ANALISIS CARA KERJA MALWARE RANSOMWARE LOOKBIT 3.0 MENGGUNAKAN METODE STATIS DAN DINAMIS

I Putu Krisna Dharma Wiguna, Muhammad Azwar ,Muhammad Innuddin, Muhammad [3]Innuddin Lilik Widyawati, Kurniadin Abd. Latif

Universitas Bumigora, Mataram, Indonesia,

Correspondence : *e-mail*: putukrisnadharmawiguna1@gmail.com

Abstrak

Perkembangan teknologi informasi turut meningkatkan risiko keamanan, salah satunya ancaman ransomware. Studi ini menganalisis cara kerja malware LookBit 3.0 melalui dua pendekatan: analisis statis menggunakan PeStudio, dan analisis dinamis dengan Any.Run. Analisis statis mengevaluasi entropi, struktur file, serta fungsi API, sementara analisis dinamis mengamati aktivitas runtime seperti perubahan registri, jaringan, dan file. LookBit 3.0 menunjukkan tingkat entropi tinggi, menyembunyikan file dalam sistem, dan memodifikasi pengaturan antarmuka serta browser. Meski tidak ditemukan koneksi ke server C2, malware ini menjalankan taktik dari kerangka MITRE ATT&CK seperti eskalasi hak akses, evasi, pengambilan kredensial, dan enkripsi data. Studi ini memberikan pemahaman mendalam tentang LookBit 3.0 sebagai dasar strategi mitigasi ransomware.

Kata kunci: *LookBit 3.0, Ransomware, Analisis Statis, Analisis Dinamis, Malware*

Abstract

The rapid advancement of information technology has also led to increased cybersecurity risks, with ransomware being one of the most prominent threats. This study analyzes how LookBit 3.0 malware operates using two approaches: static analysis with PeStudio and dynamic analysis with Any.Run. Static analysis examines entropy, file structure, and API functions, while dynamic analysis observes runtime behavior such as registry changes, network activity, and file modifications.LookBit 3.0 exhibits high entropy, hides files within the system, and modifies interface and browser settings. Although no connection to a command and control (C2) server was detected, the malware employs several MITRE ATT&CK tactics, including privilege escalation, defense evasion, credential access, and data encryption. This research provides a comprehensive understanding of LookBit 3.0, serving as a reference for future ransomware mitigation strategies.

Keywords*: LookBit 3.0, Ransomware, Static Analysis, Dynamic Analysis, Malware*

1. Pendahuluan

Ransomware telah menyebabkan kerugian besar belakangan ini. Jenis malware ini mengenkripsi data korban dan umumnya menargetkan instansi pemerintah dengan menyebar melalui jaringan lokal, setelah lebih dulu masuk lewat email atau file yang tidak terpercaya [1]. Pada tahun 2023 terjadi 361 juta serangan siber di Indonesia, dengan malware menyumbang 42,79%, dan ransomware termasuk lima besar serangan terbanyak [2].LookBit adalah ransomware yang dikembangkan oleh kelompok siber terorganisir dan memungkinkan pelaku lain membayar untuk menggunakannya. Selain mengenkripsi data dan meminta tebusan, LookBit juga mengancam akan membocorkan data korban jika permintaan tidak dipenuhi. Menurut GoodStats, dari 703 kasus ransomware pada 2023, sebanyak 4,8% terkait LookBit. Serangan ini umumnya menargetkan perusahaan besar dan institusi penting. Salah satu kasus besar terjadi pada 20 Juni 2024, ketika Pusat Data Nasional (PDN) diretas. Serangan ini menyebabkan hilangnya data 800 ribu calon

mahasiswa penerima Kartu Indonesia Pintar Kuliah (KIPK) karena tidak adanya cadangan data. Akibatnya, pendaftar harus mengunggah ulang seluruh dokumen [3].

