EVALUASI KAPABILITAS DETEKSI ANTI-SPYWARE TERHADAP PACKER SPYWARE MODE STEALTH

Proposal Tugas Akhir

Oleh

Nathaniel Liady
18222114

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

Desember 2025

LEMBAR PENGESAHAN

EVALUASI KAPABILITAS DETEKSI ANTI-SPYWARE TERHADAP PACKER SPYWARE MODE STEALTH

Proposal Tugas Akhir

Oleh

Nathaniel Liady
18222114

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 1 Desember 2025

Pembimbing

Prof. Dr. Ir. Suhardi, M.T.

NIP. 123456789

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE

BAB I

PENDAHULUAN

I.1 Latar Belakang

Ancaman siber saat ini telah berevolusi dari malware tradisional berbasis file menjadi serangan yang lebih canggih dan tersembunyi, seperti fileless *malware* dan *spyware*. Malware jenis ini dirancang khusus untuk menghindari deteksi dengan memanfaatkan fitur-fitur sah dari sistem operasi, seperti PowerShell dan Windows Management Instrumentation (WMI), untuk menjalankan kode berbahaya langsung di memori tanpa menulis file apapun ke disk. Karena tidak memiliki file yang dapat dideteksi oleh *antivirus* berbasis tanda tangan (signature-based), serangan ini seringkali luput dari pantauan sistem keamanan tradisional.

Kecanggihan ini membuat fileless malware menjadi ancaman yang sangat berbahaya bagi perusahaan manapun karena kemampuannya untuk bertahan lama dan menghindari solusi *antivirus* yang ada. Menurut penelitian, *anti-spyware* modern masih memiliki kelemahan signifikan, bahkan terhadap malware ”lama” yang dimodifikasi dengan trik baru. Misalnya, sebuah studi pada tahun 2023 menemukan bahwa hampir separuh dari 12 mesin *antivirus* yang diuji hanya mampu mendeteksi kurang dari setengah varian malware yang disamarkan. Penelitian lain juga menunjukkan bahwa metode seperti enkripsi, injeksi proses, dan penambahan data sampah ke file eksekusi (*junk data*) terbukti sangat efektif dalam menghindari deteksi. Teknik ini bahkan dapat membingungkan *antivirus* gratis dan berbayar, membuat mereka gagal mendeteksi atau mengkarantina file yang berbahaya.

Situasi ini semakin diperparah dengan temuan bahwa banyak alat keamanan, termasuk *anti-spyware*, sering kali gagal menganalisis kode yang dikemas menggunakan alat populer seperti PyInstaller untuk bahasa *Python*. Hal ini terjadi karena *antivirus* tidak dapat memahami konten kode bita *Python (Python bytecode)*, yang secara efektif menyamarkan skrip berbahaya dari analisis statis. Kurangnya deteksi yang

efektif oleh solusi keamanan yang ada, termasuk *anti-spyware* dan EDRs (*Endpoint Detection and Response*), menciptakan celah besar yang dieksploitasi oleh kelompok penjahat siber dan APTs (*Advanced Persistent Threats*), yang semakin sering menggunakan skrip *fileless PowerShell* untuk menghindari pertahanan.

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana kapabilitas sistem *anti-spyware* dalam mendeteksi aktivitas tersembunyi dari perilaku *spyware mode stealth* pada lingkungan uji terkontrol?
2. Bagaimana pendekatan paling efektif untuk menyisipkan *spyware mode stealth* ke sistem?
3. Bagaimana teknik penyamaran (obfuscation) dan metode eksekusi berbasis memori (in-memory execution) mempengaruhi kemampuan deteksi produk *anti-spyware* saat ini?
4. Apa saja celah keamanan dan kelemahan spesifik yang ditemukan pada produk *anti-spyware* dan EDR ketika dihadapkan pada serangan spyware kustom yang dirancang untuk menghindari deteksi?

I.3 Tujuan

Secara umum, tujuan dari pelaksanaan tugas akhir ini adalah untuk mengukur dan mengevaluasi efektivitas produk *anti-spyware* dan EDR komersial dalam mendeteksi *spyware mode stealth* yang dikembangkan dengan teknik-teknik penghindaran deteksi modern.

