JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 2 No: 8, Agustus 2025
E-ISSN : 3047-7824

RANSOMWARE DI SEKTOR KEUANGAN: STUDI KASUS SERANGAN TERHADAP BSI PADA TAHUN 2023

RANSOMWARE IN THE FINANCIAL SECTOR: A CASE STUDY OF ATTACKS ON BSI IN 2023

Audrey Aulia Putri[1], Hudi Yusuf[2]
Universitas Bung Karno
Email: audreyaulia2003@gmail.com[1], hoedydjoesoef@gmail.com[2]

Article Info

Article history :
Received : 14-08-2025
Revised : 16-08-2025
Accepted : 18-08-2025
Pulished : 20-08-2025

Abstract

The purpose of this study was to determine purchasing decisions influenced by price and promotion at Kierana Indah Residence 2 Housing, Bogor Regency. The method used is the associative descriptive method. Sampling using the saturated sample method in which all populations were sampled, namely 192 respondents. Data analysis using validity tests, reliability tests, classical assumption tests, quantitative analysis, simple correlation analysis and hypothesis tests. The results of the analysis found that price (X_1) has a positive effect on purchasing decisions (Y) and is significant. While promotion (X_2) has a positive effect on purchasing decisions (Y) and is significant. With the equation Y = 23.899 + 0.291 X1 + 0.195 X2 + α. The correlation value of the price and promotion variables is 0.847 (very strong). The coefficient of determination value is 73.3% while the remaining 26.7% is influenced by other factors or variables not studied. The results of the hypothesis obtained the value of F_count > F_table or (22.953 > 3.040) this is strengthened significantly (0.000 < 0.05). So H03 is rejected and Ha3 is accepted. This means that there is a significant influence simultaneously between purchasing decisions influenced by price and promotion at the Kierana Indah Residence 2 Housing, Bogor Regency.

Keywords: Price, Promotion, Purchase Decision

Abstrak

Serangan ransomware terhadap Bank Syariah Indonesia (BSI) pada tahun 2023 merupakan salah satu insiden keamanan siber terbesar di Indonesia. Pada 8 Mei 2023, kelompok hacker LockBit 3.0 berhasil mencuri data pribadi lebih dari 15 juta nasabah BSI, menimbulkan dampak signifikan terhadap kepercayaan publik dan keamanan data di sektor perbankan. Penelitian ini bertujuan untuk menganalisis serangan ransomware terhadap BSI dan dampaknya terhadap loyalitas nasabah. Hasil penelitian menunjukkan bahwa kebocoran data nasabah berpengaruh negatif dan signifikan terhadap loyalitas nasabah, sedangkan kualitas layanan dan kepercayaan berpengaruh positif dan signifikan.

Kata Kunci: Ransomware, Keuangan, BSI

PENDAHULUAN

Ransomware merupakan istilah yang berasal dari kata ransom (Bahasa Inggris) yang jika diubah ke dalam Bahasa Indonesia memiliki arti sebagai tebusan. Sementara kata ware dalam ransomware adalah singkatan yang diambil dari kata software yang diartikan sebagai perangkat lunak. Maka dapat disimpulkan bahwa arti dari kata ransomware adalah perangkat lunak yang

bertujuan untuk meminta tebusan. Secara keseluruhan ransomware memiliki arti sebagai sebuah perangkat lunak yang digunakan untuk melakukan penguncian data sehingga data tersebut tidak dapat diakses dengan tujuan untuk meminta sebuah tebusan.

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.

METODE

Metode penelitian ini adalah metode kualitatif dengan model pendekatan studi kasus. Studi kasus (case study) adalah sebuah model yang memfokuskan eksplorasi “sistem terbatas”

(bounded system) atas satu kasus khusus ataupun pada sebagian kasus secara terperinci dengan penggalian data secara mendalam. Beragam sumber informasi yang kaya akan konteks dilakukan untuk penggalian data.