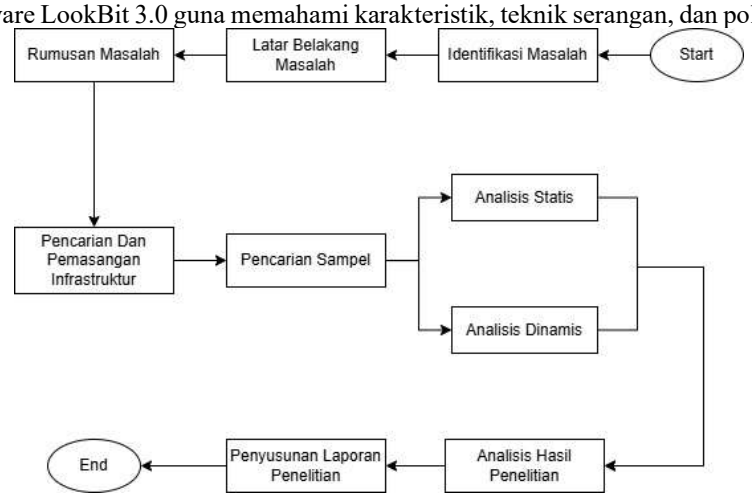
Berdasarkan kasus tersebut, penelitian ini bertujuan menganalisis ransomware LookBit 3.0 untuk memahami cara kerjanya melalui metode analisis statis dan dinamis. Tools yang digunakan adalah PeStudio dan Any.Run karena mudah dioperasikan. PeStudio digunakan untuk analisis statis, seperti melihat struktur file, string, library, dan import yang digunakan. Sementara itu, Any.Run merupakan sandbox online yang memungkinkan analisis interaktif terhadap malware secara real-time dalam lingkungan virtual yang aman [4].

Penelitian analisis malware telah dilakukan oleh beberapa peneliti di Indonesia, dalam penelitiannya berjudul "Analisis Ransomware secara Statis dan Dinamis untuk Pemetaan Evolusi Ransomware", menganalisis ransomware Gandcrab, GoldenEye, Locky, dan Ryuk menggunakan metode statis dan dinamis. Hasil analisis statis mencakup struktur file, waktu kompilasi, library, import, dan string, sementara analisis dinamis menghasilkan pohon proses, perilaku, dan signature ransomware untuk memetakan evolusinya [5]. meneliti malware pada aplikasi Android syssecApp.apk yang terinfeksi Trojan menggunakan reverse engineering, dan menemukan IP host penerima dalam source code [6]. meneliti malware pada sistem operasi Windows menggunakan teknik forensik, dengan tujuan mengungkap aktivitas dan pola serangan malware untuk membantu pengguna mengantisipasi ancaman [7].

Oleh karena itu, penelitian ini menggunakan metode deskriptif dengan pendekatan statis dan dinamis untuk menganalisis ransomware. Diharapkan hasilnya dapat menjadi acuan dalam mendeteksi ransomware baru yang memiliki pola serupa, serta memberikan kontribusi bagi pengembangan keilmuan forensik digital di masa mendatang.

2. Metode Penelitian

Penelitian ini menggunakan metode deskriptif untuk menggambarkan secara sistematis dan akurat karakteristik objek yang diteliti. Melalui pendekatan analisis statis dan dinamis, penelitian ini menganalisis perilaku ransomware LookBit 3.0 guna memahami karakteristik, teknik serangan, dan pola aktivitasnya [8].



Gambar 1. Alur Penelitian

A. Tahap Pertama

Langkah awal dalam penelitian ini adalah mengidentifikasi permasalahan. Penyusunan latar belakang didasarkan pada peristiwa yang relevan serta didukung oleh studi literatur. Berdasarkan keduanya, dirumuskan permasalahan utama yang menjadi fokus dalam penelitian ini, yaitu melakukan analisis .

B. Tahap Kedua

Tahap kedua mencakup perancangan lingkungan laboratorium penelitian, pemilihan sampel, serta pelaksanaan analisis statis dan dinamis. Adapun rincian dari tahapan ini adalah sebagai berikut:

1. Bagian yang pertama adalah perancangan dan pembangunan dari laboratorium penelitian dan kebutuhan dalam pembangunan laboratorium.
2. Tahap kedua adalah pengambilan sampel malware yang diperoleh melalui platform GitHub. Platform ini menyediakan berbagai proyek dan dataset yang dibagikan secara terbuka oleh komunitas keamanan siber untuk keperluan pendidikan dan penelitian.

3. Tahap ketiga dilakukan analisis statis dan dinamis, analisis statis dilakukan tanpa mengeksekusi malware dengan mengamati struktur file, string tersembunyi, fungsi API, dan informasi lain menggunakan tools PEStudio, sedangkan analisis dinamis dilakukan dengan menjalankan malware dalam lingkungan terkontrol (sandbox) untuk mengamati secara real-time perilakunya terhadap sistem, seperti perubahan file, aktivitas jaringan, dan modifikasi registry.

