Cerdika: Jurnal Ilmiah Indonesia, Maret 2025, 5 (3), 1147-1166
p-ISSN: 2774-6291 e-ISSN: 2774-6534

Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

MODEL PEMOLISIAN SIBER: PENDEKATAN COMMUNITY POLICING DAN E-POLICING DALAM PENANGGULANGAN KEJAHATAN RANSOMWARE

Fajri Anbiyaa
Sekolah Tinggi Ilmu Kepolisian, Indonesia
Email: fajri.anbiyaa@gmail.com

Abstrak
Penelitian ini menganalisis fenomena penyebaran ransomware melalui aplikasi palsu (APK) di Indonesia, dengan fokus pada teknik rekayasa sosial yang digunakan oleh pelaku dan dampaknya terhadap korban. Metode yang digunakan adalah kualitatif-deskriptif dengan pendekatan analisis tematik. Hasil penelitian menunjukkan bahwa penyebaran ransomware sering dilakukan melalui pesan yang tampak sah, seperti undangan pernikahan, yang memicu korban untuk mengunduh APK berbahaya. Teknik rekayasa sosial ini memanfaatkan kepercayaan dan urgensi, sehingga korban sering kali tidak menyadari bahwa mereka terinfeksi hingga data mereka dienkripsi. Dampak yang dialami korban sangat beragam, mulai dari kehilangan data pribadi dan kerugian finansial hingga stres emosional yang signifikan. Penelitian ini juga mengusulkan model pemolisian berbasis komunitas dan e-policing sebagai langkah pencegahan yang efektif. Dengan meningkatkan literasi digital masyarakat dan kolaborasi antara polisi dan masyarakat, diharapkan risiko serangan ransomware dapat diminimalkan di masa depan, sehingga menciptakan lingkungan digital yang lebih aman bagi semua.

Kata kunci: Ransomware; APK palsu; rekayasa sosial; pemolisian komunitas; e-policing

Abstract
This study analyzes the phenomenon of the spread of ransomware through fake applications (APKs) in Indonesia, focusing on the social engineering techniques used by perpetrators and their impact on victims. The method used is qualitative-descriptive with a thematic analysis approach. The results show that the spread of ransomware is often carried out through legitimate-looking messages, such as wedding invitations, which trigger victims to download malicious APKs. These social engineering techniques leverage trust and urgency, so victims often don't realize they're infected until their data is encrypted. The impact experienced by victims is very diverse, ranging from loss of personal data and financial losses to significant emotional stress. The study also proposes a community-based policing and e-policing model as effective preventive measures. By increasing people's digital literacy and collaboration between the police and the public, it is hoped that the risk of ransomware attacks can be minimized in the future, thereby creating a safer digital environment for all.

***Keywords**: Ransomware; fake APKs; social engineering; community policing; e-policing*

**Correspondence Author: Fajri Anbiyaa*
Email: fajri.anbiyaa@gmail.com

PENDAHULUAN

Kejahatan siber telah menjadi ancaman yang semakin signifikan seiring dengan perkembangan teknologi informasi dan komunikasi (Djanggih & Qamar, 2018; Fediro & Tata Sutabri, 2023; Laksana & Mulyani, 2024; Rompi & Muaja, 2021). Di antara berbagai bentuk kejahatan siber, ransomware telah muncul sebagai salah satu ancaman yang paling merusak dan menakutkan. Ransomware adalah jenis malware yang mengenkripsi data korban, sehingga tidak dapat diakses, bahkan menuntut pembayaran tebusan untuk mendekripsi data tersebut. Salah satu metode penyebaran ransomware yang semakin populer di Indonesia adalah melalui APK (Android Package) palsu yang disebarkan menggunakan aplikasi pesan instan seperti WhatsApp (Khan et al., 2022; Sulisdyantoro & Marzuki, 2023; Tamhidah, 2023).

Fenomena ini menarik perhatian karena penyebaran ransomware melalui APK palsu sangat efektif dan sulit dideteksi. Pelaku kejahatan sering menggunakan teknik rekayasa sosial (social engineering) untuk menipu korban agar mengunduh dan menginstal APK tersebut. Pesan-pesan yang dikirim oleh pelaku biasanya berisi undangan pernikahan, tawaran diskon besar, atau hadiah menarik yang sulit ditolak oleh korban (Salahdine & Kaabouch, 2019; Syafitri et al., 2022; Venkatesha et al., 2021; Wang et al., 2020). Setelah korban menginstal APK tersebut, ransomware segera menginfeksi perangkat dan mengenkripsi data penting hingga melakukan cloning. Pelaku kemudian kemudian menyalahgunakan aplikasi dalam perangkat korban untuk memperoleh keuntungan finansial melalui berbagai modus penipuan.

Kasus-kasus ransomware melalui APK palsu tidak hanya menimbulkan kerugian finansial yang besar, tetapi juga berdampak pada keamanan dan privasi individu (Arisandy, 2021; Hartono, 2023; Tajriyani, 2021; Wijanarko et al., 2023). Data pribadi yang terenkripsi mencakup informasi sensitif seperti foto, kontak, pesan, dan dokumen penting. Selain itu, serangan ransomware juga dapat merusak reputasi individu dan organisasi yang menjadi korban, serta mengganggu aktivitas bisnis dan operasional.

Dalam beberapa tahun terakhir, angka kejahatan siber di Indonesia mengalami peningkatan yang signifikan. Menurut data dari BSSN (Badan Siber dan Sandi Negara), pada tahun 2022, terdapat lebih dari 290 juta serangan siber yang terjadi di Indonesia. Di antara berbagai jenis kejahatan siber, ransomware merupakan ancaman yang paling merugikan. Berdasarkan laporan dari CS Ventures, diperkirakan bahwa serangan ransomware akan merugikan dunia hingga $20 miliar pada tahun 2021, meningkat dari $8 miliar pada tahun 2018 (Morgan, 2019).

Namun, literasi digital di kalangan masyarakat Indonesia masih relatif rendah (Firmansyah et al., 2022; Nugraha, 2022). Sebuah survei yang dilakukan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) pada tahun 2021 menunjukkan bahwa meskipun tingkat penetrasi internet di Indonesia mencapai 73,7%, kesadaran akan ancaman siber seperti ransomware masih terbatas . Survei tersebut juga mengungkapkan bahwa banyak pengguna internet di Indonesia tidak memiliki pengetahuan yang memadai tentang cara melindungi diri dari serangan siber (Levinda, 2023).

Dalam konteks pencegahan dan penegakan hukum, menanggulangi kejahatan siber, terutama ransomware, memerlukan pendekatan yang komprehensif dan kolaboratif. Community policing, atau pemolisian berbasis komunitas, muncul sebagai model yang potensial untuk mengatasi tantangan ini. Community policing menekankan pentingnya

kemitraan antara polisi dan masyarakat dalam mencegah dan menanggulangi kejahatan. Selain itu, penggunaan teknologi informasi dan komunikasi yang canggih, atau e-policing, juga dapat mendukung upaya penegakan hukum dengan memungkinkan pemantauan dan deteksi ancaman yang lebih efektif.

Namun, penerapan pemolisian dalam konteks siber juga menghadapi tantangan tersendiri. Salah satu tantangan utama adalah rendahnya tingkat kesadaran dan literasi digital di kalangan masyarakat. Banyak individu yang masih belum menyadari bahaya ransomware dan cara melindungi diri dari serangan tersebut. Oleh karena itu, edukasi dan pelatihan yang berkelanjutan sangat diperlukan untuk meningkatkan kesiapan dan respons masyarakat terhadap ancaman siber.

Penelitian ini bertujuan untuk menganalisis fenomena penyebaran ransomware melalui APK palsu di Indonesia, dengan menggunakan berbagai teori yang relevan, seperti Space Transition Theory, Social Learning Theory, dan Routine Activity Theory. Selain itu, artikel ini juga akan mengusulkan model pemolisian yang tepat untuk mencegah dan menanggulangi kejahatan siber ini melalui pendekatan community policing dan e-policing. Diharapkan, penelitian ini dapat memberikan kontribusi yang berarti bagi pengembangan ilmu kepolisian dan kebijakan keamanan siber di Indonesia.

Meskipun banyak penelitian sebelumnya telah membahas tentang ransomware dan serangan siber, masih ada kesenjangan signifikan dalam pemahaman mendalam mengenai mekanisme spesifik serangan yang dilakukan melalui aplikasi palsu (APK). Banyak studi terfokus pada aspek teknis dari ransomware, namun kurang menyoroti elemen rekayasa sosial yang menjadi kunci dalam menipu korban. Penelitian ini berupaya menjembatani kesenjangan tersebut dengan menganalisis teknik rekayasa sosial yang digunakan pelaku, sehingga memberikan wawasan yang lebih komprehensif tentang bagaimana individu dapat lebih baik dilindungi dari serangan semacam ini. Selain itu, dengan mengidentifikasi faktor-faktor yang mendorong individu menjadi pelaku kejahatan siber, penelitian ini juga mengisi kekosongan dalam literatur yang ada, yang sering kali hanya mencakup analisis dari sisi korban.

