2023 年 11 月 28 日
デジタルアーツ株式会社

PRESS RELEASE

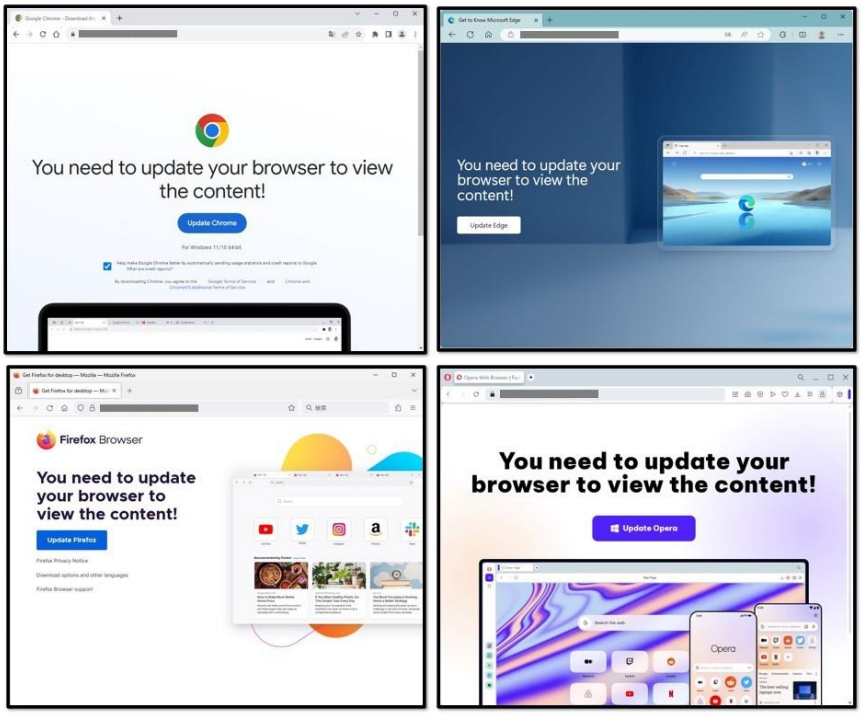
【セキュリティレポート】ブロックチェーンを悪用する「ClearFake」テイクダウンを避けるほか、ブラックリストで排除されない仕組みで安定した配信経路を確保

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、偽アップデートページを表示することでマルウェアをダウンロードさせる「ClearFake」の攻撃を分析したレポートを公開しました。

「SocGholish」に続き、「ClearFake」の攻撃手法に注目

偽アップデート（Fake Update）は、偽のアップデートページを表示してアクセスしたユーザーを騙しマルウェアをダウンロードさせる（実行させる）という攻撃です。デジタルアーツでは直近で、偽アップデートの代表的なマルウェア配信フレームワークである「SocGholish（FAKEUPDATES）」の調査結果を報告しましたが、2023 年には、その他にも多くの攻撃タイプが発見・報告されています。

なかでも 2023 年 8 月ころから確認されている「ClearFake」は、配信経路にブロックチェーンを悪用し始めました。「SocGholish」ほど解析回避の手法は取り入れていない一方で、テイクダウン避ける、複数の主要ブラウザーや多言語に対応するなどの特徴があります。「ClearFake」はターゲットを絞るのではなく、無差別的にマルウェアを配信しているといえます。この度デジタルアーツは、「ClearFake」の攻撃を独自に分析しました。