C. Tahap ketiga

Tahap ketiga merupakan tahap akhir yang meliputi analisis hasil simulasi dari analisis statis dan dinamis untuk mengidentifikasi karakteristik serta perilaku malware, kemudian dilanjutkan dengan penyusunan laporan dan penarikan kesimpulan berdasarkan data yang diperoleh.

3. Hasil dan Pembahasan

3.1. Analisis Statis

3.1.1. Analisis String

Pada tahap ini dilakukan analisis string terhadap file yang dicurigai menggunakan teknik ekstraksi string statis. Hasil analisis menunjukkan bahwa file melakukan impor sejumlah fungsi dari API Windows. Fungsi-fungsi ini memberikan petunjuk terkait aktivitas dan potensi perilaku dari file tersebut.

Encoding	Value	Penjelasan
ascii	CreateWindowExW	untuk membuat jendela grafis di lingkungan Windows, misalnya jendela aplikasi, dialog, atau antarmuka pengguna lainnya.[9]
ascii	DefWindowProcW	Memproses pesan sistem agar window tetap terlihat seperti aplikasi normal [9].
ascii	GetCommandLineW	digunakan untuk mengambil seluruh string baris perintah (command line) yang digunakan untuk menjalankan proses dalam format Unicode (wide-character).[9]
ascii	LoadLibrary	digunakan untuk memuat (load) Dynamic-Link Library (DLL) ke dalam memori selama runtime.[9]
ascii	GetLocaleInfo	Mengambil informasi tentang lokal yang ditentukan berdasarkan nama.[9]
ascii	GetUserDefaultLangID	Mengembalikan pengidentifikasi bahasa pengaturan Format Wilayah untuk pengguna saat ini.[9]

3.1.2. Analisis Library

Pada tahap analisis statis, dilakukan juga pemeriksaan terhadap library (pustaka) yang diimpor oleh file malware. Library adalah file .dll (Dynamic Link Library) yang berisi kumpulan fungsi-fungsi sistem yang dapat digunakan oleh program, termasuk malware, untuk menjalankan berbagai instruksi di sistem operasi.

No	Nama	Jumlah Fungsi	Penjelasan
1	Gdi32.dll	10	Digunakan untuk membuat program yang dapat mengekspor fungsi GDI (Graphics Device Interface), seperti menggambar ke layar atau printer [5]
2	User32.dll	7	Menyediakan fungsi untuk menampilkan dan mengelola antarmuka pengguna grafis (GUI), seperti jendela, tombol, dan menu [5]
3	Kernel32.dll	8	Kernel32 sangat umum digunakan karena memiliki fungsi penting seperti akses,

	manipulasi memori. File dan hardware [5]

3.1.3. Analisis Import

Import Table adalah bagian penting dari file PE yang menampilkan fungsi-fungsi dari library eksternal yang dipanggil program. Analisis import table memungkinkan kita mengidentifikasi potensi perilaku malware tanpa perlu menjalankannya

Fungsi yang Diimpor	Library	Fungsi
CreateWindowExW	USER32.dll	untuk membuat jendela grafis di lingkungan Windows, misalnya jendela aplikasi, dialog, atau antarmuka pengguna lainnya.[9]
GetFileAttributesW	KERNEL32.dll	digunakan untuk mengambil atribut dari sebuah file atau folder dalam format Unicode (ditandai dengan akhiran W untuk "Wide-character").[9]
GetCommandLineW	KERNEL32.dll	digunakan untuk mengambil seluruh string baris perintah (command line) yang digunakan untuk menjalankan proses dalam format Unicode (wide-character).[9]
GetProcAddress	KERNEL32.dll	digunakan untuk mengakses fungsi dalam DLL secara dinamis. Ini sangat penting dalam teknik pemrograman fleksibel dan sering disalahgunakan oleh malware agar pemanggilan fungsi sistem tidak mudah dideteksi oleh alat keamanan atau static scanner.[9]
FreeLibrary	KERNEL32.dll	digunakan untuk menyembunyikan aktivitas dan meminimalkan jejak selama eksekusi.[5]
CreateFontW, SelectObject	GDI32.dll	Mengatur elemen visual seperti teks/font dalam antarmuka [9]
CreateDialogParamW	USER32.dll	Fungsi CreateDialogParamW dalam konteks malware digunakan untuk membuat jendela dialog (dialog box) secara dinamis, dengan dukungan karakter Unicode (ditandai dengan huruf W di akhir). Fungsinya hampir sama dengan CreateWindowExW, tapi khusus untuk membuat dialog, bukan jendela utama. [9]
GetLocaleInfoW	KERNEL32.dll	Mengambil informasi lokal sistem (lokasi, zona waktu) [9]

.