Novelty dari artikel ini terletak pada pengembangan model pemolisian yang terintegrasi, yang tidak hanya berfokus pada penegakan hukum, tetapi juga pada pendekatan pencegahan melalui partisipasi masyarakat dan kolaborasi sektor swasta. Dengan memanfaatkan konsep community policing dan e-policing, penelitian ini menawarkan solusi inovatif yang melibatkan semua pemangku kepentingan dalam upaya pencegahan kejahatan siber. Penekanan pada kerjasama antara polisi, masyarakat, dan sektor swasta merupakan pendekatan baru yang diharapkan dapat meningkatkan efektivitas strategi pencegahan ransomware. Dengan demikian, artikel ini tidak hanya memberikan analisis mendalam tentang serangan ransomware, tetapi juga menawarkan rekomendasi praktis yang dapat diterapkan untuk menciptakan lingkungan digital yang lebih aman.

Selain itu penulisan artikel ini diharapkan dapat memberikan beberapa manfaat, baik secara teoritis maupun praktis. Secara teoritis, artikel ini bertujuan untuk menyumbangkan pengetahuan baru dalam literatur ilmu kepolisian dan keamanan siber, khususnya terkait dengan fenomena ransomware yang disebarkan melalui APK palsu. Secara praktis, artikel ini diharapkan dapat memberikan panduan bagi penegak hukum dalam mengidentifikasi dan menanggulangi kejahatan siber ransomware.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-deskriptif untuk menggambarkan fenomena ransomware yang disebarkan melalui APK palsu di Indonesia secara mendalam dan menyeluruh. Pendekatan ini menekankan analisis sistematis terhadap data sekunder yang relevan, bertujuan memahami pola, modus operandi, dan dampak dari kejahatan ransomware. Kualitatif dipilih karena fokus utamanya adalah pada pemahaman mendalam terhadap fenomena sosial dan perilaku yang memengaruhi kejahatan ini, sesuai dengan pandangan Creswell tentang eksplorasi makna dalam konteks sosial. Deskripsi fenomena dilakukan untuk memberikan gambaran komprehensif mengenai objek penelitian, dengan pendekatan deskriptif yang mengidentifikasi karakteristik dan hubungan antar variabel tanpa manipulasi subjek. Kombinasi pendekatan ini diharapkan dapat memberikan kontribusi signifikan dalam memahami ransomware melalui APK palsu, serta merumuskan strategi aplikatif untuk pencegahan dan penanggulangannya.

Jenis Penelitian

Penelitian ini bersifat analitis-eksploratif. Penelitian analitis dilakukan untuk memahami data dan informasi terkait fenomena ransomware melalui kerangka teori yang relevan, seperti Space Transition Theory, Social Learning Theory, dan Routine Activity Theory. Sementara itu, penelitian eksploratif bertujuan untuk menggali lebih dalam pola-pola kejahatan ransomware, khususnya yang menyebar melalui APK palsu, serta dampaknya terhadap masyarakat. Tujuan dari jenis penelitian ini adalah:

1. Mengeksplorasi pola-pola kejahatan ransomware: Melalui analisis dokumen, laporan kasus, dan putusan pengadilan.
2. Menganalisis data berdasarkan teori: Menggunakan teori-teori yang relevan untuk memahami faktor penyebab, modus operandi, dan dampak kejahatan ransomware.
3. Menyusun rekomendasi kebijakan: Mengembangkan strategi pencegahan dan penanggulangan berbasis pendekatan teoritis dan data empiris.

Sumber data

Penelitian ini menggunakan data sekunder sebagai sumber utama, dengan fokus pada dokumen dan laporan yang relevan. Sumber data yang digunakan meliputi dokumen resmi dan laporan statistik dari Badan Siber dan Sandi Negara (BSSN) mengenai tren kejahatan siber, serta laporan dari lembaga internasional seperti Cyber Security Ventures tentang dampak global ransomware. Selain itu, penelitian juga mengacu pada putusan pengadilan, seperti Putusan Pengadilan Negeri Pekalongan No. 300/Pid.Sus/2023/PN Pkl, yang memberikan gambaran tentang modus operandi ransomware melalui aplikasi palsu. Literatur ilmiah, termasuk buku dan artikel jurnal, juga menjadi sumber penting yang membahas teori kejahatan siber dan strategi penanggulangan. Terakhir, informasi dari media daring seperti Twitter dan Facebook digunakan untuk mengidentifikasi perkembangan terbaru kasus ransomware di Indonesia dan respons masyarakat. Dengan mengintegrasikan berbagai sumber data ini, penelitian dapat memberikan analisis menyeluruh dari akar masalah hingga rekomendasi solusi yang aplikatif.

Teknik pengumpulan data

Teknik pengumpulan data dalam penelitian ini berfokus pada penggunaan data sekunder dengan tahapan sistematis untuk memastikan relevansi dan validitas informasi. Metode yang digunakan meliputi studi dokumen, di mana peneliti mengumpulkan informasi dari berbagai sumber, seperti putusan Pengadilan Negeri Pekalongan No. 300/Pid.Sus/2023/PN Pkl yang memberikan gambaran konkret mengenai modus operandi dan dampak ransomware melalui aplikasi palsu, laporan resmi dari Badan Siber dan Sandi Negara (BSSN) tentang statistik kejahatan siber di Indonesia, serta publikasi akademik yang mencakup teori-teori terkait kejahatan siber seperti Space Transition Theory, Social Learning Theory, dan Routine Activity Theory. Selain itu, penelusuran media massa dilakukan untuk memperoleh informasi tambahan dari laporan berita daring yang memberikan perspektif terkini tentang kasus ransomware, termasuk kronologi peristiwa yang membantu memperkaya analisis fenomena kejahatan ini.

Teknik analisis data

Teknik analisis data dalam penelitian ini dilakukan secara kualitatif dengan pendekatan analisis tematik dan teoritis. Langkah pertama adalah reduksi data, di mana data yang diperoleh dari studi dokumen dan penelusuran media diklasifikasikan berdasarkan relevansi, sehingga informasi yang tidak relevan atau redundan dieliminasi untuk mempertajam fokus analisis. Selanjutnya, penyajian data dilakukan dalam bentuk deskripsi naratif untuk memberikan gambaran menyeluruh tentang fenomena ransomware, termasuk pola-pola kejahatan, faktor penyebab, dan dampaknya terhadap korban. Analisis tematik kemudian dilakukan untuk mengidentifikasi tema-tema utama yang muncul dari data, seperti pola penyebaran ransomware melalui aplikasi palsu, teknik rekayasa sosial yang digunakan pelaku, dan faktor yang memengaruhi kerentanan korban. Hasil analisis ini dikaitkan dengan teori-teori yang digunakan, seperti Space Transition Theory untuk memahami perilaku pelaku dalam dunia siber, Social Learning Theory untuk menganalisis pembelajaran pelaku dari komunitas daring, dan Routine Activity Theory untuk menjelaskan kondisi situasional yang memungkinkan kejahatan terjadi. Langkah terakhir adalah penarikan kesimpulan berdasarkan hasil analisis, yang digunakan untuk merumuskan rekomendasi kebijakan dalam pencegahan dan penanggulangan ransomware di Indonesia.

HASIL DAN PEMBAHASAN

1. Deskripsi Kasus Link APK Palsu yang Berisi Ransomware di Indonesia

Kejahatan siber dengan menggunakan link APK palsu yang berisi ransomware telah menjadi fenomena yang mengkhawatirkan di Indonesia. Pelaku kejahatan ini menggunakan teknik rekayasa sosial untuk menipu korban agar mengunduh aplikasi berbahaya yang dikemas dalam bentuk APK (Android Package). Modus operandi yang sering digunakan adalah mengirimkan pesan melalui aplikasi media sosial seperti WhatsApp, berisi undangan pernikahan, tawaran diskon besar, atau hadiah menarik. Pesan-pesan ini dirancang untuk menarik perhatian dan rasa ingin tahu korban, sehingga mereka terdorong untuk mengklik link dan mengunduh APK tersebut.

