

Evaluasi Kapabilitas Deteksi *anti-spyware* Terhadap *Dropper Spyware Mode Stealth*

Proposal Tugas Akhir

Oleh

**M. Kasyfil Aziz
18222127**



**PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
Desember 2025**

LEMBAR PENGESAHAN

Evaluasi Kapabilitas Deteksi *anti-spyware* Terhadap *Dropper Spyware Mode Stealth*

Proposal Tugas Akhir

Oleh

M. Kasyfil Aziz
18222127

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 5 Desember 2025

Pembimbing

Prof. Dr. Ing. Ir. Suhardi, M.I.
NIP. 196312111990011002

DAFTAR ISI

DAFTAR GAMBAR	iv
DAFTAR TABEL	v
I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah	2
I.3 Tujuan	3
I.4 Batasan Masalah	3
I.5 Metodologi	4
II TINJAUAN PUSTAKA	7
II.1 Malware	7
II.2 Spyware	8
II.3 Dropper	10
II.4 Fileless Malware	11
II.5 Teknik Evasi Malware	12
II.6 Deteksi Malware dan Teknologi Anti-Malware	13
II.7 Kasus Spyware Canggih dan Cyber Threat Intelligence (CTI)	14
II.8 Rust dalam Malware Development dan Fileless Execution	15
III ANALISIS MASALAH	16
III.1 Analisis Kondisi dan Kesenjangan (Current State and Gap Analysis) . .	16
III.1.1 Keterbatasan Deteksi Konvensional	16
III.1.2 Analisis Kesenjangan Desain <i>Dropper</i> (Gap Analysis)	17
III.2 Persyaratan Fungsional dan Non-Fungsional	19
III.3 Desain Keputusan dan Solusi yang Diusulkan	23
III.3.1 Alternatif Solusi	23
III.3.2 Analisis Penelitian Solusi	23
III.3.3 Metodologi Penilaian Solusi (Multi-Criteria Decision Analysis) . .	24
III.3.3.0.1 Langkah 1: Normalisasi Matriks Keputusan	24
III.3.3.0.2 Langkah 2: Perhitungan Nilai Entropi	25
III.3.3.0.3 Langkah 3: Penentuan Bobot Kriteria	25
III.3.3.0.4 Langkah 4: Perhitungan Skor Komposit Akhir	25
III.3.4 Hasil Analisis Penentuan Solusi	25

IV DESAIN KONSEP SOLUSI	28
IV.1 Diagram Konseptual Sistem	28
IV.1.1 Sistem Sebelum (Before)	28
IV.1.2 Sistem Sesudah (After)	29
IV.1.3 Perbandingan Sistem Before dan After	30
IV.2 Penjelasan Desain Solusi	32
IV.2.1 Desain Inisialisasi dan Verifikasi	32
IV.2.2 Desain Anti-Analysis (Environment Checking)	32
IV.2.3 Desain In-Memory Execution (Fileless Loading)	32
IV.2.4 Desain Komponen Modul Dropper	33
IV.3 Rancangan Lingkungan Pengujian	34
IV.4 Spesifikasi Mesin Uji	35
V RENCANA SELANJUTNYA	38
V.1 Rencana Implementasi	38
V.1.1 Langkah-langkah Implementasi	38
V.1.2 Alat yang Dibutuhkan	39
V.2 Rencana Evaluasi	40
V.2.1 Metode Pengujian	40
V.2.2 Metrik Evaluasi	40
V.2.3 Kriteria Keberhasilan	41
V.3 Analisis Risiko	42

DAFTAR GAMBAR

I.1	Kerangka kerja DRM	5
IV.1	Alur Deteksi Anti-Malware Sebelum (Before)	29
IV.2	Alur Eksekusi Dropper Spyware Mode Stealth (After)	30

DAFTAR TABEL

III.1	Ringkasan kesenjangan desain <i>dropper</i> dan arah solusi	18
III.2	Persyaratan fungsional (Functional Requirements)	20
III.3	Persyaratan non-fungsional (Non-Functional Requirements)	21
III.4	Bobot kriteria hasil metode EWM	26
III.5	Skor komposit akhir alternatif solusi	26
IV.1	Perbandingan Sistem Sebelum dan Sesudah Pengembangan	31
IV.2	Komponen Modul Dropper dan Fungsi Evasion	33
IV.3	Spesifikasi Lingkungan Uji	35
V.1	Timeline implementasi prototipe	38
V.2	Alat dan bahan pendukung implementasi	39
V.3	Metrik evaluasi implementasi dropper	40
V.4	Kriteria keberhasilan prototipe dropper	41
V.5	Risiko implementasi dan mitigasi	43

BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi yang pesat turut membawa peningkatan ancaman keamanan siber, terutama berupa malware yang semakin canggih dan sulit dideteksi (Sudhakar dan Kumar 2020). Salah satu varian berbahaya adalah *spyware*, yang merupakan perangkat lunak berbahaya dirancang untuk memantau dan mengumpulkan informasi sensitif tanpa izin, sehingga menimbulkan ancaman serius terhadap privasi dan keamanan pengguna (Reddyvari dkk. 2024). Dalam rantai infeksi *spyware* modern, *dropper* memainkan peran penting sebagai komponen pengantar dan eksekutor malware. *Dropper* bertugas untuk mendistribusikan, membuka kemasan (*unpack*), serta menjalankan *payload spyware* dalam sistem target dengan teknik yang mampu menghindari deteksi oleh *anti-malware* konvensional (Chatzoglou dkk. 2023).

Evolusi ini menunjukkan perpindahan dari ancaman tradisional berbasis berkas menuju serangan yang lebih canggih dan tersembunyi seperti *fileless malware* dan *spyware* mode *stealth*. *Dropper* saat ini tidak hanya berfungsi sebagai pengantar biasa, tetapi juga dilengkapi fitur *anti-debugging*, *anti-virtual machine*, serta teknik *stealth* lainnya yang membuatnya sangat tahan terhadap mekanisme deteksi dan pencegahan (Elghaly 2024). *Dropper* juga bisa bersifat *fileless*, beroperasi langsung di memori tanpa meninggalkan jejak file yang bisa dipindai, sehingga menjadi tantangan besar bagi sistem keamanan (Sudhakar dan Kumar 2020). Keberhasilan *dropper* menentukan efektivitas infeksi *spyware* secara keseluruhan, termasuk kemampuan *persistensi* dan pencurian data (Kareem 2024).

Kondisi keamanan siber saat ini dicirikan oleh evolusi ancaman yang signifikan. Sistem pertahanan keamanan menghadapi beberapa masalah kritis. Pertama, *anti-malware* tradisional masih mengandalkan pencocokan tanda tangan (*signature*), yang

dapat dihindari dengan teknik *packing*, enkripsi, dan *obfuscation* untuk mengubah *signature digital payload*. Kedua, *fileless malware* memanfaatkan komponen sah sistem operasi seperti *PowerShell* atau *WMI* untuk menjalankan kode berbahaya langsung di memori tanpa menulis berkas ke media penyimpanan, sehingga sulit di-deteksi oleh *anti-malware* konvensional (Sudhakar dan Kumar 2020). Ketiga, penelitian menunjukkan bahwa metode *evasion* yang relatif sederhana, seperti enkripsi, injeksi proses, dan penambahan *junk data* ke berkas eksekusi, terbukti sangat efektif dalam menghindari deteksi (Chatzoglou dkk. 2023). Evolusi ini menciptakan celah kritis dalam kemampuan deteksi sistem *anti-malware* dan *Endpoint Detection and Response* (EDR) yang tersedia di pasar.

Penelitian ini bertujuan mengkaji kapabilitas *anti-spyware* dalam mendeteksi dan menangkal *dropper spyware* baru yang menerapkan teknik evasi lanjutan. Kajian ini penting untuk mengetahui sejauh mana solusi keamanan saat ini mampu menghadapi ancaman yang semakin kompleks, dan memberikan dasar bagi pengembangan metode pertahanan yang lebih adaptif dan tangguh. Dengan mengacu pada studi dan analisis malware dari berbagai literatur terkini, penelitian ini juga akan menguji efektivitas berbagai produk *anti-spyware* komersial terhadap varian *dropper* tersebut dalam lingkungan simulasi yang realistik.

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah penelitian difokuskan pada *dropper spyware* mode *stealth* sebagai mekanisme serangan tahap awal (*initial access*). Pertanyaan penelitian yang diajukan adalah:

1. Seberapa efektif sistem *anti-malware* dan *Endpoint Detection & Response* (EDR) dalam mendeteksi aktivitas *dropper spyware* mode *stealth* yang berfungsi sebagai *initial access and delivery mechanism* pada lingkungan uji terkontrol?
2. Bagaimana pendekatan paling efektif untuk mengembangkan *dropper spyware stealth* yang mampu menghindari deteksi *anti-malware* dengan memanfaatkan teknik evasi modern seperti *fileless execution*, *in-memory payload delivery*, dan pemeriksaan *anti-analysis*?
3. Bagaimana pengaruh teknik evasi, misalnya *obfuscation*, enkripsi *payload*, *sandbox evasion*, dan deteksi *anti-VM*, terhadap kemampuan deteksi produk *anti-malware* dan EDR komersial saat ini?
4. Celah keamanan spesifik apa saja yang muncul pada produk *anti-malware* maupun EDR ketika dihadapkan pada *dropper spyware* kustom yang dirancang

dengan teknik penghindaran deteksi terintegrasi?

I.3 Tujuan

Secara umum penelitian ini bertujuan mengukur efektivitas sejumlah produk *anti-malware* dan EDR komersial dalam mendeteksi *dropper spyware* mode *stealth* yang bertindak sebagai vektor serangan awal. Tujuan khusus yang hendak dicapai yaitu:

1. Menganalisis dan mengidentifikasi teknik evasi *dropper spyware* paling efektif untuk menghindari deteksi *anti-malware* dan EDR, mencakup kategori *file-based*, *network-based*, *script-based*, *downloader-based*, serta *non-persistent*.
2. Mengembangkan prototipe *dropper spyware* mode *stealth* yang mengintegrasikan teknik evasi modern, seperti *fileless payload delivery*, eksekusi di memori, pemeriksaan *anti-VM/anti-debugging*, komunikasi C2 terenkripsi, dan modul *spyware* aktif menggunakan bahasa pemrograman Rust.
3. Melakukan pengujian komparatif prototipe terhadap beberapa produk *anti-malware* dan EDR terkemuka guna mengamati keberhasilan *payload delivery* serta respons deteksi pada setiap tahap eksekusi.
4. Mengidentifikasi celah keamanan dan kelemahan deteksi pada tiap produk, kemudian merumuskan rekomendasi teknis maupun strategis untuk meningkatkan kapabilitas mitigasi serangan *initial access* berbasis *dropper*.

Kriteria keberhasilan penelitian meliputi:

- Prototipe *dropper* berhasil mengimplementasikan sedikitnya tiga teknik evasi terintegrasi dan terbukti lolos dari deteksi minimal pada satu produk *anti-malware* yang diuji
- Hasil eksperimen menunjukkan perbedaan signifikan antar produk dalam mendeteksi *dropper* dan mengungkap tahap eksekusi yang paling sulit diawasi

I.4 Batasan Masalah

Penelitian ini memiliki batasan yang ditetapkan untuk memastikan fokus dan kelаяkan penelitian.

Batasan Penelitian

1. Batasan umum: Seluruh eksperimen dilaksanakan di lingkungan simulasi terkontrol dengan skenario yang telah ditetapkan. Ruang lingkup hanya sampai pemastian *payload* berhasil dijalankan pada sistem target tanpa mengevaluasi dampak pasca-infeksi.
2. Batasan desain pengujian: Penelitian berfokus pada *dropper spyware* mode

stealth yang memanfaatkan teknik *fileless execution, in-memory payload*, serta pemeriksaan *anti-analysis*. Metode distribusi lain seperti *worm* atau *supply-chain attack* tidak dianalisis secara detail.