3.2. Analisis Dinamis

3.2.1. Analisis Perilaku

Malware lb3.exe bertindak sebagai titik awal eksekusi dan segera melakukan privilege escalation dengan menjalankan proses cmstplua.exe untuk mendapatkan hak administratif memulai mekanisme bypass UAC [10], yang kemudian menghasilkan status threat dan memicu serangkaian proses turunan seperti shellexperiencehost.exe digunakan untuk menyamarkan exsekusi[10], sppextcomobj.exe yang memanggil slui.exe merupakan teknik penyamaran atau pengalihan aktivitas berbahaya dengan memanfaatkan proses resmi Windows agar tidak terdeteksi oleh sistem keamanan atau pengguna[10]. serta beberapa instance dari backgroundtransferhost.exe sering dimanfaatkan untuk menyamarkan aktivitas berbahaya, karena proses ini merupakan bagian dari sistem transfer data latar belakang Windows. Malware

modern mengeksploitasi proses ini untuk menjalankan komunikasi jaringan tersembunyi, menyimpan file, atau menyembunyikan aktivitas agar tidak dicurigai oleh antivirus atau analis forensik[10]. yang dijalankan secara parallel.

3.2.2. Taktik dan Teknik Serangan

Analisis dinamis LookBit.exe di Any.Run dipetakan dengan kerangka MITRE ATT&CK untuk mengidentifikasi taktik dan teknik serangan. MITRE ATT&CK adalah framework global untuk mengklasifikasikan perilaku penyerang siber secara sistematis.

Taktik	Teknik yang Dilakukan	Fungsi
Privilege Escalation	Bypass User Account Control (UAC)	Malware menggunakan CMSTPLUA.exe untuk memperoleh hak administratif. [10]
Defense Evasion	Bypass User Account Control	Teknik ini juga dipakai untuk menghindari deteksi sistem keamanan. [10]
Credential Access	-Unsecured Credentials in Files -From Web Browsers	Malware mencoba membaca kredensial dari file dan browser pengguna. [10]
Discovery	-Query Registry -System Information Discovery	Malware melakukan pencarian konfigurasi sistem dan informasi sistem.[10]
Impact	Data Encrypted for Impact	Aktivitas inti malware, yaitu mengenkripsi data korban sebagai bagian dari serangan ransomware. [10]

3.2.3. Aktivitas Registry

Selama proses eksekusi malware LookBit.exe dalam lingkungan virtual menggunakan Any.Run, dilakukan pemantauan terhadap aktivitas jaringan untuk mengidentifikasi kemungkinan komunikasi antara malware dan server eksternal (Command & Control / C2), serta deteksi akses terhadap sumber daya online. persingkat kalimat ini

Proses	Lokasi Registry	Keterangan
dllhost.exe	HKEY_CURRENT_USER\ SOFTWARE\Microsoft\ Windows\CurrentVersion\ Explorer	Menulis entri SlowContextMenuEntries, kemungkinan untuk mengganggu antarmuka pengguna.[10]
ShellExperience Host.exe	\REGISTRY\A{...}\ LocalState	Menulis entri PeekBadges, yang terkait dengan tampilan ikon dan GUI.[10]
BackgroundTransfer Host.exe	HKEY_CLASSES_ROOT\ Local Settings\ Software\Microsoft\ ...Internet Settings\Cache\...	Menulis beberapa entri pada cache konten, cookies, dan history.[10]

3.2.4. Aktivitas File

Malware menjatuhkan ratusan file ke direktori sistem tersembunyi $Recycle.Bin dengan nama-nama acak seperti AAAAAAAAAAAA dan HHHHHHHHHHHH, yang dihasilkan secara otomatis melalui skrip enkripsi atau obfuscation, termasuk file desktop.ini yang berpotensi digunakan untuk menyisipkan konfigurasi tersembunyi, sementara hash file yang identik menunjukkan adanya salinan file yang sama atau pola enkripsi tetap, dan dengan jumlah file mencapai ratusan (672 file mencurigakan dan 705 file teks), hal ini mengindikasikan adanya aktivitas enkripsi massal atau penyebaran payload ransomware secara luas ke dalam sistem. [10]

3.2.5. Connections

Mayoritas koneksi berasal dari proses sistem Windows yang sah seperti svchost.exe dan SIHClient.exe, yang berfungsi untuk sinkronisasi sistem, pembaruan sertifikat, atau pengecekan konektivitas, dengan seluruh koneksi menuju domain milik Microsoft, Digicert, dan Akamai yang telah dilabeli whitelisted oleh Any.Run, serta tidak ditemukan adanya koneksi mencurigakan ke domain pihak ketiga atau indikasi komunikasi dengan server Command & Control (C2).

