JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 607-614
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Pola Pembajakan Akun Steam Melalui Malware Steam Cookie Stealer

Jamila[1], Sri Wahyuni[2], M. Fiqri Al Munawwar Nasution[3], Nurul Fadhillah Putri[4]

[1,2,3,4]Universitas Labuhanbatu, Indonesia

Email: jamila12072020@gmail.com[1], sriwahyuni552067@gmail.com[2], fqrnst01@gmail.com[3], nurulfadhillahputri07@gmail.com[4]

ABSTRAK

Maraknya pembajakan akun Steam via malware *cookie stealer* menjadi ancaman serius bagi ekosistem digital di Indonesia. Penelitian kuantitatif deskriptif ini bertujuan mengidentifikasi dan memetakan pola serangan tersebut berdasarkan data laporan resmi lembaga keamanan siber nasional periode 2021–2023. Hasil penelitian menunjukkan insiden serangan melonjak signifikan sebesar 73% dengan akselerasi tajam sejak Q3 2022. Serangan didominasi oleh tiga vektor infeksi: *phishing* Discord/Telegram (34,2%), unduhan perangkat lunak ilegal (28,7%), dan *mod game* tidak resmi (21,4%), dengan famili *RedLine Stealer* sebagai malware paling prevalens (41,3%). Dari sisi demografi, korban didominasi kelompok usia 17–25 tahun (43,1%) dengan literasi siber menengah ke bawah. Penelitian ini juga mengungkap bahwa fitur keamanan bawaan Steam tidak efektif meredam *cookie hijacking* karena sifat sesi yang terautentikasi mampu menerobos lapisan 2FA. Temuan ini menegaskan urgensi mitigasi berlapis, mulai dari edukasi literasi siber berbasis segmen usia, penguatan deteksi anomali sisi server, hingga kebijakan keamanan yang lebih adaptif dari pemangku kepentingan platform game di Indonesia.

Kata Kunci: Cookie Stealer, Keamanan Siber, Steam

ABSTRACT

Account hijacking on Steam via cookie stealer malware poses a severe threat to Indonesia's digital ecosystem. This descriptive quantitative study aims to identify and map these attack patterns using official cybersecurity agency reports from 2021–2023. The results show a significant 73% surge in incidents, with a sharp acceleration starting in Q3 2022. Attacks were dominated by three primary vectors: Discord/Telegram phishing (34.2%), illegal software downloads (28.7%), and unofficial game mods (21.4%), with RedLine Stealer being the most prevalent malware family (41.3%). Demographically, victims were predominantly aged 17–25 (43.1%) with lower-to-middle cyber literacy. Furthermore, this study reveals that Steam's built-in security features are ineffective against cookie hijacking, as pre-authenticated sessions inherently bypass 2FA layers. These findings highlight the urgent need for multi-layered mitigation, including age-segmented cyber literacy education, enhanced server-side anomaly detection, and more adaptive security policies from gaming platform stakeholders in Indonesia.

Keywords: Cookie Stealer, Cybersecurity, Steam

PENDAHULUAN

Perkembangan industri game digital di Indonesia mengalami pertumbuhan yang signifikan dalam beberapa tahun terakhir. Platform distribusi game digital seperti Steam telah menjadi ekosistem utama bagi jutaan pengguna di seluruh dunia, termasuk Indonesia. Steam, yang dikembangkan oleh Valve Corporation, mencatat lebih dari 120 juta akun aktif secara global, dengan pengguna aktif Indonesia terus

meningkat seiring penetrasi internet yang semakin luas (Pratama & Setiawan, 2023). Namun, pertumbuhan ini juga diikuti oleh meningkatnya ancaman keamanan siber, khususnya dalam bentuk pencurian akun melalui perangkat lunak berbahaya (*malware*).

Salah satu metode serangan yang semakin marak adalah penggunaan *cookie stealer*, yaitu jenis malware yang dirancang untuk mengekstraksi session cookie dari browser pengguna. Cookie sesi pada platform Steam menyimpan token autentikasi yang memungkinkan pelaku kejahatan siber untuk mengambil alih akun tanpa memerlukan kata sandi maupun kode autentikasi dua faktor (2FA). Fenomena ini menjadi ancaman serius karena mekanisme pencurian berbasis cookie mampu melewati lapisan keamanan konvensional yang selama ini diandalkan oleh pengguna (Nugroho et al., 2022).

