ANALISIS DAN SIMULASI SERANGAN RANSOMWARE TERHADAP DATABASE BANK SYARIAH INDONESIA

ANALYSIS AND SIMULATION OF RANSOMWARE ATTACKS AGAINST THE BANK SYARIAH INDONESIA DATABASE

Rendi Panca Wijanarko[1*], Moch Rezeki Setiawan[1], Siti Mukaromah[1], Abdul Rezha Efrat Najaf [1]
[*]E-mail: rendi.wijanarko03@gmail.com

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Serangan ransomware telah menjadi ancaman yang signifikan dalam lingkungan keamanan komputer, terutama di sektor perbankan. Dalam penelitian ini, kami menganalisis dan mensimulasikan serangan ransomware terhadap *database* Bank Syariah Indonesia (BSI). Tujuan utama dari penelitian ini adalah untuk mengidentifikasi potensi kerentanan dan dampak serangan ransomware terhadap infrastruktur *database* sebuah organisasi. Penelitian ini melibatkan pemodelan dan simulasi serangan ransomware pada infrastruktur *database* BSI menggunakan teknik-teknik umum yang digunakan oleh penyerang dalam serangan nyata. Metode penelitian yang digunakan dalam penelitian ini mencakup studi literatur yang relevan, observasi terhadap kasus penyerangan Ransomware, hingga melakukan simulasi penyerangan terhadap sistem. Kami menganalisis serangkaian scenario penyerangan dengan teknik *Hybrid Analysis* untuk memahami bahaya serangan, mengukur dampak yang dihasilkan, hingga melakukan *backup database*. Dari hasil penelitian ini, kami merekomendasikan kepada pembaca untuk melakukan *backup* data secara rutin serta menjauhkan perangkat *backup* dari perangkat operasional utama sehingga dapat dilakukan *recovery* data pasca-serangan. Dengan mengambil langkah-langkah ini, diharapkan dapat mengurangi risiko serangan ransomware dan melindungi *database* secara efektif.
Kata kunci: Oracle, Ransomware, *backup, recovery, Malware*

Abstract

Ransomware attacks have become a significant threat in the computer security environment, especially in the banking sector. In this study, we analyzed and simulated a ransomware attack against the database of Bank Syariah Indonesia (BSI). The main objective of this research is to identify potential vulnerabilities and the impact of a ransomware attack on an organization's database infrastructure. The research involved modeling and simulating a ransomware attack on BSI's database infrastructure using common techniques used by attackers in real attacks. The research methods used in this research include the study of relevant literature and the observation of Ransomware attack cases to simulate the attack on the system. We analyzed a series of attack scenarios with Hybrid Analysis techniques to understand the danger of the attack, measure the resulting impact, and perform database backups. From the results of this research, we recommend readers perform regular data backups and keep backup devices away from the main operational devices so that post-attack data recovery can be carried out. By taking these steps, we hope to reduce the risk of ransomware attacks and protect the database effectively.
Keywords: *Oracle, Ransomware, backup, recovery, Malware*

1. PENDAHULUAN

Data merupakan aset yang sangat berharga dalam berbagai lembaga keuangan, termasuk Bank Syariah Indonesia. Dalam era digital yang semakin maju, penting untuk memprioritaskan keamanan data guna melindungi informasi sensitif pelanggan dan menjaga kelancaran integrasi

sistem perbankan. Namun, ancaman terhadap keamanan data semakin meningkat seiring dengan berkembangnya serangan yang semakin canggih dan juga risiko bencana yang tak terduga. Oleh karena itu, menjaga keamanan data menjadi tanggung jawab bersama semua elemen organisasi untuk melindungi informasi penting dari serangan yang dapat merugikan pelanggan dan lembaga keuangan (Novianti, 2021).

Dalam konteks ini, Bank Syariah Indonesia mengalami serangan langsung dari jenis serangan Ransomware pada database mereka. Kelompok peretas yang dikenal sebagai LockBit 3.0 menggunakan metode phishing dan malicious attachments untuk menyebarkan Ransomware ke dalam sistem perbankan (Wahidin, 2022). Ransomware adalah jenis serangan yang mengenkripsi data korban dan meminta pembayaran tebusan untuk mendapatkan kunci dekripsi. Dalam kasus ini, serangan ransomware telah menyebabkan kerugian data sebesar 1,5 TB, termasuk informasi sensitif pelanggan dan surat perjanjian rahasia yang dapat digunakan sebagai ancaman terhadap pengguna (R. S. Sajjan, 2017).