ANALISIS DAN HASIL

Jenis-jenis Ransomware

Ransomware pertama kali muncul pada awal tahun 1990-an dan dikenal sebagai "AIDS Trojan" atau "PC Cyborg". Ransomware awal ini mengunci akses ke sistem dengan mengenkripsi file dan meminta tebusan dalam bentuk cek yang harus dikirim ke kotak surat tertentu. Namun, ransomware modern yang menggunakan kriptocurrency sebagai metode pembayaran pertama kali muncul pada tahun 2005 dengan munculnya varian ransomware bernama "GpCode". Sejak itu, serangan ransomware telah terus berkembang dan menjadi ancaman serius di dunia digital. Adapun secara umum jenis-jenis ransomware dapat dibedakan menjadi berikut:

1. Encrypting Ransomware, Jenis ini merupakan bentuk yang paling umum dari ransomware. Ransomware ini menggunakan algoritma enkripsi yang kuat untuk mengenkripsi file pengguna sehingga tidak dapat diakses tanpa kunci dekripsi yang benar. Contoh terkenal dari encrypting ransomware adalah WannaCry dan CryptoLocker.
2. Locker Ransomware, berbeda dengan encrypting ransomware, locker ransomware tidak mengenkripsi file, tetapi memblokir akses ke sistem secara keseluruhan. Biasanya, locker ransomware akan menampilkan pesan yang menghalangi pengguna untuk mengakses komputer mereka. Ransomware jenis ini sering kali menyamar sebagai pemberitahuan palsu dari pihak berwenang, seperti kepolisian atau badan keamanan.
3. MBR Ransomware, Ransomware yang menyerang Master Boot Record (MBR) komputer atau perangkat. MBR berperan dalam proses booting sistem operasi, dan ransomware jenis ini akan menggantikan MBR dengan kode yang memblokir akses ke sistem. Hal ini menyebabkan perangkat menjadi tidak dapat digunakan hingga tebusan dibayar atau MBR dikembalikan.
4. Mobile Ransomware, Ransomware yang dirancang khusus untuk menyerang perangkat mobile, seperti smartphone atau tablet. Mobile ransomware dapat mengenkripsi data pada perangkat atau memblokir akses ke aplikasi dan fungsi penting. Salah satu contohnya adalah Android/Filecoder.C, yang menargetkan perangkat Android.
5. Scareware, Ransomware yang menggunakan taktik penipuan dengan menampilkan pesan ancaman palsu kepada pengguna. Pesan ini berisi peringatan palsu tentang pelanggaran hukum atau kegiatan ilegal yang diduga dilakukan oleh pengguna. Tujuannya adalah untuk menakut-nakuti pengguna agar membayar tebusan.

Kejahatan terorganisir dapat mencakup beragam aktivitas kriminal yang mencapai tingkat kompleksitas dan keseriusan tertentu. Kejahatan berbasis pasar biasanya melibatkan penyediaan barang atau jasa ilegal. Kejahatan predator ditandai dengan interaksi yang merugikan antara pelaku dan korban, termasuk kejahatan keuangan (misalnya, penipuan) dan eksploitasi (misalnya, perdagangan manusia). Terakhir, kejahatan regulasi atau tata kelola ditandai dengan penetapan dan

penegakan norma perilaku serta penyelesaian sengketa. Serangan ransomware sangat kompleks, membutuhkan rencana terpadu, beberapa tahapan aktivitas yang saling terkait, dan beragam keahlian khusus. Serangan ransomware seringkali membutuhkan waktu berbulan-bulan untuk diselesaikan. Serangan ransomware merupakan kejahatan berbasis pasar (pengembangan dan penjualan ransomware) dan kejahatan predator (pencurian dan pemerasan). Serangan ini merupakan kejahatan berbasis pasar karena melibatkan pasar gelap untuk barang dan jasa yang banyak diminati (misalnya, kode berbahaya), dan merupakan kejahatan predator karena melibatkan kerugian yang ditimbulkan oleh pelaku kepada korban.