Secara spesifik, tujuan yang ingin dicapai adalah:

1. Menganalisis dan mengidentifikasi teknik-teknik evasi yang paling efektif digunakan oleh *spyware* untuk menghindari deteksi dari *anti-spyware* dan EDR.
2. Mengembangkan sebuah prototipe *spyware mode stealth*, termasuk *reverse shell fileless PowerShell*, yang menggabungkan teknik-teknik evasif yang telah diidentifikasi.
3. Melakukan pengujian komparatif prototipe *spyware* pada sejumlah produk *anti-spyware* dan EDR komersial untuk mengevaluasi tingkat keberhasilan dan kegagalan deteksi.
4. Mendokumentasikan dan mempublikasikan celah keamanan yang ditemukan pada produk *anti-spyware*, serta menyusun rekomendasi mitigasi untuk pe-

ngembangan sistem pertahanan yang lebih adaptif dan tangguh.

kriteria keberhasilan dari pelaksanaan tugas akhir ini adalah:

- Prototipe *spyware* berhasil dikembangkan dengan setidaknya dua teknik evasif (misalnya, enkripsi dan obfuscation) dan mampu menghindari deteksi oleh salah satu produk *anti-spyware* yang diuji.
- Hasil pengujian menunjukkan bahwa ada perbedaan signifikan dalam tingkat deteksi antara format skrip dan *anti-spyware* yang berbeda.

Kedua kriteria tersebut menjadi indikator utama untuk menilai efektivitas penelitian, serta menunjukkan sejauh mana solusi yang ditawarkan mampu mengungkap kelemahan sistem keamanan siber saat ini. Pencapaian terhadap kriteria ini diharapkan dapat menjadi dasar pertimbangan dalam peningkatan kapabilitas deteksi *anti-spyware* dan EDR di masa depan

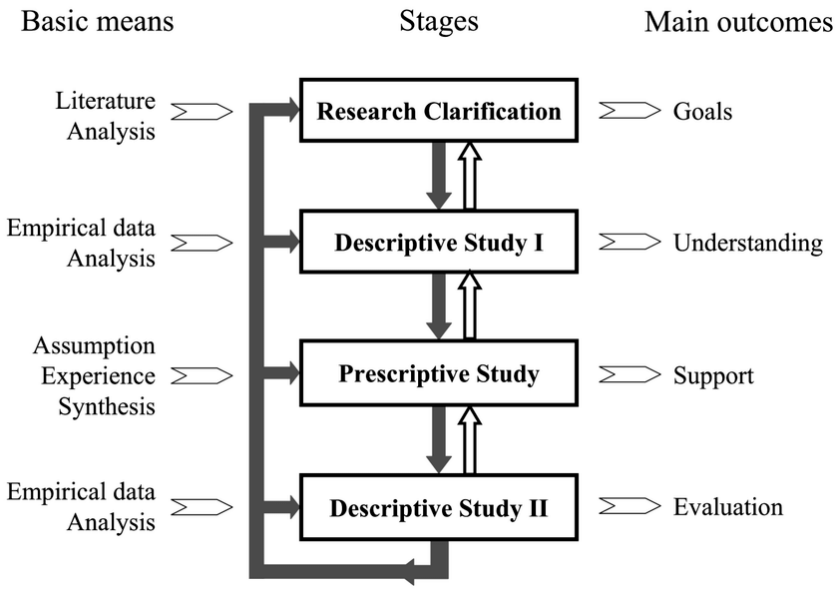
I.4 Batasan Masalah

Batasan masalah dalam pelaksanaan tugas akhir adalah sebagai berikut:

1. Penelitian ini hanya berfokus pada pengujian kapabilitas deteksi *anti-spyware* terhadap aktivitas awal (*Initial Access*) yang dilakukan oleh *spyware mode stealth* pada sistem operasi *desktop*.
2. Evaluasi hanya mencakup perangkat anti *spyware* yang dipilih sesuai kriteria penelitian, tidak membandingkan seluruh produk anti malware yang ada.
3. Aktivitas *malware* yang diujikan dibatasi secara ketat pada tahap penyusupan, enkripsi *payload*, *fileless execution*, dan upaya *persistence*.
4. 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 yang digunakan adalah *Design Research Methodology* (DRM) dikenalkan oleh Blessing **and** Chakrabarti (2009). DRM dibuat dengan tujuan supaya riset dilakukan dengan lebih efektif dan efisien. Metodologi ini terdiri dari empat tahap utama yaitu Research Clarification (RC), Descriptive Study I (DS-I), Perspective Study (PS), dan Descriptive Study II (DS-II). Berikut ini adalah gambaran dari kerangka kerja DRM.