Setelah APK palsu diinstal, ransomware segera menginfeksi perangkat korban dan mengenkripsi data penting. Selain itu, ransomware ini juga mengkloning perangkat korban,

memungkinkan pelaku untuk mengakses daftar kontak dan mengirimkan pesan kepada kontak-kontak tersebut dengan modus meminjam uang atau meminta bantuan finansial, seolah-olah pesan tersebut dikirimkan oleh korban sendiri. Hal ini menambah kompleksitas kejahatan, karena banyak kontak korban yang tidak menyadari bahwa pesan tersebut sebenarnya berasal dari pelaku.

Untuk memberikan gambaran lebih jelas tentang fenomena ini, berikut adalah contoh konkret dari kasus yang telah terjadi di Indonesia beserta dampaknya terhadap korban, berdasarkan data Putusan Pengadilan Negeri Pekalongan No. 300/Pid.Sus/2023/PN Pkl

Dalam kasus ini, terdakwa Rizki Darmawan bin Umar diadili karena terbukti mengirimkan link APK palsu melalui WhatsApp kepada korban. Rizki menggunakan pesan yang berisi undangan pernikahan untuk menipu korban agar mengunduh APK tersebut. Setelah korban menginstal aplikasi, ransomware segera mengenkripsi semua data penting di perangkatnya dan mengkloning perangkat tersebut. Selanjutnya, Rizki mengirimkan pesan kepada seluruh kontak korban, meminta pinjaman uang dengan alasan mendesak.

Pada 27 Juni 2023, Saksi Reno Yulensi membeli file APK undangan pernikahan secara online dari seseorang bernama Asek melalui WhatsApp seharga Rp.500.000. Tujuannya adalah untuk mengambil alih akun WhatsApp milik orang lain tanpa sepengetahuan pemiliknya. Reno kemudian memberikan nomor handphone miliknya yang terkoneksi dengan aplikasi Telegram untuk menerima kode OTP yang akan digunakan untuk mengaktifkan akun WhatsApp milik orang lain pada perangkat lain.

Setelah mendapatkan file APK undangan pernikahan, Reno dan Iswani Bin Sanusi membuat rencana untuk mendapatkan uang dari orang lain dengan cara berpura-pura meminjam uang menggunakan akun WhatsApp milik orang lain yang telah diambil alih. Reno bertugas untuk mengirimkan file APK dan mengambil alih akun WhatsApp milik orang lain serta menyiapkan nomor rekening untuk menampung atau menerima uang, sedangkan Iswani bertugas mengirim pesan seolah-olah dari pemilik akun sebenarnya yang berisi permintaan bantuan dengan modus meminjam uang.

Pada 24 Juli 2023, Saksi Nabila Fanessa menerima telepon dari nomor yang digunakan oleh Kapolda Jawa Tengah, Drs. Ahmad Luthfi, namun tidak sempat terangkat. Kemudian nomor tersebut mengirimkan pesan WhatsApp meminta bantuan transfer uang sebesar Rp. 3.000.000 dan kemudian Rp. 10.000.000 dengan janji akan dikembalikan malam itu juga. Nabila, yang mengenal nomor tersebut sebagai nomor Kapolda, tidak menaruh curiga dan melakukan transfer sesuai permintaan.

Pelaku menggunakan teknik rekayasa sosial dengan mengirimkan pesan yang berisi undangan pernikahan melalui WhatsApp. Setelah korban mengunduh dan menginstal APK tersebut, ransomware segera menginfeksi perangkat korban dan mengkloning perangkat tersebut. Pelaku kemudian mengirimkan pesan kepada seluruh kontak korban dengan modus meminjam uang atau meminta bantuan finansial. Dalam eksekusi kejahatannya, pelaku menggunakan identitas yang dikenal oleh korban (dalam kasus ini, nomor telepon Kapolda Jawa Tengah) untuk menipu korban agar melakukan transfer uang.

Motif utama dari kejahatan ini adalah keuntungan finansial. Pelaku menggunakan ransomware untuk mengenkripsi data korban dan mengkloning perangkat korban, kemudian memanfaatkan akses ke kontak-kontak korban untuk meminta uang. Uang yang didapat dari hasil kejahatan ini digunakan untuk membayar hutang dan memenuhi kebutuhan sehari-hari pelaku.

Dampak dari kejahatan ini sangat merugikan korban, baik dari segi finansial maupun psikologis. Dalam kasus Nabila Fanessa, kerugian finansial yang dialami mencapai Rp. 13.000.000. Selain kerugian finansial, korban juga mengalami tekanan psikologis karena harus menghubungi semua kontak untuk menjelaskan bahwa pesan tersebut adalah hasil dari kejahatan siber. Kejahatan ini tidak hanya merugikan korban secara individu, tetapi juga menimbulkan dampak yang lebih luas pada masyarakat. Kepercayaan terhadap komunikasi digital dan transaksi online dapat menurun, yang pada akhirnya mempengaruhi berbagai aspek kehidupan digital di Indonesia.

Pelaku dalam kasus ini tidak bertindak sendirian. Mereka bekerja dalam sebuah jaringan yang terorganisir dengan baik. Reno Yulensi bekerja sama dengan Iswani Bin Sanusi untuk mengirimkan pesan palsu dan meminta transfer uang. Mereka juga menggunakan pihak ketiga untuk mendapatkan rekening bank yang akan digunakan untuk menampung uang hasil kejahatan. Dalam hal ini, mereka membeli rekening bank atas nama Rizki Darmawan dari Hidayat Ainur Riski.

Kasus ini menunjukkan betapa canggih dan terorganisirnya kejahatan siber dengan modus link APK palsu yang berisi ransomware. Pelaku memanfaatkan teknik rekayasa sosial dan kelemahan dalam sistem keamanan digital untuk menipu korban dan mendapatkan keuntungan finansial.

2. Bagaimana Kejahatan Siber Bisa Terjadi Khususnya Ransomware di Indonesia

Cyber Culture adalah studi tentang budaya di ruang siber atau internet. Menurut Nasrullah, cyber culture ini berlangsung secara global dan universal melalui medium internet. Dalam konteks Indonesia, cyber culture memainkan peran penting dalam bagaimana kejahatan siber seperti ransomware dapat terjadi dan menyebar. Budaya siber mencakup norma, nilai, dan praktik yang berkembang di dalam komunitas online.

Budaya Indonesia memiliki ciri khas yang kuat dalam hal penghormatan dan interaksi sosial. Misalnya, undangan pernikahan, acara keluarga, dan pertemuan sosial lainnya sangat dihargai dan dianggap penting. Orang Indonesia cenderung merasa senang dan dihormati jika mereka diundang ke suatu acara. Dalam konteks cyber culture, pelaku kejahatan siber memanfaatkan aspek ini dengan mengirimkan undangan pernikahan palsu melalui WhatsApp yang mengandung ransomware. Undangan ini menarik perhatian korban karena sesuai dengan norma budaya yang ada, di mana undangan dianggap sebagai bentuk penghormatan.

Pelaku memanfaatkan kelemahan ini dengan menggunakan teknik rekayasa sosial untuk menipu korban agar mengunduh APK palsu yang berisi ransomware. Begitu APK diunduh dan diinstal, ransomware menginfeksi perangkat korban dan mengenkripsi data penting. Selain itu, ransomware juga mengkloning perangkat korban, memungkinkan pelaku untuk mengakses daftar kontak dan mengirimkan pesan kepada kontak-kontak tersebut dengan modus meminjam uang atau meminta bantuan finansial.

Dalam budaya siber, anonimitas yang diberikan oleh internet memungkinkan individu untuk berperilaku dengan cara yang mereka tidak akan lakukan di dunia nyata. Anonimitas ini mengurangi hambatan sosial dan moral, memungkinkan pelaku untuk bertindak dengan lebih bebas dan agresif. Budaya siber yang mendukung kebebasan berekspresi dan berbagi informasi juga menciptakan lingkungan yang kondusif bagi perilaku kriminal. Misalnya, pelaku dapat belajar teknik kejahatan siber dari forum-forum

online atau komunitas hacker, dan kemudian menerapkan pengetahuan tersebut dalam serangan mereka.

3. Analsis Mengapa Seseorang Menjadi Pelaku

Space Transition Theory dikemukakan oleh Jaishankar pada tahun 2008 dan menjelaskan bagaimana perilaku konformitas dan non-konformitas seseorang dapat berpindah dari dunia nyata ke dunia siber dan sebaliknya. Teori ini sangat relevan dalam memahami mengapa seseorang menjadi pelaku kejahatan siber.

Dunia siber menawarkan ruang yang berbeda dari dunia fisik, di mana individu dapat berpindah dengan mudah dan anonim (space mobility). Pelaku kejahatan siber, yang mungkin memiliki dorongan kriminal yang tertekan di dunia nyata karena takut akan konsekuensi, dapat menemukan kebebasan untuk bertindak di dunia siber di mana identitas mereka dapat disembunyikan (anonimity). Dalam kasus Rizki Darmawan, identitasnya bisa disembunyikan di dunia siber, memungkinkan dia untuk melakukan kejahatan tanpa takut akan konsekuensi sosial dan hukum yang ada di dunia nyata.

