Bincang Sains dan Teknologi (BST) **E-ISSN 2961-8746**
DOI: 10.56741/bst.v2i02.353 **P-ISSN 2961-8932**

Ransomware: Memahami Ancaman Keamanan Digital

[1]Budi Hartono *
Corresponding Author: *mybdhart@solusipintar.com
[1] Amartaraya Solusi Utama, Jakarta, Indonesia

Abstrak

Ransomware merupakan jenis perangkat lunak berbahaya yang mengenkripsi data dan menuntut pembayaran tebusan. Ancaman ransomware telah menyebabkan kerugian finansial yang signifikan dan mengganggu operasi bisnis serta individu. Kasus-kasus ransomware terkenal seperti WannaCry, NotPetya, GandCrab, Ryuk, dan REvil/Sodinokibi telah menunjukkan dampak negatif dari serangan tersebut. Dalam kajian ini dijelaskan pengertian ransomware, beberapa kasus terkenal yang terjadi di masa lalu, serta uraian cara kerja ransomware. Dijelaskan pula langkah-langkah pencegahan yang dapat diambil untuk melindungi diri dari serangan ransomware, seperti melakukan pencadangan data, memperbarui perangkat lunak, menggunakan solusi keamanan yang kuat, dan meningkatkan kesadaran pengguna. Dengan mengambil langkah-langkah pencegahan yang tepat, individu dan organisasi dapat meningkatkan keamanan sistem mereka dan mengurangi risiko terkena serangan ransomware. Penting untuk memahami ancaman ransomware dan mengimplementasikan tindakan pencegahan yang diperlukan guna melindungi data dan menjaga keamanan digital di dunia yang semakin kompleks ini.

Kata kunci: *ancaman keamanan digital, enkripsi data, kesadaran pengguna digital, ransomware*

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 [1]. 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 [2]. Negara lain seperti Rusia dan Turki juga menjadi sasaran utama serangan di sektor perbankan [3].

Serangan ransomware tidak hanya terbatas pada perbankan online, tetapi juga menargetkan sektor lainnya, termasuk perangkat Internet of Things (IoT) [3]. 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 [4]. 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 [5]. 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 [6].

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.

Sekilas Ransomware

Ransomware adalah jenis perangkat lunak berbahaya (malware) yang dirancang untuk mengenkripsi data pada sistem komputer atau perangkat lainnya, dan kemudian menuntut pembayaran tebusan (ransom) kepada korban agar data tersebut dapat dikembalikan atau didekripsi (Lihat Fig. 1). Ransomware umumnya masuk ke dalam sistem melalui tautan atau lampiran yang mencurigakan dalam email, situs web yang terinfeksi, atau melalui eksploitasi kerentanan dalam perangkat lunak atau sistem operasi [7],[8].

(Source: https://as1.ftcdn.net/v2/jpg/01/69/43/56/1000_F_169435664_wqdoKsEshVHog98XiSDndFzfjCLMBcVy.jpg)

Fig. 1. Ilustrasi Ransomware

Ransomware menjadi salah satu ancaman keamanan yang signifikan karena dapat menyebabkan kerugian finansial yang besar dan mengganggu operasi bisnis atau individu. Beberapa varian ransomware juga mungkin memiliki kemampuan untuk menyebar ke jaringan lain di dalam organisasi atau mengunci seluruh sistem, yang dapat membuat dampaknya semakin parah.

Kasus Ransomware

Ada beberapa kasus terkenal ransomware yang telah terjadi dalam beberapa tahun terakhir. Berikut adalah beberapa contoh kasus ransomware yang signifikan:

1. WannaCry: Pada tahun 2017, serangan ransomware WannaCry menyerang ribuan organisasi di seluruh dunia. Ransomware ini mengeksploitasi kerentanan dalam sistem operasi Windows yang tidak diperbarui dan menyebar dengan cepat melalui jaringan. Serangan ini mengenkripsi data dan menuntut pembayaran tebusan dalam Bitcoin [9].
2. NotPetya: Pada tahun 2017, serangan ransomware NotPetya menargetkan perusahaan-perusahaan besar di seluruh dunia, termasuk Ukraina, di mana serangan itu pertama kali dimulai. NotPetya menggunakan metode yang sama dengan WannaCry, yaitu memanfaatkan kerentanan dalam sistem operasi Windows. Namun, NotPetya sebenarnya lebih merupakan serangan perusak daripada upaya pemerasan, karena tidak memberikan kemungkinan dekripsi setelah pembayaran tebusan [10].
3. GandCrab: GandCrab merupakan salah satu keluarga ransomware yang aktif antara tahun 2018 dan 2019. Ransomware ini menyebar melalui kampanye spam email dan exploit kit [11]. GandCrab mengenkripsi data korban dan menuntut pembayaran tebusan dalam bentuk mata uang kripto. Meskipun operasi GandCrab telah dihentikan setelah para peneliti keamanan berhasil memecahkan algoritma enkripsinya, ransomware ini telah menimbulkan kerugian finansial yang signifikan [12].
4. Ryuk: Ransomware Ryuk pertama kali muncul pada tahun 2018 dan telah menyerang banyak organisasi, terutama dalam sektor keuangan dan kesehatan [13]. Serangan ini biasanya dimulai

dengan infeksi awal menggunakan Trojan Emotet atau TrickBot. Ryuk kemudian mengenkripsi data dan menuntut pembayaran tebusan yang besar dalam Bitcoin [14].

5. REvil/Sodinokibi: Ransomware REvil atau Sodinokibi adalah keluarga ransomware yang telah aktif sejak 2019 [15]. Serangan ini sering kali ditujukan pada perusahaan besar dan penyedia layanan TI. REvil mengenkripsi data dan meminta pembayaran tebusan dalam bentuk Bitcoin. Ransomware ini juga dikenal karena melakukan praktik "double extortion", yaitu mencuri data sebelum mengenkripsi dan mengancam untuk mempublikasikannya jika tebusan tidak dibayar [16].

Kasus-kasus tersebut hanya merupakan contoh dari banyak serangan ransomware yang terjadi secara global. Penting bagi organisasi dan individu untuk tetap waspada terhadap ancaman ransomware dan mengambil langkah-langkah keamanan yang tepat untuk melindungi data mereka.

Cara Kerja Ransomware

Ransomware adalah jenis perangkat lunak berbahaya yang mengenkripsi data pada sistem komputer atau perangkat lainnya, lalu menuntut pembayaran tebusan agar data tersebut dapat dikembalikan atau didekripsi. Cara kerja ransomware umumnya melibatkan beberapa langkah. Pertama, ransomware masuk ke dalam sistem korban melalui tautan atau lampiran yang mencurigakan dalam email, situs web yang terinfeksi, atau melalui eksploitasi kerentanan dalam perangkat lunak atau sistem operasi. Setelah masuk, ransomware mulai mengenkripsi data dengan menggunakan algoritma enkripsi yang kuat, sehingga data tidak dapat diakses oleh pemiliknya. Kemudian, ransomware menampilkan pesan tebusan yang berisi instruksi kepada korban untuk membayar tebusan, biasanya dalam bentuk mata uang kripto seperti Bitcoin, sebagai syarat untuk mendapatkan kunci dekripsi yang diperlukan untuk mengembalikan data [17]. Berikut adalah langkah-langkah umum cara kerja ransomware:

1. Infeksi awal: Ransomware biasanya masuk ke dalam sistem melalui beberapa metode, termasuk tautan atau lampiran berbahaya dalam email phishing, situs web yang terinfeksi, atau menggunakan eksploitasi kerentanan dalam perangkat lunak atau sistem operasi yang tidak diperbarui. Infeksi awal sering kali terjadi ketika pengguna tidak menyadari atau tidak berhati-hati saat berinteraksi dengan konten berbahaya.
2. Penyebaran: Setelah berhasil memasuki sistem target, ransomware akan berusaha menyebar ke perangkat lain dalam jaringan yang terhubung. Ini dapat dilakukan dengan memanfaatkan kerentanan dalam sistem atau menggunakan metode seperti memanfaatkan password yang lemah atau konfigurasi jaringan yang tidak aman.
3. Enkripsi data: Setelah ransomware menyebar, langkah berikutnya adalah mengenkripsi data yang ada di sistem atau perangkat target. Ransomware akan mengenkripsi file dengan menggunakan algoritma enkripsi yang kuat dan membuat file tersebut tidak dapat diakses oleh pemiliknya. Proses enkripsi ini dapat mempengaruhi berbagai jenis file, termasuk dokumen, gambar, video, dan file penting lainnya.
4. Peringatan atau pesan tebusan: Setelah selesai mengenkripsi data, ransomware akan menampilkan pesan atau peringatan pada layar korban. Pesan ini akan memberi tahu

