**Technologia : Jurnal Ilmiah**
p-ISSN: 2086-6917, e-ISSN: 2656-8047
Homepage: https://ojs.uniska-bjm.ac.id/index.php/JIT/index
**Vol. 14, No. 4, Oktober 2024**

# IDENTIFIKASI ANCAMAN KEAMANAN SIBER DARI PENYALAHGUNAAN SUMBER DAYA TIK: STUDI KASUS PERUSAHAAN POLYMER

**Eko Haryadi[1*], Diah Wijayanti[2], Eka Chandra Ramdhani[3], Indria Widyastuti[4]**
[1,2,3] Program Sistem Informasi, Fakultas Teknik dan Informatika, UBSI, Indonesia.
[4]Program Studi Akuntansi, Fakultas Ekonomi dan Bisnis,UBSI, Indonesia.

**Informasi Artikel:**
Dikirim: 23-09-2024; Diterima: 29-09-2024; Diterbitkan: 10-10-2024
Doi : http://dx.doi.org/10.31602/tji.v15i4.16429

**ABSTRAK**

**Masalah:** Mengklik tautan secara acak atau membuka situs web yang tidak dikenal di komputer atau perangkat seluler dapat membahayakan perangkat karena mengunduh perangkat lunak berbahaya Penggunaan model keamanan lama tidak memadai terhadap risiko keamanan siber yang berkembang,
**Tujuan:** Mengidentifikasi dan menganalisis ancaman-ancaman akibat dari penyalahgunaan sumberdaya TIK, dengan fokus pada kerentanan yang dieksploitasi oleh pelaku kejahatan. Ancaman-ancaman utama seperti serangan phishing, infeksi malware dan pencurian data dibahas secara terperinci. Metode eksploitasi, termasuk rekayasa sosial, kerentanan perangkat lunak, dan pencurian kredensial, dibahas untuk memberikan pemahaman yang komprehensif tentang lanskap ancaman. Makalah ini juga mengeksplorasi dampak dari ancaman-ancaman ini terhadap organisasi, dengan menyoroti kerugian finansial, kerusakan reputasi, dan gangguan operasional.
**Metode:** Penelitian menggunakan lima kerangka penelitian operasional yang meliput persiapan, desain, pengumpulan data, analisis data dan penulisan.
**Hasil:** . Hasil peneitian ini memberikan pengelompokan berbagai macam ancaman ke dalam lima besar malware yaitu remote access trojan, information stealer, banking trojan, ramsomware dan botnet.
**Kesimpulan:** Upaya yang terbaik dalam pencegahan ancaman ini adalah dengan peningkatan teknologi keamanan jaringan, memperbaharui regulasi dan kebijakan serta peningkatan kesadaran keamanan siber melalui proses pelatihan yang regular dan terdokumentasi.
**Kata Kunci:** Siber, Malware, TIK



## Pendahuluan

Proses perkantoran dan perusahaan sangat dipengaruhi oleh teknologi informasi (TI), yang meningkatkan produktivitas dan memfasilitasi pengambilan keputusan (Waruwu & Sundari, 2024). Saat ini, seiring teknologi terus berkembang dan mengubah kehidupan kita sehari-hari, dunia digital telah menjadi aspek penting dari jati diri kita (Jony & Hamim, 2024). Keamanan siber adalah pertahanan jaringan dan sistem komputer terhadap serangan pelaku jahat yang dapat mengakibatkan kebocoran informasi, pencurian, atau penurunan kualitas perangkat keras, perangkat lunak, atau data, serta gangguan atau kesalahan arah layanan yang ditawarkan. Dalam keamanan siber, ancaman terhadap semua jenis aktivitas dapat memengaruhi fungsi, prosedur, sistem, atau, data organisasi secara negatif. Pelaku kejahatan, seperti peretas dan

penipu, memanipulasi kerentanan dalam sistem perlindungan digital untuk memperoleh informasi, mengganggu prosedur, dan melakukan kejahatan seperti penipuan dan pencurian identitas (Coursera, 2023).

Keamanan internet merupakan salah satu masalah terpenting di abad ke-21. Hal ini disebabkan oleh fakta bahwa kemajuan teknologi, perluasan komunikasi, dan terciptanya internet siber telah menghasilkan revolusi dalam perdagangan elektronik dan transmisi data serta informasi. Menemukan solusi untuk melindungi data dan informasi di internet, serta dompet elektronik dan rekening uang, menjadi sangat penting sebagai hasilnya. Kata "keamanan siber" secara umum mencakup keamanan jaringan, keamanan aplikasi, keamanan operasi elektronik, dan keamanan informasi di Internet (Asaad & Saeed, 2022). Keamanan organisasi menghadapi masalah baru sebagai akibat dari konvergensi risiko cyber dan digitalisasi, di antara kemajuan pesat di ranah digital (Safitra et al., 2023). Teknologi informasi dan komunikasi (TIK) telah meningkatkan penyebaran pengetahuan dan arus informasi dan komunikasi, yang berdampak signifikan pada kehidupan pribadi dan profesional kita. Pertumbuhan TIK masih terus berlangsung, dan hal ini menimbulkan banyak masalah bagi masyarakat (Al-Rahmi et al., 2020).