Serangan Ransomware ini juga memiliki dampak yang signifikan dalam proses pemulihan pasca-serangan (Ferdiansyah, F, 2018). Proses pemulihan data melibatkan pemulihan dari cadangan data yang ada serta dekripsi data yang terenkripsi, yang dapat memakan waktu yang lama dan mengganggu operasional bank secara keseluruhan. Selain itu, ancaman terhadap pelanggan melalui surat perjanjian rahasia yang dicuri juga menimbulkan kekhawatiran terhadap kepercayaan pelanggan terhadap Bank Syariah Indonesia (Sulistiadi, 2023).

Dalam penelitian ini, kami bertujuan untuk melakukan analisis mendalam terhadap serangan Ransomware yang terjadi pada database Bank Syariah Indonesia serta dampaknya terhadap keamanan data. Tujuan utama dari penelitian ini adalah memberikan pemahaman yang komprehensif tentang serangan ransomware, termasuk cara serangan ini terjadi, dampaknya terhadap keamanan data, serta tantangan yang dihadapi dalam proses pemulihan pasca-serangan. Dengan demikian, penelitian ini akan memberikan kontribusi ilmiah dalam pemahaman tentang serangan ransomware dan upaya perlindungan data dalam konteks lembaga keuangan.

2. METODOLOGI

Metode yang digunakan dalam penelitian ini bukan untuk memberi panduan kepada pembaca untuk melakukan penyebaran Ransomware kepada perangkat manapun, melainkan untuk memberi pengetahuan kepada pembaca terkait bagaimana Ransomware bekerja, pencegahan, dan melakukan tindakan pasca-serangan.

2.1 Landasan Teori

2.1.1 Ransomware

Ransomware merupakan salah satu cabang dari perangkat lunak berbahaya (*malware*) yang menggunakan konsep kriptografi (Kurniawan, 2021). Penyebaran Ransomware dapat melalui berbagai metode seperti *phising, malicious attachments,* pesan email palsu, dan sebagainya. Jenis *malware* ini memungkinkan object targetnya menjadi tidak bisa diakses atau terenkripsi (E. Tansen, 2020). Setelah serangan berhasil, korban diminta untuk menebus sebuah *key* untuk melakukan dekripsi dengan mengirimkan sejumlah *bitcoin* atau mata uang elektronik lain yang sulit untuk dilacak.

2.1.2 *Social Engineering*

Social Engineering adalah teknik atau upaya yang dilakukan untuk memperoleh sebuah informasi atau otorisasi terhadap sebuah file bahkan sistem (Hastuti, 2021). Teknik ini biasa dilakukan oleh praktisi dalam bidang IT dengan tujuan beragam seperti pengembangan sistem, penghimpunan data, dan sebagainya.

2.1.3 *Static Analysis*

Static Analysis merupakan upaya yang dilakukan untuk menganalisis sebuah file *executable* dengan memahami strukturnya (Hariyadi, 2022). Dengan teknik ini, kita dapat melihat dan memahami alur kerja terkait bagaimana sebuah file dapat mempengaruhi sistem. Sebagai output

dari analisis ini, kita dapat menilai apakah sebuah file itu tergolong ke dalam ransomware atau bukan.

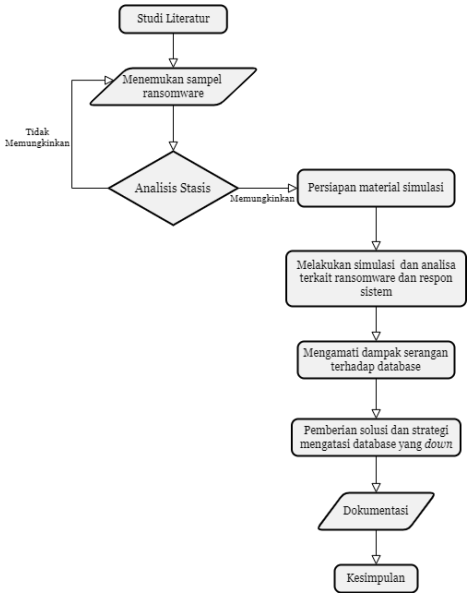
2.1.4 *Dynamic Analysis*

Dynamic Analysis merupakan teknik pemahaman sebuah file baik *secure files* maupun *malware files* dengan cara mengeksekusi file tersebut di dalam sebuah sistem yang jauh dari penyimpanan *datafiles* penting (Nastiti, 2019). Dengan teknik ini, kita bisa mendapatkan lebih banyak informasi dan meningkatkan kemampuan untuk mengidentifikasi Ransomware. Dalam praktik eksekusinya, perilaku dari file tersebut akan diperiksa secara ekstensif (A. Dewi, 2022).