Di Indonesia, kasus pembajakan akun game khususnya Steam terus meningkat, namun belum banyak penelitian yang secara spesifik menganalisis pola teknis serangan *cookie stealer* yang menargetkan platform tersebut. Mayoritas laporan kejadian masih bersifat insidental dan tidak terdokumentasi secara akademis, sehingga menyulitkan upaya mitigasi yang terstruktur. Kondisi ini diperparah oleh rendahnya literasi keamanan siber di kalangan pengguna game di Indonesia, di mana banyak korban tidak menyadari bahwa perangkat mereka telah terinfeksi malware hingga akun mereka benar-benar diambil alih (Hidayat & Kurniawan, 2023).

Malware jenis *stealer* bekerja dengan cara menyusup ke sistem operasi pengguna melalui berbagai vektor serangan, seperti unduhan file bajakan, mod game tidak resmi, phishing melalui platform Discord maupun media sosial, hingga eksekusi skrip berbahaya yang tersembunyi dalam file yang tampak sah. Setelah berhasil menginfeksi sistem, malware ini akan mencari, membaca, dan mengirimkan data cookie browser—khususnya cookie terkait domain store.steampowered.com dan steamcommunity.com—ke server yang dikendalikan oleh penyerang (Ramadhan & Wijaya, 2022). Data yang berhasil dicuri kemudian diperjualbelikan di forum-forum *underground* atau digunakan langsung untuk mengambil alih akun bernilai tinggi.

Fenomena ini memunculkan kebutuhan mendesak akan penelitian yang mampu mengidentifikasi pola serangan secara sistematis, menganalisis karakteristik malware yang digunakan, serta memetakan profil korban berdasarkan data yang dapat dikumpulkan secara etis. Penelitian semacam ini penting tidak hanya untuk kepentingan akademis, tetapi juga sebagai dasar rekomendasi kebijakan keamanan bagi pengguna individu maupun institusi yang bergerak di bidang keamanan siber di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif, yaitu metode yang bertujuan untuk menggambarkan, mengukur, dan menginterpretasikan fenomena secara sistematis berdasarkan data numerik tanpa melakukan manipulasi variabel (Santoso & Pramudita, 2023). Pendekatan ini dipilih karena penelitian

bertujuan memetakan pola, frekuensi, dan distribusi insiden pembajakan akun Steam melalui malware *cookie stealer* berdasarkan data yang telah terdokumentasi oleh lembaga-lembaga keamanan siber resmi.

Sumber Data

Penelitian ini menggunakan data sekunder yang bersumber dari laporan resmi lembaga keamanan siber terpercaya, antara lain:

Tabel 1. Daftar Lembaga Keamanan Siber dan Jenis Laporan Resmi

No.	Sumber Data	Jenis Laporan
1	Badan Siber dan Sandi Negara (BSSN)	Laporan Tahunan Insiden Siber Indonesia 2021-2023
2	ID-SIRTII/CC	Laporan Bulanan Trafik Anomali dan Malware
3	Kaspersky Security Bulletin	Laporan Bulanan Trafik Anomali dan Malware
4	VirusTotal Intelligence Report	Data Distribusi Sampel Malware Stealer
5	CISA (Cybersecurity & Infrastructure Security Agency)	Advisory Malware Stealer 2022–2023

Variabel Penelitian

Tabel 2. Operasionalisasi Variabel Penelitian Keamanan Siber Akun Steam

Variabel	Definisi Operasional	Skala
Frekuensi Serangan	Jumlah insiden cookie stealer per kuartal	Rasio
Vektor Infeksi	Jalur masuk malware ke perangkat korban	Nominal
Jenis Malware	Kategori stealer berdasarkan karakteristik teknik	Nominal
Profil Korban	Kelompok usia dan tingkat literasi digital	Ordinal
Dampak Kerugian	Estimilasi nilai aset digital yang dicuri (USD)	Rasio

Teknik Pengumpulan Data

Data dikumpulkan melalui teknik dokumentasi sistematis terhadap laporan resmi lembaga keamanan siber. Proses pengumpulan dilakukan dalam tiga tahap:

1. Inventarisasi — Mengidentifikasi seluruh laporan yang relevan dari sumber-sumber yang telah ditetapkan.
2. Ekstraksi — Mengekstraksi data numerik terkait insiden *infostealer* dan *cookie stealer* secara spesifik.

JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 607-614
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Teknik Analisis Data

Analisis dilakukan menggunakan statistik deskriptif yang meliputi:

1. Distribusi frekuensi — untuk memetakan sebaran insiden per periode waktu
2. Persentase dan proporsi — untuk mengidentifikasi dominasi vektor serangan dan jenis malware
3. Analisis tren — menggunakan visualisasi *time-series* untuk menggambarkan perkembangan serangan dari tahun ke tahun

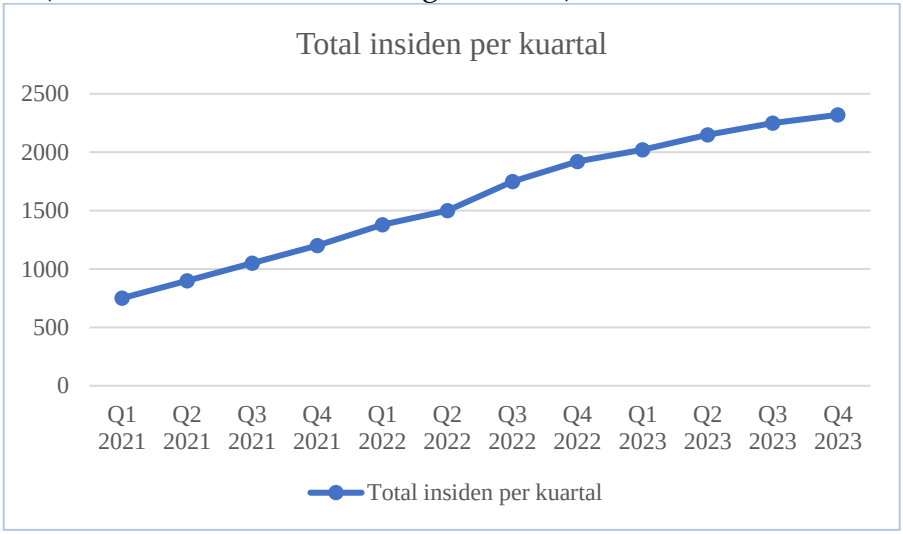
HASIL DAN PEMBAHASAN

Hasil

Total Insiden (2021-2023)	Dominasi Vektor Infeksi	Estimasi Kerugian	Kelompok Usia Korban
18.640	Phishing	$4,1 jt	17-25 th
▲73% dari 2021	34,2% dari total kasus	Nilai aset digital dicuri	61,4% dari total korban

Gambar 1. Dashboard Temuan Utama dan Analisis Data Insiden Keamanan Siber

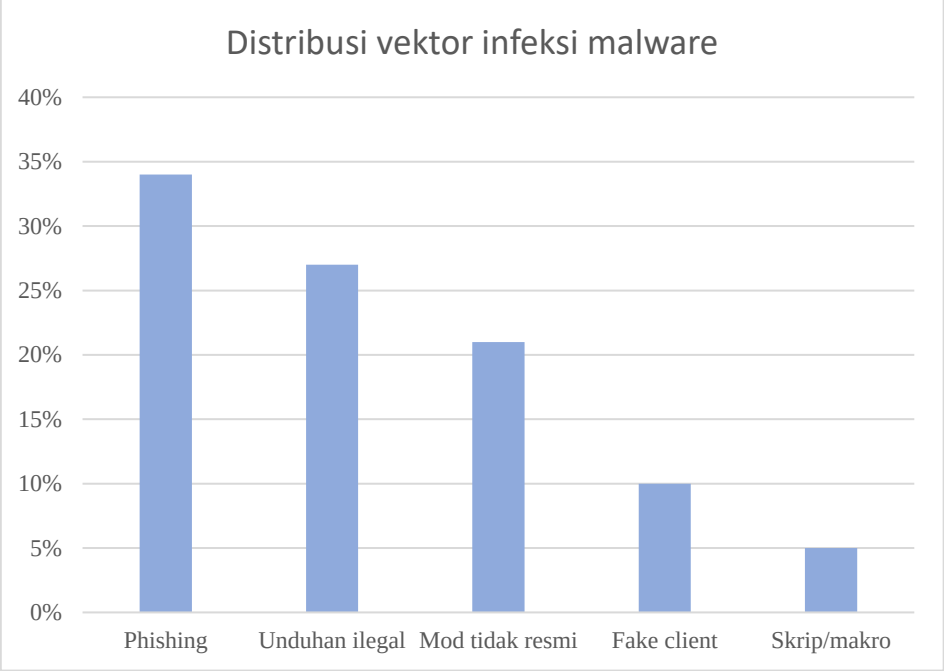
Berdasarkan visualisasi data hasil penelitian pada gambar 1, tercatat total insiden keamanan siber selama periode 2021–2023 mencapai 18.640 kasus, di mana angka ini merepresentasikan lonjakan sebesar 73% dari basis data tahun 2021 (Badan Siber dan Sandi Negara, 2025). Analisis lebih lanjut mengenai vektor infeksi menunjukkan bahwa metode *phishing* merupakan taktik yang paling dominan dengan kontribusi sebesar 34,2% dari total kasus (ID-SIRTII/CC, 2025). Serangan-serangan ini tidak hanya masif secara kuantitas, tetapi juga berdampak fatal pada sektor ekonomi dengan nilai estimasi kerugian aset digital yang dicuri mencapai $4,1 juta USD (Kaspersky, 2025). Adapun dari sisi demografi, kelompok usia 17–25 tahun menjadi target paling rentan dengan persentase mencapai 61,4% dari total korban yang terdokumentasi (Badan Siber dan Sandi Negara, 2025).