Bahaya yang terkait dengan keamanan informasi meningkat secara signifikan akibat meluasnya penggunaan teknologi informasi dan komunikasi, atau TIK. Faktanya, keamanan siber menjadi isu yang lebih besar di masyarakat saat ini sebagai akibat dari meningkatnya kuantitas dan variasi serangan siber. Selain individu, bisnis, dan bahkan organisasi pemerintah pun terdampak oleh fenomena ini. Meskipun "digitalisasi" masyarakat ini memiliki banyak manfaat, ada juga beberapa kekhawatiran. Ini termasuk pencurian identitas, email atau panggilan telepon palsu, penipuan internet, konten yang menghasut, dan pornografi anak, mendorong ujaran kebencian berdasarkan ras atau agama, memiliki akses ke layanan daring, meretas akun email, dan menggunakan perbankan daring pemerasan siber, penipuan, atau perangkat lunak berbahaya (Carvalho et al., 2023).

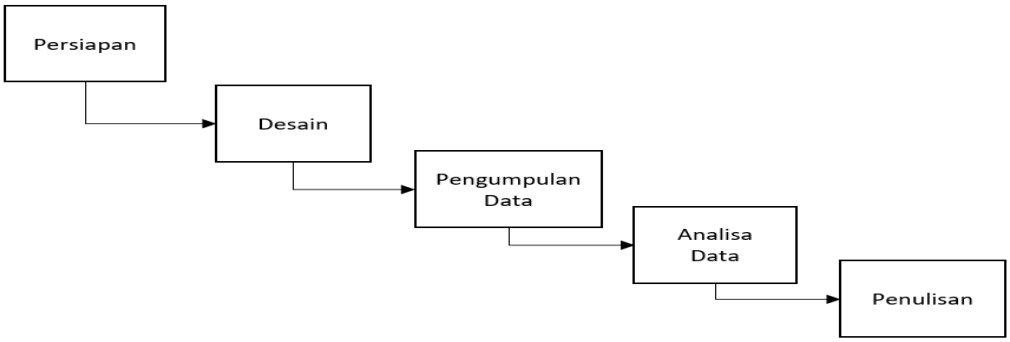
Terdapat beberapa penelitian yang telah membahas mengenai ancaman keamanan siber dan menjadi dasar dalam pembuatan penelitrian ini Penelitian yang dibuat oleh Hama Saeed (2020), dengan tujuan meningkatkan pemahaman dan persepsi terhadap ancaman keamanan terkini dan tindakan pencegahan serta meramalkan tren masa depan dalam keamanan siber sistem informasi dan mengidentifikasi langkah-langkah keamanan masa depan yang andal. Penelitian dari Asaad dan Saeed (2022) memberikan kontribusi berupa usulan model klasifikasi baru untuk ancaman keamanan guna menggeneralisasi dampaknya ke dalam beberapa kelas, bukan ancaman individual. Makalah ini mengulas berbagai model klasifikasi ancaman dan menganalisis berbagai ancaman keamanan siber, tindakan pencegahan, dan tren masa depan. Pada penelitian ini terdapat kesenjangan penelitian (*research gap*) berupa penggunaan model keamanan lama tidak memadai terhadap risiko keamanan siber yang berkembang. Berikutnya penelitian yang dilakukan oleh Khanna (2023) dengan tujuan memberikan pemahaman menyeluruh tentang ancaman keamanan siber terkini dan taktik yang digunakan oleh penjahat siber serta untuk mengeksplorasi dan mengevaluasi efektivitas tindakan penanggulangan saat ini dan yang sedang berkembang sehingga memberikan kontribusi memberikan tinjauan menyeluruh terhadap ancaman keamanan siber yang