Gambar 1.1 *Design Research Methodology* Framework

1. *Research Clarification (RC)*

   Fase ini akan dimulai dengan identifikasi masalah utama: adanya celah yang signifikan antara teknik serangan siber modern, khususnya *spyware mode stealth*, dan kemampuan deteksi solusi keamanan yang ada. Pengumpulan data awal akan dilakukan melalui tinjauan literatur komprehensif, termasuk laporan industri, artikel akademis, dan berita, untuk memahami lanskap ancaman dan teknik evasif yang digunakan untuk menghindari deteksi *anti-spyware* dan EDR. Hasil dari fase ini adalah rumusan masalah yang jelas dan terperinci, yang akan menjadi landasan untuk seluruh penelitian.
2. *Descriptive Study I (DS-I)*

   Pada fase ini, analisis mendalam terhadap masalah yang telah dirumuskan akan dilakukan dengan mengumpulkan data dan informasi yang relevan. Ini mencakup analisis rinci mengenai teknik-teknik evasi canggih, seperti penggunaan *PowerShell* dan obfuscation, untuk memahami bagaimana ancaman ini bekerja dan mengapa mereka sulit dideteksi. Selain itu, studi-studi terdahulu yang telah menguji bypass *antivirus* akan dikaji untuk mendapatkan wawasan mengenai metode dan potensi hasil. Sebagai bagian penting dari fase ini, alur kerja atau arsitektur teknis dari serangan *spyware* akan disusun, yang akan menjelaskan fase-fase seperti *Initial Access, Establish Foothold, Persistence, Data Collection*, dan *Exfiltration*. Diagram alur yang telah ada akan menjadi representasi visual dari arsitektur ini.
3. *Perspective Study (PS)*

   Fase ini merupakan inti dari DRM, di mana solusi untuk masalah yang telah

didefinisikan akan dirancang dan dikembangkan. Artefak yang akan dibuat adalah prototipe *spyware mode stealth* dengan fungsi-fungsi spesifik seperti *keylogging* dan *screen capture*. Desain prototipe akan mengintegrasikan teknik evasi yang telah diidentifikasi pada fase sebelumnya, seperti enkripsi *payload* dan penggunaan PowerShell untuk menjalankan kode langsung di memori. Berbagai modul, termasuk Packer untuk menyamarkan *payload*.

4. *Descriptive Study II (DS-II)*

   Fase terakhir ini bertujuan untuk menguji dan mengevaluasi efektivitas solusi yang telah dikembangkan. Serangkaian pengujian eksperimental akan dilakukan dalam lingkungan virtual yang terisolasi untuk mengukur tingkat deteksi berbagai produk *anti-spyware* terhadap prototipe *spyware*. Hasil pengujian akan dianalisis untuk mengidentifikasi teknik evasi mana yang paling efektif dan mengapa produk keamanan tertentu gagal atau berhasil dalam mendeteksi ancaman. Analisis ini akan memvalidasi temuan awal dan memberikan kontribusi nyata pada pemahaman tentang kerentanan sistem keamanan modern, yang akan menjadi dasar untuk rekomendasi perbaikan dan penelitian lebih lanjut.

BAB II

STUDI LITERATUR

Bab ini membahas landasan teori dan kajian literatur yang relevan untuk mendukung penelitian ini. Studi literatur dilakukan untuk memahami konsep, teori, dan teknologi yang mendasari penelitian, termasuk *information gathering, social engineering, cyber security, Anti-Spyware, malware*, dan *spyware*. Selain itu, kajian terhadap penelitian terdahulu yang berkaitan juga dilakukan untuk mengidentifikasi solusi yang sudah ada, celah penelitian, serta pendekatan yang dapat diadopsi atau dikembangkan lebih lanjut. Hasil dari studi literatur ini akan menjadi dasar dalam merumuskan solusi desain yang diusulkan dalam penelitian ini.

II.1 *Information Gathering*

Information gathering merupakan tahap awal yang sangat penting dalam proses pengujian keamanan siber maupun kegiatan intelijen digital. Tahap ini bertujuan untuk mengumpulkan informasi sebanyak mungkin mengenai target, baik berupa sistem, jaringan, organisasi, maupun individu, dengan tujuan memahami permukaan serangan yang tersedia. Verma **andothers** (2021) menjelaskan bahwa kegiatan *information gathering* dilakukan untuk memetakan aset dan mengidentifikasi potensi kerentanan sebelum serangan atau pengujian keamanan dilakukan. Secara umum, proses ini terbagi menjadi dua pendekatan utama, yaitu pasif dan aktif. Pengumpulan informasi secara pasif dilakukan tanpa melakukan interaksi langsung dengan sistem target, misalnya dengan memanfaatkan data publik dari mesin pencari, basis data domain, atau sumber intelijen terbuka (*Open Source Intelligence/OSINT*). Sebaliknya, pendekatan aktif melibatkan aktivitas langsung seperti *port scanning, service enumeration*, atau *banner grabbing* untuk memperoleh data teknis yang lebih spesifik, namun metode ini berisiko lebih tinggi untuk terdeteksi oleh sistem keamanan target.