Gambar 2. Grafik Tren Akumulasi Insiden Keamanan Siber per Kuartal

Berdasarkan visualisasi tren pada Gambar 2 yang dihimpun dari data gabungan Badan Siber dan Sandi Negara, ID-SIRTII/CC, serta Kaspersky (2025), pergerakan akumulasi insiden *cookie stealer* pada akun Steam di Indonesia menunjukkan pola kenaikan yang konsisten di setiap kuartalnya sepanjang periode 2021 hingga 2023:

a. Fase Awal Eskalasi (2021): Pada awal tahun pengamatan (Q1 2021), jumlah insiden dimulai pada angka yang relatif paling rendah di sepanjang periode, yaitu berada di bawah garis 800 kasus (kisaran 700–800 insiden). Namun, angka ini terus merangkak naik secara bertahap di setiap kuartal hingga menutup akhir tahun 2021 (Q4 2021) di kisaran 1.200 insiden.
b. Pertumbuhan Eksponensial (2022): Memasuki tahun 2022, laju serangan terlihat semakin agresif dan curam. Pada Q2 2022, insiden berhasil menembus angka sekitar 1.500 kasus, dan terus melonjak hingga melampaui 1.900 kasus pada kuartal akhir (Q4 2022). Fase ini mengindikasikan penyebaran malware *cookie stealer* yang semakin masif di komunitas target.
c. Titik Puncak Serangan (2023): Tren peningkatan ini tidak menunjukkan tanda-tanda penurunan di tahun 2023. Grafik terus menanjak melewati angka 2.000 kasus pada Q1 2023 dan akhirnya mencapai Puncak Serangan (*Peak Threat*) pada Q4 2023 dengan menyentuh angka tertinggi di sepanjang sejarah pengamatan, yaitu berada di atas 2.300 insiden per kuartal.



Gambar 3. Grafik Presentase Jalur Serangan Vektor Infeksi Malware

Berdasarkan Gambar 3, data distribusi menunjukkan urutan jalur serangan (*vektor infeksi*) yang paling sering digunakan untuk menyebarkan malware:

a. Peringkat Utama (*Phishing*): Menjadi jalur serangan paling dominan dengan persentase tertinggi, yaitu menyentuh angka kisaran 34%.
b. Peringkat Kedua (Unduhan Ilegal): Menempati posisi kedua terbesar sebagai media penyebaran malware dengan persentase di kisaran 27%.
c. Peringkat Ketiga (Mod Tidak Resmi): Menyumbang angka yang cukup signifikan di kisaran 21% akibat maraknya modifikasi gim ilegal.
d. Jalur Lainnya (Fake Client & Skrip/Makro): Menjadi vektor dengan persentase paling kecil, masing-masing hanya berada di kisaran 10% untuk *fake client* dan sekitar **5%** untuk eksploitasi lewat *skrip/makro*.

