PENERAPAN METODOLOGI FORENSIK DIGITAL NIST SP 800-86 PASCA SERANGAN RANSOMWARE LOCKBIT 3.0
Implementation of the NIST SP 800-86 Digital Forensic Methodology After the LockBit 3 Ransomware Attack

[1]ROMMI KAESTRIA, [2]ANGGRI LUKMAN DJATTA, [3]MUHAMMAD ERFAN, [4]ELOK FAIQOTUL HIMMAH
STMIK PALANGKARAYA
Email: [1]rokafordev@gmail.com, [2]anggrilukman@gmail.com , [3]muhammad651@gmail.com , [4]el.faiqotul@gmail.com

ABSTRAK

Serangan ransomware yang semakin meningkat menjadi ancaman serius bagi keamanan sistem informasi, seperti yang terjadi pada Pusat Data Nasional Sementara (PDNS) Indonesia pada tanggal 20 Juni 2024. Serangan ini menggunakan varian ransomware LockBit 3.0 yang berhasil melumpuhkan layanan lebih dari 210 institusi pemerintahan. Oleh karena itu, Penelitian ini bertujuan untuk menerapkan metodologi forensik digital NIST SP 800-86 dalam mengidentifikasi dan menganalisis jejak digital yang ditinggalkan oleh serangan Ransomware LockBit 3.0. Penelitian dilakukan dengan metode eksperimental menggunakan pendekatan One Shot Case Study Design dalam lingkungan virtual. Akuisisi data dilakukan secara statis menggunakan perangkat lunak FTK Imager dan Belkasoft RAM Capturer, kemudian dianalisis dengan Autopsy. Analisis dilakukan dengan mengikuti empat tahap utama dari NIST SP 800-86, yaitu Collection, Examination, Analysis, dan Reporting.Hasil penelitian menunjukkan bahwa metodologi NIST SP 800-86 efektif dalam mengidentifikasi artefak digital seperti file terenkripsi, proses mencurigakan, dan perubahan sistem. Selain itu, penelitian ini memberikan rekomendasi untuk meningkatkan keamanan sistem informasi guna mencegah serangan serupa di masa depan.

Kata kunci: Forensik Digital, NIST SP 800-86, LockBit 3.0, Ransomware, Investigasi Siber

ABSTRACT

The escalating ransomware attacks pose a serious threat to information system security, as experienced by Indonesia's Temporary National Data Center (PDNS) on June 20, 2024. This attack employed the LockBit 3.0 ransomware variant, successfully paralyzing services for over 210 government institutions. Therefore, this research aims to implement the NIST SP 800-86 digital forensic methodology to identify and analyze the digital footprints left by the LockBit 3.0 ransomware attack. The research was conducted using an experimental method with a One Shot Case Study Design approach in a virtual environment. Data acquisition was performed statically using FTK Imager and Belkasoft RAM Capturer software, and subsequently analyzed with Autopsy. The analysis followed the four main phases of NIST SP 800-86, namely Collection, Examination, Analysis, and Reporting. The research results indicate that the NIST SP 800-86 methodology is effective in identifying digital artifacts such as encrypted files, suspicious processes, and system changes. Furthermore, this research provides recommendations for improving information system security to prevent similar attacks in the future.

Keywords: Digital Forensics, NIST SP 800-86, LockBit 3.0, Ransomware, Cyber Investigation

Pendahuluan

Keamanan sistem informasi merupakan aspek penting dalam dunia digital modern. Salah satu insiden besar di Indonesia adalah serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) menggunakan varian LockBit 3.0. Keamanan sistem informasi merupakan aspek penting dalam dunia digital modern. Salah satu insiden besar di Indonesia adalah serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) menggunakan varian LockBit 3.0. Serangan ini melumpuhkan lebih dari 210 institusi pemerintah.

