UNIVERSITAS
GADJAH MADA
IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

IMPLEMENTASI *MULTI-STAGE RISK DETECTION TOOL* PADA *BROWSER EXTENSION* DENGAN *ACTIVE TERMINATION*

Salma Nur Jihan
22/504279/SV/21621

Browser extension membawa ancaman keamanan yang sulit dideteksi oleh perangkat lunak antivirus konvensional, diperburuk oleh teknik *obfuscation*, keterbatasan visibilitas pengguna terhadap penggunaan izin, serta serangan *supply chain* terhadap ekstensi yang sah. Mekanisme pemeriksaan yang ada belum mampu memberikan penilaian risiko yang memadai maupun *response* aktif terhadap ancaman yang sudah terinstal. Penelitian ini mengembangkan CXT-SCAN, sebuah alat deteksi ancaman *browser extension* multitahap berbasis CLI yang mengintegrasikan *static analysis*, *runtime sandbox* dan Playwright yang diintegrasikan dengan mitmproxy untuk menginspeksi aktivitas jaringan ekstensi dalam lingkungan terisolasi. CXT-Scan juga memanfaatkan *permission management* yang terhubung melalui *native messaging host* untuk melakukan *active termination* apabila terdeteksi *malicious browser extension*. Tujuan penelitian dibuat agar CXT-Scan mampu mendeteksi dan membedakan ekstensi *benign* dan *malicious* berdasarkan parameter statis, perilaku *runtime*, dan aktivitas jaringan, sekaligus memungkinkan *active termination* terhadap *extension* yang sudah terinstal tanpa memerlukan intervensi manual yang kompleks.

Kata Kunci: *Browser Extension, Detection Tool, Security Risk, Native messaging Host, Command Line Interface*

UNIVERSITAS
GADJAH MADA
IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

IMPLEMENTATION OF MULTI-STAGE RISK DETECTION TOOL FOR BROWSER EXTENSIONS WITH ACTIVE TERMINATION

Salma Nur Jihan
22/504279/SV/21621

Browser extensions pose security threats that are difficult to detect using conventional antivirus software. This challenge is further exacerbated by code obfuscation techniques, limited user visibility into permission usage, and supply chain attacks targeting legitimate extensions. Existing inspection mechanisms are unable to provide adequate risk assessment or actively respond to threats that have already been installed. This research presents CXT-SCAN, a multi-stage browser extension threat detection tool implemented as a Command line interface (CLI) application. CXT-SCAN integrates static analysis, a runtime sandbox, and Playwright combined with mitmproxy to inspect extension network activity within an isolated environment. In addition, the system employs a permission management mechanism connected through a native messaging host to perform active termination when a malicious browser extension is detected. The objective of this research is to enable CXT-SCAN to detect and distinguish between benign and malicious browser extensions based on static characteristics, runtime behavior, and network activity. Furthermore, the system provides active termination capabilities for installed malicious extensions without requiring complex manual intervention.
Keyword: Browser Extension, Detection Tool, Security Risk, Native messaging Host, Command Line Interface

,