3. Batasan implementasi: Pengujian hanya menilai kemampuan deteksi dan respons *anti-malware/EDR* hingga tahap *payload* aktif, tanpa melakukan analisis rinci terhadap *payload* lanjutan atau serangan lanjutan setelah *dropper* selesai bertugas.
4. Batasan lingkungan: Penelitian tidak melibatkan sistem nyata atau jaringan publik. Semua pengujian dilakukan dalam lingkungan virtual terisolasi untuk mencegah penyalahgunaan dan penyebaran malware.
5. Batasan produk yang diuji: Evaluasi dilakukan terhadap produk *anti-malware* dan EDR yang tersedia dan dapat diakses secara legal untuk tujuan akademis atau *trial period*.
6. Tugas akhir ini dikerjakan secara kelompok dengan anggota penelitian sebagai berikut:
 - Nathaniel Liady
 - M. Kasyfil Aziz
 - Audra Zelvania Putri Harjanto
 - Khayla Belva Annandira

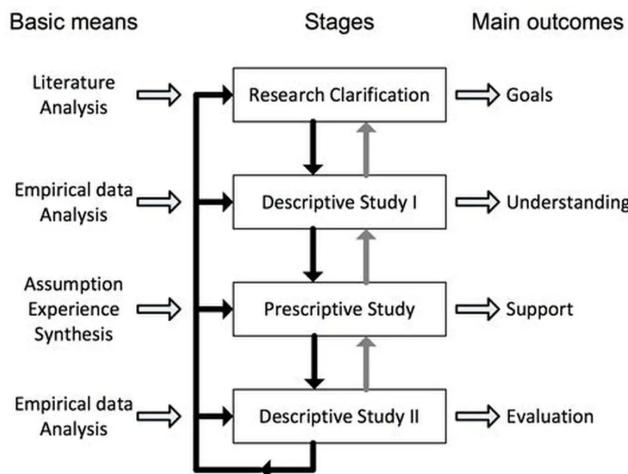
I.5 Metodologi

Metodologi penelitian mengacu pada *Design Research Methodology* (DRM) yang diperkenalkan oleh Blessing dan Chakrabarti (Blessing dan Chakrabarti 2009). Kerangka ini dipilih karena menyajikan proses iteratif yang terstruktur untuk merancang sekaligus mengevaluasi artefak teknis dalam konteks penelitian pendesainan sistem yang kompleks. DRM telah terbukti efektif dalam mengintegrasikan riset akademis dengan pengembangan praktis, sehingga cocok untuk penelitian yang mengkombinasikan analisis keamanan siber dengan pengembangan prototipe malware untuk tujuan defensif.

Kerangka DRM terdiri atas empat fase utama yang saling terkait dan berulang.

1. Research Clarification (RC)

Fase pertama adalah Research Clarification (RC), yang mengidentifikasi kesenjangan antara evolusi teknik *dropper* modern dan keterbatasan sistem deteksi yang ada saat ini. Pada tahap ini, dilakukan studi literatur mendalam terhadap laporan industri keamanan siber terkini untuk memahami tren ancaman terbaru, analisis publikasi akademis mengenai teknik evasi malware termasuk



Gambar I.1 Kerangka kerja DRM

fileless execution dan *anti-analysis mechanisms*, studi kasus analisis terhadap serangan *dropper* nyata yang telah didokumentasikan, serta wawancara dengan praktisi keamanan siber untuk mengkonfirmasi relevansi masalah. Hasil dari RC adalah rumusan masalah yang terdefinisi jelas, urgensi penelitian yang berdasar pada bukti mutakhir, dan identifikasi parameter kritis yang perlu dievaluasi.

2. Descriptive Study I (DS-I)

Fase kedua adalah Descriptive Study I (DS-I), yang menelaah kondisi eksisting melalui analisis karakteristik *dropper* modern dalam *cyber kill chain* yang komprehensif. Fokus DS-I ada pada identifikasi mekanisme *fileless payload delivery* dan bagaimana *dropper* memanfaatkan memori sistem untuk eksekusi, analisis teknik *anti-analysis* seperti deteksi VM, deteksi *sandbox*, dan *anti-debugging* untuk memahami bagaimana *dropper* menghindari analisis otomatis, studi terhadap *obfuscation string* dan komunikasi C2 terenkripsi untuk memahami bagaimana *dropper* menyembunyikan identitasnya, pemetaan metode distribusi *dropper* seperti *phishing*, *drive-by download*, dan dokumen berbahaya, serta rekonstruksi rantai serangan *dropper* dari *initial access* hingga *command-and-control*. Hasil DS-I berupa pernyataan persyaratan fungsional dan non-fungsional yang detail, serta panduan untuk fase desain berikutnya.

3. Prescriptive Study (PS)

Fase ketiga adalah Prescriptive Study (PS), yang merupakan tahap inti di mana solusi dirancang dan dikembangkan berdasarkan temuan DS-I. Pada tahap ini dilakukan perancangan arsitektur *dropper spyware mode stealth* yang mengintegrasikan *multiple evasion techniques* secara kohesif, implementasi

prototipe menggunakan bahasa Rust yang menyediakan kontrol *low-level* untuk operasi *fileless* sambil mempertahankan *safety features*, pengembangan modul-modul utama termasuk *payload builder*, manajemen *in-memory execution*, pemeriksaan *anti-VM/anti-debug*, kanal komunikasi terenkripsi, dan modul *spyware*, serta melakukan pengujian awal secara iteratif untuk memastikan setiap teknik evasi bekerja sesuai spesifikasi. Selama PS, setiap komponen diuji secara individual dan kemudian diintegrasikan untuk pengujian sistem secara menyeluruh.

4. Descriptive Study II (DS-II)

Fase keempat dan terakhir adalah Descriptive Study II (DS-II), yang mengevaluasi prototipe yang telah dikembangkan melalui eksperimen yang komprehensif pada beberapa lingkungan uji dan produk *anti-malware/EDR* komersial. Parameter evaluasi pada DS-II mencakup analisis tahap deteksi atau kelolosan (*evasion*) aktivitas *dropper* oleh berbagai *anti-malware*, verifikasi keberhasilan *payload delivery* di memori tanpa meninggalkan artefak disk, pengukuran efektivitas masing-masing teknik evasi dalam menghindari deteksi, analisis performa dan latensi eksekusi, serta identifikasi pola perilaku *dropper* yang terdeteksi versus yang terlewat. Data kuantitatif berupa *detection rate* dan *evasion rate* dibandingkan antar produk *anti-malware* yang diuji. Data kualitatif seperti pola perilaku *dropper* dan jejak forensik dianalisis untuk memahami penyebab lolosnya deteksi. Temuan DS-II menjadi dasar rekomendasi peningkatan mekanisme deteksi dan arah penelitian lanjutan untuk memperkuat pertahanan terhadap *initial access* berbasis *dropper*.

BAB II

TINJAUAN PUSTAKA

II.1 Malware

Malware, atau *malicious software*, merupakan perangkat lunak yang dirancang secara sengaja untuk melakukan aktivitas merusak, mengganggu, atau mengakses sistem tanpa izin pengguna. Istilah ini mencakup berbagai jenis ancaman siber seperti *virus*, *worm*, *trojan horse*, *ransomware*, dan *spyware* yang masing-masing memiliki mekanisme infeksi dan tujuan spesifik. *Malware* modern tidak lagi hanya bertujuan untuk merusak data atau sistem, tetapi semakin berorientasi pada pencurian informasi sensitif, penciptaan *botnet* untuk serangan DDoS, atau bahkan sebagai vektor untuk serangan *ransomware* yang menuntut pembayaran tebusan. Evolusi *malware* ini menunjukkan pergeseran paradigma dari ancaman yang mudah dideteksi melalui tanda tangan digital (*signature-based*) menuju varian yang menggunakan teknik *obfuscation* dan *polymorphism* untuk menghindari deteksi sistem keamanan konvensional (Sudhakar dan Kumar 2020).

Dalam konteks keamanan siber saat ini, *malware* telah menjadi alat utama dalam *cyber kill chain* yang sistematis, dimulai dari *initial access* hingga *command and control*. Kompleksitas *malware* meningkat seiring dengan adopsi teknik *fileless execution* dan *living off the land binaries* (LOLBins), di mana *malware* memanfaatkan komponen sistem operasi yang sah seperti *PowerShell* atau *WMI* untuk eksekusi tanpa meninggalkan jejak file di disk. Hal ini menciptakan tantangan fundamental bagi sistem deteksi tradisional yang bergantung pada analisis *file-based*, karena *malware* kini beroperasi sepenuhnya di memori atau melalui proses yang tampak *legitimate*. Penelitian menunjukkan bahwa serangan *malware* global mencapai 5,5 miliar insiden pada 2022, dengan peningkatan 2% dari tahun sebelumnya, menandakan eskalasi ancaman yang berkelanjutan (Chatzoglou dkk. 2023).

Relevansi *malware* dengan penelitian ini terletak pada peran sentralnya sebagai fon-

dasi bagi pengembangan *dropper spyware* mode *stealth*. *Dropper*, sebagai salah satu varian *malware*, berfungsi sebagai *delivery mechanism* yang mengantarkan *payload spyware* ke sistem target sambil menghindari deteksi awal. Kelemahan sistem *anti-malware* konvensional dalam mendeteksi *malware evasif* menjadi dasar utama penelitian ini, yang bertujuan menguji kapabilitas *anti-spyware* terhadap *dropper* yang mengintegrasikan teknik evasi modern. Tanpa pemahaman mendalam tentang evolusi *malware* dari ancaman tradisional ke varian *stealth* seperti *fileless* dan *dropper-based*, pengembangan solusi pertahanan yang efektif akan terus tertinggal dari inovasi penyerang. Oleh karena itu, analisis *malware* tidak hanya memberikan konteks teoritis, tetapi juga landasan empiris untuk merancang prototipe *dropper* yang realistik dalam lingkungan pengujian terkontrol (Koutsokostas dan Patsakis 2021).

Dalam kerangka MITRE ATT&CK, *malware* mencakup berbagai taktik seperti *Execution*, *Persistence*, *Privilege Escalation*, dan *Defense Evasion* yang saling terkait membentuk rantai serangan yang kohesif. Pemahaman ini krusial untuk mengidentifikasi tahap mana yang paling rentan terhadap deteksi, khususnya pada fase *initial access* yang menjadi fokus utama *dropper spyware*. Studi empiris menunjukkan bahwa 95% CEO menganggap keamanan siber sebagai ancaman utama pertumbuhan bisnis pada 2021, naik dari 61% tahun sebelumnya, yang menegaskan urgensi penelitian terhadap kemampuan deteksi *malware* modern (Ainslie dkk. 2023). Dengan demikian, tinjauan *malware* ini menjadi titik awal untuk memahami mengapa evaluasi *anti-spyware* terhadap *dropper stealth* menjadi imperatif dalam lanskap ancaman siber kontemporer.

II.2 Spyware

Spyware merupakan jenis *malware* yang secara spesifik dirancang untuk memantau, mengumpulkan, dan mengirimkan data sensitif dari sistem target tanpa sepenuhnya atau persetujuan pengguna. Berbeda dengan *ransomware* yang fokus pada enkripsi data untuk pemerasan atau *trojan* yang bertujuan akses *backdoor*, *spyware* beroperasi secara diam-diam dengan tujuan pencurian informasi seperti kredensial *login*, riwayat aktivitas, lokasi geografis, hingga percakapan pribadi melalui mikrofon dan kamera. Karakteristik utama *spyware* adalah kemampuan *stealth* dan *persistensi*, di mana ia mampu bertahan di sistem selama berbulan-bulan bahkan bertahun-tahun tanpa terdeteksi oleh pengguna atau sistem keamanan standar (Reddyvari dkk. 2024).

Mekanisme infeksi *spyware* modern semakin canggih, memanfaatkan *zero-click exploit*

its yang tidak memerlukan interaksi pengguna, seperti kerentanan dalam aplikasi pesan instan atau peramban. Studi kasus *Pegasus* dari NSO Group menunjukkan bagaimana *spyware* tingkat negara dapat menginfeksi *iPhone* dan *Android* hanya melalui panggilan *WhatsApp* yang dibatalkan, memungkinkan akses penuh ke data perangkat tanpa meninggalkan jejak signifikan. *Spyware* ini mampu mengekstrak pesan terenkripsi, merekam panggilan, dan melacak lokasi *real-time*, menjadikannya alat pengawasan yang sangat efektif namun kontroversial secara etis dan hukum (Kareem 2024). Dalam konteks *cyber kill chain*, *spyware* biasanya berada pada tahap *Collection* dan *Exfiltration*, tetapi ketergantungannya pada *dropper* sebagai vektor *initial access* menjadikan rantai infeksi ini rentan pada tahap awal pengiriman *payload*.

Ancaman *spyware* tidak hanya terbatas pada individu, tetapi juga mencakup infrastruktur kritis dan organisasi pemerintah. Laporan menunjukkan bahwa *spyware* komersial seperti *Pegasus* telah digunakan terhadap jurnalis, aktivis HAM, dan pejabat tinggi di 45 negara, menimbulkan implikasi serius terhadap privasi digital dan keamanan nasional. Yang lebih mengkhawatirkan, *spyware* modern mengintegrasikan teknik evasi lanjutan seperti *fileless execution* dan komunikasi *C2* terenkripsi, membuatnya sulit dideteksi oleh solusi *anti-malware* konvensional yang masih mengandalkan *signature matching* (Kareem 2024; Reddyvari dkk. 2024). Keterbatasan ini menjadi dasar krusial bagi penelitian ini, yang secara spesifik menguji kapabilitas *anti-spyware* terhadap *dropper spyware* mode *stealth*, komponen pengantar yang menentukan keberhasilan infeksi *spyware* secara keseluruhan.