Dari insiden tersebut, muncul kebutuhan untuk melakukan penelitian lebih lanjut dalam menjawab bagaimana teknik dan metode investigasi yang tepat dalam menghadapi

serangan siber serupa. Proses pencarian jejak digital pasca serangan sering kali terkendala oleh kompleksitas serangan yang dirancang untuk menghindari deteksi dan menutupi asal-usul serta metode yang digunakan oleh penyerang. Oleh karena itu, diperlukan pendekatan metodologis yang terstruktur untuk memperoleh hasil investigasi yang akurat dan komprehensif.

Penelitian ini bertujuan untuk menerapkan metodologi forensik digital NIST SP 800-86 untuk menganalisis dan mendokumentasikan bukti digital pasca serangan, dengan tujuan memberikan panduan sistematis bagi penanganan insiden serupa di masa depan

Metode

Penelitian ini menggunakan metode eksperimen dengan pendekatan One Shot Case Study Design dalam lingkungan virtual (Virtual Machine). Tujuannya adalah mensimulasikan serangan ransomware LockBit 3.0 secara realistis dan melakukan investigasi forensik digital menggunakan metode NIST SP 800-86.

Langkah-langkah penelitian mengikuti tahapan sistematis:

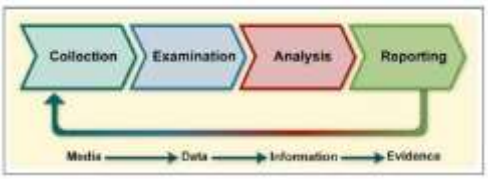
Identifikasi Masalah : Menentukan bagaimana serangan LockBit 3.0 memengaruhi sistem dan bagaimana metode forensik digital dapat mendeteksi, menganalisis, serta menjaga integritas bukti.

Studi Literatur : Menelaah penelitian terdahulu dan dokumen NIST SP 800-86 untuk memahami teknik pengumpulan dan analisis bukti digital.

Pembuatan Skenario Kasus : Simulasi serangan dilakukan dengan dua sistem: Server korban (Windows 10 Ghost Spectre) dan Server penyerang/phishing (Kali Linux)

Admin pada server korban secara tidak sadar mengunduh file berbahaya dari situs phishing sehingga sistem terenkripsi oleh ransomware.

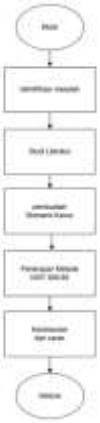
Penerapan Metodologi NIST SP 800-86, Proses investigasi mengikuti empat tahap utama: Collection (Pengumpulan) Akuisisi data volatil (RAM) menggunakan Belkasoft RAM Capturer, dan non-volatil (disk) menggunakan FTK Imager. Hasil akuisisi diverifikasi dengan teknik hashing untuk menjaga integritas.



Gambar 1.Tahapan NIST SP 800-86

Examination (Pemeriksaan) :

Analisis artefak, file, dan metadata menggunakan Autopsy dan FTK Imager untuk menemukan perubahan sistem, proses mencurigakan, dan file terenkripsi. Analysis (Analisis):Interpretasi hasil pemeriksaan untuk mengidentifikasi pola enkripsi, aktivitas malware, registry, dan komunikasi jaringan ransomware. Reporting (Pelaporan): Menyusun laporan investigasi lengkap berisi Chain of Custody, hasil analisis, kesimpulan, dan rekomendasi keamanan sistem. Menyusun hasil akhir mengenai efektivitas penerapan metode NIST SP 800-86 serta rekomendasi mitigasi terhadap serangan ransomware.Seperti pada gambar 1 berikut ini.



Gambar 2. Desain Penelitian

Kemudian menggunakan instrumen penelitian seperti pada tabel 1 berikut ini.

