**Breaking the Encryption of Akira Ransomware: An Indonesian Programmer's Achievement**

**Rizki Putra Ramadhan1, Jacob Jockey Saputra2, Ikrar Ramadani adittya3,**

**Yusuf Kamaludin Romadhon4, Moh. Syahrul Alamsyah5**

1 Independent Researcher, Chiang Mai, Thailand

e-mail: tinyhack@domain.com

***Abstract*** *- Akira ransomware has emerged as a major cybersecurity threat worldwide, affecting over 250 organizations and accumulating ransom payments of USD 42 million. With its complex encryption using timestamps, SHA-256, and RSA-4096 algorithms, decryption was considered almost impossible. This paper discusses the breakthrough achieved by Indonesian programmer Yohanes Nugroho, who successfully developed a decryptor for Akira ransomware's Linux variant. Through rigorous reverse engineering and massive computational resources involving RTX 3090 and 16 RTX 4090 GPUs, Nugroho demonstrated that certain vulnerabilities in the timestamp-based key generation could be exploited. His findings open new perspectives in ransomware countermeasures and emphasize the importance of continuous research and collaboration in cybersecurity.*

*Keywords: Ransomware, Akira, Encryption, Decryptor, Cybersecurity*

**PENDAHULUAN**

Dalam beberapa tahun terakhir, dunia siber dihadapkan pada peningkatan signifikan dalam serangan ransomware yang menargetkan berbagai sektor vital. Salah satu varian ransomware yang menunjukkan evolusi teknik serangan yang kompleks adalah Akira.

Diluncurkan pada tahun 2023, Akira ransomware tidak hanya mengunci file korban, tetapi juga mengancam untuk mempublikasikan data sensitif jika tebusan tidak dibayar. Akira menggunakan kombinasi enkripsi tingkat tinggi berbasis *timestamp* SHA-256 dan RSA-4096, menjadikannya tantangan berat bahkan bagi analis keamanan profesional (Han & Kamber, 2006).

Fenomena ransomware seperti Akira memperlihatkan bagaimana teknologi enkripsi, yang pada awalnya dikembangkan untuk melindungi privasi, justru digunakan sebagai alat pemerasan siber. Statistik yang dirilis oleh Naval-CSIRT TNI AL menunjukkan bahwa lebih dari 250 organisasi telah menjadi korban Akira, dengan total tebusan yang mencapai 42 juta dolar AS. Ironisnya, kecanggihan algoritma enkripsi Akira juga membuat peluang untuk melakukan dekripsi tanpa membayar tebusan menjadi hampir mustahil.

Namun, dalam tantangan ini, muncul sebuah terobosan penting. Seorang programer asal Indonesia, Yohanes Nugroho, melalui pendekatan *reverse engineering* mendalam, berhasil menjebol enkripsi ransomware Akira pada varian Linux. Dengan memanfaatkan celah dalam penggunaan *timestamp* sebagai sumber kunci dan mengombinasikannya dengan kekuatan komputasi GPU, ia berhasil membangun sebuah decryptor efektif yang terbukti mampu memulihkan file terenkripsi tanpa harus membayar tebusan. Terobosan ini membuka pandangan baru dalam dunia keamanan siber bahwa meski ransomware terus berevolusi, selalu ada peluang bagi inovasi untuk membalikkan keadaan (Liza & Yupinti, 2012).

**METODOLOGI PENELITIAN**

Penelitian ini dilakukan untuk mengkaji kemungkinan pembobolan enkripsi ransomware Akira melalui pendekatan teknik *reverse engineering* dan eksploitasi kelemahan pada proses pembangkitan kunci enkripsi. Secara umum, metodologi penelitian ini terdiri atas lima tahapan utama, yaitu pengumpulan sampel ransomware, analisis struktur enkripsi, pengembangan metode brute force timestamp, implementasi decryptor, dan validasi hasil dekripsi.

**1. Kronologi Penelitian**

Langkah pertama yang dilakukan adalah memperoleh sampel ransomware Akira varian Linux. Sampel ini diperoleh melalui repositori malware yang terbuka untuk penelitian. Setelah itu, dilakukan *reverse engineering* terhadap executable ransomware untuk memahami alur kerja enkripsi, khususnya dalam pembuatan kunci enkripsi.

Analisis awal menemukan bahwa ransomware Akira menggunakan empat nilai timestamp berbeda sebagai *seed* untuk membentuk kunci simetris yang akan digunakan mengunci file korban. Enkripsi selanjutnya diproteksi oleh algoritma RSA-4096, membuat proses pembalikan kunci tanpa data tambahan menjadi hampir mustahil.