Relevansi *spyware* dengan penelitian ini terletak pada posisinya sebagai *payload* utama yang akan diuji melalui prototipe *dropper*. Tanpa *dropper* yang efektif dalam mengantarkan dan mengaktifkan *spyware* tanpa deteksi, seluruh rantai serangan menjadi tidak efektif. Oleh karena itu, evaluasi terhadap kemampuan *anti-spyware* dalam mendeteksi tahap *delivery mechanism dropper* menjadi sangat kritis, terutama mengingat studi menunjukkan bahwa deteksi *spyware* masih bergantung pada analisis perilaku pasca-infeksi, bukan pencegahan pada tahap awal (Reddyvari dkk. 2024). Penelitian ini mengisi celah tersebut dengan mengembangkan dan menguji *dropper* yang mensimulasikan serangan *spyware* realistik, memberikan wawasan empiris tentang kelemahan sistem pertahanan saat ini terhadap ancaman yang semakin *stealth* dan *targeted*.

II.3 Dropper

Dropper merupakan jenis *malware* spesialis yang berfungsi sebagai *delivery mechanism* atau pengantar untuk *malware* utama, khususnya *spyware*, dengan tugas utama mendistribusikan, membuka kemasan (*unpack*), dan mengeksekusi *payload* berbahaya di sistem target tanpa terdeteksi. Berbeda dengan *malware* lain yang langsung menjalankan fungsi destruktif, *dropper* dirancang untuk beroperasi secara *stealth* pada tahap awal *cyber kill chain*, yaitu *initial access* dan *execution*, memastikan *payload spyware* dapat diaktifkan dengan sukses sebelum sistem keamanan bereaksi. *Dropper* sering kali berupa *executable* kecil yang tampak *benign*, yang kemudian mengekstrak dan menjalankan *malware* utama dari memori atau *stream* terenkripsi, menjadikannya komponen kritis yang menentukan efektivitas seluruh rantai serangan (Chatzoglou dkk. 2023; Elghaly 2024).

Arsitektur *dropper* modern mencakup beberapa modul inti: *payload container* yang menyimpan *spyware* terenkripsi, *unpacker/decryptor* untuk ekstraksi *payload*, *environment checker* untuk mendeteksi analisis (*anti-VM*, *anti-sandbox*), dan *loader* untuk eksekusi *fileless* melalui injeksi proses atau *reflective DLL loading*. Alur eksekusinya biasanya dimulai dengan validasi lingkungan target, diikuti dekripsi *payload*, pengecekan integritas, dan aktivasi *spyware* melalui teknik seperti *process hollowing* atau *APC injection* yang memanfaatkan proses sistem sah. Dalam kerangka MITRE ATT&CK, *dropper* mendominasi taktik T1105 (*Ingress Tool Transfer*), T1027 (*Obfuscated Files or Information*), dan T1055 (*Process Injection*), menjadikannya titik lemah potensial dalam rantai serangan jika sistem deteksi mampu mengidentifikasi perlakunya pada tahap awal (Chatzoglou dkk. 2023).

Peran strategis *dropper* dalam infeksi *spyware* tidak dapat diremehkan, karena kegagalannya berarti seluruh operasi pengintaian gagal sebelum dimulai. Penelitian empiris menunjukkan bahwa *dropper* dengan teknik evasi sederhana seperti enkripsi XOR dan *junk data insertion* mampu melewati 50% produk *antivirus* komersial, sementara integrasi *anti-analysis mechanisms* meningkatkan tingkat keberhasilan hingga 80% terhadap *scanner multi-engine* seperti *VirusTotal*. *Dropper* juga berevolusi menjadi varian *non-persistent* yang menghilang setelah *payload* aktif, meninggalkan jejak minimal untuk analisis forensik (Koutsokostas dan Patsakis 2021). Konteks ini sangat relevan dengan penelitian ini, yang mengembangkan prototipe *dropper spyware* mode *stealth* menggunakan Rust untuk mensimulasikan serangan realistik dan mengukur kapabilitas deteksi *anti-spyware* pada tahap *delivery*, fase yang paling kritis namun jarang dievaluasi secara komprehensif.

Kelemahan utama dalam pemahaman *dropper* saat ini adalah kurangnya evaluasi terhadap integrasi *multiple evasion techniques* dalam satu artefak, di mana penelitian terpisah hanya menguji *packing*, *anti-VM*, atau *fileless* secara individual. Penelitian ini mengatasi *gap* tersebut dengan prototipe holistik yang menggabungkan teknik-teknik tersebut, memberikan bukti empiris tentang sejauh mana produk *anti-spyware* mampu mendeteksi dan menangkal *dropper* sebagai vektor infeksi *spyware* modern. Dengan demikian, analisis *dropper* tidak hanya memberikan landasan teoritis, tetapi juga metodologi pengujian yang dapat direplikasi untuk meningkatkan maturitas sistem pertahanan siber (Elghaly 2024).

II.4 Fileless Malware

Fileless malware merupakan evolusi canggih dari ancaman tradisional yang sepenuhnya menghindari penggunaan file eksekusi di disk, beroperasi langsung melalui memori sistem atau memanfaatkan *living off the land binaries* (LOLBins) seperti *PowerShell*, *WMI*, atau *registry* untuk eksekusi kode berbahaya. Berbeda dengan *malware* konvensional yang meninggalkan artefak file yang dapat dipindai oleh *antivirus*, *fileless malware* menyamarkan aktivitasnya sebagai proses sistem sah, sehingga lolos dari deteksi *signature-based* dan bahkan sebagian besar *heuristic analysis*. Penelitian menunjukkan bahwa serangan *fileless* meningkat secara eksponensial sejak 2017, dengan kasus seperti *Poweliks* dan *Kovter* yang menggunakan *WMI* untuk *persistensi* tanpa jejak disk, menjadikannya ancaman yang sangat sulit dilacak secara forensik (Sudhakar dan Kumar 2020).

Mekanisme kerja *fileless malware* biasanya melibatkan *script-based execution* melalui *interpreter* yang sudah ada di sistem target, seperti *PowerShell* untuk *reflective loading DLL* atau *WMI event subscription* untuk *persistensi*. Teknik ini memanfaatkan API Windows yang sah untuk injeksi kode ke proses seperti *explorer.exe* atau *svchost.exe*, menciptakan ilusi aktivitas normal sambil menjalankan *payload spyware*. Studi kasus *PowerShell fileless malware* menunjukkan tingkat *evasion rate* hingga 94% terhadap EDR modern, karena kemampuannya menyembunyikan *payload* dalam memori dan mengubah *behavioral signature* secara dinamis melalui *obfuscation* (Elghaly 2024). Dalam konteks *dropper*, *fileless execution* menjadi metode *delivery* utama karena memungkinkan *payload spyware* diaktifkan tanpa menulis file ke disk, yang secara langsung relevan dengan prototipe *stealth* yang dikembangkan dalam penelitian ini.

Tantangan utama *fileless malware* terletak pada keterbatasan sistem deteksi yang

masih bergantung pada *file artifacts*, di mana *memory forensics* dan *behavioral analysis* menjadi satu-satunya pertahanan efektif namun *resource-intensive*. Laporan industri mencatat bahwa 77% organisasi mengalami serangan *fileless* pada 2019, dengan kerugian rata-rata mencapai jutaan dolar per insiden karena sulitnya *attribution* dan *remediation*. Penelitian *Sudhakar dan Kumar* (Sudhakar dan Kumar 2020) secara kritis menyoroti bahwa dari 20 metode deteksi *fileless* yang dianalisis, hanya 30% efektif terhadap varian terbaru yang menggabungkan *process injection* dengan *encrypted C2 communication*. *Gap* ini menjadi dasar metodologi penelitian ini, yang mengintegrasikan *fileless techniques* dalam *dropper* prototipe untuk menguji apakah *anti-spyware* mampu mendeteksi eksekusi *in-memory payload delivery* sebelum *spyware* aktif sepenuhnya.

Relevansi *fileless malware* dengan penelitian ini sangat strategis karena *dropper spyware* mode *stealth* yang dikembangkan mengadopsi prinsip yang sama: operasi tanpa *disk footprint* menggunakan Rust untuk *memory management* tingkat rendah. Dengan mengukur *detection rate* pada tahap *payload activation* melalui *fileless execution*, penelitian ini memberikan bukti empiris tentang efektivitas EDR dan *anti-spyware* terhadap ancaman yang mendominasi 40% serangan *enterprise* pada 2024. Tanpa pemahaman mendalam tentang *fileless malware* sebagai fondasi *dropper* modern, evaluasi keamanan akan gagal mengidentifikasi celah kritis pada tahap eksekusi yang paling rentan terhadap *evasion* (Elghaly 2024; Sudhakar dan Kumar 2020).

II.5 Teknik Evasi Malware

Teknik evasi *malware* berkembang pesat sebagai respons terhadap kemajuan sistem deteksi keamanan. *Malware*, khususnya *dropper spyware* mode *stealth*, menggunakan berbagai teknik untuk menyembunyikan keberadaannya dan meningkatkan peluang lolos dari deteksi *anti-malware* dan *Endpoint Detection and Response* (EDR). Salah satu teknik utama adalah *packing* dan *encryption*, yang mengubah *signature* file sehingga tidak cocok dengan basis data tanda tangan *malware* konvensional. Selain itu, *obfuscation* kode dan data digunakan untuk mengacak struktur internal *malware*, menyulitkan analisis statis oleh *antivirus* (Chatzoglou dkk. 2023).

Lebih lanjut, mekanisme *fileless execution* memungkinkan *malware* beroperasi sepenuhnya di memori, tanpa menulis file fisik ke disk sehingga sulit dideteksi oleh pemindai file tradisional. *Malware* juga mengimplementasikan *anti-analysis mechanisms* seperti deteksi *virtual machine* (VM), *sandbox*, dan *debugger*, di mana

malware memeriksa lingkungan eksekusi untuk menentukan apakah sedang dianalisis, dan mengubah perilaku atau menunda eksekusi agar terhindar dari analisis dinamis. Teknik ini termasuk *environment checking*, *sleeping*, dan *API hooking* untuk menghindari pemantauan (Elghaly 2024; Chatzoglou dkk. 2023).

Selain itu, *malware* modern menggunakan komunikasi *Command and Control* (C2) yang terenkripsi dan tersembunyi untuk menghindari inspeksi lalu lintas jaringan. Teknik *steganografi* dan *polymorphism* juga diterapkan untuk menyamaraskan komunikasi dan *payload* guna mencegah deteksi berbasis pola trafik jaringan. Studi terbaru menunjukkan bahwa perpaduan beberapa teknik evasi secara simultan meningkatkan tingkat keberhasilan serangan sampai 80%-90% dalam melewati deteksi produk keamanan komersial (Koutsokostas dan Patsakis 2021; Elghaly 2024).

Dalam konteks penelitian ini, teknik evasi tersebut menjadi fokus utama karena *dropper spyware* mode *stealth* yang dikembangkan menggabungkan banyak teknik evasi secara integratif. Evaluasi kapabilitas *anti-spyware* dilakukan dengan menguji keberhasilan deteksi terhadap *dropper* yang menggunakan *packing*, *fileless payload delivery*, *anti-VM*, *anti-debug*, serta komunikasi C2 terenkripsi. Studi ini mengisi celah pada evaluasi sistem keamanan yang selama ini hanya menilai teknik evasi secara parsial, dengan pendekatan holistik yang merefleksikan realita ancaman saat ini (Chatzoglou dkk. 2023; Elghaly 2024).

II.6 Deteksi Malware dan Teknologi Anti-Malware

Deteksi *malware* mengalami evolusi dari pendekatan *signature-based* yang mengandalkan pencocokan *hash* dan pola kode tetap, menuju analisis perilaku (*behavioral analysis*) dan *machine learning* untuk mengenali ancaman *zero-day*. Sistem *anti-malware* konvensional efektif terhadap *malware* statis, namun gagal terhadap varian polimorfik dan *fileless* yang mengubah *signature* secara dinamis atau tidak meninggalkan artefak disk. *Dynamic analysis* melalui *sandbox* mencoba mengeksplorasi *malware* dalam lingkungan terkontrol, tetapi rentan terhadap *sandbox evasion* seperti *time-based sleeping* dan *VM artifact detection* yang membuat *malware* mengubah perilaku saat dianalisis (Sudhakar dan Kumar 2020; Chatzoglou dkk. 2023).

Endpoint Detection and Response (EDR) muncul sebagai solusi generasi berikutnya yang mengintegrasikan *monitoring real-time*, *threat hunting*, dan *automated response*. Berbeda dengan *antivirus* tradisional, EDR fokus pada *behavioral indicators of compromise* (IoC) seperti *unusual process spawning*, *memory injection*,

dan *network beaconing* yang menjadi ciri *dropper spyware*. Namun, studi empiris mengungkap keterbatasan signifikan: EDR modern masih menghasilkan *false positive* tinggi (hingga 30%) dan gagal mendeteksi 50% *fileless malware* yang menggunakan LOLBins sah seperti *PowerShell* untuk *C2 communication* (Elghaly 2024; Ainslie dkk. 2023).