2.1.5 Backup and Recovery

Metode ini dilakukan untuk proses pencadangan basis data dan operasi pemulihan secara efisien (Rosano, 2020). Hal ini dilakukan oleh organisasi atau perusahaan ketika sistem mereka down atau terkena bencana. Dalam penelitian ini, setelah simulasi serangan ransomware berhasil dilakukan, kita bisa menguji efektivitas pemulihan cadangan yang ada serta memberikan opsi lain untuk solusi pasca-serangan.

2.2 Metode Penelitian



Gambar 1. Metode Penelitian Hybrid Analysis

Pada **Gambar 1**, dijelaskan bahwasannya metode penelitian ini menggunakan teknik Hybrid Analysis guna mendapatkan informasi sebanyak mungkin mengenai alur Ransomware serta dampaknya terhadap *database* target. Dengan adanya simulasi ini diharapkan pembaca dapat memiliki gambaran serta peluang untuk mencegah bahkan menghadapi serangan Ransomware di kemudian hari. Selain itu, praktik simulasi penyerangan dilakukan untuk memperoleh pemahaman praktis tentang bagaimana Ransomware beroperasi, dampaknya pada *database*, serta menemukan upaya mitigasi yang efektif terhadap *database*.

2.3 Metode Pengumpulan Data

1. Observasi

Observasi dilakukan dengan pengamatan secara sistematis terhadap beberapa kejadian serangan Ransomware, dalam kasus ini adalah Bank Syariah Indonesia. Kami mengumpulkan data dan mencatat informasi yang relevan tentang bagaimana kasus Ransomware pada Bank Syariah Indonesia dapat terjadi.

2. Studi Literatur

Studi literatur dilakukan dengan mengumpulkan, mengevaluasi, dan menganalisis literatur yang relevan dan tersedia secara tertulis mengenai Ransomware dan dampaknya terhadap sebuah *database*. Dengan melakukan hal ini, kami dapat secara kritis mengevaluasi dan menganalisis berbagai hal tentang bagaimana *database* dapat *down* sebagai akibat dari serangan Ransomware.

3. HASIL DAN PEMBAHASAN

3.1 *Required Tools*

3.1.1 Visual Studio

Untuk membuat sebuah ransomware dibutuhkan aplikasi dekstop yang bernama visual studio. Visual studio digunakan untuk membuat rancangan aplikasi berbasis desktop untuk membuat Ransomware dari awal hingga selesai dan bisa di *running* pada laptop atau komputer. *Software* visual studio digunakan untuk membuat source code atau codingan yang berisi perintah untuk membuat Ransomware untuk mengenkripsi file - file yang diinginkan.

3.1.2 *Database*

Untuk *database* bisa menggunakan jenis *database* apapun, baik *database* Oracle, MySQL, Mongodb dan yang lainnya. Tujuan dibutuhkannya *software database* adalah untuk menyerang *database* tersebut dan mengetahui bagaimana penyerangan Ransomware bekerja saat menyerang ke dalam *database*.

3.2 *Source Code*

```
0 references
class Program
{
    private const bool DELETE_ENCRYPTED_FILE = true; /* CAUTION */
    private const bool DECRYPT_DESKTOP = true;
    private const bool DECRYPT_DOCUMENTS = true;
    private const bool DECRYPT_PICTURES = true;
    private const string ENCRYPTED_FILE_EXTENSION = ".jcrypt";
    private const string ENCRYPT_PASSWORD = "Password1";

    private static string DESKTOP_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory);
    private static string DOCUMENTS_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);
    private static string PICTURES_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.MyPictures);
    private static string DECRYPTION_LOG = "";
    private static int decryptedFileCount = 0;
    0 references
    static void Main(string[] args)
    {
        if (DECRYPT_DESKTOP)
        {
            decryptFolderContents(DESKTOP_FOLDER);
        }

        if (DECRYPT_PICTURES)
        {
            decryptFolderContents(PICTURES_FOLDER);
        }

        if (DECRYPT_DOCUMENTS)
        {
            decryptFolderContents(DOCUMENTS_FOLDER);
        }
```

Gambar 2. Tampilan potongan source code decrypt

Pada **Gambar 2** terlihat sebuah potongan *source code* yang mampu mengembalikan (dekripsi) file-file yang sebelumnya telah terenkripsi oleh Ransomware. Kode ini ditujukan untuk mengembalikan semua file yang terdapat dalam direktori file desktop, picture, dan document. Dengan menggunakan kode ini, file-file yang terkena dampak Ransomware akan dikembalikan ke keadaan semula melalui proses dekripsi. Selain itu, file-file yang memiliki ekstensi (.jcrypt), yang menunjukkan bahwa mereka telah terinfeksi oleh Ransomware, akan dihapus dan digantikan dengan file-file yang sudah berhasil didekripsi.