Teknik *information gathering* secara tradisional terdiri atas tiga tahap utama, yaitu *footprinting, scanning*, dan *enumeration*. Pada tahap *footprinting*, peneliti mengumpulkan informasi dasar seperti alamat IP, nama domain, sistem operasi, serta teknologi yang digunakan. Tahap *scanning* bertujuan untuk menemukan *host* aktif dan *port* terbuka, sementara *enumeration* melibatkan eksplorasi lebih dalam terhadap layanan, pengguna, atau konfigurasi sistem yang dapat dimanfaatkan dalam tahap berikutnya. Seiring berkembangnya teknologi, berbagai alat bantu seperti Nmap, Wireshark, The Harvester, Netcraft, dan Metagoofil banyak digunakan untuk mendukung proses pengumpulan informasi ini. Studi Verma **andothers** (2021) juga menyoroti pentingnya kombinasi antara OSINT dan pemindaian aktif untuk meningkatkan efektivitas deteksi potensi risiko, meskipun penggunaan metode ini harus dibatasi dalam ruang lingkup yang legal dan etis.

Selain aspek teknis, penelitian terbaru menekankan pentingnya aspek etika dan hukum dalam kegiatan *information gathering*. Pengumpulan data secara berlebihan atau tanpa izin dapat melanggar privasi individu maupun regulasi keamanan informasi. Oleh karena itu, para peneliti dianjurkan untuk melakukan kegiatan ini dalam lingkungan laboratorium yang terisolasi, dengan batasan yang jelas dan persetujuan dari pihak terkait. Di sisi lain, hasil pengumpulan informasi juga harus dikelola dengan prinsip *responsible disclosure*, yaitu melaporkan temuan yang berpotensi sensitif kepada pihak yang berwenang tanpa menyebarkannya secara publik. Dengan demikian, *information gathering* tidak hanya berfungsi sebagai tahapan teknis untuk mendukung pengujian keamanan, tetapi juga sebagai fondasi penting dalam membangun kesadaran, kebijakan, dan strategi pertahanan siber yang lebih komprehensif.

II.2 *Social Engineering*

Social engineering adalah teknik manipulasi psikologis yang mengeksploitasi kelemahan manusia, bukan kerentanan teknis pada sistem keamanan. Dalam lanskap siber yang terus berkembang, *social engineering* menjadi salah satu ancaman paling signifikan dan efektif. Sejak tahun 2021, serangan *social engineering* telah meningkat baik dari segi volume maupun kecanggihan, dengan penjahat siber dan kelompok terorganisir mengeksploitasi bias kognitif dan emosi manusia untuk menipu. Ini menjadikan faktor manusia sebagai mata rantai terlemah dalam keamanan siber

Penelitian terbaru mengidentifikasi berbagai metode serangan *social engineering*,

mulai dari yang sederhana hingga yang sangat canggih. *Phishing, spear phishing*, dan *whaling* adalah serangan yang menggunakan email atau pesan palsu yang disesuaikan untuk menipu individu atau target tingkat tinggi. Serangan *phishing* di media sosial juga dapat menjangkau audiens yang lebih luas daripada email konvensional. Selain itu, *pretexting* adalah ketika penyerang menciptakan skenario palsu untuk mendapatkan informasi sensitif atau akses, sering kali dengan menyamar sebagai rekan kerja atau figur otoritas. Ada juga metode *baiting* yang menggunakan umpan (seperti file berbahaya) atau manipulasi suara untuk memancing korban agar mengambil tindakan yang membahayakan. Penyerang juga dapat melakukan *impersonation*, yaitu menyamar sebagai individu yang dikenal atau dipercaya, sebuah taktik yang lebih mudah dilakukan di media sosial karena melimpahnya informasi korban. Untuk meningkatkan presisi dan skalabilitas, penjahat siber kini juga memanfaatkan teknologi canggih seperti kecerdasan buatan (AI) dan *deepfake* untuk membuat serangan *social engineering* lebih meyakinkan.

Berbagai studi telah mengidentifikasi beberapa faktor yang membuat individu rentan terhadap serangan *social engineering*. Kesadaran keamanan yang rendah adalah salah satu faktor utama. Penyerang juga mengeksploitasi emosi seperti ketakutan, urgensi, rasa ingin tahu, dan kepercayaan untuk mendorong korban membuat keputusan yang salah. Kepercayaan berlebihan pada figur otoritas juga membuat korban lebih mudah dimanipulasi. Serangan-serangan ini memiliki dampak yang signifikan, termasuk kerugian finansial, kerusakan reputasi, dan hilangnya data. Studi kasus skema penipuan keuangan yang menargetkan Google dan Facebook menunjukkan bahwa organisasi dengan sistem keamanan yang kuat pun tidak kebal terhadap *social engineering*.