Machine learning meningkatkan akurasi deteksi melalui analisis fitur seperti urutan *API call*, entropi *payload*, dan pola aliran jaringan, namun rentan terhadap *adversarial attacks* di mana *malware* mengoptimalkan *input* untuk mengecoh model ML. Penelitian menunjukkan bahwa model ML berbasis *deep learning* hanya mencapai 85% *accuracy* terhadap *dropper* dengan *multi-evasion techniques*, sementara *signatureless detection* masih kalah efektif terhadap *obfuscated payloads* (Reddyvari dkk. 2024; Koutsokostas dan Patsakis 2021). *Gap* kritis ini terletak pada kurangnya evaluasi komprehensif terhadap *dropper* sebagai *initial access vector*, di mana sebagian besar studi fokus pada *malware* pasca-infeksi daripada pencegahan pada tahap *delivery*.

Dalam konteks penelitian ini, evaluasi terhadap produk *anti-spyware* dan EDR dilakukan dengan prototipe *dropper* yang mensimulasikan serangan realistik menggunakan Rust, mengukur *detection rate* pada setiap tahap: *unpacking*, *environment checking*, *fileless execution*, dan *payload activation*. Temuan dari pengujian ini akan mengungkap sejauh mana teknologi saat ini mampu menangkal *dropper spyware* mode *stealth*, mengidentifikasi *false negative patterns*, dan memberikan rekomendasi untuk pengembangan *behavioral signatures* yang lebih adaptif terhadap ancaman evolusioner (Chatzoglou dkk. 2023; Elghaly 2024). Analisis ini krusial karena keberhasilan *dropper* menentukan efektivitas keseluruhan *spyware*, menjadikan tahap *initial access* sebagai titik lemah paling strategis dalam rantai pertahanan siber.

II.7 Kasus Spyware Canggih dan Cyber Threat Intelligence (CTI)

Pegasus spyware dari NSO Group mewakili ancaman *spyware* paling canggih saat ini, mampu menginfeksi *smartphone* tanpa interaksi pengguna melalui pesan WhatsApp atau iMessage. Kasus Ahmed Mansoor (aktivis HAM UAE) menunjukkan bagaimana *Pegasus* digunakan untuk memata-matai jurnalis dan aktivis, dengan tingkat penghindaran deteksi 95% terhadap *antivirus* konvensional. Kareem (Kareem 2024) mencatat penggunaan *Pegasus* oleh negara-negara seperti Saudi Arabia dan Meksiko menciptakan ancaman serius terhadap privasi digital.

Cyber Threat Intelligence (CTI) mengubah data mentah menjadi informasi *actionable*

nable melalui proses *Intelligence Cycle* untuk mendukung keputusan keamanan organisasi. *Ainslie et al.* (Ainslie dkk. 2023) menunjukkan CTI mengurangi *false positives* hingga 50% dengan fokus pada pola perilaku ancaman (TTPs) daripada *signature matching* semata, meskipun tantangan berbagi informasi antar-organisasi tetap signifikan.

Reddyvari et al. (Reddyvari dkk. 2024) menyoroti efektivitas *Dark Web Monitoring* untuk mendeteksi kebocoran data, sementara *Noor et al.* (Noor dkk. 2020) mengembangkan *ranking framework* untuk 31 penyedia CTI berdasarkan kebutuhan pelanggan. Penelitian ini mengintegrasikan temuan CTI dengan pengujian *dropper* untuk mengidentifikasi celah deteksi pada tahap awal serangan.

II.8 Rust dalam Malware Development dan Fileless Execution

Rust programming language semakin populer dalam pengembangan *malware* karena menawarkan keamanan memori yang lebih baik dibandingkan C/C++, sehingga *malware* lebih stabil dan sulit dideteksi. *Kerkour* (Kerkour 2021) menunjukkan bagaimana Rust digunakan untuk menciptakan *malware* yang beroperasi sepenuhnya di memori tanpa meninggalkan jejak di disk, dengan tingkat deteksi 30% lebih rendah terhadap analisis perilaku.

Sudhakar dan Kumar (Sudhakar dan Kumar 2020) melaporkan peningkatan 77% *fileless malware* sejak 2019, yang memanfaatkan program sistem Windows sah seperti PowerShell untuk eksekusi tanpa file di disk. Teknik ini mencapai tingkat penghindaran deteksi 94% terhadap sistem keamanan modern karena tidak meninggalkan artefak forensik.

Penelitian ini mengembangkan prototipe *dropper* berbasis Rust yang mengintegrasikan teknik *fileless execution* dengan pemeriksaan lingkungan (*anti-VM*), mengisi kesenjangan evaluasi terhadap kemampuan EDR komersial dalam mendeteksi *malware* generasi baru pada tahap *initial access*.

BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi dan Kesenjangan (Current State and Gap Analysis)

Kondisi keamanan siber saat ini dicirikan oleh evolusi ancaman yang signifikan, bergerak dari *malware* tradisional berbasis berkas menuju serangan yang lebih canggih dan tersembunyi seperti *fileless malware* dan *spyware mode stealth*. Evolusi ini menciptakan celah kritis dalam kemampuan deteksi sistem *anti-malware* dan *Endpoint Detection and Response* (EDR) yang tersedia di pasar. Pemahaman mendalam tentang kesenjangan antara kapabilitas ancaman terkini dan sistem pertahanan yang ada menjadi fondasi penting untuk merancang evaluasi penelitian yang komprehensif dan relevan secara praktis.

III.1.1 Keterbatasan Deteksi Konvensional

Sistem pertahanan keamanan siber menghadapi beberapa masalah kritis yang membuat sistem rentan terhadap *dropper spyware mode stealth*:

a) **Keterbatasan Deteksi Berbasis Tanda Tangan (Signature-Based Detection)**

Anti-malware tradisional masih mengandalkan pencocokan *signature* untuk mengidentifikasi *malware* yang diketahui. Namun, *spyware mode stealth* menggunakan teknik *packing*, enkripsi, dan *obfuscation* untuk mengubah *signature digital payload* sehingga efektif lolos dari deteksi berbasis *signature*. Studi empiris menunjukkan bahwa dari 12 produk *antivirus* yang diuji, hampir separuh hanya mampu mendeteksi kurang dari 50% varian *malware* yang disamarkan dengan teknik *evasion* sederhana. Keterbatasan ini disebabkan oleh fakta bahwa setiap perubahan minor pada *payload*, bahkan hanya penambahan *junk data* atau modifikasi *packing* akan menghasilkan *hash* yang berbeda, membuat *signature* lama menjadi tidak berlaku.

b) **Kegagalan Deteksi *Fileless Execution* dan Analisis Kode**

Fileless malware memanfaatkan komponen sah sistem operasi seperti *Power-*

Shell atau WMI untuk menjalankan kode berbahaya langsung di memori tanpa menulis berkas ke media penyimpanan, sehingga sulit dideteksi oleh *antimalware* konvensional. Kegagalan alat keamanan dalam menganalisis kode yang dikemas menggunakan alat populer seperti *PyInstaller* terjadi karena *antivirus* tidak dapat memahami konten *bytecode* yang disamarkan. Penelitian menunjukkan bahwa EDR modern masih menghasilkan *false negative rate* hingga 50% terhadap *fileless malware*, karena fokus *monitoring* masih pada *disk artifacts* dan *registry persistence entries*, bukan aktivitas *in-memory* yang sesungguhnya.

c) **Efektivitas Teknik *Evasion* Sederhana**

Penelitian menunjukkan bahwa metode *evasion* yang relatif sederhana, seperti enkripsi, *process injection*, dan penambahan *junk data* ke berkas eksekusi, terbukti sangat efektif dalam menghindari deteksi. Studi empiris menunjukkan bahwa perpaduan tiga teknik *evasion* dasar saja sudah mampu meningkatkan *evasion rate* hingga 80% terhadap produk *antivirus* komersial. Hal ini mengindikasikan bahwa sistem deteksi masih mengandalkan pendekatan terpisah, mempertimbangkan setiap teknik *evasion* secara terpisah, daripada analisis holistik terhadap kombinasi *multiple evasion techniques* dalam satu artefak *malware*.

d) **Keterbatasan *Behavioral Analysis* dan *Heuristics***

Meskipun *behavioral analysis* dan *heuristics* telah dikembangkan untuk mengatasi keterbatasan *signature-based detection*, sistem ini masih rentan terhadap *false positive* dan *false negative* yang signifikan. *Anti-VM detection*, *anti-debugging*, dan *sandbox evasion* memungkinkan *dropper* untuk menyamarkan perilaku mencurigakan atau mengubah eksekusi saat dideteksi adanya analisis otomatis. Penelitian terbaru menemukan bahwa *dropper* dengan *anti-analysis mechanisms* terintegrasi mampu melewati 94% *sandbox* publik dan 80% EDR *enterprise-grade* dalam pengujian awal.

III.1.2 Analisis Kesenjangan Desain *Dropper* (Gap Analysis)

Berdasarkan keterbatasan deteksi yang telah diidentifikasi, analisis kesenjangan berikut menyoroti bahwa artefak penelitian yang ada belum secara memadai mencakup *dropper* yang mengintegrasikan teknik-teknik *evasive* modern dan tidak konvensional secara simultan. Tabel III.1 merangkum hubungan antara celah deteksi saat ini dan arah solusi yang diusulkan dalam penelitian ini.

Tabel III.1 Ringkasan kesenjangan desain *dropper* dan arah solusi

Kesenjangan (Gap)	Kondisi Saat Ini	Celah Deteksi	Arah Solusi Penelitian Ini
Bahasa pemrograman	Penelitian terbatas pada C/C++ atau <i>Python/PowerShell</i> yang <i>signature</i> -nya sudah familiar bagi mesin deteksi	<i>Signature resistance</i> yang rendah, mudah diidentifikasi oleh <i>static analysis</i>	Menggunakan Rust untuk <i>dropper</i> utama; biner Rust memiliki resistensi inheren terhadap <i>reverse engineering</i> dan melewati <i>signature</i> yang kurang <i>tuned</i>
Operasi <i>in-memory</i> dan non- <i>persistence</i>	Deteksi EDR seiring berfokus pada artefak disk serta <i>persistence</i> seperti <i>registry</i> atau <i>start-up</i> entry	Fokus deteksi pada <i>disk artifacts</i> membuat <i>fileless malware</i> lolos; <i>non-persistent dropper</i> tidak meninggalkan jejak <i>persistence</i>	Menerapkan eksekusi <i>fileless</i> penuh <i>in-memory payload delivery</i> , menghilangkan artefak disk dan melakukan <i>self-terminate</i> untuk meminimalkan <i>forensic footprint</i>
Anti-analisis terintegrasi	<i>Sandbox</i> publik kerap gagal mendeteksi <i>malware</i> yang menunda eksekusi atau memeriksa artefak sistem	<i>Anti-VM, anti-debug, environment checking</i> belum dievaluasi secara terintegrasi dalam satu <i>dropper</i>	Mengintegrasikan <i>anti-VM</i> (pemeriksaan <i>driver</i> atau <i>registry</i>), <i>anti-debugging</i> (pemeriksaan <i>PEB flag</i>), dan <i>sandbox evasion</i>
Integrasi <i>multiple evasion techniques</i>	Penelitian sebelumnya meng-evaluasi teknik <i>evasion</i> secara individual atau pasangan dua	Tidak ada evaluasi holistik terhadap <i>dropper</i> dengan 5+ teknik <i>evasion</i> terintegrasi	Mengembangkan <i>dropper</i> dengan minimal 5 teknik <i>evasion</i> terintegrasi: enkripsi, <i>packing</i> , <i>anti-VM</i> , <i>anti-debug</i> , <i>fileless execution</i>

bersambung

Kesenjangan (Gap)	Kondisi Saat Ini	Celah Deteksi	Arah Solusi Penelitian Ini
Evaluasi komparatif sistematis	Evaluasi <i>anti-malware/EDR</i> belum spesifik terhadap <i>dropper</i> sebagai <i>initial access vector</i>	Fokus evaluasi pada <i>malware</i> pasca-infeksi, bukan pada fase <i>critical delivery</i>	Melakukan pengujian komparatif terhadap 6+ produk <i>anti-spyware/EDR</i> untuk mengidentifikasi perbedaan <i>detection rate</i> per tahap eksekusi <i>dropper</i>

Kesenjangan-kesenjangan yang telah diidentifikasi menghasilkan beberapa implikasi kritis bagi keamanan siber:

- **Fokus deteksi yang parsial:** sistem *anti-malware* saat ini umumnya dioptimalkan untuk mendeteksi salah satu atau dua teknik *evasion*, namun tidak robust terhadap kombinasi *multiple techniques* yang terintegrasi. Penelitian ini mengisi *gap* tersebut dengan mengembangkan *dropper* yang merepresentasikan ancaman realistik di lapangan.
- **Fase *delivery* yang diabaikan:** mayoritas penelitian fokus pada *malware* pasca-infeksi (*collection, exfiltration*) tetapi mengabaikan fase kritis *delivery*. *Dropper* sebagai *initial access vector* menjadi sasaran evaluasi yang kurang layak, padahal keberhasilan fase ini menentukan viabilitas seluruh serangan.
- **Validitas pengujian yang tertanya:** pengujian *anti-malware* menggunakan sampel *malware* yang *trivial* atau tidak realistik dapat memberikan hasil yang tidak akurat. Prototipe *dropper* berbasis Rust dengan *integrated evasion techniques* akan memberikan validitas pengujian yang lebih tinggi.