Selain itu, dunia siber memungkinkan individu untuk beradaptasi dengan norma dan aturan yang berbeda (behavorial flexibility). Pelaku kejahatan siber seperti Rizki mungkin berperilaku sesuai dengan norma kriminal di dunia siber yang berbeda dari norma konformitas yang mereka ikuti di dunia nyata. Dunia siber memberikan mereka lingkungan di mana perilaku non-konformitas lebih diterima atau bahkan didorong.

Anonimitas dan fleksibilitas identitas di dunia siber memungkinkan individu untuk menciptakan identitas baru yang berbeda dari identitas mereka di dunia nyata (identity flexibility). Pelaku seperti Rizki dapat menggunakan identitas palsu atau anonim untuk melakukan tindakan kriminal tanpa takut akan dikenali. Dalam kasus ransomware, Rizki dapat menyamar sebagai teman atau anggota keluarga korban untuk meminta uang.

Kontrol sosial di dunia siber lebih lemah dibandingkan dengan dunia nyata (diminished social control). Pelaku kejahatan siber seperti Rizki merasa lebih bebas untuk bertindak tanpa takut akan penegakan hukum yang efektif. Ketika mekanisme pengawasan dan penegakan hukum di dunia siber tidak sekuat di dunia nyata, pelaku merasa lebih aman untuk melakukan kejahatan.

Menggunakan Space Transition Theory, kita dapat melihat bahwa dunia siber memberikan ruang bagi pelaku untuk berperilaku berbeda dari dunia nyata. Rizki Darmawan, dalam kasus putusan Pengadilan Negeri Pekalongan, mungkin tidak akan melakukan kejahatan di dunia nyata karena takut akan konsekuensi sosial dan hukum. Namun, di dunia siber, identitasnya bisa disembunyikan, dan kontrol sosial lebih lemah. Fleksibilitas identitas dan anonimitas di dunia siber memungkinkan Rizki untuk melakukan kejahatan tanpa takut dikenali. Anonimitas ini juga memberikan rasa aman yang lebih besar, mendorong Rizki untuk melanjutkan aktivitas kriminalnya.

Selanjutnya dengan menggunakan Social Learning Theory yang diperkenalkan oleh Albert Bandura pada tahun 1977 kita mencoba untuk memahami bagaimana pelaku kejahatan siber belajar dan menyempurnakan teknik mereka.

Pelaku kejahatan siber sering kali belajar teknik dan metode serangan melalui observasi. Rizki dan komplotannya dapat mengamati tutorial video, membaca panduan di forum hacker, atau belajar dari komunitas online lainnya (observational learning). Misalnya, seorang individu yang tertarik untuk melakukan serangan ransomware dapat

belajar cara membuat dan menyebarkan malware dengan mengamati tutorial yang tersedia di dark web atau forum hacker.

Setelah mempelajari teknik tertentu, individu mungkin menirunya (imitation) jika mereka melihat bahwa perilaku tersebut menghasilkan hasil yang diinginkan. Dalam konteks kejahatan siber, Rizki mungkin meniru teknik yang digunakan oleh hacker berpengalaman setelah melihat bahwa teknik tersebut berhasil dalam serangan sebelumnya. Proses imitasi ini membantu pelaku baru mengembangkan keterampilan mereka dengan cepat.

Penguatan yang positif atau negatif mempengaruhi apakah perilaku yang dipelajari akan diulangi. Jika Rizki menerima penguatan positif, seperti mendapatkan uang dari serangan ransomware, dia akan lebih cenderung mengulanginya. Sebaliknya, jika mereka tertangkap atau mengalami kegagalan, mereka mungkin menghindari perilaku tersebut. Misalnya, seorang hacker yang berhasil mendapatkan tebusan dalam bentuk uang tanpa tertangkap akan merasa termotivasi untuk melanjutkan aktivitas kriminalnya.

Ketika melihat orang lain mendapatkan reward atau punishment juga dapat mempengaruhi perilaku individu (vicarious reinforcement). Rizki dan komplotannya tidak hanya belajar dari pengalaman pribadi mereka tetapi juga dari mengamati konsekuensi yang dialami oleh orang lain. Misalnya, ketika seorang hacker melihat berita tentang keberhasilan serangan ransomware yang menghasilkan tebusan besar, mereka mungkin merasa terdorong untuk mencoba metode serupa.

Dari perspektif Social Learning Theory, Rizki dan komplotannya mungkin belajar teknik dan metode serangan ransomware dari komunitas online. Mereka dapat mengamati tutorial video, membaca panduan di forum hacker, atau belajar dari pengalaman orang lain di komunitas hacker. Modus operandi yang mereka gunakan, yaitu mengirimkan link APK palsu melalui WhatsApp, mungkin merupakan hasil dari proses observasi dan imitasi teknik yang telah terbukti berhasil. Penguatan positif dalam bentuk keuntungan finansial dari serangan sebelumnya akan memperkuat motivasi mereka untuk melanjutkan kejahatan ini.

Selanjutnya, melalui Routine Activity Theory Lawrence E. Cohen dan Marcus Felson yang menyatakan bahwa kejahatan terjadi ketika tiga elemen utama bertemu dalam ruang dan waktu: pelaku yang termotivasi, target yang cocok, dan ketiadaan penjaga yang mampu. Kita akan memahami motivasi pelaku dalam melakukan kejahatan siber.

Individu yang memiliki niat atau kecenderungan untuk melakukan kejahatan. Dalam konteks kejahatan siber, Rizki yang termotivasi (motivated offender) mungkin didorong oleh berbagai faktor seperti keuntungan finansial, keinginan untuk merusak, atau sekadar tantangan intelektual. Keuntungan finansial adalah salah satu motivasi utama bagi pelaku ransomware, di mana mereka meminta tebusan dalam bentuk uang untuk mengembalikan akses data yang dienkripsi.

Objek atau individu yang menjadi sasaran kejahatan dan menarik bagi pelaku. Dalam konteks ransomware, target yang cocok adalah individu atau organisasi yang memiliki data penting yang dapat dienkripsi dan digunakan sebagai alat untuk pemerasan. Target sering kali dipilih berdasarkan seberapa mudah mereka dapat dieksploitasi (suitable target). Misalnya, individu yang tidak memiliki pengetahuan tentang keamanan siber atau organisasi yang tidak memiliki sistem keamanan yang kuat adalah target yang ideal.

Selain itu kurangnya pengawasan atau perlindungan yang dapat mencegah kejahatan. Di dunia siber, ketiadaan penjaga yang mampu dapat berupa kurangnya perangkat lunak keamanan, rendahnya kesadaran tentang ancaman siber, atau kelemahan

dalam sistem keamanan (absence of capable guardian). Ketika pelaku mengetahui bahwa target tidak memiliki proteksi yang memadai, mereka akan lebih cenderung untuk melakukan serangan.

Routine Activity Theory membantu kita memahami motivasi dan kondisi yang memungkinkan terjadinya kejahatan ini. Rizki dan komplotannya adalah pelaku yang termotivasi oleh keuntungan finansial. Mereka mencari target yang cocok, yaitu individu yang tidak waspada dan tidak memiliki proteksi yang memadai terhadap serangan siber. Dalam kasus ini, Nabila Fanessa menjadi target yang cocok karena tidak curiga terhadap pesan dari nomor yang dikenalnya sebagai nomor Kapolda Jawa Tengah. Ketiadaan penjaga yang mampu, seperti kurangnya kesadaran tentang ancaman siber dan lemahnya proteksi perangkat, membuat serangan ini lebih mudah dilakukan.

4. Analisis Mengapa Seseorang Menjadi Korban

Cyber Culture adalah budaya yang terbentuk dalam komunitas virtual dan berdampak pada perilaku siber individu. Menurut Nasrullah (2014), Cyber Culture berlangsung secara global dan universal melalui medium internet, mencakup norma, nilai, dan praktik yang berkembang di komunitas online. Dalam konteks kejahatan siber, Cyber Culture memainkan peran penting dalam membentuk perilaku dan kerentanan individu terhadap serangan siber, termasuk ransomware.