II.3 *Cyber Security*

Cyber security merupakan disiplin ilmu dan praktik yang berfokus pada perlindungan sistem komputer, jaringan, data, serta perangkat digital dari berbagai ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Menurut Ainslie **andothers** (2023), keamanan siber tidak hanya menjadi isu teknis, melainkan juga tantangan strategis yang berpengaruh terhadap pengambilan keputusan di tingkat organisasi. Dalam konteks modern, setiap keputusan bisnis harus mempertimbangkan potensi risiko siber, karena ancaman digital kini dapat berdampak langsung pada keberlanjutan operasional dan reputasi perusahaan. Oleh karena itu, *cyber security* mencakup kombinasi aspek teknologi, manusia, dan kebijakan organisasi yang bekerja secara terpadu untuk mencegah, mendeteksi, dan merespons

insiden keamanan secara efektif.

Komponen utama dalam *cyber security* meliputi perlindungan data dan privasi, pengelolaan risiko, deteksi serta respons terhadap insiden, hingga penerapan *Cyber Threat Intelligence (CTI)* yang berfungsi untuk mengidentifikasi pola serangan dan memberikan wawasan bagi pengambilan keputusan keamanan Ainslie **andothers** (2023). Selain itu, munculnya ancaman baru seperti fileless malware turut memperluas ruang lingkup keamanan siber. Berdasarkan penelitian Sudhakar **and** Kumar (2020), *fileless malware* beroperasi langsung di memori tanpa menyimpan file berbahaya di sistem, sehingga sulit dideteksi oleh *antivirus* tradisional yang berbasis tanda tangan. Ancaman ini menunjukkan bahwa sistem pertahanan harus bergeser dari deteksi berbasis file menuju pendekatan berbasis perilaku dan analisis memori.

Dalam penerapannya, pendekatan holistik menjadi kunci keberhasilan manajemen keamanan siber. FLECO, sebuah kerangka kerja yang dikembangkan oleh Domínguez-Dorado **andothers** (2024), menekankan pentingnya integrasi antara aspek teknologi, tata kelola, dan budaya organisasi untuk membangun sistem keamanan yang berkelanjutan. Pendekatan ini membantu organisasi dalam mengukur kesiapan keamanan siber dan memperkuat koordinasi lintas departemen agar setiap unit memahami tanggung jawabnya dalam menjaga keamanan digital. Dengan demikian, *cyber security* tidak hanya berfungsi untuk merespons ancaman yang terjadi, tetapi juga sebagai strategi proaktif yang melibatkan seluruh komponen organisasi dalam menciptakan ketahanan siber yang adaptif dan menyeluruh.

II.4 *Anti-Spyware*

Sistem *anti-spyware* modern menghadapi tantangan signifikan dalam lanskap keamanan siber yang terus berevolusi, beralih dari malware tradisional menuju serangan stealth yang canggih. Menurut Sudhakar dan Kumar (2020), fileless malware beroperasi langsung di memori, menjadikannya sulit dideteksi oleh antivirus tradisional yang berbasis tanda tangan. Spyware merupakan ancaman yang beroperasi tersembunyi, dirancang untuk memantau dan mengumpulkan informasi pengguna secara rahasia, dan dikategorikan sebagai ancaman cyber espionage. Ancaman ini terus berkembang: vektor serangan meluas hingga menyasar fitur modern seperti asisten suara smartphone dan spyware disebarkan melalui injeksi pada aplikasi palsu. Selanjutnya, Ainslie **andothers** (2023) menekankan bahwa keamanan siber bukan hanya isu teknis, tetapi tantangan strategis yang memengaruhi pengambilan keputusan di tingkat organisasi, sehingga pentingnya *Cyber Threat Intelligence (CTI)*

semakin krusial.

Kelemahan deteksi pada sistem *anti-spyware* timbul dari metode evasi canggih yang memanfaatkan celah arsitektur keamanan. E. **andothers** (2023) menjelaskan bahwa spyware menggunakan teknik *packing* dan *obfuscation* untuk mengubah tanda tangan digitalnya, secara efektif menghindari deteksi berbasis tanda tangan. Bahkan, Koutsokostas **and** Patsakis (2021) menunjukkan bahwa malware dapat memanfaatkan *obfuscation bytecode* Python karena kegagalan alat keamanan dalam memprosesnya. Lebih lanjut, ancaman *fileless* mengandalkan skrip bawaan sistem operasi, terutama PowerShell, untuk evasi, karena eksekusi langsung di memori (*in-memory*) menghindari deteksi berbasis file tradisional. Kareem (2024) menggarisbawahi bahwa spyware tingkat lanjut menunjukkan kapabilitas *zero-click* dan memerlukan mekanisme deteksi yang jauh lebih kompleks.