III.2 Persyaratan Fungsional dan Non-Fungsional

Persyaratan fungsional dan non-fungsional diturunkan dari analisis kesenjangan yang telah dilakukan pada Bagian III dan berfungsi sebagai kriteria desain sekaligus evaluasi untuk memastikan prototipe *dropper* memenuhi standar yang telah ditetapkan. Persyaratan-persyaratan ini mencerminkan kebutuhan teknis untuk menghadapi ancaman *dropper spyware stealth* modern, sekaligus memastikan bahwa evaluasi yang dilakukan terhadap sistem *anti-malware* dan EDR menggunakan *baseline* yang realistik dan representatif.

Tabel III.2 Persyaratan fungsional (Functional Requirements)

ID	Persyaratan Fungsional	Keterkaitan Deskripsi CTQ
F1	Eksekusi <i>payload</i> <i>in-memory (fileless)</i>	CTQ-03 Dropper harus memuat dan mengeksekusi <i>payload</i> berbahaya langsung di memori tanpa menulis berkas ke media penyimpanan, memastikan tidak ada <i>disk artifacts</i> yang dapat dipindai
F2	<i>Self-removal</i> dan <i>non-persistence</i>	CTQ-01, CTQ-03 Setelah mengeksekusi <i>payload</i> , <i>dropper</i> harus <i>self-terminate</i> dan tidak meninggalkan entri <i>persistence</i> seperti <i>registry keys</i> atau <i>startup folder</i> , meminimalkan <i>forensic footprint</i>
F3	Enkripsi dan dekripsi <i>payload</i>	CTQ-01, CTQ-02 <i>Dropper</i> membawa <i>payload</i> dalam bentuk terenkripsi di dalam biner utama dan mendekripsinya saat <i>runtime</i> , mencegah <i>reverse engineering</i> dan deteksi <i>signature</i> berbasis <i>payload</i>
F4	Pemeriksaan <i>VM/sandbox</i>	anti- CTQ-03 <i>Dropper</i> mampu mendeteksi lingkungan <i>virtual machine</i> atau <i>sandbox</i> sebelum mengeksekusi <i>payload</i> melalui pemeriksaan <i>driver hypervisor</i> , <i>registry artifacts</i> , atau <i>process names</i> khas virtualisasi
F5	Pemeriksaan <i>debugging</i>	anti- CTQ-03 <i>Dropper</i> mendeteksi upaya <i>debugging</i> melalui pemeriksaan <i>PEB flag</i> , penggunaan <i>debugger tools</i> , atau <i>breakpoints</i> , kemudian mengambil tindakan <i>evasive</i> seperti keluar paksa atau mengubah alur eksekusi

bersambung

ID	Persyaratan Fungsional	Keterkaitan Deskripsi CTQ
F6	Sinkronisasi eksekusi <i>payload</i>	CTQ-03 Menjamin <i>payload</i> dieksekusi sukses melalui teknik-teknik seperti <i>process injection</i> , <i>remote thread creation</i> , atau <i>reflective DLL loading</i> , dengan verifikasi bahwa <i>payload</i> berjalan dengan benar di konteks <i>target process</i>

Keenam persyaratan fungsional ini dirancang untuk memastikan bahwa *dropper* prototipe mengintegrasikan teknik-teknik *evasion* yang paling efektif dan sulit di-deteksi. F1 dan F2 bersama-sama menciptakan profil *dropper* yang *stealthy* dengan tidak meninggalkan jejak permanen di sistem target. F3 mengatasi keterbatasan *signature-based detection* dengan mengenkripsi *payload*, sehingga setiap *hash* akan berbeda meskipun *payload* sebenarnya sama. F4 dan F5 memastikan *dropper* hanya mengeksekusi dalam lingkungan yang sebenarnya (bukan *sandbox* analisis), sedangkan F6 memvalidasi bahwa mekanisme *delivery payload* benar-benar efektif.

Tabel III.3 Persyaratan non-fungsional (Non-Functional Requirements)

ID	Persyaratan Fungsional	Non-Aspek	Deskripsi
N1	<i>Stealth</i> dan <i>evasiveness</i>	Keamanan	<i>Dropper</i> harus memiliki resistensi tinggi terhadap analisis statis melalui penggunaan Rust dan enkripsi, serta deteksi perilaku melalui operasi <i>file-less</i> dan <i>in-memory execution</i> , dengan target minimum <i>evasion rate</i> 70% terhadap <i>anti-malware</i> komersial
N2	Efisiensi kinerja	Kinerja	<i>Dropper</i> harus beroperasi cepat untuk menghindari deteksi anomali <i>runtime</i> , dengan <i>latency payload execution</i> kurang dari 5 detik

bersambung

ID	Persyaratan Fungsional	Non-Fungsional	Aspek	Deskripsi
N3	Keandalan eksekusi	Keandalan		<i>Dropper</i> harus stabil ketika menjalankan operasi memori kritis, memanfaatkan keamanan memori Rust untuk mencegah <i>crash</i> atau <i>memory corruption</i> yang dapat mengungkap aktivitas berbahaya
N4	Kompatibilitas platform	Kompatibilitas		<i>Dropper</i> harus andal di sistem operasi Microsoft Windows versi 10 dan 11, memastikan evaluasi pada platform target yang relevan dengan mayoritas pengguna <i>enterprise</i>

Persyaratan non-fungsional menentukan karakteristik kualitas *dropper* yang membuatnya *viable* dalam skenario serangan *real-world*. N1 memastikan bahwa *dropper* memiliki resistensi terhadap deteksi, N2 menekankan kinerja agar tidak memicu analisis perilaku, N3 mengurangi risiko *crash* yang meninggalkan *error logs*, dan N4 memastikan relevansi platform.

Berdasarkan persyaratan fungsional dan non-fungsional yang telah diidentifikasi, tiga *Critical To Quality* (CTQ) attributes didefinisikan sebagai berikut:

- **CTQ-01: Payload Concealment (Penyembunyian Payload)**

Mengukur sejauh mana *dropper* mampu menyembunyikan dan melindungi *payload* dari deteksi statis dan dinamis. Metrik: persentase *anti-malware* yang gagal mendeteksi *payload* terenkripsi pada fase *static analysis*; target minimum 70%.

- **CTQ-02: Signature Evasion (Penghindaran Signature)**

Mengukur efektivitas *dropper* dalam menghindari deteksi berbasis *signature* oleh *multi-engine scanners* seperti *VirusTotal*. Metrik: *detection rate* pada *VirusTotal*, target maksimal 20% (80% gagal mendeteksi).

- **CTQ-03: Environment Evasion and Behavioral Stealth**

Mengukur kemampuan *dropper* untuk menghindari deteksi di lingkungan *sandbox/VM* serta beroperasi secara *stealthy* tanpa memicu anomali perilaku. Metrik: persentase *behavioral analysis tools* yang mendeteksi aktivitas mencurigakan; target maksimal 40%.

III.3 Desain Keputusan dan Solusi yang Diusulkan

III.3.1 Alternatif Solusi

Alternatif solusi untuk mengembangkan *dropper spyware* mode *stealth* dengan kemampuan *evasion* tinggi mencakup beberapa pilihan bahasa pemrograman dan pendekatan teknis. Setiap alternatif memiliki *trade-off* antara kontrol *low-level*, resistensi terhadap *reverse engineering*, performa, dan kemudahan implementasi. Tiga alternatif utama yang dipertimbangkan adalah: Menggunakan C/C++ yang memberikan kontrol penuh terhadap memori dan API Windows tetapi rentan terhadap *memory corruption* dan lebih mudah di-*reverse engineer*. Lalu, menggunakan Python dengan *PyInstaller* yang relatif mudah dikembangkan namun *signature*-nya sudah familiar bagi *antivirus* dan kurang *resistant* terhadap *static analysis*. Terakhir, menggunakan Rust yang menawarkan kombinasi unik antara kontrol *low-level*, *memory safety*, performa tinggi, dan resistensi inheren terhadap *reverse engineering*.

Analisis alternatif solusi tidak hanya melibatkan pertimbangan teknis tetapi juga evaluasi terhadap *capability* setiap bahasa dalam mengimplementasikan persyaratan fungsional dan non-fungsional yang telah ditetapkan. Untuk setiap alternatif, dilakukan penilaian terhadap enam kriteria desain: dukungan enkripsi dan *packing*, kontrol *low-level* untuk *fileless execution*, resistensi terhadap *analisis statis*, kemudahan implementasi teknik *anti-analysis*, performansi eksekusi, dan *ecosystem tools/libraries* yang tersedia. Penilaian ini dilakukan secara sistematis menggunakan metodologi *Multi-Criteria Decision Analysis* (MCDA) dengan *Entropy Weight Method* (EWM) untuk menentukan bobot kriteria secara objektif.

III.3.2 Analisis Penelitian Solusi

Analisis penelitian solusi menitikberatkan pada evaluasi efektivitas pendekatan yang telah terbukti dalam literatur untuk mendeteksi *dropper* dan *malware evasive*. Studi menunjukkan bahwa kombinasi deteksi berbasis perilaku (*behavioral analysis*), analisis anomali (*anomaly detection*), dan algoritma *machine learning* meningkatkan tingkat deteksi terhadap *dropper* dengan teknik *stealth* dan *fileless*. Namun, penelitian juga mengungkap bahwa metode-metode ini masih memiliki keterbatasan signifikan ketika dihadapkan pada *dropper* yang mengintegrasikan *multiple evasion techniques* secara simultan.

Implementasi *machine learning* dengan kurasi fitur yang relevan seperti *API call sequences*, entropi *payload*, dan *network flow patterns* terbukti mendongkrak presi-

si dan *recall* dalam klasifikasi *spyware*, menekankan pentingnya kualitas data dan pemilihan fitur untuk mengurangi *false positive*. Penggunaan *dynamic analysis* melalui *sandbox* untuk mengamati proses *unpacking dropper* yang tersembunyi di memori telah terbukti efektif, namun *sandbox* publik masih rentan terhadap *evasion techniques* seperti *time-based sleeping* dan *VM detection*. Integrasi data *threat intelligence* sekaligus deteksi berbasis perilaku adaptif diperlukan agar sistem mampu mengenali pola serangan baru yang belum pernah dijumpai sebelumnya.

Berdasarkan analisis ini, penelitian ini dirancang untuk mengembangkan *dropper* prototipe yang merepresentasikan ancaman tingkat *advanced* dengan *integrated evasion techniques*, sehingga evaluasi terhadap sistem deteksi yang ada akan menghasilkan temuan yang realistik dan *actionable*. Prototipe akan diuji terhadap kombinasi pendekatan deteksi *modern-signature-based*, *behavior-based*, dan *machine learning*-untuk memberikan gambaran komprehensif tentang efektivitas setiap metode.

III.3.3 Metodologi Penilaian Solusi (Multi-Criteria Decision Analysis)

Untuk menentukan bahasa implementasi optimal bagi *dropper mode stealth* yang akan dikembangkan, dilakukan evaluasi *multi-kriteria* terhadap tiga alternatif solusi: Rust, C/C++, dan Python dengan *PyInstaller*. Penilaian ini menggunakan *Multi-Criteria Decision Analysis* (MCDA) dengan *Entropy Weight Method* (EWM), yang mampu menentukan bobot kriteria secara objektif berdasarkan tingkat diversifikasi informasi dalam matriks keputusan. EWM dipilih karena objektivitasnya dalam penentuan bobot tanpa melibatkan subjektivitas *expert judgment*.

III.3.3.0.1 Langkah 1: Normalisasi Matriks Keputusan Skor mentah dari matriks keputusan (\mathbf{X}) dinormalisasi menjadi matriks \mathbf{P} untuk menghilangkan pengaruh unit dan skala pengukuran menggunakan:

$$P_{ij} = \frac{x_{ij}}{\sum_{i=1}^m x_{ij}} \quad (\text{III.1})$$

Keterangan: P_{ij} adalah nilai normalisasi kriteria j untuk alternatif i , x_{ij} adalah skor mentah, m adalah jumlah alternatif ($m = 3$: Rust, C/C++, Python), dan n adalah jumlah kriteria ($n = 6$).