Anonimitas adalah salah satu elemen utama yang membentuk Cyber Culture. Anonimitas memungkinkan individu untuk menyembunyikan identitas asli mereka dan berperilaku dengan cara yang berbeda dari dunia nyata. Bagi pelaku kejahatan, anonimitas ini memberikan kebebasan untuk melakukan tindakan kriminal tanpa takut akan konsekuensi langsung. Namun, bagi korban, anonimitas ini juga berarti mereka tidak dapat dengan mudah mengidentifikasi dan menghindari pelaku. Selain itu, identitas daring atau online identity memungkinkan individu untuk menciptakan dan mengelola identitas yang berbeda dari identitas asli mereka. Pelaku kejahatan siber sering kali menggunakan identitas palsu atau anonim untuk menipu korban. Misalnya, dalam kasus ransomware dengan modus link APK palsu, pelaku dapat berpura-pura menjadi teman, anggota keluarga, atau pihak berwenang untuk memanipulasi korban agar mengunduh aplikasi berbahaya. Norma dan nilai bersama dalam komunitas siber mengatur perilaku individu. Norma ini dapat mencakup etiket komunikasi, keamanan informasi, dan etika penggunaan teknologi. Namun, di banyak komunitas online, norma-norma ini mungkin tidak sekuat di dunia nyata, dan perilaku yang merugikan seperti penyebaran malware atau penipuan dapat lebih diterima atau bahkan didorong. Budaya berbagi informasi dan sumber daya dalam komunitas hacker, misalnya, dapat memfasilitasi penyebaran teknik dan metode kejahatan siber. Bagi korban, ketidakpahaman atau ketidaktahuan tentang norma-norma keamanan siber yang diperlukan dapat meningkatkan kerentanan mereka terhadap serangan. Individu yang tidak terbiasa dengan praktik keamanan siber yang baik, seperti verifikasi sumber pesan atau kewaspadaan terhadap link yang mencurigakan, lebih mudah menjadi target serangan.

Partisipasi aktif dalam komunitas online adalah aspek penting dari Cyber Culture. Di satu sisi, partisipasi ini dapat memberikan keuntungan, seperti akses ke informasi dan dukungan sosial. Namun, di sisi lain, partisipasi ini juga dapat mengekspos individu kepada risiko kejahatan siber. Pelaku dapat memanfaatkan informasi yang dibagikan secara publik atau dalam grup tertutup untuk menargetkan korban dengan lebih efektif. Misalnya, pelaku

ransomware dapat mengumpulkan informasi tentang target potensial dari media sosial atau forum online untuk menyesuaikan serangan mereka. Informasi seperti detail pribadi, hubungan sosial, dan kebiasaan online dapat digunakan untuk membuat pesan phishing yang lebih meyakinkan dan meningkatkan kemungkinan korban akan mengklik link berbahaya.

Dalam konteks Indonesia, budaya siber sangat mempengaruhi bagaimana seseorang dapat menjadi korban kejahatan siber. Budaya sosial Indonesia yang menghargai undangan pernikahan dan acara sosial lainnya dimanfaatkan oleh pelaku kejahatan siber. Misalnya, dalam kasus Rizki Darmawan yang mengirimkan undangan pernikahan palsu melalui WhatsApp, korban seperti Nabila Fanessa menjadi rentan karena norma sosial yang mendorong mereka untuk membuka dan menerima undangan tersebut tanpa kecurigaan. Budaya siber di Indonesia, di mana orang cenderung mempercayai informasi yang diterima melalui aplikasi media sosial dan berinteraksi secara aktif tanpa mempertimbangkan risiko keamanan, juga memperbesar peluang terjadinya kejahatan. Anonimitas dan fleksibilitas identitas yang diberikan oleh dunia siber membuat pelaku lebih mudah menipu korban dengan teknik rekayasa sosial, seperti berpura-pura menjadi teman atau anggota keluarga untuk meminta bantuan finansial.

Disamping itu Routine Activity Theory, yang diperkenalkan oleh Lawrence E. Cohen dan Marcus Felson pada tahun 1979, menyatakan bahwa kejahatan terjadi ketika tiga elemen utama bertemu dalam ruang dan waktu: pelaku yang termotivasi, target yang cocok, dan ketiadaan penjaga yang mampu. Teori ini dapat digunakan untuk menganalisis bagaimana dan mengapa seseorang menjadi korban kejahatan siber.

Dalam konteks kejahatan siber, pelaku yang termotivasi adalah individu yang memiliki niat atau kecenderungan untuk melakukan kejahatan. Faktor-faktor yang memotivasi pelaku dapat bervariasi, termasuk keuntungan finansial, keinginan untuk merusak, atau tantangan intelektual. Pelaku ransomware, misalnya, termotivasi oleh potensi mendapatkan uang dari korban yang bersedia membayar untuk mendapatkan kembali akses ke data mereka. Target yang cocok adalah individu atau objek yang menarik bagi pelaku kejahatan. Dalam kasus ransomware, target yang cocok adalah individu atau organisasi yang memiliki data penting dan rentan terhadap serangan siber. Faktor-faktor yang membuat seseorang menjadi target yang cocok termasuk rendahnya kesadaran dan pengetahuan tentang keamanan siber, kurangnya proteksi teknis, dan tingginya nilai data. Individu yang tidak memiliki pengetahuan tentang ancaman siber dan cara melindungi diri mereka lebih rentan terhadap serangan. Mereka mungkin tidak mengenali tanda-tanda phishing atau link berbahaya dan dengan mudah mengklik link yang mencurigakan. Sistem yang tidak dilindungi oleh perangkat lunak keamanan yang memadai, seperti antivirus dan firewall, lebih mudah disusupi oleh ransomware. Individu yang tidak secara teratur memperbarui perangkat lunak keamanan mereka juga lebih rentan terhadap serangan. Individu atau organisasi yang menyimpan data penting dan sensitif, seperti informasi keuangan atau data pribadi, menjadi target yang lebih menarik bagi pelaku ransomware. Data ini dapat digunakan untuk pemerasan atau dijual di pasar gelap.

Penjaga yang mampu adalah individu, teknologi, atau sistem yang dapat mencegah kejahatan. Ketiadaan penjaga yang mampu meningkatkan peluang terjadinya kejahatan. Dalam konteks kejahatan siber, ketiadaan penjaga yang mampu dapat berupa kurangnya sistem keamanan yang kuat, rendahnya tingkat kepatuhan terhadap praktik keamanan, dan kurangnya edukasi dan kesadaran. Tanpa perlindungan seperti perangkat lunak antivirus,

firewall, dan enkripsi, perangkat dan data menjadi lebih rentan terhadap serangan. Sistem keamanan yang lemah memudahkan pelaku untuk menyusup dan menginfeksi perangkat dengan ransomware. Individu yang tidak mengikuti praktik keamanan siber yang baik, seperti menggunakan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, dan memverifikasi sumber pesan, lebih rentan terhadap serangan. Tanpa edukasi yang memadai tentang ancaman siber dan cara menghindarinya, individu mungkin tidak menyadari risiko yang mereka hadapi dan tidak tahu bagaimana melindungi diri mereka. Program edukasi dan kampanye kesadaran yang efektif dapat berfungsi sebagai penjaga yang mampu dengan meningkatkan pengetahuan dan kewaspadaan masyarakat terhadap ancaman siber.

Dengan menggabungkan konsep Cyber Culture dan Routine Activity Theory, kita dapat memahami lebih baik mengapa seseorang menjadi korban kejahatan siber, khususnya ransomware. Cyber Culture menciptakan lingkungan di mana perilaku non-konformitas dan anonimitas dapat berkembang, sementara Routine Activity Theory menekankan pada kondisi situasional yang memungkinkan kejahatan terjadi. Budaya siber yang mendukung anonimitas, fleksibilitas identitas, dan partisipasi komunitas meningkatkan kerentanan individu terhadap kejahatan siber. Individu yang tidak waspada atau tidak memiliki pengetahuan tentang praktik keamanan siber yang baik lebih mudah tertipu oleh teknik rekayasa sosial yang digunakan oleh pelaku ransomware. Partisipasi aktif dalam komunitas online juga dapat mengekspos individu kepada risiko, karena informasi pribadi mereka dapat digunakan oleh pelaku untuk menargetkan mereka dengan lebih efektif. Routine Activity Theory menunjukkan bahwa kejahatan terjadi ketika pelaku yang termotivasi bertemu dengan target yang cocok dan tidak ada penjaga yang mampu. Dalam konteks kejahatan siber, pelaku ransomware termotivasi oleh keuntungan finansial, mencari target yang tidak dilindungi dengan baik dan memiliki data penting, serta memanfaatkan ketiadaan sistem keamanan yang memadai untuk menyerang.