korban bahwa data mereka telah dienkripsi dan menuntut pembayaran tebusan agar kunci dekripsi diberikan. Pesan ini biasanya berisi instruksi tentang cara membayar tebusan, termasuk alamat dompet Bitcoin atau instruksi lainnya.

5. Pembayaran tebusan: Ransomware biasanya menuntut pembayaran tebusan dalam bentuk mata uang kripto seperti Bitcoin, Ethereum, atau Monero. Pembayaran ini dimaksudkan untuk membuat transaksi sulit dilacak dan meningkatkan anonimitas penyerang. Namun, penting untuk dicatat bahwa tidak ada jaminan bahwa data akan dikembalikan setelah pembayaran tebusan dilakukan.

Penting untuk diingat bahwa membayar tebusan tidak dijamin akan mengembalikan data dan dapat mendorong kegiatan kriminal lebih lanjut. Penanganan kasus ransomware sebaiknya melibatkan pihak berwenang dan langkah-langkah pencegahan yang tepat harus diambil untuk melindungi sistem dan data dari serangan ransomware.

Antisipasi Ransomware

Ransomware merupakan ancaman serius dalam dunia digital yang dapat menyebabkan kerugian finansial dan kerugian data yang signifikan. Oleh karena itu, penting bagi individu dan organisasi untuk mengambil langkah-langkah pencegahan guna melindungi diri mereka dari serangan ransomware. Beberapa langkah yang dapat diambil untuk mengantisipasi ransomware [18]-[21].

Penerapan langkah-langkah pencegahan dapat membantu individu dan organisasi untuk mengurangi risiko terhadap serangan ransomware. Namun, penting juga untuk tetap waspada dan mengikuti perkembangan terkini dalam keamanan digital guna memastikan perlindungan yang optimal. Untuk mengantisipasi serangan ransomware, berikut adalah beberapa langkah pencegahan yang dapat diambil:

1. Backup data secara teratur: Lakukan pencadangan data penting secara teratur ke lokasi yang terpisah dan aman, seperti penyimpanan eksternal atau cloud. Pastikan pencadangan dilakukan secara otomatis dan diverifikasi keabsahannya. Dengan melakukan ini, Anda memiliki salinan data yang dapat dipulihkan jika terjadi serangan ransomware.
2. Perbarui perangkat lunak dan sistem operasi: Pastikan sistem operasi, perangkat lunak aplikasi, dan perangkat keras yang digunakan selalu diperbarui dengan rilis terbaru. Perbarui secara teratur agar kerentanan yang diketahui dapat diperbaiki dan mencegah eksploitasi yang memungkinkan ransomware masuk.
3. Gunakan solusi keamanan yang kuat: Instal perangkat lunak keamanan yang terpercaya, seperti antivirus, antispyware, dan firewall. Pastikan perangkat lunak ini diperbarui secara teratur dengan definisi virus terbaru untuk mendeteksi dan menghalangi ancaman ransomware.
4. Waspadai email dan tautan yang mencurigakan: Jangan mengklik tautan atau membuka lampiran yang mencurigakan dalam email yang tidak dikenal atau tidak diharapkan. Verifikasi sumber email terlebih dahulu sebelum mengambil tindakan. Hindari mengklik tautan yang tidak dipercaya atau mencurigakan di situs web yang tidak terpercaya.

