2023 年 11 月 14 日
デジタルアーツ株式会社

PRESS RELEASE

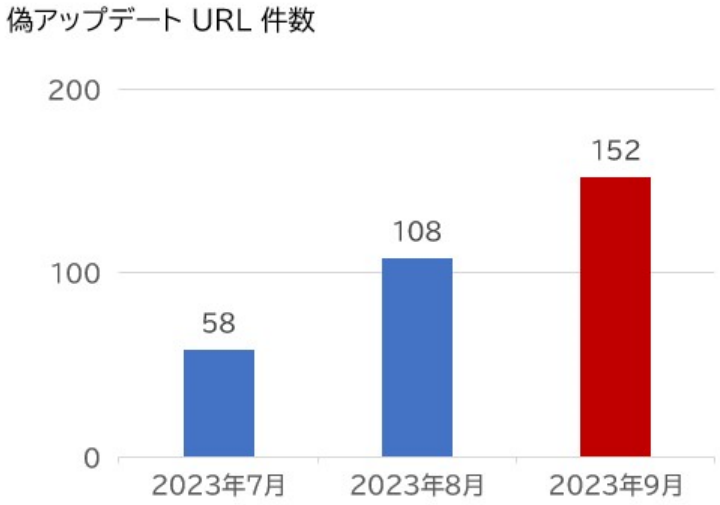
【セキュリティレポート】
偽アップデートの代表的マルウェア配信フレームワーク「SocGholish」を独自分析
ターゲットのブラウザー上で繰り返し HTML を置き換えページを改ざん

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させてアクセスしたユーザーを騙すことでマルウェアをダウンロードさせる「SocGholish」の攻撃を分析したレポートを公開しました。

■日本国内でも観測が増える偽アップデート

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て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。偽アップデートにはいくつか異なるパターンがあり、今年観測されているものは、「SocGholish」、「ClearFake」、「SmartApeSG（ZPHP）」「FakeSG（RogueRaticate）」、「FakeUpdateRU」などが挙げられます。

日本においても、今年は特に新たな攻撃タイプが出現し、これまで以上に偽アップデートが観測されています。デジタルアーツが観測した偽アップデートの URL 件数は、2023年7月で58件、2023年8月で108件、2023年9月で152件と、直近3ヶ月でも右肩上がりに増加していることがわかります。

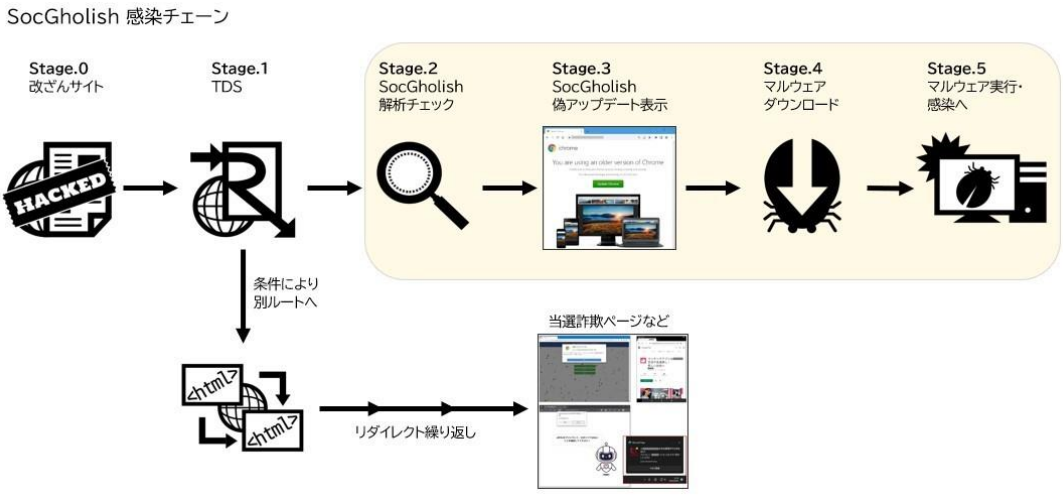


■様々なマルウェアを配信するフレームワーク「SocGholish」

「SocGholish」は、様々なマルウェアを配信するために使用されている JavaScript フレームワークであり、偽アップデートの中で代表的な攻撃手法の1つです。2017 年末頃から観測されており、2022 年に米国の 250 以上のニュースサイトを改ざんしたのも「SocGholish」であったことがわかっています。そこでデジタルアーツは、「SocGholish」の攻撃を独自に分析しました。