muncul dan tindakan pencegahan yang digunakan untuk mengurangi risiko tersebut dan mengevaluasi efektivitas kemajuan teknologi seperti AI, pembelajaran mesin, dan blockchain dalam meningkatkan pertahanan keamanan siber. Penelitian ini menerapkan tinjauan pustaka dan analisis. Sebuah penelitain dilakukan yang bertujuan untuk mengusulkan pendekatan baru terhadap manajemen risiko siber berdasarkan konsep rantai pembunuhan siber yang diperkenalkan oleh Lockheed Martin yang ditulis oleh Hoffmann (2020). Kontribusi dari penelitian Hoffmann (2020) ini adalah proses manajemen risiko yang diusulkan adalah baru dan tidak tercermin dalam literatur yang tersedia dan pendekatan ini dapat digunakan oleh organisasi untuk menerapkan mekanisme keamanan dan mengurangi risiko cyber ke tingkat yang dapat diterima. Kesenjangan penelitian ini menyebutkan tidak tersedia data empiris untuk umum guna memperkirakan kemungkinan ancaman siber tertentu secara akurat dan proses penilaian tingkat transisi dalam model Markov sangat bergantung pada pendapat ahli, yang dapat menimbulkan subjektivitas.

Penelitian yang dilakukan oleh Asaad dan Saeed (2022) mengatasi berbagai ancaman, kerentanan, dan tantangan keamanan siber yang dihadapi oleh individu, organisasi, dan negara. Penelitian Asaad dan Saeed (2022) ini melakukan tinjauan komprehensif terhadap penelitian yang ada tentang ancaman dan kerentanan keamanan siber juga meneliti studi kasus spesifik untuk menggambarkan dampak serangan siber dan efektivitas solusi yang diusulkan. Makalah ini memberikan gambaran rinci tentang keadaan keamanan siber saat ini, termasuk ancaman umum, kerentanan, dan teknik mitigasi. Sedangkan kekurangan dalam penelitian ini adalah diperlukan lebih banyak data empiris untuk memvalidasi efektivitas langkah-langkah keamanan siber yang diusulkan. Tujuan penelitian yang penulis lakukan adalah mengidentifikasi jenis ancaman keamanan siber yang bersumber dari penyalahgunaan sumber daya TIK yang mempunyai pengaruh langsung terhadap ancaman keamanan siber. Sebagai kontribusi praktis untuk penelitian ini, adalah membuat berbagai klasifikasi ancaman keamanan siber akibat penyalahgunaan TIK telah diketahui serta menentukan mekanisme untuk mendeteksi dan mencegah ancaman dari sisi organisasi dan menawarkan rekomendasi untuk meningkatkan langkah-langkah keamanan siber.

## Metode

Proses penelitian menggambarkan urutan langkah-langkah yang harus dilakukan sesuai dengan urutannya (Singh, 2021). Semua kegiatan dan hasil yang diharapkan diidentifikasi.




**Gambar 1.** Kerangka penelitian operasional.

Cara yang efektif untuk merencanakan, mengoordinasikan, dan mengawasi operasi penelitian dikenal sebagai kerangka kerja operasional. Untuk meningkatkan nilai dan dampak penelitian dalam skala besar, diperlukan koordinasi dan pengoptimalan orang, prosedur, dan sumber daya. Untuk menjamin bahwa penelitian dilakukan secara metodis, efektif, dan etis, kerangka kerja ini sangat penting.

1. Tahap persiapan dalam kerangka operasional penelitian sangat penting untuk menetapkan dasar proyek penelitian. Tahap ini melibatkan beberapa kegiatan utama adalah menetapkan tujuan dengan menguraikan tujuan dan sasaran penelitian dengan jelas. Melakukan proses tinjauan pustaka: yaitu melakukan tinjauan menyeluruh terhadap pustaka yang ada untuk memahami status pengetahuan terkini dan mengidentifikasi kesenjangan.
2. Tahap desain dalam kerangka operasional penelitian sangat penting untuk membentuk struktur dan metodologi proyek penelitian. Tahap ini melibatkan beberapa aktivitas utama yaitu merumuskan pertanyaan penelitian atau hipotesis yang ingin dijawab oleh penelitian secara jelas. Memilih metode penelitian yang tepat (metode kualitatif) yang sejalan dengan tujuan penelitian. Membuat alat untuk pengumpulan data, seperti panduan wawancara.
3. Tahap pengumpulan data dalam kerangka operasional penelitian adalah tempat pengumpulan informasi yang sebenarnya berlangsung. Tahap ini sangat penting untuk memperoleh data yang dibutuhkan untuk menjawab pertanyaan penelitian atau menguji hipotesis. Kegiatan utama dalam tahap ini meliputi penggunaan alat dan teknik yang dirancang pada tahap sebelumnya, seperti wawancara dan observasi.
4. Tahap analisis data dalam kerangka operasional penelitian adalah tahap saat data yang terkumpul diperiksa dan diinterpretasikan untuk menarik kesimpulan yang bermakna. Tahap ini sangat penting untuk mengubah data mentah menjadi wawasan yang berharga. Aktivitas utama dalam tahap ini meliputi memeriksa dan mengoreksi kesalahan atau ketidakkonsistenan dalam data untuk memastikan keakuratan. Mengorganisasikan data ke dalam kategori atau tema, terutama untuk data kualitatif. Analisis kualitatif menggunakan metode seperti analisis tematik, analisis konten, atau analisis wacana untuk menginterpretasikan data kualitatif.
5. Tahap penulisan dalam kerangka operasional penelitian adalah tahap saat temuan dan wawasan dari penelitian didokumentasikan dan dikomunikasikan. Tahap ini sangat penting untuk berbagi hasil penelitian dengan audiens yang dituju. Aktivitas utama dalam tahap ini meliputi mengatur konten yaitu menyusun laporan atau makalah secara logis, biasanya mencakup bagian-bagian seperti pendahuluan, tinjauan pustaka, metodologi, hasil, diskusi, dan kesimpulan. Kemudian menulis draf awal, memastikan bahwa semua poin dan temuan utama diartikulasikan dengan jelas merevisi dan menyunting yatu dengan meninjau draf untuk kejelasan, koherensi, dan