Tabel 1. Instrumen Penelitian

Jenis	Alat/Software	Keterangan
Akuisisi Data	Belkasoft RAM Capturer, FTK Imager, USB Write Blocker	Mengambil data volatil dan non-volatil dengan menjaga integritas
Analisis Data	Autopsy, HashMyFiles, VirusTotal	Menganalisis artefak, memverifikasi hash, mendeteksi malware

Jenis	Alat/Software	Keterangan
Simulasi Lingkungan	VirtualBox	Menjalankan dua VM: Windows 10 Ghost Spectre (korban) dan Kali Linux (penyerang)

Selanjutnya melakukan Skenario Simulasi untuk Server korban menjalankan web aplikasi berbasis PHP menggunakan XAMPP. Server penyerang meniru situs judi online yang menyebarkan file ransomware (phishing site). Setelah file dijalankan, seluruh data di server korban terenkripsi dan ditampilkan pesan tebusan (ransom note).

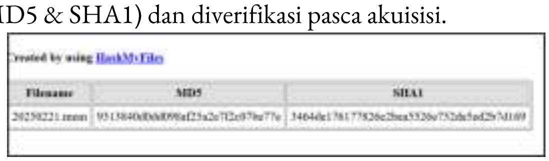
Gambar 3. Skenario Kasus

Hasil Dan Pembahasan

Penelitian ini mensimulasikan serangan LockBit 3.0 dalam lingkungan virtual untuk menguji efektivitas metodologi NIST SP 800-86 dalam investigasi forensik digital. Terdapat dua VM yang digunakan, yaitu VM korban (Windows 10 Ghost Spectre) dan VM pelaku (Kali Linux), masing-masing berperan sebagai target sistem dan penyebar ransomware melalui halaman phishing. Penerapan Metodologi NIST SP 800-86 telah dilakukan kemudian menunjukkan hasil bahwa:

Collection

Akuisisi data dilakukan dalam dua tahap: data volatil dikumpulkan menggunakan Belkasoft RAM Capturer dan data non-volatil menggunakan FTK Imager dari image disk VirtualBox. Integritas data dijaga melalui proses hashing (MD5 & SHA1) dan diverifikasi pasca akuisisi.



Created by using HashMyFiles

Filename	MD5	SHA1
[illegible]	[illegible]	[illegible]

Gambar 4.Hasil Hash file dump RAM

Menunjukkan hasil akuisisi memori volatil dan validasi integritas melalui hash. Ini sangat penting karena menegaskan keaslian data hasil akuisisi.

Examination

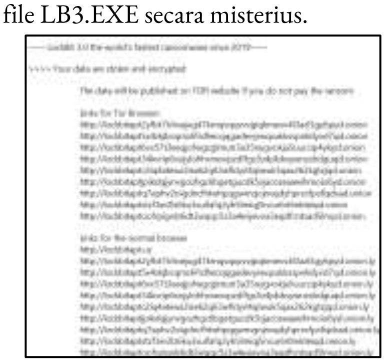
Pemeriksaan dilakukan menggunakan FTK Imager (untuk data RAM) dan Autopsy (untuk image disk). Ditemukan aktivitas mencurigakan seperti eksekusi LB3.EXE, akses situs judi online, perubahan file sistem, penghapusan log, dan penyebaran ransom note (WY3kdVRvm.README.txt) di ribuan lokasi. Beberapa URL lokal dan eksternal serta artefak program cmd.exe, svchost.exe, dan 7za.exe juga terdeteksi.

Gambar 5.Data Artifacts

Visualisasi hasil penyaringan artefak digital dalam disk image menggunakan Autopsy. Representatif untuk menunjukkan proses pemeriksaan terhadap file, metadata, dan log aktivitas.

Analysis

Dari hasil analisis, disusun kronologi serangan yang dimulai dari akses phishing hingga enkripsi data dan penghapusan log sistem. Ditemukan bukti anti-forensic behavior seperti manipulasi timestamp, pembuatan file kosong, dan hilangnya file LB3.EXE secara misterius.