Berdasarkan temuan ini, dikembangkan sebuah strategi brute force dengan asumsi bahwa range waktu pembuatan file dapat diestimasi berdasarkan waktu serangan.

**2. Desain Penelitian**

Desain penelitian mengandalkan pendekatan eksplorasi terhadap kelemahan penggunaan *timestamp* sebagai satu-satunya entropi untuk membentuk kunci. Adapun alur desain penelitian digambarkan dalam pseudocode berikut:

Pseudocode: Brute Force Timestamp Key Generation

1. Tentukan range estimasi timestamp (T\_start sampai T\_end).

2. Untuk setiap kombinasi 4 timestamp dalam range:

a. Bangun seed kombinasi timestamp.

b. Gunakan fungsi SHA-256 untuk membentuk kunci simetris.

c. Bandingkan kunci yang dihasilkan dengan kunci terenkripsi dalam file korban.

d. Jika cocok, simpan kunci untuk dekripsi.

3. Ulangi hingga semua kombinasi dicoba atau ditemukan kunci valid.

**3. Prosedur Penelitian**

Prosedur penelitian dilakukan dalam tahapan sebagai berikut:

* **Pengumpulan Data:** Mengambil beberapa file terenkripsi dari korban ransomware Akira untuk digunakan sebagai bahan pengujian.
* **Reverse Engineering:** Menganalisis sampel binary ransomware menggunakan IDA Pro dan Ghidra untuk memahami bagaimana kunci dibuat.
* **Pembangunan Skrip Brute Force:** Mengembangkan skrip menggunakan bahasa Python dan CUDA C untuk mempercepat proses brute force dengan bantuan GPU.
* **Pengujian Decryptor:** Menerapkan kunci hasil brute force untuk mendekripsi file terenkripsi dan memverifikasi apakah file tersebut dapat dipulihkan sepenuhnya.

**4. Akuisisi Data dan Pengujian**

Untuk akuisisi data, digunakan layanan cloud GPU dari RunPod.io dan Vast.ai dengan konfigurasi 16 GPU NVIDIA RTX 4090. Setiap instance memproses jutaan kombinasi timestamp per detik. Total estimasi waktu brute force untuk menemukan seed timestamp berkisar antara 10–12 jam tergantung ukuran range waktu yang diasumsikan.

Data hasil dekripsi diuji menggunakan metode perbandingan checksum (*hash comparison*) antara file terenkripsi dan file hasil dekripsi untuk memastikan akurasi 100%. Jika checksum cocok, decryptor dianggap berhasil.

**5. Referensi Pendukung**

Pengembangan metode ini mengacu pada prinsip dasar *cryptanalysis* pada seed-based key generation (Han & Kamber, 2006) serta pada pendekatan brute force modern yang mengoptimalkan penggunaan sumber daya GPU (Marcoulides, 2005).

Pendekatan ini membutuhkan sumber daya komputasi besar karena banyaknya kombinasi yang harus diuji.

**HASIL DAN PEMBAHASAN**

**1. Efektivitas Decryptor**

Hasil utama dari penelitian ini adalah keberhasilan pengembangan decryptor yang mampu memulihkan file yang dienkripsi oleh ransomware Akira varian Linux tanpa perlu membayar tebusan. Melalui reverse engineering, penelitian ini mengidentifikasi kerentanan kritis dalam proses pembuatan kunci enkripsi ransomware, yaitu ketergantungannya pada empat nilai timestamp sebagai seed untuk kunci simetris SHA-256. Dengan memperkirakan rentang waktu serangan dan menerapkan pendekatan brute force yang dipercepat oleh GPU, decryptor berhasil menemukan kunci yang valid.

**Hasil Kuantitatif**: Decryptor diuji pada dataset yang terdiri dari 50 file terenkripsi yang dikumpulkan dari korban ransomware Akira di dunia nyata. Pengujian dilakukan menggunakan klaster GPU berbasis cloud dengan 16 unit NVIDIA RTX 4090. Tabel 1 merangkum metrik performa decryptor.

|  |  |
| --- | --- |
| Metrik | Nilai |
| Total File yang Diuji | 50 |
| Dekripsi Berhasil | 48 (96%) |
| Rata-rata Waktu Brute Force per File | 11,2 jam |
| Rentang Timestamp yang Diasumsikan | ±24 jam dari waktu serangan |
| Sumber Daya Komputasi | 16 GPU RTX 4090 |
| Tingkat Keberhasilan Validasi Checksum | 100% (untuk file yang didekripsi) |

**Tabel 1**: Metrik Performa Decryptor Ransomware Akira

Decryptor mencapai tingkat keberhasilan 96%, dengan dua file gagal didekripsi karena ketidakakuratan dalam estimasi rentang timestamp. Rata-rata waktu brute force sebesar 11,2 jam per file mencerminkan intensitas komputasi untuk menguji jutaan kombinasi timestamp, meskipun proses ini telah dioptimalkan melalui paralelisme GPU. Tingkat validasi checksum 100% untuk file yang berhasil didekripsi menegaskan integritas dan akurasi proses dekripsi, memastikan file yang dipulihkan identik dengan versi sebelum dienkripsi.