4. Kesimpulan

Malware LookBit 3.0 menyerang sistem melalui metode eksekusi berlapis, dimulai dari file utama lb3.exe. Setelah dijalankan, malware segera melakukan eskalasi hak akses menggunakan proses sah Windows seperti CMSTPLUA.exe untuk melewati User Account Control (UAC) tanpa memunculkan peringatan. Setelah memperoleh hak administratif, LookBit 3.0 menjatuhkan banyak file acak ke direktori tersembunyi seperti $Recycle.Bin, serta memodifikasi registry dan cache browser untuk menyembunyikan jejak dan berpotensi mengakses data sesi pengguna. Untuk menghindari deteksi antivirus, malware ini menyamar sebagai proses sistem resmi seperti sppextcomobj.exe, ShellExperienceHost.exe, dan BackgroundTransferHost.exe. Selain itu, nilai entropi yang tinggi menunjukkan adanya teknik obfuscation atau enkripsi untuk menghindari analisis statis, sementara ketiadaan digital signature tidak menghalanginya menampilkan GUI guna menipu pengguna. Aktivitas jaringan dan DNS yang digunakan pun terlihat normal karena hanya mengarah ke domain sah seperti Digicert dan Microsoft, sehingga mampu menghindari sistem deteksi berbasis reputasi. Berdasarkan pemetaan MITRE ATT&CK, LookBit 3.0 menggunakan teknik privilege escalation, defense evasion, credential access, dan data encryption, yang menandakan bahwa malware ini dirancang secara sistematis untuk menyerang, menyembunyikan diri, dan memaksimalkan kerusakan sebelum berhasil terdeteksi.

Daftar Pustaka

[1] G. W. Wahidin, S. Syaifuddin, and Z. Sari, “Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox,” *J. Repos.*, vol. 4, no. 1, pp. 83–94, 2022, doi: 10.22219/repositor.v4i1.1373.

[2] Naufal Zuhdi, “361 Juta Serangan Siber Masuk ke Indonesia Per Oktober 2023,” Media indonesia. [Online]. Available: https://mediaindonesia.com/teknologi/630255/361-juta-serangan-siber-masuk-ke-indonesia-per-oktober-2023#goog_rewarded

[3] Agnes Z. Yonatan, “Sektor Bisnis Paling Banyak Diserang Ransomware Global 2024,” GoodStats. [Online]. Available: http://goodstats.id/article/sektor-bisnis-paling-banyak-diserang-ransomware-global-2024-sySqT

[4] Brad Slavin, “Malware Analysis in ANY.RUN: The Ultimate Guide,” ANY RUN. Accessed: Mar. 26, 2025. [Online]. Available: https://any.run/cybersecurity-blog/authors/

[5] C. F. Fahriza, “Analisis Ransomware Secara Statis dan Dinamis Untuk Pemetaan Evolusi Ransomware Analisis Ransomware Secara Statis dan Dinamis Untuk Pemetaan Evolusi Ra nsomware,” 2022.

[6] D. Prayitno, “Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware,” *Simetris*, vol. 16, no. 2, pp. 53–57, 2022, [Online]. Available: https://www.sttrcepu.ac.id/jurnal/index.php/simetris/article/view/255%0Ahttps://www.sttrcepu.ac.id/jurnal/index.php/simetris/article/download/255/165

[7] Y. Ilhamdi and Y. N. Kunang, “Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik,” *Bina Darma Conf. Comput. Sci.*, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

[8] Adenta Rubian Qiyas Syahwidi, S. Cahyono, and R. N. Yasa, “Analisis Aplikasi Cryptowallet Tiruan Terhadap Indikasi Android Malware,” *Info Kripto*, vol. 17, no. 1, pp. 23–31, 2023, doi: 10.56706/ik.v17i1.61.

[9] Microsoft, “Gambaran umum teknologi Akses Data dan Penyimpanan,” Microsoft. Accessed: Nov. 20, 2024. [Online]. Available: https://learn.microsoft.com

[10] MITRE, “ATT&CK Matrix for Enterprise,” MITRE. [Online]. Available: https://attack.mitre.org/