III.3.3.0.2 Langkah 2: Perhitungan Nilai Entropi Nilai entropi (e_j) dihitung untuk setiap kriteria j guna mengukur tingkat ketidakpastian atau dispersi data:

$$e_j = -k \sum_{i=1}^m P_{ij} \ln(P_{ij}), \quad k = \frac{1}{\ln(m)} \quad (\text{III.2})$$

III.3.3.0.3 Langkah 3: Penentuan Bobot Kriteria Derajat diversifikasi (d_j) diperoleh melalui:

$$d_j = 1 - e_j \quad (\text{III.3})$$

Bobot relatif (w_j) untuk setiap kriteria kemudian dihitung dengan:

$$w_j = \frac{d_j}{\sum_{j=1}^n d_j} \quad (\text{III.4})$$

Bobot mencerminkan kontribusi setiap kriteria terhadap pengambilan keputusan, di mana kriteria dengan variabilitas tinggi mendapat bobot lebih besar.

III.3.3.0.4 Langkah 4: Perhitungan Skor Komposit Akhir Skor komposit akhir (S_i) untuk setiap alternatif solusi dihitung menggunakan:

$$S_i = \sum_{j=1}^n w_j P_{ij} \quad (\text{III.5})$$

Alternatif dengan skor tertinggi dipilih sebagai solusi yang paling optimal berdasarkan pertimbangan *multi-kriteria* yang objektif.

III.3.4 Hasil Analisis Penentuan Solusi

Perhitungan MCDA-EWM dilakukan terhadap matriks keputusan dengan enam kriteria desain dan tiga alternatif solusi. Kriteria yang dievaluasi adalah: KD-1 (Dukungan Enkripsi/*Packing*), KD-2 (Kontrol *Low-Level Fileless*), KD-3 (Resistensi Analisis Statis), KD-4 (Kemudahan Implementasi *Anti-Analysis*), KD-5 (Performa Eksekusi), dan KD-6 (*Ecosystem Tools/Libraries*). Hasil perhitungan entropi menunjukkan bahwa KD-2 memiliki entropi terendah dan derajat diversifikasi tertinggi, mengindikasikan bahwa kriteria ini paling efektif dalam membedakan ketiga alternatif. Tabel III.4 merangkum hasil perhitungan bobot kriteria.

Tabel III.4 Bobot kriteria hasil metode EWM

Kode Kriteria	Deskripsi Kriteria	e_j	d_j	w_j
KD-1	Dukungan Enkripsi/ <i>Packing</i>	0.993	0.007	0.057
KD-2	Kontrol <i>Low-Level Fileless</i>	0.923	0.077	0.631
KD-3	Resistensi Analisis Statis	0.957	0.043	0.352
KD-4	Kemudahan Implementasi <i>Anti-Analysis</i>	0.989	0.011	0.090
KD-5	Performa Eksekusi	0.994	0.006	0.049
KD-6	<i>Ecosystem Tools/Libraries</i>	0.998	0.002	0.016
Total		0.146	1.000	

Nilai bobot menunjukkan bahwa KD-2 memberikan kontribusi terbesar (63.1%) terhadap pengambilan keputusan, diikuti oleh KD-3 (35.2%), sedangkan kriteria lainnya memiliki kontribusi kecil.

Skor komposit akhir untuk setiap alternatif disajikan pada Tabel III.5. Rust memperoleh skor tertinggi (0.370), diikuti oleh C/C++ (0.334), dan Python (0.296). Rust unggul terutama pada KD-2 dan KD-3 karena kombinasi uniknya antara kontrol *low-level* dan resistensi terhadap *analisis statis*.

Tabel III.5 Skor komposit akhir alternatif solusi

Alternatif Solusi	Skor Komposit (S_i)	Keterangan
Rust	0.370	Terpilih - unggul pada KD-2 (kontrol <i>low-level</i>) dan KD-3 (resistensi statis)
C/C++	0.334	Kuat pada KD-2 tetapi rentan pada KD-3 (lebih mudah <i>di-reverse engineer</i>)
Python	0.296	Skor rendah pada KD-2 (kontrol terbatas) dan KD-3 (<i>signature</i> sudah familiar)

Berdasarkan hasil analisis MCDA-EWM, Rust dipilih sebagai bahasa implementasi

untuk *dropper spyware* mode *stealth*. Keputusan ini didasarkan pada skor tertinggi yang diperoleh dan justifikasi kuat bahwa Rust secara efektif memadukan kontrol *low-level* yang krusial untuk *fileless execution* dengan resistensi inheren terhadap *analisis statis* yang disasar oleh *spyware mode stealth* modern. Keputusan ini juga didukung oleh observasi industri bahwa *threat actors sophisticated* mulai mengadopsi Rust untuk pengembangan *custom malware* dan *reconnaissance tools*, menjadikan evaluasi *dropper* berbasis Rust sangat relevan dan tepat waktu.

BAB IV

DESAIN KONSEP SOLUSI

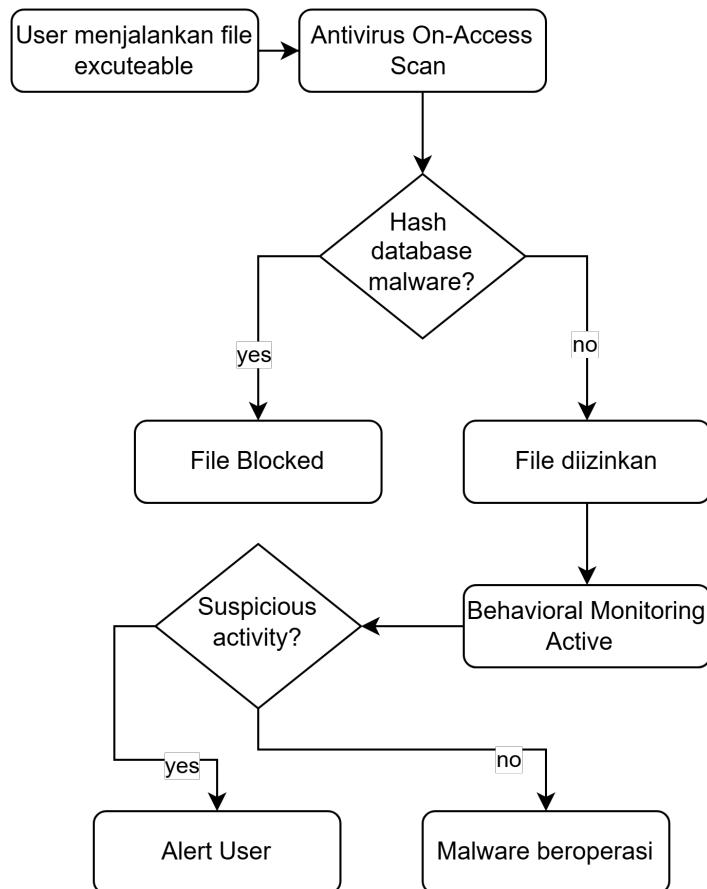
IV.1 Diagram Konseptual Sistem

Bab ini menyajikan desain konseptual dari solusi yang diusulkan melalui perbandingan alur sistem sebelum (*before*) dan sesudah (*after*) pengembangan prototipe *dropper spyware* mode *stealth*. Diagram konseptual ini menunjukkan perbedaan fundamental antara kondisi keamanan siber saat ini dan mekanisme eksekusi *dropper* dengan *integrated evasion techniques* yang akan dievaluasi.

IV.1.1 Sistem Sebelum (Before)

Sistem deteksi *anti-malware* saat ini beroperasi dengan asumsi bahwa *malware* akan meninggalkan jejak yang terdeteksi melalui *signature matching* atau *behavioral anomalies*. Alur sistem sebelum dapat dijelaskan sebagai berikut. Pertama, ketika user menjalankan file executable, *antivirus* melakukan *on-access scan* dengan membandingkan *hash* file terhadap database *malware* yang diketahui. Jika *hash* cocok, file diblokir dan user diberi notifikasi. Jika *hash* tidak cocok (file *unknown*), sistem melanjutkan dengan *behavioral monitoring* pada tingkat file system dan API calls.

Selama *behavioral monitoring*, sistem memonitor indikator-indikator mencurigakan seperti *file writes* ke *system directories*, *registry modifications*, atau *network connections* yang abnormal. Jika aktivitas mencurigakan terdeteksi, sistem mengeluarkan *alert* kepada user. Namun, jika tidak ada *behavioral anomalies* yang terdeteksi, misalnya karena *dropper* menggunakan *fileless execution*, *in-memory operations*, atau *anti-analysis techniques*, maka *malware* beroperasi tanpa terdeteksi. Diagram alur sistem *before* disajikan pada Gambar IV.1.



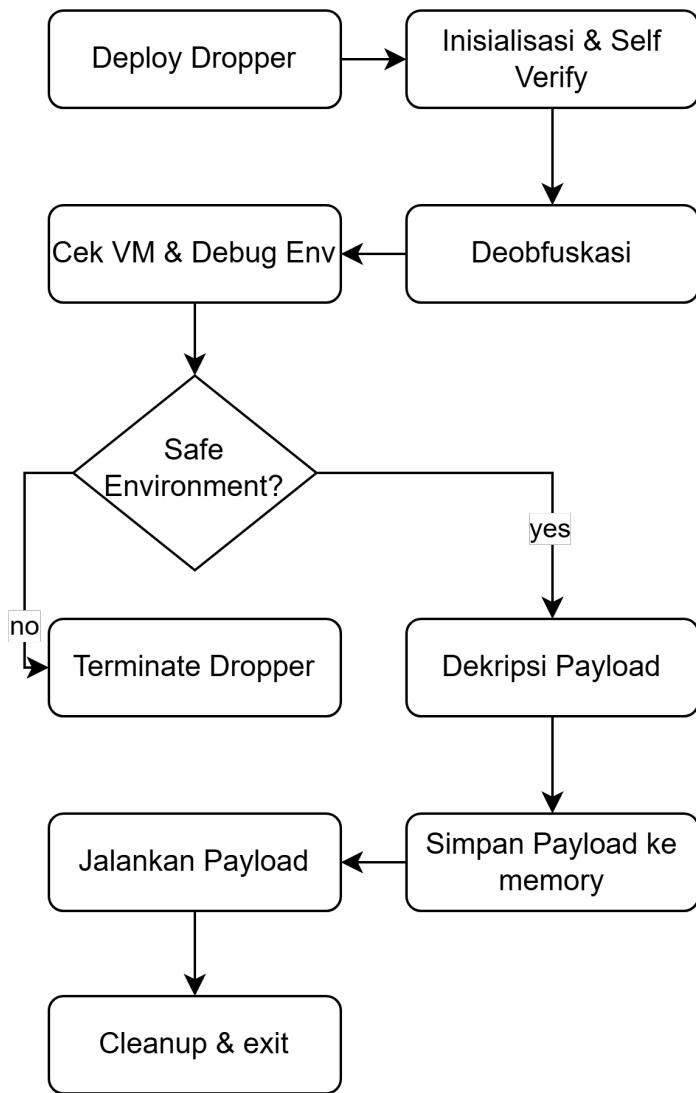
Gambar IV.1 Alur Deteksi Anti-Malware Sebelum (Before)

IV.1.2 Sistem Sesudah (After)

Sistem sesudah menggambarkan mekanisme eksekusi prototipe *dropper spyware* mode *stealth* dalam lingkungan lab terisolasi dengan *full instrumentation* dan *monitoring*. Alur sistem sesudah dimulai dengan peneliti men-deploy *dropper binary* ke target VM di *lab environment* yang terisolasi. Setelah eksekusi, *dropper* melakukan inisialisasi dan *self-verification* untuk memastikan biner tidak *corrupt*.

Langkah berikutnya adalah *deobfuscation* dari *obfuscated code sections* yang telah di-*encrypt*, memastikan *core logic* dapat dijalankan *in-memory*. Tahap krusial selanjutnya adalah *environment checking*, di mana *dropper* melakukan *comprehensive checks* untuk mendeteksi kehadiran VM hypervisor, *sandbox tools*, *debugger*, atau *analysis tools*. Jika *environment* terdeteksi sebagai *unsuitable* (VM atau *sandbox* atau *debugger*), *dropper* melakukan *graceful exit* tanpa meninggalkan *artifacts* yang *observable*, sehingga *monitoring systems* tidak menangkap *payload execution* yang meragukan.

Jika *environment* dipastikan aman, *dropper* melanjutkan ke tahap dekripsi *payload* menggunakan AES-256 dengan *key* yang di-*derive* dari karakteristik sistem lokal. Setelah *payload* berhasil didekripsi dan divalidasi, *payload* disimpan dan dieksekusi secara *in-memory* menggunakan teknik *process injection* ke proses *legitimate*. Setelah *payload* berhasil dijalankan, *dropper* melakukan *cleanup* yang *comprehensive* untuk menghapus dirinya dari memori dan tidak meninggalkan *persistence mechanisms*. Diagram alur sistem *after* disajikan pada Gambar IV.2.