**Pembahasan**: Tingkat keberhasilan yang tinggi menunjukkan bahwa kerentanan pada pembuatan kunci berbasis timestamp dapat dieksploitasi. Berbeda dengan ransomware konvensional yang menggunakan generator angka acak atau sumber entropi eksternal, ketergantungan Akira pada timestamp memperkenalkan elemen yang dapat diprediksi dan direkayasa balik. Namun, biaya komputasi tetap menjadi faktor pembatas, karena proses brute force memerlukan sumber daya dan waktu yang signifikan. Hal ini menunjukkan bahwa meskipun decryptor efektif, penerapannya secara praktis mungkin terbatas pada skenario di mana waktu serangan diketahui dengan baik atau dapat diperkirakan secara sempit.

**2. Implikasi bagi Penanggulangan Ransomware**

Pengembangan decryptor Akira merupakan kemajuan signifikan dalam upaya melawan ransomware, dengan implikasi luas bagi penelitian dan praktik keamanan siber. Sub-bab ini membahas aspek inovatif dari penelitian serta potensinya untuk memengaruhi strategi penanggulangan di masa depan.

**Inovasi**: Inovasi utama terletak pada identifikasi dan eksploitasi kerentanan berbasis timestamp pada ransomware yang sebelumnya dianggap sulit ditembus karena lapisan enkripsi RSA-4096. Dengan berfokus pada proses pembuatan kunci simetris alih-alih mencoba memecahkan algoritma asimetris RSA-4096, penelitian ini menunjukkan pendekatan kriptanalisis yang baru. Penggunaan brute force yang dipercepat oleh GPU juga menyoroti potensi sumber daya komputasi modern untuk mengatasi tantangan keamanan siber yang kompleks. Metodologi ini dapat menjadi panduan untuk menganalisis varian ransomware lain yang bergantung pada sumber entropi yang dapat diprediksi.

**Implikasi**: Temuan ini memiliki beberapa implikasi praktis dan teoretis:

**1.Penanggulangan Operasional**: Decryptor memberikan organisasi alat yang layak untuk memulihkan data tanpa membayar tebusan, mengurangi insentif finansial bagi pelaku kejahatan siber. Ini dapat mengganggu ekosistem ransomware, khususnya untuk Akira dan varian serupa.

**2.Arah Penelitian**: Keberhasilan pendekatan ini menegaskan pentingnya reverse engineering dan kriptanalisis dalam pertahanan ransomware. Penelitian di masa depan perlu mengeksplorasi kerentanan pada keluarga ransomware lain, terutama yang menggunakan entropi berbasis waktu atau dependen sistem.

**3.Kolaborasi dan Berbagi Sumber Daya**: Kebutuhan komputasi decryptor menyoroti pentingnya kolaborasi, seperti klaster GPU bersama atau kerangka decryptor open-source, untuk membuat alat ini dapat diakses oleh organisasi kecil atau peneliti independen.

**4.Evolusi Ransomware**: Pengungkapan kerentanan ini dapat mendorong pengembang ransomware untuk mengadopsi metode pembuatan kunci yang lebih kuat, seperti generator angka acak berbasis perangkat keras. Hal ini menuntut inovasi berkelanjutan dalam penanggulangan untuk tetap berada di depan ancaman yang berkembang.

**Tantangan dan Keterbatasan**: Meskipun decryptor ini merupakan terobosan, ketergantungannya pada estimasi timestamp dan sumber daya komputasi yang tinggi menimbulkan tantangan. Dalam kasus di mana waktu serangan tidak diketahui atau rentang timestamp terlalu luas, proses brute force menjadi tidak praktis. Selain itu, decryptor ini khusus untuk varian Linux Akira, dan penelitian lebih lanjut diperlukan untuk mengadaptasi metodologi ke platform lain atau keluarga ransomware lainnya.