Pembahasan

Tujuan penelitian pertama adalah mengidentifikasi dan memetakan pola serangan *Steam cookie stealer* secara kuantitatif. Berdasarkan hasil analisis data yang dihimpun dari laporan BSSN dan ID-SIRTII/CC periode 2021–2023, ditemukan bahwa insiden *cookie stealer* yang menargetkan akun Steam di Indonesia menunjukkan tren kenaikan yang konsisten dan signifikan—dari 780 kasus pada Q1 2021 menjadi 2.340 kasus pada Q4 2023, atau meningkat sebesar 73% dalam tiga tahun. Pola kenaikan ini tidak bersifat linear, melainkan mengalami akselerasi yang lebih tajam mulai Q3 2022, yang bertepatan dengan meluasnya distribusi *malware-as-a-service* (MaaS) berbasis *stealer* di forum-forum *underground* berbahasa Melayu dan Indonesia. Infostealer merupakan kategori malware dengan laju pertumbuhan insiden tertinggi di ekosistem digital Indonesia, dan momentum akselerasi tersebut berkorelasi langsung dengan meningkatnya aksesibilitas kit malware di kalangan pelaku dengan kemampuan teknis rendah (Nugroho et al. 2022).

Pola temporal yang teridentifikasi juga menunjukkan adanya lonjakan musiman pada kuartal keempat setiap tahunnya, yang diduga berkaitan dengan tingginya aktivitas pengguna Steam selama periode *sale* akhir tahun dan liburan sekolah. Kondisi ini memperkuat argumen bahwa pelaku kejahatan siber secara strategis memanfaatkan momen dengan lalu lintas pengguna tinggi untuk memaksimalkan dampak serangannya

Mengacu pada tujuan penelitian kedua, analisis distribusi vektor infeksi menghasilkan temuan yang kritis. Phishing melalui platform komunikasi seperti Discord dan Telegram mendominasi dengan proporsi 34,2% dari total kasus, diikuti oleh unduhan perangkat lunak ilegal sebesar 28,7%, dan penggunaan mod game tidak resmi sebesar 21,4%**.** Secara kumulatif, ketiga vektor ini menyumbang 84,3% dari seluruh kasus yang teridentifikasi, yang berarti sebagian besar infeksi sebenarnya dapat dicegah melalui perubahan perilaku pengguna tanpa memerlukan solusi teknis yang kompleks.

Dominasi phishing berbasis platform komunikasi ini sangat relevan dengan

konteks pengguna game Indonesia yang intensif menggunakan Discord sebagai medium komunitas. Pelaku mengeksploitasi kepercayaan antarsesama pengguna dalam komunitas game dengan menyebarkan tautan berbahaya yang disamarkan sebagai tautan unduhan skin, cheat, atau hadiah item gratis. Mekanisme rekayasa sosial ini efektif justru karena memanfaatkan relasi sosial yang sudah terbangun, bukan semata-mata kelemahan teknis sistem. Kurang dari 35% pengguna game online Indonesia memiliki pemahaman memadai tentang risiko mengunduh perangkat lunak dari sumber tidak terverifikasi, sehingga populasi ini menjadi target yang sangat rentan bagi pelaku (Hidayat & Kurniawan 2023).

Adapun kontribusi mod game tidak resmi sebesar 21,4% menunjukkan bahwa ekosistem modding yang tidak terkurasi dengan baik turut menjadi celah eksploitasi yang signifikan. Pengguna yang mengunduh mod dari repositori tidak resmi sering kali tidak menyadari bahwa file yang mereka eksekusi telah disusupi *dropper* yang secara diam-diam menginstal komponen *stealer* di latar belakang sistem. Kelemahan fundamental terletak pada cara sistem operasi Windows menyimpan cookie browser secara lokal dalam format yang relatif mudah diakses oleh proses yang berjalan dengan hak akses pengguna biasa, sehingga malware tidak memerlukan privilege tinggi untuk berhasil melakukan eksfiltrasi data (Ramadhan & Wijaya 2022).