Mengingat kompleksitas ancaman yang ada, strategi *anti-spyware* harus beralih dari deteksi pasif menuju pendekatan yang lebih proaktif dan holistik. Dalam konteks pengembangan alat offensive security, Kerkour (2021) memilih bahasa pemrograman modern seperti Rust sebagai pilihan unggulan karena unggul dalam menciptakan tool yang tangguh dan sulit dilacak. Koutsokostas2021PythonMalware serta Elghaly (2024) sama-sama menekankan bahwa inti dari penguatan *anti-spyware* adalah adopsi pendekatan deteksi berbasis perilaku (*behavior-based*) untuk mengenali anomali aktivitas sistem, alih-alih hanya menandai *file*. Selain itu, Domínguez-Dorado **andothers** (2024) menyoroti bahwa manajemen keamanan siber harus berfokus pada integrasi aspek teknologi, tata kelola, dan budaya organisasi, didukung oleh kerangka kerja holistik seperti FLECO.

II.5 *Malware*

Malware merupakan salah satu ancaman utama dalam dunia keamanan siber yang terus berevolusi dari generasi ke generasi. Secara umum, *malware* adalah perangkat lunak berbahaya yang dirancang untuk menyusup, merusak, atau mencuri data dari sistem komputer tanpa sepengetahuan pengguna. Sudhakar **and** Kumar (2020) menjelaskan bahwa evolusi malware telah bergeser dari bentuk tradisional berbasis *file* menuju *fileless malware* yang beroperasi sepenuhnya di memori. Jenis *malware* ini tidak meninggalkan jejak *file* di sistem, sehingga sulit dideteksi oleh antivirus berbasis tanda tangan. *Fileless malware* sering memanfaatkan komponen sah dari sistem operasi, seperti *Windows Management Instrumentation (WMI)* dan PowerShell, untuk melancarkan serangan tanpa menulis *file* berbahaya ke *disk*. Teknik

ini memungkinkan pelaku untuk melakukan aksi seperti *reconnaissance*, pencurian data, dan persistensi tanpa terdeteksi oleh solusi keamanan konvensional.

E. **andothers** (2023) menambahkan bahwa dalam "permainan kucing dan tikus" antara pembuat *malware* dan pembuat *antivirus*, berbagai teknik penghindaran deteksi terus berkembang. Teknik-teknik seperti *code obfuscation, polymorphism, packing*, dan *process injection* digunakan untuk mengubah struktur dan perilaku kode agar tidak mudah dikenali. Studi mereka menunjukkan bahwa dari 16 sampel *malware* yang diujikan dengan tujuh teknik penghindaran klasik, hanya sebagian kecil antivirus yang mampu mendeteksi lebih dari separuh variasi *malware* tersebut. Hal ini menegaskan bahwa bahkan *malware* "lama" dengan trik penyamaran baru masih mampu menembus sistem deteksi modern. Lebih jauh lagi, peneliti juga menemukan bahwa penggunaan model pembelajaran mesin (ML) untuk deteksi *malware* masih rentan terhadap serangan *adversarial*, di mana pembuat *malware* dapat menghasilkan varian baru yang tampak seperti program sah.

Koutsokostas **and** Patsakis (2021) berfokus pada pengembangan *malware stealth* berbasis Python yang mampu menghindari deteksi tanpa menggunakan *obfuscation*. Mereka menemukan bahwa keterbatasan pada mesin deteksi statis, seperti VirusTotal dan sandbox analisis dinamis, dapat dimanfaatkan untuk menciptakan *malware* yang "bersih" dari hasil pemindaian puluhan antivirus. Studi tersebut mengungkapkan bahwa PyInstaller—alat populer untuk membungkus program Python menjadi *executable* dapat dimodifikasi agar menghasilkan *malware* yang tidak terdeteksi karena kelemahan inheren dalam cara antivirus memproses bytecode Python. Selain itu, mereka menemukan bahwa sandbox publik sering kali gagal mendeteksi *malware* yang menunda eksekusi, mendeteksi lingkungan virtual, atau memeriksa artefak sistem sebelum beraksi.

Berdasarkan literatur tersebut, tren utama dalam penelitian *malware* modern menyoroti bahwa ancaman kini tidak hanya berasal dari varian baru, tetapi dari kemampuan *malware* untuk beradaptasi terhadap mekanisme pertahanan yang ada. Dengan kombinasi teknik *living-off-the-land*, penghindaran berbasis memori, dan eksploitasi terhadap celah dalam sistem analisis otomatis, *malware* modern semakin sulit diidentifikasi. Oleh karena itu, studi-studi ini menegaskan perlunya pendekatan deteksi berbasis perilaku dan kecerdasan buatan yang mampu mengenali pola aktivitas abnormal alih-alih bergantung semata pada tanda tangan statis. Dengan demikian, penelitian mengenai *malware* tidak hanya penting untuk memahami sifat serangan, tetapi juga menjadi dasar dalam merancang sistem pertahanan yang lebih adaptif

dan tangguh terhadap ancaman siber generasi baru.