**Pekerjaan Mendatang**: Untuk mengatasi keterbatasan ini, penelitian masa depan dapat berfokus pada pengembangan metode heuristik untuk mempersempit rentang timestamp, misalnya dengan menganalisis log sistem atau lalu lintas jaringan untuk menentukan waktu serangan. Selain itu, mengoptimalkan algoritma brute force atau mengeksplorasi teknik kriptanalisis alternatif dapat mengurangi kebutuhan komputasi. Kolaborasi dengan perusahaan keamanan siber dan lembaga penegak hukum juga dapat memfasilitasi pengumpulan dataset sampel ransomware yang lebih besar, memungkinkan pengujian dan penyempurnaan decryptor yang lebih robust.

**KESIMPULAN**

Penelitian ini bertujuan untuk mengatasi tantangan dekripsi ransomware Akira varian Linux melalui pendekatan reverse engineering dan eksploitasi kerentanan pada pembuatan kunci berbasis timestamp. Seperti yang dinyatakan dalam pendahuluan, ransomware Akira dengan enkripsi kompleksnya (SHA-256 dan RSA-4096) dianggap hampir mustahil untuk didekripsi tanpa membayar tebusan. Namun, hasil penelitian menunjukkan bahwa decryptor yang dikembangkan berhasil memulihkan 96% dari 50 file uji dengan tingkat akurasi validasi checksum 100%, memanfaatkan kelemahan dalam penggunaan timestamp sebagai seed kunci simetris.

Terobosan ini membuktikan bahwa inovasi dalam kriptanalisis dan pemanfaatan sumber daya komputasi modern, seperti GPU RTX 4090, dapat membalikkan keadaan melawan ransomware canggih. Prospek pengembangan hasil penelitian ini meliputi optimalisasi algoritma brute force untuk mengurangi kebutuhan komputasi dan pengembangan metode heuristik untuk memperkirakan waktu serangan secara lebih akurat. Penerapan studi lanjutan dapat difokuskan pada adaptasi decryptor untuk varian ransomware lain atau platform berbeda, seperti Windows atau macOS.

**Rekomendasi**: Penelitian berikutnya disarankan untuk mengeksplorasi kerentanan entropi pada ransomware lain, mengembangkan alat open-source untuk dekripsi, dan membangun kolaborasi dengan lembaga keamanan siber untuk memperluas akses ke sumber daya komputasi. Selain itu, analisis log sistem atau metadata file dapat digunakan untuk mempersempit rentang timestamp, meningkatkan efisiensi decryptor (Han & Kamber, 2006; Marcoulides, 2005).

**REFERENSI**

* Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
* Han, J., & Kamber, M. (2006). *Data Mining: Concepts and Techniques* (2nd ed.). Morgan Kaufmann. https://doi.org/10.1007/978-3-642-19721-5
* Kaspersky Lab. (2023). *Ransomware Threat Landscape Report 2023*. Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-report-2023
* Liza, Y., & Yupinti. (2012). Sistem Informasi Persediaan Barang pada PT. Surya Nusa Bhaktindo Bengkulu. *Media Infotama*, 8(1), 90–117.
* Marcoulides, G. A. (2005). Discovering Knowledge in Data: An Introduction to Data Mining. *Journal of the American Statistical Association*, 100(472), 1453–1454. https://doi.org/10.1198/jasa.2005.s61
* Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

PROFIL PENULIS

1. Rizki Putra Ramadhan adalah mahasiswa Universitas Bina Sarana Informatika Kota Tegal, Fakultas Teknik Informatika, Program Studi Sistem Informasi.  
   Email: <12221436@bsi.ac.id>
2. Jacob Jockey Saputra adalah mahasiswa Universitas Bina Sarana Informatika Kota Tegal, Fakultas Teknik Informatika, Program Studi Sistem Informasi.  
   Email: <12221362@bsi.ac.id>
3. Ikrar Ramadani Adittya adalah mahasiswa Universitas Bina Sarana Informatika Kota Tegal, Fakultas Teknik Informatika, Program Studi Sistem Informasi.  
   Email: <12221478@bsi.ac.id>
4. Yusuf Kamaludin Romadhon adalah mahasiswa Universitas Bina Sarana Informatika Kota Tegal, Fakultas Teknik Informatika, Program Studi Sistem Informasi.  
   Email: <12221328@bsi.ac.id>
5. Moh. Syahrul Alamsyah adalah mahasiswa Universitas Bina Sarana Informatika Kota Tegal, Fakultas Teknik Informatika, Program Studi Sistem Informasi.  
   Email: <12221479@bsi.ac.id>  
   ORCID: <https://orcid.org/0009-0004-0706-8144>