi.org/10.25157/justisi.v10i1.7236

Siddiq, A., Yudiastuti, H., & Panjaitan, F. (2020). Analisis Perilaku Malware Dengan Metode Surface Analysis Dan Runtime Analysis. Journal of Software Engineering Ampera, 160-174. https://doi.org/10.51519/journalsea.v1i3.53