II.6 *Spyware*

Spyware merupakan salah satu bentuk *malware* yang dirancang untuk memantau, mengumpulkan, dan mengirimkan informasi pengguna tanpa izin atau kesadaran mereka. Perangkat lunak ini biasanya berjalan secara tersembunyi di latar belakang sistem dan dapat merekam aktivitas pengguna, seperti penekanan tombol (*keylogging*), riwayat peramban, data *login*, serta *file* sensitif. Dalam literatur keamanan siber, *spyware* sering dikategorikan sebagai ancaman yang bersifat *stealth*, karena kemampuannya untuk beroperasi tanpa menimbulkan indikasi mencolok bagi pengguna maupun sistem keamanan. Menurut Koutsokostas **and** Patsakis (2021), kemampuan *stealth* seperti ini muncul karena *malware* modern, termasuk *spyware*, memanfaatkan teknik penghindaran analisis dan deteksi baik dalam bentuk statis maupun dinamis. Mereka menunjukkan bahwa banyak *antivirus* gagal mengenali kode berbahaya yang dikemas menggunakan alat seperti PyInstaller karena keterbatasan dalam menganalisis *bytecode Python*. Hal ini menyebabkan sebagian besar *multi-engine scanner*, termasuk VirusTotal, dapat memberikan hasil "bersih" terhadap *file* yang sebenarnya mengandung komponen *spyware*.

E. **andothers** (2023) dalam studi "*Bypassing Antivirus Detection: Old-school Malware, New Tricks*" menguatkan temuan tersebut dengan menyoroti bagaimana teknik klasik seperti *code obfuscation, packing*, dan *process injection* masih sangat efektif untuk menghindari deteksi *antivirus* modern. Mereka menguji berbagai varian *malware*, termasuk *spyware*, terhadap beberapa produk *antivirus* dan menemukan bahwa sebagian besar sistem deteksi hanya mampu mengenali sebagian kecil varian yang dimodifikasi. Temuan ini menunjukkan bahwa banyak mesin *antivirus* masih mengandalkan pencocokan tanda tangan (*signature-based detection*), yang tidak mampu mengidentifikasi pola perilaku baru dari *spyware* yang berevolusi. Selain itu, metode penghindaran berbasis lingkungan—seperti deteksi sandbox atau penundaan eksekusi (*delayed execution*) membuat spyware semakin sulit teridentifikasi melalui analisis dinamis tradisional.

Dari sisi karakteristik perilaku, *spyware* modern cenderung memanfaatkan teknik *living-off-the-land*, yaitu memanfaatkan fungsi atau layanan sah dari sistem operasi seperti PowerShell, WMI, atau API Windows untuk melaksanakan aksinya tanpa mengunduh *file* berbahaya tambahan. Pendekatan ini menjadikan *spyware* semakin sulit dilacak, karena aktivitasnya tampak seperti proses sistem yang normal. Kout-

sokostas **and** Patsakis (2021) menegaskan bahwa pola serangan semacam ini tidak hanya menunjukkan kelemahan sistem deteksi *antivirus*, tetapi juga menyoroti perlunya pendekatan baru berbasis perilaku (*behavior-based detection*) yang mampu mengenali anomali aktivitas sistem, bukan sekadar menandai *file* berbahaya.

Secara keseluruhan, literatur menunjukkan bahwa *spyware* merupakan evolusi dari malware tradisional menuju ancaman yang lebih canggih, tersembunyi, dan adaptif. Dengan kemampuan memanfaatkan celah pada sistem deteksi statis maupun dinamis, *spyware* modern menjadi tantangan utama dalam bidang keamanan siber. Oleh karena itu, penelitian dan pengembangan sistem pertahanan di masa depan perlu berfokus pada integrasi antara analisis perilaku, pembelajaran mesin, dan *threat intelligence* untuk mendeteksi aktivitas mencurigakan secara proaktif. Pendekatan ini diharapkan dapat menutup celah yang selama ini dimanfaatkan oleh *spyware* untuk beroperasi tanpa terdeteksi di berbagai *platform*, baik *desktop* maupun *mobile*.

BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Kondisi keamanan siber saat ini ditandai dengan evolusi ancaman yang signifikan, bergerak dari *malware* tradisional berbasis *file* 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 (AV)* dan *Endpoint Detection and Response (EDR)* yang masih berpegangan pada mekanisme pertahanan konvensional.