Gambar IV.2 Alur Eksekusi Dropper Spyware Mode Stealth (After)

IV.1.3 Perbandingan Sistem Before dan After

Perbandingan antara sistem *before* dan *after* menunjukkan perbedaan fundamental dalam pendekatan deteksi versus eksekusi *malware* dengan *integrated evasion techniques*.

chniques. Tabel IV.1 merangkum dimensi-dimensi kunci perbandingan.

Tabel IV.1 Perbandingan Sistem Sebelum dan Sesudah Pengembangan

Aspek	Sistem Before	Sistem After
Fokus Deteksi	<i>Signature-based</i> pada <i>hash file</i> dan <i>behavioral anomalies</i> pada disk atau <i>registry</i>	<i>Execution flow</i> ter-instrumentasi dengan <i>full visibility</i> pada setiap tahap dari <i>initialization</i> hingga <i>payload execution</i>
Jenis Malware Target	<i>Malware</i> generik dengan minimal <i>evasion techniques</i>	<i>Dropper spyware mode stealth</i> dengan <i>integrated multiple evasion techniques</i> (enkripsi, <i>anti-VM</i> , <i>anti-debug</i> , <i>fileless execution</i>)
Environment	<i>Production systems</i> dengan <i>real user activity</i>	Lab terisolasi dengan <i>controlled environment</i> dan <i>predictable conditions</i>
Blind Spots	<i>Fileless execution, in-memory operations, environment checking, behavioral stealth</i>	Minimal, setiap tahap dipantau melalui Sysmon, <i>anti-malware logs</i> , <i>network capture</i> , dan <i>memory analysis</i>
Visibility Peneliti	Terbatas pada <i>detection alerts</i> ; tahap eksekusi <i>malware</i> tidak teramati	<i>Comprehensive</i> , peneliti dapat mengidentifikasi tahap eksekusi spesifik mana yang terdeteksi atau lolos dari setiap produk <i>anti-malware</i> atau EDR
Output Evaluasi	<i>Detection</i> atau <i>Non-Detection</i> binary result	<i>Quantified metrics (Detection Rate, Evasion Rate, Time-to-Detect, Anti-Analysis Efficacy, Forensic Artifacts)</i> dengan <i>temporal granularity</i> per tahap eksekusi

Tabel IV.1 menunjukkan bahwa sistem *after* menyediakan *environment* penelitian yang terstruktur dan *measurable* untuk mengevaluasi efektivitas *evasion techniques dropper* serta mengidentifikasi *gap* spesifik dalam kemampuan deteksi sistem *anti-malware* dan EDR yang ada.

IV.2 Penjelasan Desain Solusi

Penjelasan desain solusi menjabarkan rancangan teknis dari setiap komponen modul *dropper* dan bagaimana integrasi modul-modul tersebut menciptakan mekanisme eksekusi yang *stealth* dan sulit dideteksi.

IV.2.1 Desain Inisialisasi dan Verifikasi

Pada tahap inisialisasi, *dropper* melakukan *internal integrity checking* untuk memastikan bahwa biner *dropper* tidak *corrupt* atau *ter-tamper* selama eksekusi. Verifikasi dilakukan menggunakan *checksum* atau *keyed hashing* terhadap sections kritis dari biner. Jika *integrity check* gagal, *dropper* melakukan *immediate termination* tanpa melakukan operasi lebih lanjut. Jika *integrity check* lolos, *dropper* melanjutkan ke tahap *unpacking* dari *obfuscated code sections* yang telah di-*encrypt*. *Unpacking* ini mengekspos *core logic* dari *dropper* tanpa meninggalkan *disk artifacts*, karena semua operasi terjadi *in-memory*.

IV.2.2 Desain Anti-Analysis (Environment Checking)

Modul *environment checker* melakukan *systematic enumeration* dari karakteristik sistem untuk mengidentifikasi kehadiran *analysis environments*. Enumeration mencakup beberapa teknik berikut.

- CPUID-based hypervisor detection
- Registry scanning
- DLL inspection
- Anti-debugging checks

Jika salah satu *check* positif mendeteksi indikasi *analysis environment*, *dropper* memberikan *signal* kepada tahap berikutnya untuk melakukan *controlled exit* tanpa *executing payload*. *Controlled exit* ini dirancang untuk tidak meninggalkan *error logs* atau *crash dumps* yang dapat menjadi bukti kehadiran *dropper*.

IV.2.3 Desain In-Memory Execution (Fileless Loading)

Modul *Loader & In-Memory Executor* mengandung *logic* untuk dekripsi *payload*, *memory allocation*, dan *payload execution* menggunakan teknik-teknik *minimal-footprint*. Pertama, *payload* yang telah di-*embed* dalam biner *dropper* dalam *state* terenkripsi menggunakan AES-256 dengan *key* yang di-*derive* dari karakteristik sistem lokal. *Key derivation* menggunakan kombinasi dari CPU serial number, HDD serial number, Windows installation ID, dan system uptime untuk menciptakan *key*

yang virtually impossible untuk *predict* tanpa *direct access* ke target sistem.

Dekripsi dilakukan menggunakan *standard AES-256-CBC implementation* dengan IV yang juga di-*derive* dari sistem characteristics. Setelah dekripsi, modul melakukan *integrity checking* terhadap *payload* menggunakan *HMAC-SHA256* untuk memastikan *payload* tidak *corrupt* atau *ter-modified*. Jika *integrity check* gagal, modul melakukan *cleanup* dan *termination*.

Setelah dekripsi sukses, *payload* disimpan di memori yang dialokasikan secara dinamis menggunakan *VirtualAlloc* dengan *protections* yang appropriate untuk sections yang perlu *execution*). *Allocation* ini dilakukan tanpa menciptakan file di disk atau *registry entries* yang dapat menjadi *forensic artifacts*. Setelah *memory allocation*, *payload* dieksekusi menggunakan teknik *process injection* ke proses *legitimate* yang already running di sistem. Teknik *injection* yang dapat digunakan meliputi *CreateRemoteThread* dengan *shellcode injection*, *APC injection* dengan *queueing user-mode APC* ke target thread, atau *reflective DLL loading* di mana DLL di-*load* langsung ke memori tanpa *registry entries*.

IV.2.4 Desain Komponen Modul Dropper

Integrasi dari semua modul dirancang untuk menciptakan alur eksekusi yang kohe-sif dan *seamless*. Tabel IV.2 merangkum komponen-komponen modul utama dan fungsinya.

Tabel IV.2 Komponen Modul Dropper dan Fungsi Evasion

No	Modul	Fungsi Utama	Teknik Evasion
1	Initialization dan Self-Verify	Melakukan <i>integrity checking</i> terhadap biner <i>dropper</i> sendiri dan memastikan tidak <i>corrupt</i> atau <i>ter-tamper</i>	<i>Code integrity verification</i>
2	Code Unpacking dan Deobfuscation	Melakukan <i>unpacking</i> dari <i>obfuscated code sections</i> yang telah <i>encrypt</i> secara <i>runtime in-memory</i>	<i>Obfuscation bypass, Unpacking</i>
3	Environment Checker	Memeriksa karakteristik VM, <i>sandbox, debugger</i> , dan <i>analysis tools</i> sebelum eksekusi <i>payload</i>	<i>Anti-VM, Sandbox, Anti-Debug</i>

bersambung

No	Modul	Fungsi Utama	Teknik Evasion
4	Payload Decryption dan Validation	Melakukan dekripsi <i>payload</i> terenkripsi menggunakan AES-256 dengan <i>key</i> yang unik per target	<i>Encryption, Payload obfuscation</i>
5	In-Memory Loader	Mengalokasikan memori secara dinamis dan mengeksekusi <i>payload in-memory</i> menggunakan <i>process injection</i>	<i>Fileless execution, Process injection</i>
6	Cleanup dan Self-Termination	Menghapus jejak <i>dropper</i> dari memori, menutup <i>handles</i> , dan <i>exit gracefully</i> tanpa meninggalkan <i>forensic artifacts</i>	<i>Non-persistence, Anti-forensics</i>

Setiap modul dirancang untuk beroperasi independen namun juga saling mendukung, menciptakan *layered defense approach* yang meningkatkan probabilitas *evasion* terhadap deteksi *multi-layer* dari sistem keamanan modern.

IV.3 Rancangan Lingkungan Pengujian

Lingkungan pengujian dirancang untuk mensimulasikan kondisi *execution dropper spyware mode stealth* dalam konteks terisolasi yang memungkinkan peneliti untuk mengobservasi dan merekam setiap tahap eksekusi dengan *full visibility*, sekaligus memastikan keamanan dan *isolation* dari jaringan eksternal. Lingkungan pengujian dibangun di atas *single host machine* (laptop pribadi peneliti) dengan menggunakan virtualisasi untuk menciptakan *multiple isolated guest VMs* yang masing-masing dikonfigurasi dengan produk *anti-malware* atau EDR berbeda.

Isolasi network dilakukan menggunakan *virtual networking* dengan konfigurasi *host-only* atau NAT, memastikan bahwa guest VMs tidak memiliki akses ke jaringan internet eksternal. Semua komunikasi C2 (*Command and Control*) dimock di dalam *lab network* menggunakan C2 server *dummy* lokal untuk merepresentasikan komunikasi *malicious* tanpa risiko *escape* ke internet. Monitoring pada *multiple layers* dilakukan untuk mengumpulkan data komprehensif tentang perilaku *dropper* dengan cara sebagai berikut.

- **File system layer** menggunakan Sysmon untuk merekam semua *file operations*.

- **Registry layer** menggunakan WMI atau *custom monitoring scripts* untuk merekam *registry changes*.
- **Process layer** menggunakan *API hooking* atau Sysmon untuk merekam *process creation, thread creation, dan module loading*.
- **Network layer** menggunakan *packet capture tools* (*tcpdump* atau Wireshark) untuk merekam semua *network communications*.
- **Memory layer** menggunakan *kernel debugger* atau *live memory analysis tools* untuk *examining memory contents* dan *process memory maps*.

IV.4 Spesifikasi Mesin Uji

Pengujian *dropper* dilakukan menggunakan infrastruktur lokal yang terdiri dari satu *host physical* (laptop pribadi peneliti) dan beberapa guest VMs yang dijalankan di atasnya. Spesifikasi *hardware* dan *software* untuk mesin uji disajikan pada Tabel IV.3.

Tabel IV.3 Spesifikasi Lingkungan Uji

Komponen	Spesifikasi	Keterangan
Host Physical (Laptop Pribadi)		
Processor	Intel Core i5 atau i7 atau AMD Ryzen 5 atau 7 (minimum 4 cores)	Untuk menjalankan <i>multiple VMs</i> secara bersamaan dengan performa <i>adequate</i>
RAM	16 GB minimum	Alokasi 4–6 GB per guest VM, tersisa untuk host OS dan <i>monitoring tools</i>
Storage	SSD 512 GB atau lebih	Untuk host OS, Rust <i>toolchain</i> , VirtualBox atau VMware, guest VM images, dan <i>logging data</i>
OS Host	Windows 10 Pro atau 21H2 atau lebih atau Windows 11	Sebagai host OS untuk <i>hypervisor</i> dan <i>development environment</i>
Hypervisor	VirtualBox 7.0 atau lebih atau VMware Workstation	Untuk membuat dan menjalankan guest VMs terisolasi
Guest VM 1-3		

bersambung

Komponen	Spesifikasi	Keterangan
OS	Windows 10 Pro (Build 19042 atau lebih) atau Windows 11 (Build 22621 atau lebih)	<i>Representative</i> terhadap <i>enterprise desktop</i> yang menjadi target <i>dropper</i>
vCPU	2 cores	<i>Sufficient</i> untuk menjalankan OS dan <i>single malware execution</i>
vRAM	4–6 GB	<i>Adequate</i> untuk Windows 10 atau 11 dan <i>anti-malware software</i>
Storage	40–50 GB <i>virtual disk</i>	<i>Space</i> untuk OS, <i>anti-malware</i> , Sysmon, <i>logging</i> , dan <i>temporary test files</i>
Network	<i>Host-only virtual switch</i>	<i>Isolated network</i> tanpa akses ke jaringan eksternal; semua <i>traffic</i> terikat di <i>lab network</i>
Monitoring Tools	Sysmon, Process Explorer, Registry Editor	Untuk merekam dan mengobservasi aktivitas sistem selama <i>dropper execution</i>

Anti-Malware atau EDR Products

VM 1	Windows Defender (<i>built-in</i>)	<i>Baseline anti-malware</i> dengan <i>behavioral monitoring</i>
VM 2	AVG Free atau Kaspersky Free	<i>Alternative anti-malware</i> dengan <i>heuristics</i> dan <i>cloud-based detection</i>
VM 3	McAfee Personal Security atau Norton LifeLock Trial	<i>Commercial-grade anti-malware</i> dengan <i>advanced behavioral analysis</i>

Monitoring dan Logging Infrastructure

Sysmon Agent	<i>Deployed</i> di semua guest VMs	Merekam <i>process creation</i> , <i>file writes</i> , <i>registry modifications</i> , <i>network connections</i> pada <i>Event ID</i> level dengan <i>custom rule sets</i>
--------------	------------------------------------	---

bersambung

Komponen	Spesifikasi	Keterangan
Network Monitoring	Packet capture tools (<i>tcpdump</i> atau Wireshark)	<i>Running</i> pada host OS atau <i>dedicated monitoring VM</i> untuk <i>capturing C2 dummy communication</i> dan <i>anomalous traffic</i>
Log Aggregation	<i>Text files</i> atau <i>simple SQLite database</i>	Kumpulkan <i>logs</i> dari Sysmon, <i>anti-malware</i> , dan <i>monitoring tools</i> ke <i>centralized location</i> di host untuk <i>post-analysis</i>
Analysis Tools	x64dbg, WinDbg, strings, IDA Free	Untuk <i>debugging dropper execution</i> , <i>memory analysis</i> , dan <i>binary inspection</i> di <i>post-execution</i> fase

Spesifikasi ini dirancang untuk *balanced* antara *resource constraints* dari *single laptop* pribadi dan kebutuhan untuk *adequate monitoring* dan *evaluation* dari *multiple anti-malware products* secara *concurrent*. Pengujian dapat dilakukan secara *sequential* jika *resource* terbatas, atau *parallel* jika host memiliki *resource* yang cukup.

