悪性ブラウザ拡張機能の検知を目的としたEDR支援手法の提案

A Proposal of EDR support method for detecting malicious browser extensions

伊藤朝美・マネジメント分科会・情報セキュリティ大学院大学

In modern web browsers, users can install third-party programs called browser extensions. While browser extensions enhance usability, there have been reports of security risks associated with their malicious use, as they can access sensitive data stored in the browser and the contents of website input forms. The methods of attack have become more complex. Some extensions are malicious from the start, while others have been modified through hijacked developer accounts or have turned malicious via updates after release. Previous studies have primarily focused on analyzing browser extension files before installation, making it difficult to detect malicious behavior that occurred during runtime. Despite these growing risks, there are currently insufficient discussions regarding the monitoring of internal browser behavior. EDR (Endpoint Detection and Response) solutions are unable to adequately monitor deep-level internal activities within the browser, leading to a critical gap in detecting extension-related incidents. To address this problem, we propose a method to support malicious behavior detection through EDR using Chromium, and investigate threat models for malicious browser extensions. The proposed method is based on the assumption that it could be implemented by browser and EDR vendors in the future.

背景と目的

ブラウザ拡張機能はブラウザの機能を拡張するサードパーティ製プログラムであり，ManifestファイルやHTML，JavaScriptファイルなどから構成される．便利な一方でブラウザ内の情報や閲覧中のWebサイトにアクセスできるため悪用される．

【例①】RedDirecion キャンペーン[1]
- 公式ストアの拡張がアップデートを通じ悪性化した事例
- ブラウザ遷移を監視し攻撃者サイトへリダイレクトする挙動

【例②】ChromeAlone[2]
- Chrome標準機能を利用したエンドポイント保護の回避手法の紹介
- ブラウザ拡張によるWebAssembly (WASM)の動的実行を利用

- 既存研究は拡張を構成するファイルへの事前検査手法が主流 → インストール後の悪性化を発見することが困難
- エンドポイントでブラウザ内部の挙動を直接監視する技術が不足

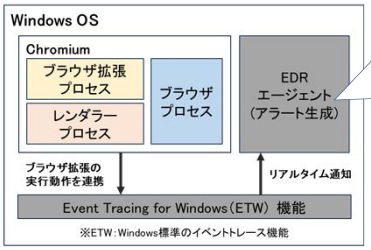
目的　**ブラウザ拡張に関連したインシデント検知やインシデント対応者による分析を可能とすること**

本提案の位置づけ：ブラウザベンダおよびEDRベンダによる将来的な実装を視野に入れたもの

提案内容

提案システムの構成

Windows OSにChromiumとEDRエージェントが存在する環境を想定



EDRは受信したブラウザ拡張の実行動作ログから，事前定義した悪性挙動に該当する一連の流れを発見した場合にアラート生成

以下の拡張動作取得のためChromiumソースコード改変(計15ファイル)
- Extensions APIの実行動作 (cookies.getAllやtabs.update等)
- HTTP/HTTPS通信
- Webサイトのパスワード入力欄の入力値読み取り動作

対象とする悪性挙動とEDRのアラート定義

対象とする悪性挙動	EDRのアラート定義
Cookie情報の外部送信	1. cookies.getAll/cookies.get実行 2. HTTP/HTTPS通信
ユーザの入力パスワードの外部送信	1. パスワード入力欄の値読み取り 2. HTTP/HTTPS通信
ブラウザ閲覧行動監視とリダイレクト	1. tabs.onUpdated（タブ監視）実行 2. HTTP/HTTPS通信 3. tabs.update（タブ更新）実行 4. HTTP/HTTPS通信
	1. tabs.onUpdated（タブ監視）実行 2. HTTP/HTTPS通信 3. tabs.create（新規タブ作成）実行 4. HTTP/HTTPS通信 5. tabs.remove（タブ削除）実行
WASMモジュールの追加ダウンロードと動的実行	1. HTTP/HTTPS通信 2. レスポンスのContent-Typeがapplication/wasm

評価と考察

評価

1. 対象とする悪性挙動を持つ自作の拡張でアラート生成に必要なログを取得できるか
2. Chrome Web Storeに存在する拡張で誤検知が発生するか
3. 悪性拡張の戦略に対して本研究のログ取得方法は耐性があるか

No.	観点	対象	結果
1	ログ有効性	対象とする悪性挙動を持つ自作の拡張	一部を除き，アラート生成に必要なログの取得を確認 ※tabs.createを利用したHTTP/HTTPS通信については拡張起因と判断できず
2	誤検知	対象とする悪性挙動と類似挙動を持つ可能性がある拡張 ※Cookie管理ツールや生産性向上ツール等の拡張3個	アラート生成に用いるログの利用範囲によっては，「ブラウザ閲覧行動監視とリダイレクト」の誤検知が発生
		インターネットで推奨されている拡張 ※翻訳ツールやタブ管理ツール等の拡張10個	自サービスのドメインに紐づくCookie情報の取得と自サービスへのHTTPS通信が発生した場合，「Cookie情報の外部送信」の誤検知が発生
3	戦略への耐性	拡張によるリクエストヘッダのオリジン削除 拡張のJavaScriptコード難読化	取得ログに影響なし

考察

- ブラウザの改変でこれまで取得困難であったブラウザ拡張の実行動作を可視化でき，EDRなどの監視機能を担うアプリケーションに対してログ連携することが可能であることを実証
- 本手法のソースコード改変範囲では取得できない実行動作あり
- ·誤検知が発生しやすいアラート定義あり

今後の課題

- ブラウザ拡張の実行動作ログの網羅性確保
- 悪性挙動発見時の挙動停止や拡張無効化などの追加処理
- 悪性および良性のブラウザ拡張からなる大規模データセットを用いた検証とアラート定義の精度向上
- Chromiumベース以外のブラウザへの適用検討

参考文献
[1] Idan Dardikman: Google and Microsoft Trusted Them. 2.3 Million Users Installed Them. They Were Malware., Koi Security (オンライン)，入手先(https://www.koi.ai/blog/google-and-microsoft-trusted-them-2-3-million-users-installed-them-they-were-malware)(参照 2026-01-18)．
[2]Mike Weber: CHROME ALONE Transforming a Browser into a C2 Platform, DEF CON 33(オンライン)，入手先(https://media.defcon.org/DEF%20CON%2033/DEF%20CON%2033%20presentations/Michael%20Weber%20-%20ChromeAlone%20-%20Transforming%20a%20Browser%20into%20a%20C2%20Slides.pdf)(参照 2026-01-18)．