Dalam konteks kasus Rizki Darmawan, Nabila Fanessa menjadi korban karena memenuhi ketiga elemen tersebut. Pertama, Rizki sebagai pelaku termotivasi oleh keuntungan finansial. Kedua, Nabila adalah target yang cocok karena dia menerima pesan undangan pernikahan, sebuah konteks yang sangat dipercaya dalam budaya Indonesia. Ketiga, tidak adanya penjaga yang mampu, dalam hal ini, kurangnya kesadaran Nabila tentang ancaman siber dan lemahnya proteksi perangkatnya, membuat serangan ini lebih mudah dilakukan. Nabila tidak memiliki perangkat lunak keamanan yang memadai untuk mendeteksi APK berbahaya dan tidak menyadari pentingnya verifikasi sumber pesan sebelum mengunduh aplikasi. Kurangnya edukasi dan kesadaran tentang ancaman siber di kalangan masyarakat umum memperbesar kemungkinan mereka menjadi korban kejahatan seperti ransomware.

Budaya siber yang mendukung anonimitas, fleksibilitas identitas, dan partisipasi komunitas meningkatkan kerentanan individu terhadap kejahatan siber. Individu yang tidak waspada atau tidak memiliki pengetahuan tentang praktik keamanan siber yang baik lebih mudah tertipu oleh teknik rekayasa sosial yang digunakan oleh pelaku ransomware. Partisipasi aktif dalam komunitas online juga dapat mengekspos individu kepada risiko, karena informasi pribadi mereka dapat digunakan oleh pelaku untuk menargetkan mereka dengan lebih efektif.

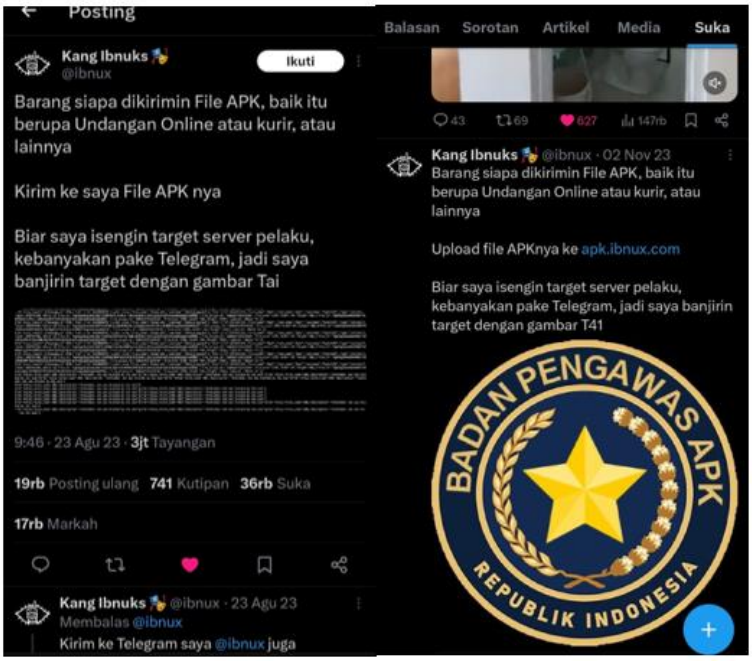
Routine Activity Theory menunjukkan bahwa kejahatan terjadi ketika pelaku yang termotivasi bertemu dengan target yang cocok dan tidak ada penjaga yang mampu. Dalam konteks kejahatan siber, pelaku ransomware termotivasi oleh keuntungan finansial, mencari

target yang tidak dilindungi dengan baik dan memiliki data penting, serta memanfaatkan ketiadaan sistem keamanan yang memadai untuk menyerang.

5. Pemberdayaan Komunitas dalam Konteks Cyber

1) Fenomena “Badan Pengawas APK”

Fenomena "Badan Pengawas APK" yang dipelopori oleh Kang Ibnuks (@ibnux) di jejaring X (Twitter) merupakan contoh nyata dari inisiatif komunitas dalam melawan kejahatan siber, khususnya ransomware dan aplikasi palsu (APK palsu). Melalui akun Twitternya, Kang Ibnuks menawarkan bantuan untuk memeriksa nomor dan akun yang dicurigai sebagai pelaku ransomware atau penyebar APK palsu. Ia melakukan kegiatan ini dengan tujuan membantu para korban kejahatan ransomware dan memberikan edukasi kepada pengikutnya tentang bagaimana cara menghindari kejahatan tersebut.



Gambar 1. Laman Akun X (Twitter) Kang Ibnuks (@ibnux)

Dalam serangkaian cuitan, Kang Ibnuks mengajak para pengikutnya untuk mengirimkan file APK yang mencurigakan kepadanya. Misalnya, dalam salah satu cuitannya, ia menulis, "Barang siapa dikirimin File APK, baik itu berupa Undangan Online atau kurir, atau lainnya, kirim ke saya File APK nya." Melalui unggahan ini, ia menerima file APK yang mencurigakan dan melakukan analisis mendalam terhadap file tersebut untuk mengidentifikasi sumber dan metode serangan yang digunakan oleh pelaku.

Kang Ibnuks juga memberikan edukasi kepada pengikutnya tentang cara mengenali dan menghindari APK palsu yang berpotensi mengandung ransomware. Ia menjelaskan langkah-langkah pencegahan, seperti tidak sembarangan mengunduh file dari sumber yang tidak dikenal dan selalu memeriksa keaslian pesan yang diterima. Edukasi semacam ini sangat penting untuk meningkatkan literasi digital dan kesadaran masyarakat terhadap ancaman siber.

Selain melakukan analisis dan edukasi, Kang Ibnuks secara aktif melaporkan hasil temuan kepada pihak berwenang, yaitu Divhumas Polri (@DivHumas_Polri). Ia

menggunakan tag dan caption untuk menarik perhatian pihak kepolisian terhadap akun-akun yang dicurigai sebagai pelaku kejahatan siber. Langkah ini mempercepat proses pelaporan dan memfasilitasi tindakan hukum terhadap pelaku kejahatan.

Fenomena ini menjadi semakin menarik ketika Kang Ibnuks mulai melakukan serangan balik terhadap pelaku ransomware. Ia menggunakan berbagai teknik serangan seperti DoS (Denial of Service) attack, flooding attack, dan message bombing untuk merusak perangkat pelaku. Misalnya, dalam salah satu cuitannya, ia menyebutkan bahwa ia akan membanjiri target dengan pesan "bom pesan" sebagai bentuk serangan balik. Teknik ini dirancang untuk mengganggu operasional pelaku ransomware dan menyebabkan kerugian material bagi mereka.

Kegiatan Kang Ibnuks mendapat respons positif dari banyak pengguna Twitter yang mengapresiasi usahanya dalam membantu korban dan melawan pelaku kejahatan siber. Banyak pengguna yang mengirimkan file APK mencurigakan dan meminta bantuannya untuk memeriksa dan melaporkan pelaku. Sebagai contoh, salah satu pengguna bernama Amelia Martira (@irasjafii) mengirim pesan kepada Kang Ibnuks, meminta bantuan setelah menerima kiriman APK mencurigakan. Kang Ibnuks dengan sigap merespons dan memberikan instruksi lebih lanjut tentang apa yang harus dilakukan.

Figure 2. Respon Akun Kang Ibnuks (@ibnux) terhadap follower

Inisiatif ini menunjukkan bahwa kolaborasi antara individu, komunitas, dan pihak berwenang sangat penting dalam memerangi kejahatan siber. Kang Ibnuks tidak hanya bertindak sebagai pendidik dan pelapor, tetapi juga sebagai seorang aktivis yang menggunakan keahliannya untuk melawan pelaku kejahatan secara langsung. Fenomena

"Badan Pengawas APK" ini menyoroti peran vital masyarakat dalam meningkatkan keamanan siber dan melindungi diri serta komunitas dari ancaman digital.

Dengan menggunakan media sosial sebagai platform untuk edukasi dan aksi, Kang Ibnuks berhasil menciptakan dampak yang signifikan dalam meningkatkan kesadaran dan respons terhadap kejahatan siber. Inisiatif ini juga menekankan pentingnya literasi digital dan kolaborasi antara berbagai pihak untuk menciptakan lingkungan digital yang lebih aman dan tangguh. Melalui upaya konsisten dan dukungan dari komunitas serta otoritas, inisiatif semacam ini dapat memberikan perlindungan yang lebih baik bagi masyarakat dan mengurangi jumlah korban kejahatan siber.