5. Gunakan sandi yang kuat dan unik: Gunakan kata sandi yang kompleks, terdiri dari kombinasi huruf, angka, dan karakter khusus. Hindari menggunakan kata sandi yang mudah ditebak atau umum. Gunakan manajer kata sandi untuk mengelola sandi yang kuat dan unik untuk setiap akun yang Anda miliki.
6. Batasi hak akses: Berikan hak akses yang sesuai kepada pengguna dan kelompok pengguna. Batasi akses administrator hanya kepada mereka yang membutuhkannya. Ini akan membantu mencegah penyebaran ransomware dari akun yang terbatas.
7. Perhatikan pembaruan firmware: Selain memperbarui perangkat lunak, penting juga untuk memperbarui firmware perangkat keras seperti router, switch, dan perangkat jaringan lainnya. Firmware yang diperbarui dapat membantu melindungi perangkat keras dari kerentanan yang dapat dimanfaatkan oleh ransomware.
8. Tingkatkan kesadaran pengguna: Berikan pelatihan dan edukasi kepada pengguna tentang praktik keamanan digital yang aman. Ajarkan mereka untuk tidak mengklik tautan atau membuka lampiran yang mencurigakan, serta pentingnya melaporkan aktivitas yang mencurigakan kepada tim keamanan.
9. Gunakan firewall dan filter lalu lintas: Aktifkan firewall pada perangkat jaringan Anda dan gunakan filter lalu lintas untuk membatasi akses ke situs web berbahaya atau mencurigakan yang dapat menjadi sumber infeksi ransomware.
10. Monitor dan deteksi ancaman: Implementasikan sistem pemantauan dan deteksi ancaman yang kuat untuk mengmengidentifikasi dan menangani serangan ransomware secepat mungkin. Gunakan perangkat lunak atau solusi deteksi ancaman yang canggih untuk mendeteksi perilaku atau pola yang mencurigakan dari ransomware.

Dengan mengambil langkah-langkah pencegahan ini, maka dapat ditingkatkan keamanan sistem dan mengurangi risiko terkena serangan ransomware. Tetap mengikuti praktik keamanan yang baik dan tetap waspada terhadap ancaman yang mungkin muncul akan membantu melindungi data dari serangan ransomware.

Kesimpulan

Ransomware merupakan ancaman serius dalam dunia digital yang dapat menyebabkan kerugian finansial dan gangguan operasional yang signifikan bagi individu dan organisasi. Kasus-kasus ransomware terkenal seperti WannaCry, NotPetya, GandCrab, Ryuk, dan REvil/Sodinokibi telah memperlihatkan dampak yang merugikan dari serangan ini. Ransomware dapat mengenkripsi data penting dan menuntut pembayaran tebusan dalam bentuk mata uang kripto, seringkali Bitcoin. Penting bagi organisasi dan individu untuk mengambil langkah-langkah pencegahan yang tepat guna melindungi diri dari serangan ransomware. Beberapa langkah yang dapat diambil termasuk melakukan pencadangan data secara teratur, memperbarui perangkat lunak dan sistem operasi, menggunakan solusi keamanan yang kuat, waspada terhadap email dan tautan mencurigakan, menggunakan sandi yang kuat dan unik, membatasi hak akses, memperbarui firmware perangkat keras, meningkatkan kesadaran pengguna, menggunakan firewall dan filter lalu lintas, serta mengimplementasikan sistem pemantauan dan deteksi ancaman yang canggih.