Aktivitas kelompok ransomware lainnya tidak begitu mudah dikarakterisasi dalam kerangka kejahatan terorganisir. Misalnya, serangan Conti terhadap Kosta Rika pada pertengahan 2022 yang disebutkan di atas tampaknya lebih dimotivasi oleh publisitas daripada keuntungan finansial, mungkin juga karena itu adalah serangan terakhir sebelum kelompok tersebut dilaporkan terpecah dan kemudian diluncurkan kembali dalam komponen yang lebih kecil. Demonstrasi kekuatan yang terang-terangan terhadap negara ini tidak berbeda dengan modus operandi kartel narkoba Amerika Tengah dan Selatan yang sering menggunakan tindakan kekerasan spektakuler untuk menunjukkan kekuatan mereka, merongrong legitimasi negara, dan semakin memperkuat posisi mereka dalam ekonomi gelap. Oleh karena itu, aktivitas kelompok ransomware seperti Conti, DarkSide, dan REvil tampaknya analog dengan aktivitas kriminal kelompok kejahatan terorganisir lainnya. Oleh karena itu, kami berpendapat bahwa kelompok ransomware dapat dan harus diperiksa melalui lensa kejahatan terorganisir dan pemeriksaan tersebut akan memperkaya pemahaman kita tentang kelompok-kelompok tersebut.

Cara Kerja Ransomware

Pada 8 Mei 2023 layanan Bank Syariah Indonesia (BSI) tidak dapat diakses. Gangguan layanan berlanjut sampai beberapa hari berikutnya. Nasabah tidak dapat melakukan transaksi baik melalui ATM, maupun aplikasi mobile. Gangguan layanan berlangsung sampai beberapa hari berikutnya. Kelompok hacker ransomware Lockbit mengklaim sebagai penyerang BSI tersebut. Dalam klaimnya, mereka berhasil mencuri 1,5 TB data meliputi database data pribadi lebih dari 15 juta pengguna (meliputi nomor telepon, alamat, saldo, nomor kartu, transaksi dan lainnya), dokumen keuangan, dokumen hukum, NDA, dan password layanan internal dan eksternal yang digunakan bank. Lockbit juga meminta pihak BSI untuk menghubungi para peretas dalam waktu 72 jam untuk menyelesaikan masalah.

LockBit 3.0 dikenal sebagai 'LockBit Black' lebih sulit ditangani daripada versi sebelumnya dan memiliki kemiripan dengan Ransomware Blackmatter dan Blackcat. LockBit 3.0 berfungsi sebagai model Ransomware-as-a-Service (RaaS) sehingga dapat disewakan atau menjalin afiliasi dengan kelompok lain. Lockbit 3 merupakan kelanjutan dari versi ransomware sebelumnya, LockBit 2.0, dan LockBit. Dalam imbauan keamanan dari Cybersecurity & Infrastructure Security Agency (CISA), badan keamanan siber Amerika Serikat, LockBit sebelumnya yang dikenal sebagai ransomware "ABCD" adalah subkelas ransomware yang dikenal sebagai 'crypto virus'. Menurut CISA, LockBit 3.0 hanya akan menginfeksi mesin yang tidak memiliki pengaturan bahasa yang cocok dalam daftar, kecuali telah ditentukan sebelumnya. Daftar pengecualian bahasa yaitu, tapi tidak terbatas pada, Rumania (Moldova), Arab (Suriah), dan Tatar (Rusia). Jika bahasa dari daftar pengecualian terdeteksi, LockBit 3.0 akan menghentikan eksekusi tanpa menginfeksi sistem.

Peneliti keamanan juga telah menemukan jenis dan bukti baru bahwa kelompok yang bertanggung jawab atas LockBit 3.0 berencana memperluas kapasitas infeksi malware. Sementara varian terbaru LockBit 3.0, sebelumnya telah menargetkan server Windows, Linux, dan VMware ESXi, dugaan versi baru dari enkripsi LockBit telah diidentifikasi yang juga dapat memengaruhi macOS, ARM, FreeBSD, MIPS, dan CPU SPARC.