2) Analisis Fenomena BPA Akun Kang Ibnux (@ibnux)

Upaya Kang Ibnux dalam melawan kejahatan siber, khususnya ransomware dan APK palsu, sangat relevan dalam konteks cyber culture. Dalam komunitas online, anonimitas dan identitas daring memainkan peran penting dalam membentuk perilaku. Anonimitas memungkinkan individu untuk berperilaku dengan cara yang berbeda dari dunia nyata, sering kali tanpa takut akan konsekuensi langsung. Kang Ibnux memanfaatkan elemen-elemen ini untuk mendeteksi dan melaporkan pelaku kejahatan siber. Dengan menggunakan akun anonim, ia mampu mengidentifikasi sumber serangan dan memberikan edukasi kepada pengikutnya tanpa takut akan ancaman balik dari pelaku. Selain itu, identitas daring yang ia bangun sebagai "Badan Pengawas APK" memberikan kredibilitas dan kepercayaan di antara komunitas online, memungkinkan dia untuk mengumpulkan informasi dan melaporkannya dengan efektif.

Norma dan nilai bersama dalam komunitas siber, seperti keamanan informasi dan etika penggunaan teknologi, menjadi fokus utama dari edukasi yang diberikan oleh Kang Ibnux. Ia mengajarkan pengikutnya tentang pentingnya praktik keamanan siber yang baik dan cara mengenali serta menghindari APK palsu yang berpotensi mengandung ransomware. Dengan membangun kesadaran dan pengetahuan di antara komunitas online, ia membantu menciptakan norma baru yang lebih aman dan waspada terhadap ancaman siber.

Dalam Routine Activity Theory menyatakan bahwa kejahatan terjadi ketika tiga elemen utama bertemu: pelaku yang termotivasi, target yang cocok, dan ketiadaan penjaga yang mampu. Upaya Kang Ibnux berfokus pada menghilangkan motivasi pelaku (motivated offender) dengan mengurangi peluang mereka untuk mendapatkan keuntungan dari kejahatan mereka.

Pertama, dengan mendeteksi dan melaporkan pelaku kejahatan siber kepada pihak berwenang seperti Divhumas Polri, Kang Ibnux membantu memastikan bahwa pelaku menghadapi konsekuensi hukum atas tindakan mereka. Ancaman penegakan hukum ini mengurangi motivasi pelaku untuk melanjutkan kejahatan mereka karena risiko tertangkap dan dihukum meningkat. Selain itu, dengan melakukan serangan balik seperti DoS attack, flooding attack, dan message bombing, Kang Ibnux secara langsung merusak perangkat pelaku. Kerusakan ini tidak hanya mengganggu operasional mereka tetapi juga menyebabkan kerugian material yang signifikan, mengurangi potensi keuntungan yang mereka harapkan dari serangan ransomware.

Kedua, dengan meningkatkan kesadaran dan literasi digital di kalangan masyarakat, Kang Ibnux membantu menciptakan "penjaga yang mampu" (capable guardian) dalam komunitas online. Ketika individu lebih waspada dan dilengkapi dengan pengetahuan tentang praktik keamanan siber yang baik, mereka menjadi target yang lebih sulit bagi

pelaku kejahatan. Dengan demikian, peluang bagi pelaku untuk berhasil melakukan serangan ransomware berkurang.

Disamping itu dalam Social Learning Theory Albert Bandura (1977) menekankan bahwa individu belajar perilaku melalui observasi dan imitasi, dan penguatan (reinforcement) memainkan peran penting dalam menentukan apakah perilaku tersebut akan diulang. Upaya Kang Ibnux dapat dianalisis dalam konteks teori ini melalui konsep penguatan negatif (punishment).

Dengan mengidentifikasi dan melaporkan pelaku kejahatan siber, Kang Ibnux memberikan penguatan negatif yang kuat. Pelaku yang tertangkap dan dihukum oleh pihak berwenang mengalami konsekuensi langsung dari tindakan mereka, yang berfungsi sebagai penguatan negatif. Selain itu, serangan balik yang dilakukan oleh Kang Ibnux, seperti DoS attack dan message bombing, menyebabkan kerusakan pada perangkat pelaku, menambah elemen penguatan negatif. Pelaku yang perangkatnya rusak akan mengalami kerugian finansial dan teknis, yang mengurangi motivasi mereka untuk melanjutkan perilaku kriminal.

Penguatan negatif ini tidak hanya mempengaruhi pelaku yang secara langsung ditargetkan oleh Kang Ibnux tetapi juga memberikan contoh kepada pelaku potensial lainnya. Melihat bahwa pelaku kejahatan siber dapat dikenai konsekuensi serius, baik melalui penegakan hukum maupun kerusakan teknis, pelaku potensial mungkin berpikir dua kali sebelum melakukan tindakan kriminal serupa. Dengan demikian, upaya Kang Ibnux memiliki efek jera yang lebih luas dalam komunitas hacker dan pelaku kejahatan siber.

6. Analisa Community Policing Konteks Fenomena BPA Kang Ibnuks (@ibnux)

Community Policing adalah pendekatan pemolisian yang melibatkan kemitraan antara polisi dan masyarakat untuk mengidentifikasi dan menyelesaikan masalah kejahatan dan gangguan sosial. Dalam konteks siber, community policing memainkan peran yang sangat penting dalam pencegahan kejahatan siber seperti ransomware dan APK palsu. Fenomena Badan Pengawas APK (BPA) yang dipelopori oleh Kang Ibnuks (@ibnux) adalah contoh nyata bagaimana prinsip-prinsip community policing dapat diterapkan dalam dunia digital untuk memerangi kejahatan siber.

1) Partnership (Kemitraan)

Kemitraan adalah inti dari community policing. Kerjasama antara kepolisian dan masyarakat sangat penting untuk menciptakan lingkungan yang aman. Kang Ibnuks telah membangun kemitraan yang kuat dengan masyarakat online melalui akun Twitternya. Dengan menawarkan bantuan untuk memeriksa file APK yang mencurigakan, ia menjalin hubungan kepercayaan dengan para pengikutnya. Selain itu, kemitraan ini diperkuat dengan komunikasi yang efektif antara Kang Ibnuks dan Divhumas Polri (@DivHumas_Polri). Dengan melaporkan akun-akun dan nomor telepon yang dicurigai, Kang Ibnuks membantu kepolisian dalam mengidentifikasi dan menangani pelaku kejahatan siber. Contoh nyata dari kemitraan ini terlihat dalam berbagai cuitan di mana Kang Ibnuks mengarahkan pengikutnya untuk mengirimkan informasi yang mencurigakan ke akun Telegram atau WhatsApp-nya untuk dianalisis lebih lanjut.

2) Problem Solving (Pemecahan Masalah)

Community policing menekankan pemecahan masalah secara kolaboratif. Kang Ibnuks memfokuskan usahanya pada identifikasi dan analisis masalah yang berkaitan

dengan ransomware dan APK palsu. Dengan menerima laporan dari masyarakat dan menganalisis file yang mencurigakan, ia dapat mengidentifikasi pola dan teknik yang digunakan oleh pelaku. Informasi ini kemudian dibagikan dengan pengikutnya dan pihak berwenang untuk mencari solusi yang efektif. Contohnya, dalam salah satu cuitannya, Kang Ibnuks menjelaskan bagaimana ia membuka APK menggunakan aplikasi Dexplorer untuk menemukan token Telegram dan ID pengguna yang mencurigakan, yang kemudian dapat digunakan untuk melacak dan melaporkan pelaku.

3) Proaktif

Salah satu prinsip penting dari community policing adalah proaktivitas. Tindakan pencegahan sebelum kejahatan terjadi sangat penting dalam konteks siber. Kang Ibnuks secara proaktif mengedukasi pengikutnya tentang ancaman ransomware dan APK palsu serta cara menghindarinya. Edukasi ini mencakup langkah-langkah praktis seperti tidak mengunduh file dari sumber yang tidak dikenal, memverifikasi keaslian pesan yang diterima, dan menggunakan perangkat lunak keamanan yang memadai. Dengan meningkatkan kesadaran dan pengetahuan masyarakat, Kang Ibnuks membantu mencegah kejahatan siber sebelum terjadi. Contohnya, ia memberikan tips dan saran tentang bagaimana mengenali dan menghindari pesan phishing dan link berbahaya.

4) Creative (Kreatif)

Pendekatan kreatif adalah kunci dalam pencegahan dan penanggulangan kejahatan siber. Kang Ibnuks menggunakan metode inovatif untuk melawan pelaku kejahatan siber. Selain menganalisis file APK dan melaporkannya kepada pihak berwenang, ia juga menggunakan serangan balik seperti DoS attack, flooding attack, dan message bombing untuk merusak perangkat pelaku. Metode ini tidak hanya mengganggu operasional pelaku tetapi juga memberikan efek jera yang signifikan. Penggunaan taktik kreatif ini menunjukkan bagaimana inisiatif individu dapat menjadi bagian integral dari strategi pencegahan kejahatan siber yang lebih luas.