Referensi

[1] Fakta-Fakta BSI Kena Serangan Siber Kelompok Ransomware Lockbit. Natasha Khairunisa AmaniNatasha Khairunisa Amani. Diperbarui 16 Mei 2023, 18:50 WIB. https://www.liputan6.com/bisnis/read/5288741/fakta-fakta-bsi-kena-serangan-siber-kelompok-ransomware-lockbit
[2] Sharma, P., Zawar, S., & Patil, S.B. (2016). Ransomware analysis: Internet of things (IoT) security issues, challenges and open problems in the context of worldwide scenario of security of systems. Retrieved from http://ijirse.com.
[3] Farhat, D., & Awan, M.S. (2021). A brief survey on ransomware with the perspective of internet security threat reports. In Proceedings of the 2021 International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
[4] Custers, B.H.M., Pool, R.L.D., et al. (2019). Banking malware and the laundering of its profits. European Journal of Criminology, 16(6), 651-671. Retrieved from journals.sagepub.com.
[5] Wilner, A., Jeffery, A., Lalor, J., Matthews, K., et al. (2019). On the social science of ransomware: Technology, security, and society. Comparative Sociology, 18(2), 215-242. Retrieved from Taylor & Francis.
[6] Wazid, M., Zeadally, S., & Das, A.K. (2019). Mobile banking: evolution and threats: malware threats and security solutions. IEEE Consumer Electronics Magazine, 8(6), 72-81. Retrieved from ieeexplore.ieee.org.
[7] Kaspersky. (2021). Ransomware. Diakses pada 20 Mei 2023, dari https://www.kaspersky.com/resource-center/definitions/what-is-ransomware
[8] US-CERT. (2016). Ransomware. Diakses pada 20 Mei 2023, dari https://www.us-cert.gov/Ransomware
[9] Kaspersky. (2021). WannaCry ransomware. Diakses pada 20 Mei 2023, dari https://www.kaspersky.com/resource-center/threats/wannacry-ransomware
[10] Cisco Talos. (2017). Threat Spotlight: NotPetya. Diakses pada 20 Mei 2023, dari https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html
[11] Liao, H., Wang, W., Qiu, M., & Li, J. (2018). Dissecting GandCrab: Unveiling the TTPs of the most popular Ransomware in 2018. Diakses pada 20 Mei 2023, dari https://ieeexplore.ieee.org/document/8553856
[12] Europol. (2019). Internet Organized Crime Threat Assessment (IOCTA) 2019. Diakses pada 20 Mei 2023, dari https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019
[13] CrowdStrike. (2019). 2019 CrowdStrike Global Threat Report. Diakses pada 20 Mei 2023, dari https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
[14] Dienst, S. (2019). What is Ryuk Ransomware? How to Prevent Ryuk Ransomware Attacks. Diakses pada 20 Mei 2023, dari https://heimdalsecurity.com/blog/ryuk-ransomware/
[15] Trend Micro. (2021). Ransomware REvil/Sodinokibi. Diakses pada 20 Mei 2023, dari https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/revil-sodinokibi-ransomware-threat-and-mitigation-strategies
[16] Arditama, Y. (2020). REvil Ransomware: Mengguncang Dunia Digital dengan Model Ransomware "Double Extortion". Diakses pada 20 Mei 2023, dari https://www.netskope.com/blog/revil-ransomware-mengguncang-dunia-digital-dengan-model-ransomware-double-extortion
[17] Reilly, K. (2020). Understanding Ransomware: How it Works and How to Prevent It. Retrieved May 20, 2023, from https://heimdalsecurity.com/blog/what-is-ransomware/
[18] Cisco. (2020). Protecting Against Ransomware. Retrieved May 20, 2023, from https://www.cisco.com/c/en/us/products/security/ransomware.html
[19] McAfee. (2020). How to Protect Yourself and Your Devices Against Ransomware. Retrieved May 20, 2023, from https://www.mcafee.com/blogs/consumer/how-to-protect-yourself-and-your-devices-against-ransomware/
[20] National Cyber Security Centre. (2021). Ransomware: Recovering Your Files. Retrieved May 20, 2023, from https://www.ncsc.gov.uk/guidance/ransomware-recovering-your-files
[21] US-CERT. (2021). Ransomware Guidance and Resources. Retrieved May 20, 2023, from https://www.us-cert.gov/ncas/tips/ST19-001

Bincang Sains dan Teknologi (BST) **E-ISSN 2961-8746**
DOI: 10.56741/bst.v2i02.353 **P-ISSN 2961-8932**

Penulis

Budi Hartono merupakan praktisi teknologi informati di Solusi Pintar Indonesia, PT. Amartaraya Solusi Utama di Jakarta, Indonesia. Ia adalah alumni dari program sarjana di Teknik Fisika dan program magister di Teknik Informatika, Institut Teknologi Bandung (ITB). Ia memiliki pengetahuan dan keahlian yang luas dalam pengembangan teknologi, dan telah memberikan konsultasi serta berkontribusi dalam pengembangan teknologi di berbagai perusahaan. Ia telah terlibat dalam proyek-proyek penting yang melibatkan implementasi dan pengembangan solusi teknologi informasi. (email: mybdhart@solusipintar.com).