Untuk menginfeksi mesin korban, peretas biasanya melalui eksploitasi protokol desktop jarak jauh (RDP), *drive-by compromise*, serangan phishing, penyalahgunaan akun valid, dan eksploitasi aplikasi yang terkoneksi internet.

Untuk mengonfirmasi lokasi sistem yang ditargetkan, ransomware LockBit menggunakan fungsi:

GetSystemDefaultUILanguage()

GetUserDefaultUILanguage()

Beberapa bahasa yang dikecualikan adalah Rumania (Moldova), Arab (Suriah), dan Tatar (Rusia). Grup Ransomware LockBit pertama kali diamati pada September 2019, menjadi grup ransomware paling aktif tahun 2022.

Payload LockBit 3.0 adalah Windows PE standar sama dengan versi sebelumnya. Payload didesain untuk dieksekusi dengan hak akses administrator, jika belum memiliki hak akses administrator maka akan dicoba untuk membypass nya. Lockbit akan terinstal pada system service, dan setiap eksekusi payload akan menginstal beberapa layanan termasuk SecurityHealthService dan EventLog. Pada versi sevelemnya, LockBit3.0 akan mengidentifikasi dan mematikan layanan yang ditemukan termasuk backup dan sql.

lockbit membutuhkan passphrase tertentu untuk eksekusi yang meuprakan sampel atau kampanye seperti Egregor dan BlackCat.

LockBit mengcopy dirinya pada direktori *%programdata%* dan dijalankan dari proses ini. Enkripsi dilakukan sangat cepat dan dapat menyebar ke host yang berdekatan. Payload ransomware mampu mengenkripsi dalam waktu kurang dari satu menit. Ekstensi ditambahkan pada file baru hasil enkripsi yang juga akan berbeda untuk tiap contoh. Mesin yang terinfekai akan mati kira-kira 10 menit setelah payload ransomware dijalankan. Setelah infeksi selesai, korban diperintahkan untuk menghubungi penyerang melalui portal berbasis TOR.

Konten terenkripsi ada di payload LockBit 3 dan di dekripsi saat runtime dengan XOR mask. LockBit 3.0 juga menyimpan di heap memory kemudian menggunakan trampoline untuk menjalankan fungsi misalnya Windows System memanggil NtSetInformationThread dan ZwProtectVirtualMemory. Selanjutnya ransomware akan mengaburkan alamat dengan *obfuscate.* LockBit mengacak penerapan fungsi DbgUiRemoteBreakin untuk menonaktifkan debugger yang melampirkan proses ransomware.

Upaya Pencegahan

Langkah Pengamanan bagi Nasabah BSI

1. Tetap bersikap tenang karena BSI merupakan bank yang terdaftar sebagai peserta penjaminan pada Lembaga Penjamin Simpanan (LPS) sehingga dana yang disimpan di

BSI dijamin oleh LPS

2. Mengganti kredensial mobile banking, internet banking dan PIN ATM
3. Memantau aktivitas pada rekening untuk mendeteksi apabila terdapat transaksi mencurigakan
4. Jika terdapat aktivitas mencurigakan segera laporkan ke BSI melalui kontak resmi.
5. Waspada terhadap percobaan phishing yang mengatasnamakan BSI dengan modusnya bisa mengatasnamakan *Customer Service.*
6. Melakukan update/pacthing aplikasi perbankan yang di gunakan
7. Menggunakan antivirus/antimalware pada perangkat yang digunakan