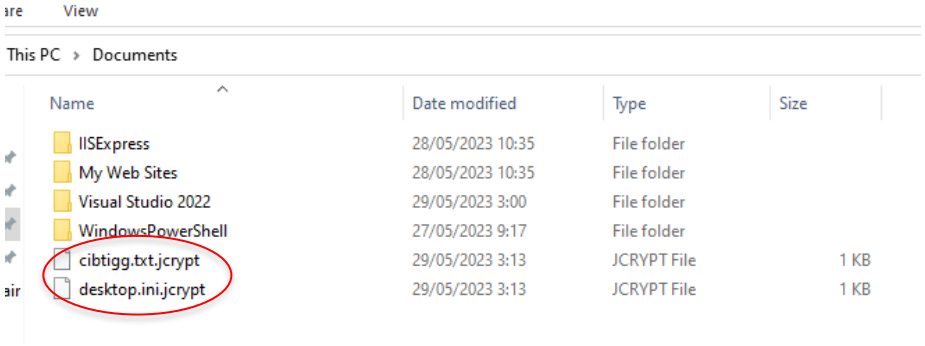
```
private const bool DELETE_ALL_ORIGINALS = true; /* CAUTION */
private const bool ENCRYPT_DESKTOP = true;
private const bool ENCRYPT_DOCUMENTS = true;
private const bool ENCRYPT_PICTURES = true;
private const string ENCRYPTED_FILE_EXTENSION = ".jcrypt";
private const string ENCRYPT_PASSWORD = "Password1";
private const string BITCOIN_ADDRESS = "1BtUL5dhVXHwKLqSdhjyjK9Pe64Vc6CEH1";
private const string BITCOIN_RANSOM_AMOUNT = "1";
private const string EMAIL_ADDRESS = "21082010004@student.upnjatim.ac.id";

private static string ENCRYPTION_LOG = "";
private string RANSOM_LETTER =
   "All of your files have been encrypted.\n\n" +
   "To unlock them, please send " + BITCOIN_RANSOM_AMOUNT + " bitcoin(s) to BTC address: " + BITCOIN_ADDRESS + "\n" +
   "Afterwards, please email your transaction ID to: " + EMAIL_ADDRESS + "\n\n" +
   "Thank you and have a nice day!\n\n" +
   "Encryption Log:\n" +
   "----------------------------------------\n";
private string DESKTOP_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.DesktopDirectory);
private string DOCUMENTS_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments);
private string PICTURES_FOLDER = Environment.GetFolderPath(Environment.SpecialFolder.MyPictures);
private static int encryptedFileCount = 0;

1 reference
public Form1()
{
    InitializeComponent();
}
```

Gambar 3. Tampilan potongan source code encrypt

Pada **Gambar 3** terlihat sebuah potongan *source code* yang akan mengenkripsi semua file yang terdapat dalam direktori file desktop, gambar, dan dokumen. Akibat dari enkripsi Ransomware, semua file akan mengalami kerusakan dan tidak dapat diakses dengan jelas karena kontennya akan berubah menjadi kombinasi angka dan huruf yang tidak dapat dibaca.

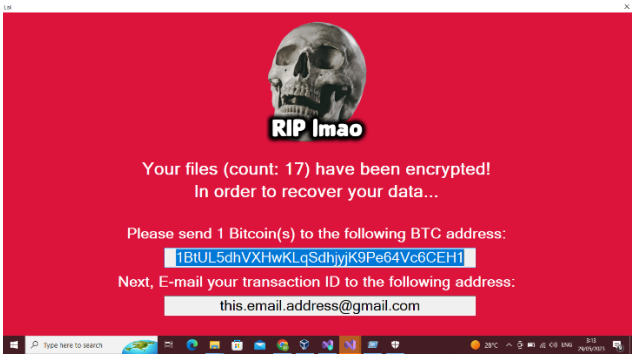
3.3 Implementasi Praktik Penyerangan Ransomware

Setelah kita menyelesaikan pembuatan Ransomware, langkah selanjutnya adalah mengeksekusi kode yang telah kita buat. Pada **Gambar 4**, terlihat hasil dari file enkripsi atau *encrypt* yang telah dijalankan. Kemudian, tunggu beberapa saat agar Ransomware dapat bekerja dengan baik untuk mengubah ekstensi file yang ditarget menjadi .jcrypt.