konsistensi. Ini termasuk memeriksa kesalahan tata bahasa, menyempurnakan argumen, dan memastikan bahwa tulisannya ringkas dan tepat. Mempersiapkan versi akhir dokumen, memastikan bahwa semua bagian lengkap dan sempurna.

Teknik pengumpulan data adalah metode yang digunakan untuk mengumpulkan informasi untuk penelitian, analisis, atau pengambilan keputusan. Pada penelitian ini teknik pengumpulan data yang digunakan adalah sebagai berikut:

1. Wawancara adalah metode pengumpulan data di mana pewawancara mengajukan pertanyaan untuk mengumpulkan informasi langsung dari responden. Dengan menggunakan teknik semi-terstruktur yaitu campuran pertanyaan yang telah ditentukan sebelumnya dan tindak lanjut spontan, tujuannya adalah untuk memperoleh wawasan mendalam tentang pengalaman, pendapat, atau perilaku seseorang. Untuk mengeksplorasi isu-isu kompleks yang tidak dapat dicakup melalui survei atau kuesioner
2. Observasi. Observasi dalam penelitian adalah teknik di mana peneliti secara sistematis mengamati, mendengarkan, dan mencatat perilaku serta peristiwa yang terjadi secara alami. Berikut ini adalah beberapa aspek penting: jenis observasi yang digunakan adalah observasi tidak terstruktur yautu peneliti mencatat semua perilaku dan peristiwa yang relevan tanpa rencana yang telah ditetapkan sebelumnya

**Hasil**

Penelitian di lakukan pada salah satu perusahaan swasta yang bergerak dibidang polymer. Proses observasi dilakukan sebelum wawancara. Pendekatan observasi dilakukan dengan cara berkunjung dan menilai langsung kantor tersebut, tempat karyawan tersebut bekerja. Beberapa kali observasi yang sama dilakukan dengan melihat ke berbagai tempat, ruang server, infrastruktur teknologi Informasi, area kerja karyawan, pusat CCTV, dan ruang kerja staf semuanya masuk dalam proses pengawasan. Observasi ini dilakukan untuk mendukung hasil wawancara dan mencegah bias. Koneksi internet khusus melalui ASTINet milik Telkom—layanan akses internet 24 jam dengan rasio lebar pita terjamin 1:1 ke titik referensi menggunakan gateway internet default dan alamat internet protocol publik milik Telkom Indonesia—digunakan untuk koneksi cadangan, dengan berbagai penyedia layanan internet (ISP) lokal yang menawarkan kecepatan antara 50 Mbps dan 100 Mbps. Perangkat kerasnya terdiri dari server IBM, router Cisco, switch Cisco, dan FORTINET FortiGate Firewall FG-200E. Sistem operasinya terdiri dari server Windows, Linux, dan klien Windows. Wawancara semi-terstruktur menggabungkan kesempatan bagi pewawancara untuk menggali lebih dalam tema atau tanggapan dengan serangkaian pertanyaan terbuka yang telah ditentukan sebelumnya. Pada kesempatan interview ditemukan beberapa fakta bahwa koneksi internet belum dimanfaatkan secara maksimal untuk mencapai tujuan yang diinginkan. Mengklik tautan secara acak atau membuka situs web yang tidak dikenal di komputer atau perangkat seluler dapat membahayakan perangkat karena mengunduh perangkat lunak berbahaya secara tersembunyi.