Langkah Pengamanan bagi Organisasi

1. Administrator organisasi melakukan updating/ *patching* otomatis pada semua *software* dan *hardware* yang digunakan
2. Menerapkan kebijakan konservatif pada firewall, terapkan sensor dalam setiap sisi
3. Memisahkan DMZ (*demilitarized zone)* yang merupakan pengaman jaringan dari trafik yang tidak tepercaya—dengan intranet
4. Melakukan pembatasan terhadap user yang memiliki akses terhadap data kritikal untuk mengakses internet
5. Selalu buat bakcup (cadangan) data
6. Lakukan simulasi serangan dan menyiapkan rencana tindakan untuk pemulihan insiden
7. Melakukan edukasi kepada pegawai mengenai pentingnya keamanan informasi

Tindakan Pengamanan bagi Masyarakat Umum

1. Menginstal aplikasi hanya dari sumber resmi
2. Tidak mengunjungi situs web berbahaya, mengunduh lampiran berbahaya, atau melalui add-on yang tidak diinginkan selama pengunduhan
3. Menginstal antivirus/antimalware pada perangkat yang digunakan
4. Melakukan update terhadap aplikasi yang digunakan
5. Jangan pernah mengikuti tuntutan dari pelaku kejahatan

KESIMPULAN

Ransomware termasuk dalam kualifikasi tindakan pemerasan dan/atau pengancaman sesuai dengan ketentuan Pasal 27 ayat (4) UU ITE. Tindakan ini dalam Pasal 368 ayat (1) KUHP disebutkan: “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa seorang dengan kekerasan atau ancaman kekerasan untuk memberikan barang sesuatu, yang seluruhnya atau sebagian adalah kepunyaan orang itu atau orang lain, atau supaya membuat hutang maupun menghapuskan piutang, diancam karena pemerasan, dengan pidana penjara paling lamasembilan tahun.”

Unsur-unsur yang ada dalam pasal ini adalah sebagai berikut:

1. Memaksa orang lain;
2. Untuk memberikan barang yang sama sekali atau sebagian termasuk kepunyaan orang itu sendiri atau kepunyaan orang lain, atau membuat utang atau menghapuskan piutang;
3. Dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak;
4. Memaksanya dengan memakai kekerasan atau ancaman kekerasan

Definisi kejahatan Ransomware memenuhi unsur-unsur Pasal 368 Ayat (1) KUHP tersebut diatas. Walaupun terjadi di ruang siber, tidak kasat mata, tindakan ini tetap dianggap nyata dan digolongkan kedalam tindakan pemerasan yang didalamnya terdapat unsur paksaan dan ancaman kekerasan. Paksaan dan ancaman yang di lakukan kepada korban Ransomware, bukan tindakan fisik secara nyata, tetapi dilakukan di ruang siber dengan mengunci data dan meminta uang tebusan melalui email korban. Apabila uang tebusan tidak dibayarkan, maka selamanya korban tidak dapat mengakses datanya. Kekerasan yang diderita korban bukan kekerasan fisik, tetapi kekerasan secara psikologis. Pelaku menekan korban untuk memenuhi tebusan yang diminta sebagai syarat untuk dapat membuka data korban yang telah terkunci.

DAFTAR PUSTAKA

Creswell, J. W. (2015). Penelitian kualitatif & desain riset. Yogyakarta: Pustaka Pelajar.

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.

Fakta-Fakta BSI Kena Serangan Siber Kelompok Ransomware Lockbit. Natasha KhairunisaAmaniNatasha Khairunisa Amani. Diperbarui 16 Mei 2023, 18:50 WIB.

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.

https://www.liputan6.com/bisnis/read/5288741/fakta-fakta-bsi-kena-serangan-siber-kelompok-ransomware-lockbit

James Martin, Reconceptualising organised (cyber)crime: The case of ransomware https://csirt.magelangkota.go.id/posts/mengenal-lockbit-3-0-ransomware-yang-membuat-layanan-bsi-lumpuh

Kevin Anthony, KEJAHATAN PEMERASAN MENGGUNAKAN VIRUS RANSOMWARE DIKAITKAN DENGAN KEJAHATAN ITE

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.

Soesilo, R. (1988). Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal. Bogor: Politeia.

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.

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.