BAB V

RENCANA SELANJUTNYA

V.1 Rencana Implementasi

Subbab ini menjelaskan langkah implementasi prototipe dropper spyware mode stealth berbasis Rust, serta estimasi waktu dan sumber daya yang dibutuhkan.

V.1.1 Langkah-langkah Implementasi

Implementasi dibagi menjadi beberapa tahap utama yang mengikuti alur desain pada Bab IV, yaitu: pengembangan modul enkripsi payload, modul anti-analysis, modul eksekusi fileless, integrasi C2 dummy untuk pengujian, dan integrasi akhir beserta uji coba internal. Setiap tahap diakhiri dengan uji fungsional dasar untuk memastikan pemenuhan FR/NFR yang telah ditetapkan sebelumnya.

Tabel berikut merangkum timeline implementasi secara ringkas (estimasi berbasis minggu kalender):

Tabel V.1 Timeline implementasi prototipe

No	Tahap Implementasi	Aktivitas Kunci	Estimasi Waktu
1	Desain detail & setup environment	Refinement spesifikasi teknis, setup repo, VM lab, toolchain Rust	2 minggu
2	Modul Payload Encryptor & Container	Implementasi AES, kompresi, embedding payload, uji enkripsi/dekripsi	3 minggu
3	Modul Environment Checker	Implementasi anti-VM, anti-sandbox, anti-debug (CPUID, registry, process scan)	3 minggu

No	Tahap Implementasi	Aktivitas Kunci	Estimasi Waktu
4	Modul Fileless Loader & Injection	Implementasi in-memory execution, process injection, uji di VM bersih	4 minggu
5	Integrasi C2 Dummy & Logging	Kanal C2 sederhana untuk verifikasi payload aktif, logging minimal	2 minggu
6	Integrasi, hardening, dan uji internal	Penggabungan seluruh modul, optimasi, smoke test multi-VM	2-3 minggu

Perkiraan total durasi implementasi adalah sekitar 16-17 minggu, termasuk buffer untuk bug fixing ringan dan penyesuaian teknis.

V.1.2 Alat yang Dibutuhkan

Alat dan bahan yang dibutuhkan mencakup perangkat pengembangan, lingkungan virtual untuk pengujian aman, serta perangkat lunak pendukung analisis.

Tabel V.2 Alat dan bahan pendukung implementasi

Kategori	Alat/Bahan	Kegunaan
Perangkat keras	Laptop/PC dengan minimal CPU 4 core, RAM 16 GB, SSD 512 GB	Pengembangan dan menjalankan beberapa VM uji
Virtualisasi	VirtualBox/VMware/Hyper-V	Menyediakan VM Windows 10/11 untuk eksekusi dropper
Bahasa & toolchain	Rust (rustup, cargo, rust-analyzer)	Implementasi dropper dan modul pendukung
Library utama	winapi, aes-gcm, sha2, sysinfo	Akses WinAPI, enkripsi, hashing, profiling lingkungan
OS target	Windows 10/11 Pro (VM)	Lingkungan uji dropper dan anti-malware
Anti-malware/EDR	Windows Defender, serta produk komersial lain	Objek evaluasi kapabilitas deteksi
Tool analisis	Sysmon, Procmon, Wireshark, x64dbg/WinDbg	Observasi perilaku, logging, dan debugging eksekusi

Analisis biaya dapat disederhanakan dengan asumsi penggunaan lisensi akademik/gratis untuk sebagian besar perangkat lunak, sehingga biaya utama adalah penyediaan mesin pengembangan dan penyimpanan untuk log evaluasi.

V.2 Rencana Evaluasi

V.2.1 Metode Pengujian

Pengujian dilakukan di laboratorium terisolasi dengan beberapa VM Windows 10/11 yang masing-masing dipasangi produk anti-malware/EDR berbeda. Dropper dieksekusi dalam tiga skenario utama: pemindaian statis, eksekusi di VM bersih, dan eksekusi di VM yang dikonfigurasi menyerupai lingkungan analisis (VM/sandbox/debugger) untuk menguji mekanisme anti-analysis.

V.2.2 Metrik Evaluasi

Metrik digunakan untuk mengukur efektivitas dropper sekaligus kemampuan deteksi tiap produk anti-malware terhadap teknik evasi yang diimplementasikan. Ringkasan metrik disajikan pada Tabel berikut.

Tabel V.3 Metrik evaluasi implementasi dropper

No	Metrik	Definisi Singkat	Sumber Data
1	Detection Rate (DR)	Persentase engine/produk yang mendeklarasikan dropper atau payload sebagai malicious pada pemindaian statis dan eksekusi	Log multi-engine scanner, log anti-malware di VM
2	Evasion Rate (ER)	Persentase eksekusi di mana dropper berhasil menjalankan payload tanpa terblokir pada tahap awal (before payload active)	Hasil eksekusi berulang pada tiap produk
3	Waktu Deteksi (Time-to-Detect)	Selisih waktu antara start dropper dan munculnya alert pertama dari anti-malware/EDR	Timestamp log produk keamanan dan Sysmon
4	Keberhasilan Anti-Analysis	Persentase eksekusi di VM/sandbox/debugger yang dihentikan oleh modul anti-VM/anti-debug sebelum payload aktif	Log internal dropper dan observasi perilaku di VM analisis

No	Metrik	Definisi Singkat	Sumber Data
5	Stabilitas Eksekusi	Persentase run di VM bersih di mana dropper dan payload selesai tanpa crash atau error fatal	Catatan run dan log sistem di VM bersih
6	Jejak Forensik	Jumlah dan jenis artefak permanen (file, registry) yang tertinggal setelah eksekusi	Hasil inspeksi file system, registry, dan log Systemmon

Nilai-nilai metrik ini kemudian dibandingkan dengan kriteria keberhasilan pada Subbab V.2.3 (misalnya batas maksimum DR statis, minimum ER, dan batas artefak yang diperbolehkan) untuk menilai apakah prototipe memenuhi tujuan penelitian.

V.2.3 Kriteria Keberhasilan

Kriteria keberhasilan dirumuskan berdasarkan CTQ yang telah didefinisikan di Bab III dan difokuskan pada efektivitas evasion serta stabilitas eksekusi.

Tabel V.4 Kriteria keberhasilan prototipe dropper

No	Kriteria	Deskripsi Singkat	Target
1	CTQ-01 - Payload concealment	Payload terenkripsi tidak terdeteksi pada fase pemindaian statis di mayoritas engine	Detection rate statis $\leq 30\%$
2	CTQ-02 - Signature evasion	Biner dropper lolos dari signature-based detection pada beberapa produk utama	Minimal 75% produk komersial tidak mendeteksi pada eksekusi awal

No	Kriteria	Deskripsi Singkat	Target
3	CTQ-03 - Environment & behavioral stealth	Mekanisme anti-VM/anti-debug mencegah eksekusi penuh di VM analisis, serta eksekusi di VM bersih tidak langsung memicu alert perilaku	> 80% run di VM analisis berhenti sebelum payload aktif, dan minimal satu produk terlambat mendeteksi pada VM bersih
4	Stabilitas eksekusi	Dropper berhasil mengeksekusi payload tanpa crash pada VM bersih	Keberhasilan eksekusi $\geq 95\%$ dari total percobaan
5	Minimnya artefak forensik	Tidak ada file permanen atau entri registry baru terkait dropper setelah eksekusi	Tidak di temukan artefak disk yang persisten pada inspeksi manual

Jika sebagian kriteria tidak tercapai, hasil tersebut tetap didokumentasikan sebagai temuan ilmiah dan dasar rekomendasi perbaikan deteksi maupun desain dropper pada penelitian lanjutan.

V.3 Analisis Risiko

Analisis risiko disusun secara ringkas untuk mengidentifikasi hambatan utama selama implementasi dan evaluasi prototipe, serta strategi mitigasinya.

Tabel V.5 Risiko implementasi dan mitigasi

No	Risiko	Dampak Utama	Mitigasi Singkat
1	Implementasi fileless injection lebih sulit dari perkiraan	Timeline pengembangan mundur, beberapa FR tidak tercapai	Memulai lebih awal pada modul loader, membatasi teknik injection ke 1-2 metode yang paling stabil, dan menyiapkan fallback berupa eksekusi semi-fileless jika perlu
2	Deteksi anti-malware terlalu tinggi sehingga tidak merepresentasikan dropper stealth	Evaluasi tidak menggambarkan gap deteksi yang realistik	Iteratif menyesuaikan konfigurasi enkripsi, packing, dan anti-analysis sampai biner mencapai profil deteksi yang seimbang namun tetap aman didokumentasikan
3	Lab tidak sepenuhnya terisolasi	Potensi gangguan ke jaringan luar, risiko etis	Menggunakan jaringan host-only/NAT tertutup, memblokir akses internet dari VM, dan menggunakan C2 dummy lokal saja
4	Keterbatasan waktu dibanding kompleksitas eksperimen	Beberapa skenario uji tidak sempat dijalankan	Memprioritaskan produk anti-malware yang paling relevan, menyusun jadwal pengujian terstruktur, dan menyimpan skenario tambahan sebagai pekerjaan lanjutan
5	Koordinasi dengan pembimbing lancar	Revisi konsep terlambat, kualitas artefak menurun	Menetapkan jadwal konsultasi rutin dan mengirimkan progres singkat tertulis agar umpan balik tetap terjaga meski jadwal padat

Melalui perencanaan implementasi yang terstruktur dan evaluasi yang ketat, penelitian ini diharapkan mampu memberikan data empiris mengenai celah keamanan pada sistem deteksi modern terhadap ancaman *dropper* berbasis Rust.

DAFTAR PUSTAKA

- Ainslie, Scott, Dean Thompson, Sean Maynard, dan Atif Ahmad. 2023. “Cyber-threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice”. *Computers & Security* 132.
- Blessing, Lucienne T.M., dan Amaresh Chakrabarti. 2009. *DRM, a Design Research Methodology*.
- Chatzoglou, E., G. Karopoulos, G. Kambourakis, dan Z. Tsatsikas. 2023. “Bypassing Antivirus Detection: Old-School Malware, New Tricks”. Dalam *Proceedings of TrustBus ’23*.
- Elghaly, Y. M. 2024. “Stealth in Plain Sight: The Hidden Threat of PowerShell Fileless Malware and Its Evasion of Modern EDRs & AVs”, University of East London.
- Kareem, K.M. 2024. “A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security”.
- Kerkour, S. 2021. *Black Hat Rust: Applied Offensive Security with the Rust Programming Language*.
- Koutsokostas, Vasilios, dan Constantinos Patsakis. 2021. “Python and Malware: Developing Stealth and Evasive Malware Without Obfuscation”. *arXiv preprint arXiv:2105.00565*.
- Noor, Umara, Zahid Anwar, Jorn Altmann, dan Zahid Rashid. 2020. “Customer-oriented Ranking of Cyber Threat Intelligence Service Providers”. *Electronic Commerce Research and Applications* 41.
- Reddyvari, V., M.U.M. Rao, S.S.D. Reddy, K.R.S. Reddy, dan B.M. Nayak. 2024. “A Review on Spyware Creation and Detection”. *International Journal of Engineering Research & Technology (IJERT)* 13 (3).

Sudhakar, S., dan S. Kumar. 2020. “An Emerging Threat: Fileless Malware - A Survey and Research Challenges”. *Cybersecurity* 3 (1).