Gambar 4. Tampilan File yang terkena Ransomware

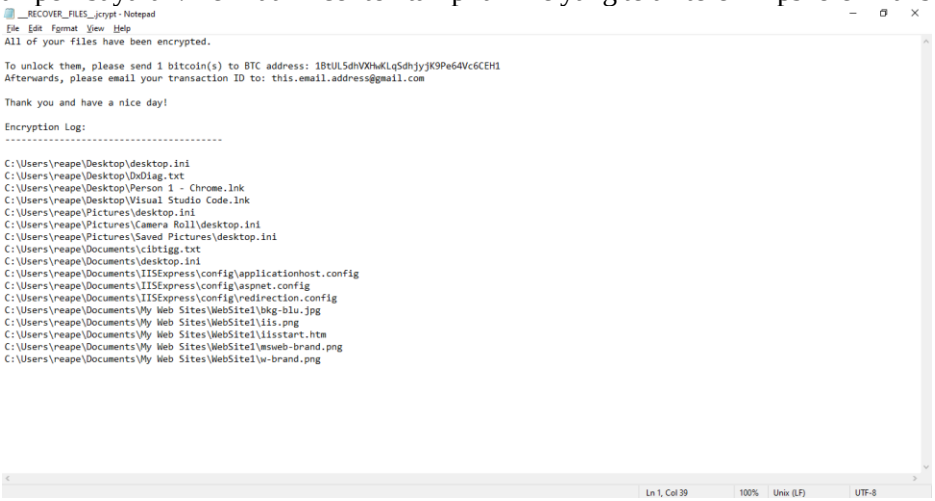
Jika Ransomware telah selesai mengenkripsi seluruh file yang dituju, maka akan muncul tampilan seperti gambar berikut:



Gambar 5. Tampilan layar dekstop korban yang terkena Ransomware

Pada **Gambar 5**, gambar tersebut akan muncul dan korban akan mendapatkan peringatan bahwa semua file dalam perangkatnya telah terenkripsi. Untuk mengembalikan file-file yang terenkripsi, korban diharuskan membayar sejumlah uang kepada pembuat Ransomware. Namun, melakukan pembayaran sangat tidak disarankan dalam penanganan serangan ini karena tidak ada jaminan bahwa hacker akan melakukan dekripsi dan bahkan membuat efek domino dimana kejadian serupa akan terulang karena hacker mendapatkan apa yang mereka inginkan. Solusi yang kami tawarkan adalah dengan segera menggunakan perangkat lunak *antimalware* seperti Windows Defender Anti-Malware.

Setelah semua file korban terenkripsi, sebuah file pemulihan dengan nama "recovery file" akan muncul di halaman desktop yang telah ditunjukan pada **Gambar 6.** File ini bertujuan untuk memberitahukan korban mengenai file-file yang telah terenkripsi sehingga terdorong untuk melakukan pembayaran. Berikut ini contoh tampilan file yang telah terenkripsi oleh Ransomware:

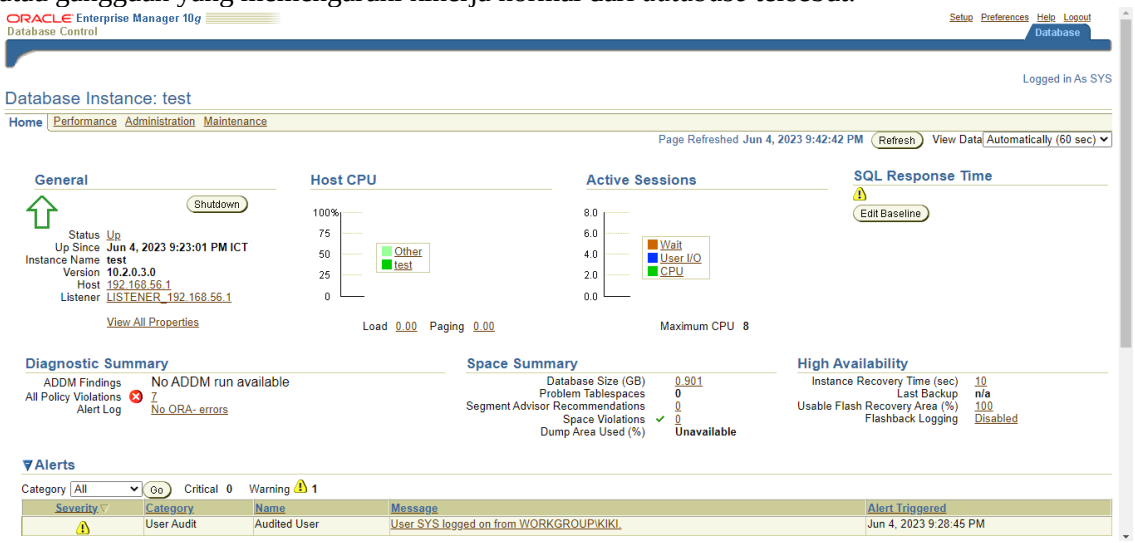


Gambar 6. Tampilan daftar file yang terkena Ransomware

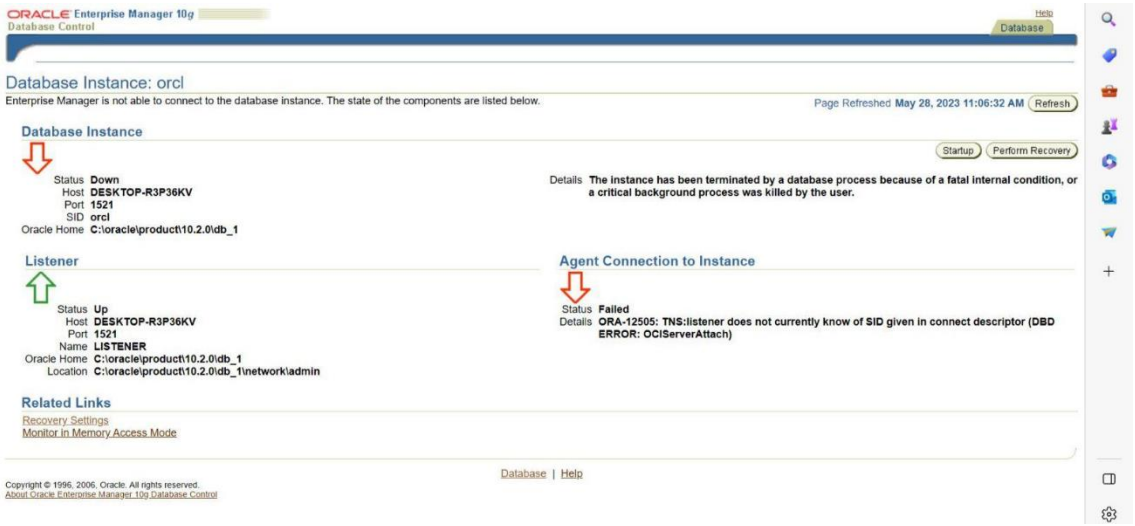
Setelah file-file tersebut terenkripsi, korban tidak dapat membukanya secara otomatis. Jika korban mencoba membuka file tersebut, akan muncul simbol-simbol atau tulisan-tulisan acak, bahkan tidak dapat dibaca karena telah terenkripsi yang ditunjukan pada **Gambar 7**

Gambar 7. Tampilan isi file yang terkena Ransomware

Selanjutnya, kita akan berfokus pada pemeriksaan tampilan *database* sebelum dan setelah terkena serangan Ransomware. Tujuan dari pemeriksaan ini adalah untuk mengetahui apakah *database* masih dapat beroperasi atau telah terpengaruh oleh Ransomware. **Gambar 8** menunjukkan contoh tampilan *database* dari perangkat lunak Oracle sebelum terkena serangan Ransomware dan sebelum mengalami proses enkripsi. Pada tampilan *database* ini, tidak terlihat adanya masalah atau gangguan yang memengaruhi kinerja normal dari *database* tersebut.



Gambar 8. Tampilan *database* Oracle yang belum terkena Ransomware



Gambar 9. Tampilan *database* Oracle yang telah terkena Ransomware

Selanjutnya, kita akan mengamati tampilan *database* Oracle yang telah terkena serangan virus Ransomware dan mengenkripsi data di dalamnya seperti tercantum pada **Gambar 9**. Jika kita perhatikan, terdapat perbedaan dalam tampilan antara *database* yang masih berfungsi normal dan belum terinfeksi oleh Ransomware, dengan *database* yang telah terkena serangan Ransomware. Pada *database* yang masih berfungsi normal, tampilan akan menunjukkan status "*up*", yang menandakan bahwa *database* tersebut sedang berjalan dan siap menerima koneksi serta menjalankan permintaan dari pengguna.

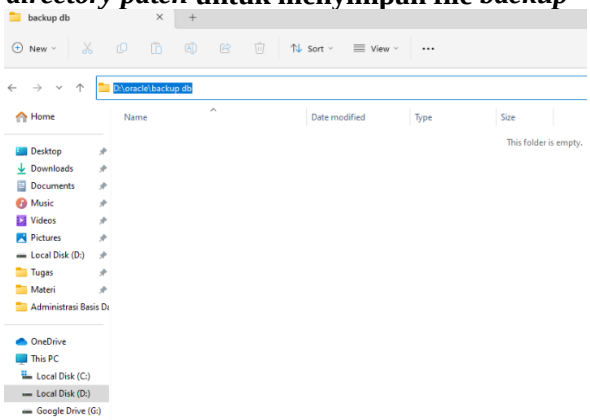
Namun, pada *database* yang telah terkena serangan virus Ransomware, tampilan akan menunjukkan status "*down*", yang mengindikasikan bahwa database tersebut tidak aktif atau tidak berjalan. Ketika *database* Oracle berada dalam status "*down*", berarti proses instance dan proses background tidak berjalan, dan *database* tidak tersedia untuk menerima koneksi atau menjalankan

permintaan pengguna. Oleh karena itu, dapat disimpulkan bahwa *database* tersebut kemungkinan telah terinfeksi oleh virus Ransomware yang menyerang *database*.