FORTINET FortiGate Firewall FG-200E memberikan data kepada penulis selama proses observasi. Informasi tentang protokol internet, port, protokol, dan nama serangan diperoleh oleh penulis. Kumpulan pedoman yang mengendalikan pengiriman dan penerimaan data melalui internet dikenal sebagai Protokol Internet (IP). Protokol ini menjamin bahwa paket data diarahkan dengan benar dari sumber ke tujuan yang dituju. Titik akhir untuk komunikasi adalah port. Port digunakan untuk memisahkan berbagai jenis lalu lintas jaringan dan memungkinkan pengoperasian beberapa layanan pada satu perangkat. Nomor port adalah nomor port, yang berkisar dari 0 hingga 65535, digunakan untuk mengidentifikasi port. Misalnya, port 80 biasanya digunakan oleh HTTP, tetapi port 443 digunakan oleh HTTPS. Dua protokol utama untuk mengirim data melalui internet adalah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). TCP berorientasi koneksi artinya sebelum mengirim data, koneksi dibuat antara pengirim dan penerima. Sedangkan UDP, tanpa koneksi artinya mengirim data tanpa membuat koneksi, yang mengurangi overhead dan latensi.

Tabel 1. Hasil scan FORTINET FortiGate Firewall FG-200E

| IP | PORT | PROTOCOL | NAME |
|---|---|---|---|
| 2.56.8.117 | 80 | TCP | AzorUlt |
| 3.120.209.58 | 80 | TCP | CoinMiner |
| 5.9.72.48 | 417 | TCP | Tofsee |
| 5.34.183.40 | 80 | TCP | Locky |
| 5.53.124.241 | 80 | TCP | Gozi |
| 5.56.133.250 | 80 | TCP | Loki |
| 5.63.10.102 | 80 | TCP | Downloader.Pony |
| 5.101.49.49 | 80 | TCP | Downloader.Pony |
| 5.101.51.28 | 80 | TCP | Gozi |
| 5.135.67.231 | 80 | TCP | AsyncRAT |
| 5.154.191.130 | 80 | TCP | AzorUlt |
| 5.164.202.78 | 80 | TCP | Malware |
| 5.182.210.45 | 80 | TCP | TrickBot |
| 5.182.210.128 | 80 | TCP | Loki |
| 5.182.210.157 | 80 | TCP | AzorUlt |
| 5.182.211.76 | 80 | TCP | Loki |
| 5.196.189.37 | 80 | TCP | Locky |
| 5.196.200.229 | 80 | TCP | Ransom.LockyV2 |
| 5.253.114.110 | 80 | TCP | RemcosRAT |
| 8.209.64.228 | 80 | TCP | Neurevt |
| 8.209.67.204 | 80 | TCP | Loki |
| 13.66.129.80 | 80 | TCP | AveMariaRAT |
| 13.69.254.90 | 80 | TCP | Adwind |
| 13.82.213.135 | 80 | TCP | Loki |
| 14.18.83.206 | 80 | TCP | Malware |
| …….. | … | …. | …….. |

Pada Tabel 1, menunjukan hasil pengamatan dari FORTINET FortiGate Firewall FG-

200E. Hasil tersebut menghasilkan sebanyak 2600 serangan yang terjadi selama satu bulan. Pada penelusuran hasil firewall maka dapat diambil kesimpulan berdasarkan port yang digunakan adalah sebagai berikut seperti yang tercantum pada tabel 2.

Tabel 2. Klasifikasi ancaman berdasarkan PortE

| **TCP** | |
|---|---|
| 80 | HTTP |
| 417 | Profil Kerentanan Internet |
| 443 | HTTPS |
| 1556 | Veritas NetBackup |
| 1960 | Cisco Unified Communications Manager (CUCM) |
| 3284 | Apple Remote Desktop (ARD) |
| 3325 | ActiveWorks Active Network |
| **UDP** | |
| 16464 | Botnet ZeroAccess |
| 16465 | Botnet ZeroAccess |
| 16470 | Botnet ZeroAccess |
| 16471 | Botnet ZeroAccess |

Berikutnya, berdasarkan jenis ancaman yang masuk ke dalam filter firewall, maka dikelompokan menjadi beberapa bagian.