Secara konseptual, serangan *spyware* modern yang berfokus pada *Initial Access* dan *Packer* melibatkan beberapa komponen utama: Target (sistem yang diserang), *Packer/Dropper* (Artefak *spyware* yang disamarkan), *Anti-Malware/EDR* (Sistem pertahanan), dan *Server* (Pengumpul informasi, seperti yang digambarkan dalam alur *General Flow*).

III.1.1 Masalah Kerentanan dan Ketertinggalan Anti-Malware Konvensional

Kondisi keamanan siber saat ini ditandai dengan evolusi ancaman yang signifikan, bergerak dari *malware* tradisional berbasis *file* 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 (AV)* dan *Endpoint Detection and Response (EDR)* yang masih berpegangan pada mekanisme pertahanan konvensional.

III.1.2 Identifikasi Masalah Pengguna

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hen-

drerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

III.1.3 Kebutuhan Fungsional

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

III.1.4 Kebutuhan Nonfungsional

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

III.2 Analisis Pemilihan Solusi

III.2.1 Alternatif Solusi

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo,

facilisis non, adipiscing quis, ultrices a, dui.

III.2.2 Analisis Penentuan Solusi

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

BAB IV

DESAIN KONSEP SOLUSI

Ilustrasikan desain konsep solusi dalam bentuk model konseptual dan penjelasan secara ringkas, beserta perbedaannya dengan sistem saat ini. Ilustrasi harus dapat dibandingkan (*before* and *after*). Karena masih berupa proposal, bab ini hanya berisi gambar desain konsep solusi tersebut dan penjelasan perbandingannya dengan gambar sistem yang ada saat ini (yang tergambar di awal Bab **??**).

BAB V

RENCANA SELANJUTNYA

Jelaskan secara detail langkah-langkah rencana selanjutnya, hal-hal yang diperlukan atau akan disiapkan, dan risiko dan mitigasinya, yang meliputi:

1. Rencana implementasi, termasuk alat dan bahan yang diperlukan, lingkungan, konfigurasi, biaya, dan sebagainya.
2. Desain pengujian dan evaluasi, misalnya metode verifikasi dan validasi.
3. Analisis risiko dan mitigasi, misalnya tindakan selanjutnya jika ada yang tidak berjalan sesuai rencana.

DAFTAR PUSTAKA

Ainslie, Scott, Dean Thompson, Sean Maynard **and** Atif Ahmad. 2023. "Cyber-threat intelligence for security decision-making: A review and research agenda for practice". *Computers & Security* 132:103352. https://doi.org/10.1016/j.cose.2023.103352.

Blessing, L. T. M. **and** A. Chakrabarti. 2009. "DRM, a Design Research Methodology". Disiniasi dari file "Design-Research-Methodology.pdf".

Domínguez-Dorado, Manuel, Francisco J. Rodríguez-Pérez, Jesús Galeano-Brajones, Jesús Calle-Cancho **and** David Cortés-Polo. 2024. "FLECO: A tool to boost the adoption of holistic cybersecurity management". *Software Impacts* 19:100614. https://doi.org/10.1016/j.simpa.2024.100614.

E., Chatzoglou, Kambourakis G., Karupoulos G. **and** Tsiatsikas Z. 2023. "Bypassing antivirus detection: old-school malware, new tricks". Disiniasi dari file "2023 Bypassing antivirus detection old-school malware, new tricks.pdf".

Elghaly, Yehia M. 2024. "Stealth in Plain Sight: The Hidden Threat of PowerShell Fileless Malware and Its Evasion of Modern EDRs & AVs". Disiniasi dari file "2024 Stealth in Plain Sight The Hidden Threat of PowerShell Fileless Malware and Its Evasion of Modern EDRs AVs.pdf".

Kareem. 2024. "A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security". Disiniasi dari file "A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security.pdf".

Kerkour, Sylvain. 2021. *Black Hat Rust: Applied offensive security with the Rust programming language.* Self-published.

Koutsokostas, V **and** C Patsakis. 2021. “Python and Malware: Developing Stealth and Evasive Malware Without Obfuscation”. Disiniasi dari file ”2021 Python and Malware Developing Stealth and Evasive Malware Without Obfuscation.pdf”.

Sudhakar, Unknown **and** Sushil Kumar. 2020. “An emerging threat Fileless malware: a survey and research challenges”. *Cybersecurity* 3 (1): 1. https://doi.org/10.1186/s42400-019-0043-x.

Verma, V., S. K. Dubey, T. Khan **and** Pandey H. Prem. 2021. “The Study on Information Gathering”. Disiniasi dari file ”2021 Cyber Security The Study on Information Gathering.pdf”.