3.4 Pengamanan Data Pada *Database*

Untuk meredam dampak dari serangan virus Ransomware pada *database*, ada beberapa langkah yang dapat dilakukan. Salah satunya adalah dengan melakukan pencadangan (*backup*) data secara berkala dan terjadwal pada *database*. Hal ini penting agar ketika data utama di dalam *database* rusak dan tidak dapat diakses karena terenkripsi oleh virus Ransomware, data dapat dipulihkan. Penting juga untuk tidak hanya menyimpan salinan data cadangan pada satu perangkat atau tempat penyimpanan saja. Disarankan untuk menyimpan salinan data cadangan dari database utama ke berbagai tempat penyimpanan yang berbeda, seperti cloud, server, *hardware* (misalnya perangkat memory), dan lainnya. Dengan melakukan ini, data *backup* akan lebih aman dan terhindar dari risiko kehilangan jika satu tempat penyimpanan mengalami masalah.
Berikut ini adalah beberapa cara untuk melakukan pencadangan data atau ekspor pada *database* Oracle:

1. **Menentukan area *directory patch* untuk menyimpan file *backup***



Gambar 10. Tampilan directory path untuk menyimpan file backup database

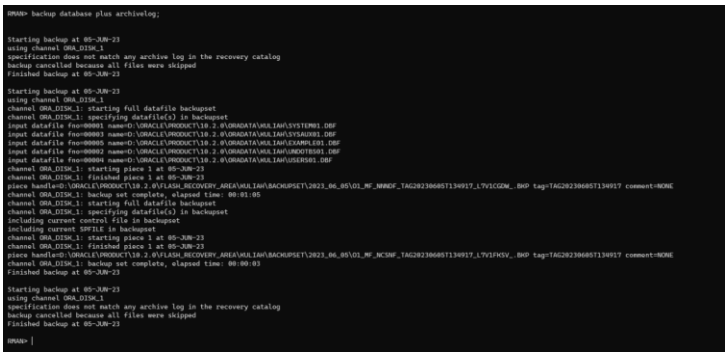
Sebelum melakukan *backup*, pengguna akan menentukan *path area* yang dibuat untuk menyimpan file hasil *backup* dari *database* utama seperti yang tertera pada **Gambar 10.**

2. **Menggunakan query untuk *database backup***

```
C:\Users\HP>sqlplus/nolog

SQL*Plus: Release 10.2.0.3.0 - Production on Mon Jun 5 13:41:56 2023

Copyright (c) 1982, 2006, Oracle.  All Rights Reserved.

SQL> conn sys as sysdba
Enter password:
Connected.
SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount
ORACLE instance started.

Total System Global Area  612368384 bytes
Fixed Size                  1292036 bytes
Variable Size             192940284 bytes
Database Buffers          411041792 bytes
Redo Buffers                7094272 bytes
Database mounted.
SQL>
```

Gambar 11. Tampilan query untuk *shutdown database*

Query pada **Gambar 11** digunakan untuk melakukan *cold backup* yang berarti kondisi *database* dalam keadaan mati atau *shutdown*. Perintah “startup mount” digunakan untuk memulai kembali database Oracle dalam mode "*mount*". Mode "*mount*" memungkinkan akses ke file kontrol database, tetapi tidak memuat database secara lengkap. Ini diperlukan sebelum melakukan backup.



Gambar 12. Tampilan query untuk *backup database*

Pada **Gambar 12,** pencadangan *database* dilakukan dengan menggunakan fitur Recovery Manager (RMAN) yang disediakan oleh Oracle . Perintah *archivelog* digunakan untuk mengubah mode database menjadi mode *archivelog*. Mode ini memungkinkan perekaman log transaksi ke dalam arsip log yang diperlukan untuk *backup database* selanjutnya secara lengkap mulai dari kondisi terakhir *database* ter-*backup* hingga jadwal pencadangan selanjutnya.