1. Remote access Trojan (RATs). Trojan adalah aplikasi yang memiliki tampilan normal tetapi menyembunyikan kode berbahaya. Trojan, yang biasanya ditampilkan sebagai program yang dapat dieksekusi, secara diam-diam memasang program jahat di samping program yang tidak berbahaya, sehingga membahayakan integritas sistem yang disusupi. Dalam domain trojan, ada subkelas penting yang perlu dipertimbangkan yaitu remote access trojan (RAT) (floroiu et al., 2024).
2. Information Stealer. Malware yang bertujuan mengumpulkan data dari perangkat korban disebut malware pencuri informasi, atau pencuri info. Identitas dan kata sandi pengguna, informasi kartu kredit, dompet mata uang kripto, file lokal, dan data peramban—termasuk cookie, riwayat pengguna, dan informasi formulir isi otomatis—semuanya dapat termasuk dalam kategori ini. Penjahat dunia maya memanfaatkan malware pencuri informasi untuk mendapatkan kata sandi pengguna dan data sistem, biasanya dengan tujuan menghasilkan uang. Dalam serangan kejahatan dunia maya terhadap berbagai organisasi dan sektor di seluruh dunia, termasuk Australia, pencuri informasi telah diamati. Panduan malware pencuri informasi, aktivitas ancaman, dan saran mitigasi untuk bisnis dan staf mereka semuanya disertakan dalam makalah ini untuk para pembaca (Complexity, 2024)
3. Banking Trojan. Tujuan dari malware trojan perbankan adalah untuk memperoleh informasi login untuk lembaga keuangan. Web injection merupakan metode yang sering digunakan untuk mempermudah pencurian ini. Web inject berfungsi dengan mengubah kode HTML halaman web atau dengan menyadap input

pengguna di dalam browser.

4. Ramsom Ware. Malware yang dikenal sebagai ransomware diciptakan untuk memungkinkan berbagai tindakan terlarang, seperti mengunci data pribadi hingga uang tebusan dibayarkan (Beaman et al., 2020).
5. Botnets. Botnet adalah instrumen untuk menyebarkan malware ke seluruh jaringan. Hal ini mencirikannya sebagai risiko signifikan bagi jaringan bisnis, yang mungkin memerlukan data, aplikasi, dan layanan agar dapat diakses setiap saat. Sumber utama serangan Denial-of-Service (DOS) adalah botnet. Botnet memiliki kemampuan untuk menghentikan pekerja mengakses data pribadi dan sensitif yang tersimpan di jaringan. Hal ini dapat berdampak buruk pada kapasitas sistem untuk mengakses data serta reputasi pengelola data (Owen et al., 2022).
6. General android malware. Malware Android adalah perangkat lunak berbahaya yang secara khusus dirancang untuk menargetkan perangkat Android. Malware ini dapat menyebabkan berbagai masalah, seperti mencuri informasi pribadi, menampilkan iklan yang tidak diinginkan, atau bahkan mengambil alih kendali Perangkat (Sabbah et al., 2023).
7. Downloader. jenis perangkat lunak berbahaya yang dirancang untuk mengunduh dan menginstal program berbahaya tambahan ke perangkat yang terinfeksi.
8. Proxy Botnets. Perangkat yang disusupi yang digunakan oleh penjahat dunia maya untuk mengarahkan lalu lintas berbahaya, sehingga secara efektif menutupi sumber lalu lintas yang sebenarnya
9. Penetration testing tools. Alat pengujian penetrasi dirancang untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem, tetapi terkadang dapat disalahgunakan atau mengandung malware itu sendiri.
10. Cryptocurrency Miner. Memecahkan kode-kode tersembunyi yang tersusun dari persamaan algoritma matematika merupakan proses penambangan mata uang kripto pada blockchain. Penambang akan mendapatkan imbalan berupa mata uang digital yang sebanding dengan jumlah kripto yang ditambang dan jenis kripto tersebut, hal ini dikarenakan setiap kripto memiliki tingkat kesulitannya masing-masing (Rakhman et al., 2023).
11. Phishing. Phishing sebagai "aktivitas penipuan yang melibatkan pembuatan situs web palsu untuk mengelabui pengguna agar memberikan informasi sensitif seperti kata sandi, informasi keuangan, atau informasi pribadi." Menurut definisi yang diberikan di atas, phishing adalah upaya untuk mengelabui seseorang agar mengungkapkan informasi pribadi, seperti nomor kartu kredit dan informasi rekening bank, dengan mengirimkan tautan berbahaya yang mengarahkan mereka ke situs web palsu (Alkhalil et al., 2021)

**Pembahasan**

Berdasarkan analisa data dan pengelompokan jenis serangan maka dapat dibuatkan satu kesimpulan bahwa terdapat 11 kelompok ancaman. Detail informasi mengenai pengelompokan ancaman tercantum dalam tabel 3. Berdasarkan hasil tersebut maka trojan mendominasi memberikan kontribusi dalam ancaman keamanan siber dari penyalahgunaan sumber daya TIK. Trojan adalah program jahat yang menyamar sebagai perangkat lunak yang sah. Aplikasi ini memiliki kemampuan untuk

menyembunyikan malware dalam item yang ingin di unduh, termasuk musik, film, permainan komputer, dan lampiran email. Jenis malware zero-access, yang dapat merusak server, jaringan, dan sistem komputer, adalah jenis yang paling umum. Jenis ini didefinisikan sebagai perangkat lunak yang memasuki komputer tanpa izin. Microsoft Windows terdampak oleh malware Trojan horse yang dikenal sebagai Zero Access.