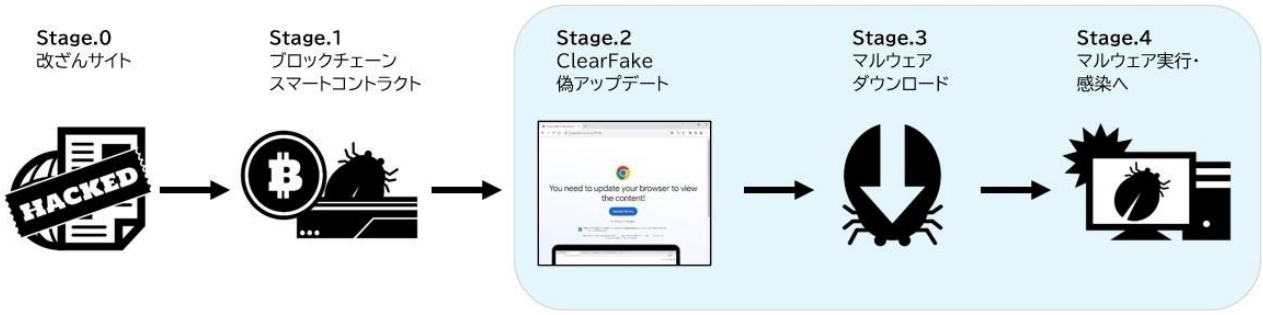


偽アップデートページ例

ブロックチェーンの特性を悪用し、削除が困難な JavaScript を展開する「ClearFake」

今回の調査において、「ClearFake」は正規のサイトを改ざんし（以下、「改ざんサイト」と記載）、あらかじめ挿入された JavaScript を起点として偽アップデートページを表示し、最終的にマルウェアのダウンロード・感染へと至ることがわかりました。

ClearFake 感染チェーン



まず、改ざんサイトにアクセスが確認されると、インターネットを介してブロックチェーンに接続し、特定のスマートコントラクト※1 にアクセスします。そして、悪意のある JavaScript コードを取得する際に、BSC※2（BNB Smart Chain）という「ブロックチェーン」を悪用していることが判明しました。

ブロックチェーンは、改ざん防止や永続性を保証するために設計されていることから、ブロックチェーン上に悪意のある JavaScript コードが展開されると、削除することはほぼ不可能であり、テイクダウンが難しくなります。加えて、本事例でアクセスする際に利用されていた URL は、一般的かつ正当な URL であったことから、これらはブラックリストではブロックされにくいものと考えられます。つまり攻撃者側には、安定した配信経路といえます。

この後、ブロックチェーン上に展開された悪意のある JavaScript がブラウザーで実行されると、新たな URL にアクセスを行い、利用しているブラウザーと利用言語に応じた偽アップデートページが表示されます。また、偽アップデートページの表示をする際はインラインフレームで元のページ全体を覆い隠しています。そのため、改ざんサイトからリダイレクトせず、アドレスバーもそのままの URL が表示されます。

最後に、偽アップデートページのダウンロードボタンをクリックすると、リダイレクトし、オンラインストレージ「Dropbox」の URL からマルウェアがダウンロードされました。また、調査時にダウンロードされた exe ファイルは、「Lumma Stealer」という情報窃取型のマルウェアであることも確認できました。ファイルを実行することでマルウェアに感染し、端末情報が盗まれる危険性があります。

※1 スマートコントラクト：ブロックチェーン上で自動的に動作するプログラムのようなもの

※2 BSC：BNB Smart Chain の略であり、ビットコインなどの仮想通貨取引で利用されるブロックチェーン

※あくまで今回ダウンロードされたファイルは調査時のものであり、環境や時期によって他のマルウェアが配信される可能性があります。

「ClearFake」は今後も新たな手法を用いる可能性あり

「ClearFake」は、解析されたとしてもテイクダウンされない経路があります。さらに偽装種類が多いということは誘導される絶対数もそれらに比例するため、結果的に偽アップデートの被害が多発することが予想できます。また、「ClearFake」は本調査を分析している短期間においても、JavaScript の記述方法を頻繁に更新するなどの動きが確認されているため、今後も変わった手法を用いてくる可能性が考えられます。

「ClearFake」に限らず他の偽アップデートも出現しており、今後も Web 経由のマルウェア感染に警戒する必要があるでしょう。

●セキュリティレポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

詳細はこちらからご覧ください。

https://www.daj.jp/security_reports/36/

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F　▶URL: https://www.daj.jp/
＜本リリースに関するお問い合わせ＞
　デジタルアーツ株式会社　広報課　関・宮内　　TEL　: 03-5220-1670／ E-mail : press@daj.co.jp