Fenomena BPA yang dipelopori oleh Kang Ibnuks menunjukkan bagaimana prinsip-prinsip community policing dapat diterapkan secara efektif dalam konteks siber. Dengan membangun kemitraan yang kuat dengan masyarakat online, Kang Ibnuks mampu mengumpulkan informasi yang berharga dan membantu penegakan hukum dalam mengidentifikasi dan menangkap pelaku kejahatan siber. Pendekatan proaktif dan kreatifnya dalam edukasi dan tindakan balik tidak hanya mencegah kejahatan tetapi juga memberikan contoh nyata bagaimana masyarakat dapat berperan aktif dalam menciptakan lingkungan digital yang aman.

Kemitraan yang dibangun oleh Kang Ibnuks dengan pengikutnya dan pihak kepolisian adalah salah satu contoh dari bagaimana community policing dapat bekerja dalam dunia digital. Kolaborasi ini menunjukkan bahwa dengan komunikasi yang efektif dan tindakan bersama, ancaman kejahatan siber dapat diminimalkan dan kepercayaan masyarakat terhadap sistem keamanan siber dapat ditingkatkan. Dengan terus mengedukasi masyarakat dan melaporkan pelaku kejahatan, Kang Ibnuks memainkan peran penting dalam menciptakan lingkungan siber yang lebih aman dan terlindungi.

Sebagaimana dijelaskan bahwa e-Policing adalah pendekatan pemolisian modern yang mengintegrasikan teknologi informasi untuk meningkatkan efisiensi dan efektivitas operasional kepolisian. Menurut Laksana (2014), e-Policing dapat dipahami sebagai model pemolisian yang membawa prinsip-prinsip community policing (CP) ke dalam sistem online, berupaya menerobos sekat-sekat ruang dan waktu, menjadi strategi inisiatif anti

korupsi, dan dilaksanakan bersama dengan model pemolisian tradisional untuk mewujudkan keamanan masyarakat. Fenomena Badan Pengawas APK (BPA) yang dipelopori oleh Kang Ibnuks (@ibnux) merupakan contoh penerapan e-Policing dalam dunia digital.

a. Membawa Community Policing (CP) pada Sistem Online
   Kang Ibnuks memanfaatkan platform media sosial seperti Twitter untuk membangun kemitraan dengan masyarakat online. Ia mengedukasi pengikutnya tentang ancaman ransomware dan APK palsu, serta memberikan bantuan dalam memeriksa file yang mencurigakan. Ini adalah bentuk nyata dari community policing yang diterapkan dalam dunia siber, di mana masyarakat dan polisi bekerja sama untuk mengidentifikasi dan menyelesaikan masalah kejahatan siber.
b. Menerobos Sekat-Sekat Ruang dan Waktu
   Dengan menggunakan media sosial, Kang Ibnuks mampu memberikan layanan kepolisian yang cepat, tepat, transparan, akuntabel, informatif, dan mudah diakses. Melalui cuitan dan interaksi online, ia dapat segera merespons laporan dari masyarakat, memberikan edukasi, dan melaporkan temuan kepada pihak berwenang. Pendekatan ini menghilangkan hambatan geografis dan temporal, memungkinkan respons yang lebih cepat terhadap ancaman siber.
c. Strategi Inisiatif dan Terobosan Kreatif
   Inisiatif Kang Ibnuks juga mencerminkan strategi dan reformasi birokrasi. Dengan transparansi yang ditawarkan melalui media sosial, setiap tindakan dan laporan dapat diakses oleh publik, mengurangi peluang terjadinya pengkaburan. Selain itu, penggunaan metode kreatif seperti serangan balik terhadap pelaku ransomware menunjukkan terobosan inovatif dalam menangani kejahatan siber.
d. d. Integrasi dengan Model Pemolisian Tradisional
   Upaya Kang Ibnuks tidak menggantikan model pemolisian tradisional tetapi melengkapinya. Ia bekerja sama dengan Divhumas Polri untuk melaporkan temuan dan memberikan informasi yang diperlukan untuk tindakan penegakan hukum. Pendekatan ini menunjukkan bahwa e-Policing dapat berjalan seiring dengan metode tradisional untuk menciptakan polisi yang profesional dan responsif.
e. e. Menyelenggarakan Tugas Kepolisian Berbasis Elektronik
   Fenomena BPA mencerminkan penyelenggaraan tugas kepolisian berbasis elektronik yang terpadu, terintegrasi, dan sistematis. Dengan analisis digital, pelaporan online, dan edukasi publik, Kang Ibnuks membantu memelihara keamanan dan rasa aman masyarakat. Inisiatif ini menunjukkan bagaimana e-Policing dapat digunakan untuk mendukung dan memperkuat upaya penegakan hukum tradisional dalam menghadapi tantangan kejahatan siber yang kompleks.

KESIMPULAN

Penelitian ini mengungkapkan cara penyebaran ransomware melalui APK palsu yang memanfaatkan teknik rekayasa sosial, di mana pelaku mengirim link tampak sah kepada korban. Setelah mengunduh APK, ransomware menginfeksi perangkat, mengenkripsi data, dan mengakses daftar kontak untuk menyebarkan pesan palsu. Faktor yang mendorong seseorang menjadi pelaku kejahatan siber meliputi motivasi finansial, tantangan intelektual, dan anonimitas. Teori-teori seperti Space Transition Theory, Social Learning Theory, dan Routine Activity Theory membantu menjelaskan perilaku jahat dan kerentanan individu. Model pemolisian yang diusulkan, "Proactive Cyber Community Policing," mengintegrasikan Community Policing dan e-Policing, meliputi pembentukan komunitas, program literasi digital, serta penegakan hukum. Temuan ini menekankan pentingnya pendekatan kolaboratif dalam penanganan kejahatan siber, dengan rekomendasi untuk memperkuat kemitraan antara polisi, masyarakat, dan sektor swasta. Selain itu, kebijakan keamanan siber di Indonesia perlu diperbarui untuk mendukung inisiatif ini, termasuk peningkatan edukasi dan literasi digital untuk meningkatkan kesadaran masyarakat tentang ancaman siber.

BIBLIOGRAFI

Arisandy, Y. O. (2021). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(3). https://doi.org/10.18196/ijclc.v1i3.11264

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1). https://doi.org/10.15294/pandecta.v13i1.14020

Fediro, B., & Tata Sutabri. (2023). Rancang Bangun Sistem Pelaporan Insiden Kejahatan Siber. *Jurnal Informatika Teknologi Dan Sains*, *5*(1). https://doi.org/10.51401/jinteks.v5i1.2210

Firmansyah, D., Saepuloh, D., & Dede. (2022). Daya Saing : Literasi Digital dan Transformasi Digital. *Journal of Finance and Business Digital*, *1*(3). https://doi.org/10.55927/jfbd.v1i3.1348

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02). https://doi.org/10.56741/bst.v2i02.353

Khan, M. A. R., Kumar, N., & Tripathi, R. C. (2022). Detection of Android Malware App through Feature Extraction and Classification of Android Image. *International Journal of Advanced Computer Science and Applications*, *13*(5). https://doi.org/10.14569/IJACSA.2022.01305103

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, *3*(01). https://doi.org/10.56127/jukim.v3i01.1143

Levinda. (2023). *APJII: Pengguna Internet Indonesia 215 Juta Jiwa pada 2023, Naik 1,17%*. Katadata.Co.Id/.

Morgan, S. (2019). 2019 Official Annual Cybercrime Report. *Cybersecurity Ventures*.

Nugraha, D. (2022). Literasi Digital dan Pembelajaran Sastra Berpaut Literasi Digital di Tingkat Sekolah Dasar. *Jurnal Basicedu*, *6*(6).

https://doi.org/10.31004/basicedu.v6i6.3318

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4).

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). https://doi.org/10.3390/FI11040089

Sulisdyantoro, D., & Marzuki, M. I. (2023). Identification of Whatsapp Digital Evidence on Android Smartphones using The Android Backup APK (Application Package Kit) Downgrade Method. *Journal of Integrated and Advanced Engineering (JIAE)*, *3*(1). https://doi.org/10.51662/jiae.v3i1.70

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3162594

Tajriyani, N. S. (2021). Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker. *Jurist-Diction*, *4*(2). https://doi.org/10.20473/jd.v4i2.25785

Tamhidah, M. A. R. (2023). Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu Dan Kejahatan Siber. *Innovative: Journal Of Social Science Research*, *3*(6).

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. In *SN Computer Science* (Vol. 2, Issue 2). https://doi.org/10.1007/s42979-020-00443-1

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2992807

Wijanarko, R. P., Moch Rezeki Setiawan, Siti Mukaromah, & Abdul Rezha Efrat Najaf. (2023). Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1). https://doi.org/10.33005/sitasi.v3i1.436