Dengan menggunakan taktik rootkit, trojan menyembunyikan dirinya di sistem yang disusupi sambil mengunduh malware tambahan dari botnet. Jenis Trojan ini menggunakan port terdaftar 16464 untuk mengeksploitasi protokol datagram pengguna.

Tabel 3. Klasifikasi ancaman berdasarkan ancaman

| Remote Access Trojans (RATs) | Information Stealers | Banking Trojans | Ransomware | Botnets | General Android Malware) | downloader | Proxy Botnet | Penetration Testing Tool | Cryptocurrency Miner | Phishing |
|---|---|---|---|---|---|---|---|---|---|---|
| Adwind | ArkeiStealer | Banload | Locky | Andromeda | Androidmal ware | Amadey | Bunitu | CobaltStrike | CoinMiner | FinancialSt atement |
| AgentTesla | AzorUlt | dridex | Ransom.Locky | Mirai | | | | | CoinMiner.XMRig | |
| AsyncRAT | AzorultBot | Emotet | Ransom.LockyV2 | ZeroAccess | | | | | DofoilV3 | |
| AveMariaRAT | Baldr | Gameover-zeus | Teslacrypt | Nitol | | | | | | |
| BabylonRAT | Fareit | Gozi | | PushdoV3 | | | | | | |
| BlackRAT | FormBook | Hancitor | | | | | | | | |
| DarkComet | KPOTStealer | Heodo | | | | | | | | |
| ImminentRAT | LokiBot | IcedID | | | | | | | | |
| NanoCore | RaccoonStealer | Kronos | | | | | | | | |
| NetWire | PredatorStealer | Ramnit | | | | | | | | |
| OrcusRAT | Zegost | TrickBot | | | | | | | | |
| ParallaxRAT | Loki | Valak | | | | | | | | |
| QuasarRAT | | Locky | | | | | | | | |
| RemcosRAT | | BlackMoon | | | | | | | | |
| RevengeRat | | DanaBot | | | | | | | | |
| XpertRAT | | Neurevt | | | | | | | | |
| LimeRAT | | Spyeye | | | | | | | | |
| Cybergate | | TinyNuke | | | | | | | | |
| FlawedAmmyyRAT | | TrickBotTier-2 | | | | | | | | |
| WSHRAT | | | | | | | | | | |
| QRat | | | | | | | | | | |
| Remcos | | | | | | | | | | |

Beberapa tahapan dalam pendeteksian meliputi hal di bawah ini:

1. Perilaku Aneh. Waspadai indikasi seperti kinerja yang lambat, pop-up yang tidak terduga, atau aplikasi yang diluncurkan sendiri.
2. Perangkat Lunak Antivirus. Jalankan pemindaian sistem secara berkala dengan perangkat lunak antivirus yang andal. Trojan dapat ditemukan dan dihilangkan oleh sebagian besar aplikasi antivirus.
3. Task Manager. Cari proses aneh di pengelola tugas. Jika ditemukan sesuatu yang tidak biasa, bisa jadi itu adalah trojan horse.

Sedangkan pencegahan yang bisa dilakukan adalah

1. Jauhi tautan dan unduhan yang mencurigakan. Jangan mengeklik tautan atau mengunduh file dari sumber yang tidak dikenal.
2. Selalu perbarui perangkat lunak. Untuk melindungi dari kerentanan, semua perangkat lunak, termasuk sistem operasi, diperbarui kata sandi yang kuat, buat kata sandi yang kuat dan unik untuk melindungi dari peretasan akun.
3. Firewall harus diaktifkan untuk mencegah pengguna yang tidak berwenang

mengakses komputer.
4. Pencadangan Sering. Data dicadangkan secara berkala ke cloud atau drive eksternal. Jadi, jika seseorang terinfeksi, sistem dapat diperbaiki.