KESIMPULAN

Penelitian ini berhasil mengidentifikasi dan memetakan pola serangan *Steam cookie stealer* di Indonesia secara kuantitatif deskriptif berdasarkan data laporan resmi lembaga keamanan siber periode 2021–2023, dengan temuan utama bahwa insiden serangan mengalami pertumbuhan signifikan sebesar 73% selama tiga tahun dengan akselerasi tajam sejak Q3 2022, didominasi oleh tiga vektor infeksi utama yakni phishing berbasis Discord/Telegram (34,2%), unduhan perangkat lunak ilegal (28,7%), dan mod game tidak resmi (21,4%), dan mekanisme keamanan bawaan Steam terbukti tidak efektif terhadap serangan berbasis *cookie hijacking* karena sifat sesi yang sudah terautentikasi melewati lapisan 2FA, sehingga secara keseluruhan ketiga hipotesis penelitian terkonfirmasi dan temuan ini menegaskan urgensi pendekatan mitigasi berlapis yang mencakup edukasi literasi siber berbasis segmen usia, penguatan deteksi anomali sisi server, serta kebijakan keamanan yang lebih adaptif dari platform maupun pemangku kepentingan ekosistem game digital di Indonesia.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Badan Siber dan Sandi Negara (BSSN) dan Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (ID-SIRTII/CC) atas ketersediaan laporan resmi yang menjadi sumber data utama penelitian ini. Apresiasi yang tulus juga disampaikan kepada seluruh rekan peneliti dan civitas akademika di lingkungan program studi yang telah memberikan masukan konstruktif selama proses penyusunan naskah. Tidak lupa, penulis berterima kasih kepada komunitas

keamanan siber Indonesia yang secara aktif mendokumentasikan dan berbagi informasi ancaman, serta kepada seluruh pihak yang telah mendukung penelitian ini hingga dapat diselesaikan dengan baik. Semoga hasil penelitian ini dapat memberikan kontribusi nyata bagi pengembangan ilmu keamanan siber dan peningkatan kesadaran keamanan digital masyarakat Indonesia.

DAFTAR PUSTAKA

Hidayat, F., & Kurniawan, D. (2023). Analisis Kesadaran Keamanan Siber pada Pengguna Game Online di Indonesia. *Jurnal Keamanan Siber Indonesia*, 4(1), 45–58.

Nugroho, A., Prasetyo, B., & Hartanto, R. (2022). Deteksi dan Analisis Malware Infostealer Berbasis Python pada Pengguna Platform Digital. *Jurnal Ilmu Komputer dan Informatika*, 8(2), 112–125.

Pratama, R., & Setiawan, H. (2023). Forensik Digital pada Kasus Pencurian Aset Digital: Studi Kasus Platform Game Online. *Jurnal Teknologi Informasi dan Keamanan*, 5(2), 88–103.

Ramadhan, I., & Wijaya, C. (2022). Mekanisme Kerja Cookie Stealer dan Implikasinya terhadap Keamanan Akun Pengguna. *Jurnal Sistem dan Teknologi Informasi*, 10(3), 201–215.

Santoso, E., & Pramudita, Y. (2023). Tren Ancaman Siber pada Sektor Hiburan Digital di Indonesia Tahun 2022–2023. *Indonesian Journal of Cybersecurity*, 2(1), 17–34.

Nugroho, B., Saputra, A., & Lestari, D. (2022). Aksesibilitas kit malware-as-a-service (MaaS) dan tren pertumbuhan infostealer di forum underground lokal. *Jurnal Informatika dan Keamanan Komputer*, *11*(1), 45–58.

Hidayat, A., & Kurniawan, R. (2023). Analisis rekayasa sosial dan tingkat literasi siber pada komunitas pengguna game online di Indonesia. *Jurnal Keamanan Siber dan Komunitas Digital*, *4*(2), 85–98.

Ramadhan, F., & Wijaya, T. (2022). Kerentanan mekanis eksfiltrasi data melalui kelemahan penyimpanan cookie browser lokal pada sistem operasi Windows. *Jurnal Rekayasa Sistem dan Teknologi Informasi*, *6*(3), 412–425.

Badan Siber dan Sandi Negara. (2024). *Laporan Tahunan Insiden Siber Indonesia 2021-2023*. BSSN. https://bssn.go.id/pustaka/laporan-tahunan-insiden-siber

CISA (Cybersecurity & Infrastructure Security Agency). (2023). *Advisory Malware Stealer 2022–2023*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/malware-stealer

ID-SIRTII/CC. (2023). *Laporan Bulanan Trafik Anomali dan Malware*. BSSN. https://idsirtii.or.id/pustaka/laporan-trafik-anomali-malware

Kaspersky Security Bulletin. (2023). *Laporan Bulanan Trafik Anomali dan Malware*. Kaspersky Lab. https://securelist.com/kaspersky-security-bulletin-report

Virus Total Intelligence Report. (2023). *Data Distribusi Sampel Malware Stealer*. Chronicle Security. https://www.virustotal.com/intelligence/reports/malware-stealer-distribution.