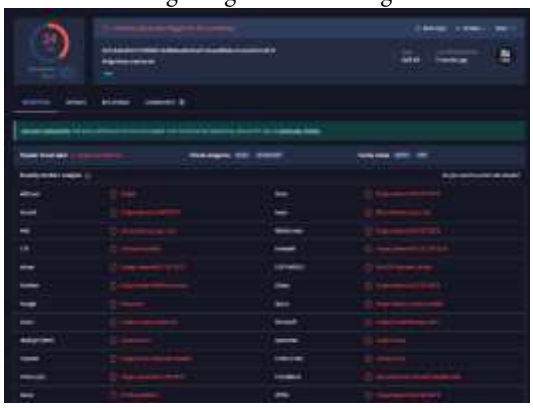


Gambar 6.Pesan dalam WY3kdVRvm.README.txt

Ini adalah ransom note yang dibuat LockBit 3.0 dan disebarkan ke seluruh sistem. Sangat khas dan identifikatif terhadap ransomware.

Selanjutnya diunggah ke virustotal.com dengan hasil pemindaian menunjukkan bahwa 24 dari 63 penyedia keamanan menandai file ini sebagai berbahaya, dengan

kategori ancaman berupa trojan dan ransomware, serta diklasifikasikan sebagai bagian dari keluarga LockBit.



Gambar 7.tampilan analisis virustotal.com

Reporting

Seluruh proses didokumentasikan dalam laporan forensik lengkap disertai chain of custody. Laporan ini dapat dijadikan acuan bagi tim keamanan siber dalam menyusun strategi mitigasi dan kebijakan penguatan sistem informasi ke depan.

Rekomendasi keamanan meliputi pelatihan keamanan siber, penggunaan backup offline, pembaruan sistem berkala, dan penerapan prinsip least privilege pada hak akses pengguna.

Simpulan Dan Saran

Penerapan metodologi NIST SP 800-86 terbukti efektif dalam mengungkap bukti digital pasca serangan ransomware LockBit 3.0. Metodologi ini membantu mengidentifikasi artefak kunci dan menyusun kronologi insiden dengan akurat. Rekomendasi yang dihasilkan dapat digunakan untuk memperkuat pertahanan sistem informasi terhadap serangan ransomware di masa depan.

Pustaka Acuan

Buku

J. Kävrestad, M. Birath, and N. Clarke, Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications, 3rd ed. Gewerbestrasse, Switzerland: Springer Nature Switzerland AG, 2024.

D. Hariyadi and et al., Buku Panduan Dasar Forensik Digital. Yogyakarta: PENERBIT BASKARA MEDIA, 2022.

I. Riadi and B. F. Muthohirin, Forensik Email, 2nd ed. Yogyakarta: Diandra Kreatif, 2022.

EC-Council, Digital Forensics Essentials, 1st ed. s.l., 2021.

C. Altheide and H. Carvey, Digital Forensics with Open Source Tools, 1st ed. Waltham: Elsevier, 2011.

A. Bhardwaj and K. Kaushik, Practical Digital Forensics. London: BPB Online, 2023.

Jurnal/Prosiding/Disertasi/Tesis/Skripsi

A. Faizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis," Journal of Information Systems and Informatics, vol. VI, no. 2, p. 705, 2024.

B. N. Nasrullayev, H. Q. Hamza ugli, T. O. Valijonovich, and D. M. Avlakulovich, "Static and Live Digital Forensics, along with Practical Examples of Tools Used for Each Approach," Texas Journal of Engineering and Technology, vol. Volume 19, pp. 21–27, 2023.

Lain-lain

K. Kent, S. Chevalier, T. Grance, and H. Dang, "NIST SP 800-86." [Online]. Available: https://csrc.nist.gov/pubs/sp/800/86/final

Kompas, "Mengenal Ransomware LockBit 3.0 Brain Cipher yang Serang PDNS dan Minta Tebusan Rp 130 Miliar." [Online]. Available: https://tekno.kompas.com/read/2024/06/25/11430077/mengenal-Ransomware-LockBit-30-brain-cipher-yang-serang-pdns-dan-minta-tebusan?page=all#google_vignette.

Socradar, "Dark Web Profile: LockBit 3.0 Ransomware." [Online]. Available: https://socradar.io/dark-web-profile-LockBit-3-0-Ransomware/.

You Need to Know." [Online]. Available: https://www.kaspersky.com/resource-center/threats/LockBit-Ransomware.