■html を置き換え偽アップデートページを表示　マルウェアダウンロードを促す「SocGholish」

今回の調査では、「SocGholish」はブラウザー上で正規サイトの html を置き換えることで、偽アップデートページを表示し、マルウェアをダウンロードさせていることが判明しました。まず、正規サイトが改ざんされてしまうきっかけには、ウェブサーバーの脆弱性を突かれたり、管理用アカウントの乗っ取りなどが考えられます。そして、その改ざんされた正規サイトにアクセスすると JavaScript が順次実行されアクセスしたブラウザー上では html の置き換えが発生します。実際に偽アップデートページを表示する際は、リダイレクトはせず、アドレスバーも元の正規サイトの URL のままであり、かつ一瞬で表示されるため、不信感を与えにくくなっています。



「SocGholish」は、アクセスした人の動作などを含め、IP アドレスや解析者・サンドボックスなどの機械的なアクセスかどうかといった様々な項目で確認を行いながら挙動を変化させます。チェック時に問題が確認され、想定するターゲ

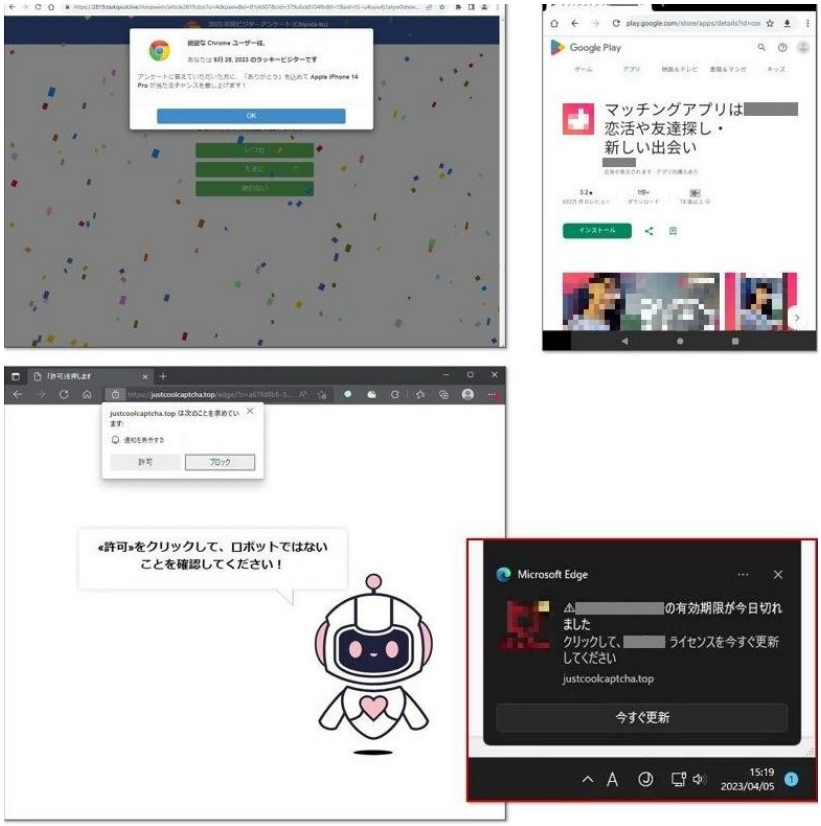
ットではないことが判明した場合は、別ルートに誘導されるか、そのステップで終了し偽アップデートページが表示されないことが分かっています。

このように、「SocGholish」は JavaScript を駆使して想定するターゲットにのみ偽アップデートページを表示させることで、様々な解析回避を行っています。

想定するターゲットの場合は最終的に html が大きく置き換えられ、偽アップデートページが表示されます。ページ内のボタンをクリックすることでファイルがダウンロードされますが、ダウンロード部分には解析回避で用いられる「HTML Smuggling」という手法も確認しました。
ダウンロードしたファイルをダブルクリックし実行すると、新たな URL に対して POST 通信を行うというところまで確認ができています。その後の挙動については、何度か情報のやりとりを繰り返したり、端末に応じたさらなるマルウェアに感染するといったことが考えられるでしょう。

■「SocGholish 」ではない別のルートへの誘導も発見

途中のチェック部分において、条件に合致しなかった際は別のルートへと進むことがわかっており、こちらでは改ざんサイトからリダイレクトが発生します。最終的にユーザー情報に応じてビジターアンケート、マッチングアプリページ、ブラウザープッシュ通知の許可を誘うページなどに誘導されることを確認しました。



今回の調査の結果、「SocGholish」を用いて偽アップデートからマルウェアを配信する攻撃は、日本以外の国を主なターゲットとしているように考えられますが、今後もあらゆる状況に備えて Web 経由のマルウェア感染に警戒する必要があります。

※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

●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/35/

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