**Kesimpulan**

Penyalahgunaan teknologi informasi dan komunikasi (TIK) dapat berdampak besar pada keamanan siber. Kejahatan siber seperti serangan ransomware, phishing, dan peretasan dapat meningkat akibat penyalahgunaan TIK. Penjahat siber memanfaatkan celah dalam sistem TIK untuk memeras uang tebusan, mencuri data rahasia, dan mengganggu layanan. Prosedur TIK yang tidak memadai dapat menyebabkan pelanggaran data, di mana informasi pribadi diakses oleh pihak yang tidak berwenang. Terdapat tiga hal yang menjadi acuan untuk pencegahan dan pendeteksian, sisi teknis dengan adopsi teknologi yang mampu menahan seranagn misalanya dengan memperbaharui firewall, yang kedua adalah regulasi dan kebijakan dari organisasi yang lebih baik lagi dan yang ketiga ada peningkatan cybersecurty awareness yang lebih ditingkatkan melalu pelatihan dan training.

**Referensi**

Al-Rahmi, W. M., Alzahrani, A. I., Yahaya, N., Alalwan, N., & Kamin, Y. Bin. (2020). Digital Communication: Information And Communication Technology (ICT) Usage For Education Sustainability. *Sustainability (Switzerland)*, *12*(12), 1–18. Https://Doi.Org/10.3390/Su12125052

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study And A New Anatomy. *Frontiers In Computer Science*, *3*(March), 1–23. Https://Doi.Org/10.3389/Fcomp.2021.563060

Asaad, R. R., & Saeed, V. A. (2022). A Cyber Security Threats, Vulnerability, Challenges And Proposed Solution. *Applied Computing Journal*, *2*(4), 227–244.Https://Doi.Org/10.52098/Acj.202260

Beaman, C., Barkworth, A., & David, T. (2020). TC 11 Briefing Papers Ransomware : Recent advances , analysis , challenges and future research directions.

Carvalho, S., Carvalho, J. V., Silva, J. C., Santos, G., & De Melo Bandeira, G. S. (2023). Concerns About Cybersecurity: The Implications Of The Use Of ICT For Citizens And Companies. *Journal Of Information Systems Engineering And Management*, *8*(2). Https://Doi.Org/10.55267/Iadt.07.13226

Complexity, C. (N.D.). *The Silent Heist : Cybercriminals Use Information Stealer Malware To Compromise Corporate Networks*.

Floroiu, I., Floroiu, M., Niga, A.-C., & TIMISICA, D. (2024). Remote Access Trojans Detection Using Convolutional And Transformer-Based Deep Learning Techniques. *Romanian Cyber Security Journal*, *6*(1), 47–58. Https://Doi.Org/10.54851/V6i1y202405

Hama Saeed, M. A. (2020). Malware In Computer Systems: Problems And Solutions. *IJID (International Journal On Informatics For Development)*, *9*(1), 1. Https://Doi.Org/10.14421/Ijid.2020.09101

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk Based Approach In Scope Of Cybersecurity Threats And Requirements. *Procedia Manufacturing*, *44*(2019), 655–662. Https://Doi.Org/10.1016/J.Promfg.2020.02.243

Jony, A. I., & Hamim, S. A. (2024). Navigating The Cyber Threat Landscape: A Comprehensive Analysis Of Attacks And Security In The Digital Age. *Journal Of Information Technology And Cyber Security*, *1*(2), 53–67. Https://Doi.Org/10.30996/Jitcs.9715

Khanna, P. (2023). *Emerging Cybersecurity Threats And Countermeasures: A Comprehensive Review*. *11*(7), 2320–2882. Www.Ijcrt.Orgwww.Ijcrt.Org

Owen, H., Zarrin, J., & Pour, S. M. (2022). A Survey On Botnets, Issues, Threats, Methods, Detection And Prevention. *Journal Of Cybersecurity And Privacy*, *2*(1), 74–88. Https://Doi.Org/10.3390/Jcp2010006

Rakhman, I., Munir, M., Musyafa'ah, N., & Minarti, S. (2023). Mining Cryptocurrency Di Blockchain. *Jurnal Riset Manajemen Dan Ekonomi (Jrime)*, *1*(1), 262–273.

Sabbah, A., Taweel, A., & Zein, S. (2023). Android Malware Detection: A Literature Review. *Communications In Computer And Information Science*, *1768 CCIS*(June), 263–278. Https://Doi.Org/10.1007/978-981-99-0272-9_18

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework For The Future Of Cybersecurity. In *Sustainability (Switzerland)* (Vol. 15, Issue 18). Https://Doi.Org/10.3390/Su151813369

Singh, A. (2021). Significance Of Research Process In Research Work. *SSRN Electronic Journal*, *March*. Https://Doi.Org/10.2139/Ssrn.3815032

Waruwu, G., & Sundari, J. (2024). Audit Teknologi Informasi Menggunakan Cobit 5 Studi Kasus PT. Global Network Dharma Jaya. *Infomatek*, *26*(1), 69–74. Https://Doi.Org/10.23969/Infomatek.V26i1.13333.