ブラウザー分離：次世代のブラウザーセキュリティ
January 20, 2022 年 1 月 20 日 Minerva のブログから

ブラウザーベース攻撃は最も共通なベクトル攻撃の一つであり、的を絞ったネットワークへ攻撃の足掛かりを作ります。この足掛かりを構築する攻撃ステージでは、攻撃者はブラウザーの脆弱性を狙いゼロデイ攻撃をしかけるのです。ブラウザー攻撃を防御する最な目的は、マルウェアがブラウザーの不正侵入や、エンドポイントへの足掛かりを防ぐためです。

攻撃者がブラウザーを狙う主な理由としては、初めにブラウザーは企業社内のネットワーク上で情報とドキュメントが行き交う中継地点であることです。これは他のソフトウェアアプリケーションよりも外部からの攻撃がよりアクセス侵入されやすくなります。次にブラウザーはアドオン機能などのアプリをインストールされやすいということです。攻撃者は機能自体にある脆弱性を利用して悪意のある拡張子を生み出し、ユーザが何の疑いもなくインストールされるのを待ち構えているのです。

Google Chrome のケースを挙げますと、市場全体の 65%以上を占めており、ソースコードは Chromium として一般公開されています。このオープンソースコードリポジットリー上で脆弱性を分析し、マルウェアのペイロード攻撃の準備をしています。Microsoft Edge もまた Chromium をベースであり、そう考えますと、市場の 75%以上が Google であり、Chromium を狙ったマルウェア攻撃が集中されるのは理にかなっているのでしょうか。しかしクローズドソースベースのブラウザーでも逆コンパイルされ APT 攻撃のターゲットになっているのも事実です。

ブラウザーベース攻撃は多様なベクターから攻撃

攻撃例としては、

◎ フィッシング&クリック攻撃 – ユーザが URL をクリックすると悪意のあるウエブへアクセスされてしまいます。または他のメディアコンテンツへアクセスされエクスプロイト攻撃の標的にされてしまいます。高度なフィッシングには、スペアーフィッシング攻撃があり、同じ社内の人間と偽り、攻撃を仕掛けたりします。

◎ トロイの木馬を仕掛けた拡張機能＆プラグイン – ユーザがブラウザー拡張機能をダウンロードすることにより、悪意のある機能も一緒にダウンロードされてしまいます。

◎ 合法なウエブサイト上に悪意の広告を埋め込む – 悪意のある広告業者が広告収入と引き換えに、悪意のソフトウェアを組み込んだ広告を掲載します。ユーザはその広告をクリックすることにより、JavaScript コードが起動し攻撃が開始されてしまいます。

クラウドベースのアプリケーションの利点

クラウドベースのアプリケーションやサービスが近年増えてきておりますが、デスクトップアプリケーションなどのネイティブアプリを利用する際にウエブアプリケーションを利用するブラウザーで実行されます。ドキュメント、スプレッドシート、プレゼンテーションや他のファイルタイプなどのやり取りにおいてブラウザーのセキュリティが強化されています。よってドキュメントへ埋め込まれた悪意のあるコードがエンドポイントへ侵入することはありません。

既存のブラウザー分離対策について
ブラウザー分離は、ブラウザーベース攻撃からローカル環境を防御することであり、主に2つの対策があります。

まず初めに仮想マシン（VM）又は Micro VM でインターネットを利用することで分離環境を整えることができます。次にスクリーニング手法でこれはブラウザーアプリケーションがリモートサーバー上で稼働し、ユーザーインターフェイスイメージがクライアントシステムへ転送されます。スクリーニング手法は、SSH 上の X11 のプロトコールを利用することで活用できます。

理論上は、いずれかの方法でブラウザーへアクセスするのは妥当な考えですが、現実には信頼性やユーザの使い心地などユーザビリティの観点から運用と性能などの課題があります。

既存ブラウザーを分離するソリューションにおいてユーザビリティとスケラビリティの欠如がユーザを疎遠してしまう要因となっているのが現状です。アプリケーションはリモートアクセスでローカル環境（VM）へ通信する方法はとても時間がかかることが多々あり、ユーザのストレス負荷がかかり接続が遅く業務効率の低下となります。

Type 2 Hypervisor の VM はハードウェアのリソースが2つのオペレーティングシステムへ切り分けられ稼働します。このことからコスト及びオペレーション負荷が増大し、通常より 2 倍の CPU と RAM が必要になります。

VM は広範囲なハードウェアドライバーサポートが無く、ハードウェアを仮想化しても機能しないことがあるかもしれません。一般的に VM ソフトウェア環境でサポートされているテスト済のマザーボードは稀です。LAN 上で通常ノード又は USB ポートへアクセスしたり VM をシームレスに機能させたりすることは非常に困難です。VM 環境でモバイル開発を実施するのは現実的ではありません。

Minerva の次世代ブラウザー分離防御モジュール

Minerva Labs では先制防御を最優先にそしてセキュリティチームの観点から容易な展開とスケラビリティを追求したシームレスな製品を提供しています。この分野において多くの調査と開発を経て、ユーザビリティとスケラビリティを軽視することなくブラウザーからの攻撃を防御する製品を開発致しました。Minerva のブラウザー防御モジュールはランサムウェア防御としても役割を兼ねており、VM環境で展開するような既存のソリューションよりも多くの攻撃から防御できる製品です。

Minerva のブラウザー防御モジュール（BIM）はブラウザーの初期プロセスから悪意のある子プロセスが発生するのを先制防御します。悪意のあるエクスプロイトがブラウザーの脆弱性を突いて侵入されても、防御モジュールが悪意のあるプロセスを先制防御しますのでマルウェア実行をストップします。ファイルレス攻撃については、ペイロード攻撃の実行前に Minerva のメモリーインジェクション攻撃防御モジュールによってブロックされます。ブラウザー上に悪意のあるファイルを仕掛けてエンドポイントへダウンロードさせるような攻撃も Minerva の悪意のあるファイル攻撃防御モジュールで阻止します。Minerva の防御プラットフォームは多種多様なマルウェアの検知挙動を見つけ先制防御します。

Minerva 製品（Minerva Armor）についてのお問い合わせは Pico Technologies（info@pico-t.co.jp）までお願い致します。