4. KESIMPULAN DAN SARAN

Dalam demikian, dapat disimpulkan bahwa Ransomware merupakan sebuah malware yang sangat berbahaya yang dapat secara langsung menyerang database penting dalam sebuah perusahaan atau organisasi. Untuk melawan serangan Ransomware, langkah-langkah yang dapat diambil antara lain adalah melakukan backup data secara rutin dan menyimpannya secara terpisah dari perangkat operasional utama, seperti yang telah dijelaskan pada subbab 3.4. Dengan demikian, proses pemulihan data pasca-serangan dapat dilakukan. Dalam tahap pencadangan database, disarankan untuk melakukan backup dalam kondisi offline atau tidak beroperasi untuk menghindari kemungkinan crash. Selain itu, jika terjadi serangan Ransomware yang berlangsung, disarankan untuk tidak membayar tebusan kepada para penyerang dan segera menjalankan perangkat lunak antimalware seperti Windows Defender Anti-Malware, seperti yang dijelaskan pada penjelasan Gambar 5.

Salah satu kekurangan penelitian ini adalah kurangnya pembahasan yang mendalam mengenai langkah-langkah konkret yang dapat diambil oleh Bank Syariah Indonesia untuk mencegah serangan Ransomware di masa depan. Oleh karena itu, penelitian ini dapat diperluas dengan memberikan panduan praktis yang lebih terperinci mengenai kebijakan keamanan yang dapat diterapkan, pelatihan karyawan yang diperlukan, serta teknologi keamanan yang dapat diimplementasikan.

Saran pengembangan untuk penelitian selanjutnya adalah melakukan analisis yang lebih mendalam mengenai faktor-faktor yang mendorong terjadinya serangan Ransomware, seperti celah keamanan yang ada dalam sistem perbankan dan kerentanan manusia dalam menghadapi serangan phishing. Selain itu, penelitian selanjutnya dapat melibatkan survei atau wawancara dengan pelanggan Bank Syariah Indonesia untuk memahami dampak serangan Ransomware terhadap kepercayaan mereka terhadap lembaga keuangan. Hal ini akan memberikan wawasan yang lebih mendalam tentang cara mengatasi kerugian reputasi dan membangun kembali kepercayaan pelanggan setelah terjadinya serangan Ransomware.

5. DAFTAR RUJUKAN

[1] Novianti (2021). “Pentingnya Keamanan Data Dalam Intelijen Bisnis ”, j-sika, 2(02), 41–48
[2] Wahidin, G. W., Syaifuddin, S., & Sari, Z. (2022). Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox. Jurnal Repositor, 4(1), 83-94.

[3] R. S. Sajjan and V. R. Ghorpade (2017), “Ransomware attacks: Radical menace for cloud computing” Informatika dan Teknologi (INTECH), vol 2(02), 19-22
[4] Ferdiansyah, F. (2018). Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware. JUSIFO (Jurnal Sistem Informasi), 4(1), 37-48.
[5] Sulistiadi, & Salman, M. (2023). Ransomware Attacks Threat Modeling Using Bayesian Network: Pemodelan Ancaman Serangan Ransomware Menggunakan Bayesian Network. Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi, 14(1), 43-56.
[6] Kurniawan, I., Mahmud, H., & Dewi, N. (2021). Penyebaran Virus Ransomware Wannacry Berdasarkan Undang-Undang No. 11 Tahun 2008. Jurnal Inovasi Penelitian, 2(2), 427-432.
[7] E. Tansen and D. W. Nurdiarto (2020) Analisis dan Deteksi Malware dengan Metode Hybrid Analysis Menggunakan Framework MOBSF. JURTI (Jurnal Teknologi Informasi), 4(2), 191-201.
[8] Hastuti, T., Djuyandi, Y., & Darmawan, W. B. (2021). Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara. Paradigma Polistaat: Jurnal Ilmu Sosial Dan Ilmu Politik, 4(1), 60–81.
[9] Hariyadi, D., Setiawan, C. B., Sahtyawan, R., Wicaksono, A. I., & Wisnuaji, A. (2022). Analisis dan Deteksi Backdoor pada Content Management System Menggunakan Metode Signature-based dan Static Analysis. INTEK : Jurnal Informatika Dan Teknologi Informasi, 5(1), 17-21.
[10] Nastiti, F. E., Hariyadi, D., & Fazlurrahman. (2019). "Telegrambot: Using Telegram To Crawling Malware Threats." CESS (Journal Of Computer Engineering System And Science), 4(1), 51-54, 2019.
[11] A. Dewi, R. Ananda, and U. Rifanti (2022), Dynamic Analysis Of The Covid-19 Model With Isolation Factors, BAREKENG: J. Math. & App., 16(1), 047-056.
[12] Rosano, A., & Sudaradjat, D. (2020). Manajemen Backup Data untuk Penyelamatan Data Nasabah pada Sistem Informasi Perbankan (Studi Kasus : PT Bank XYZ). REMIK: Riset Dan E-Jurnal Manajemen Informatika Komputer, 4(2), 210-217.