DigitalArts

セキュリティレポート

NewsLetter

2020 7/16

デジタルアーツ株式会社

セキュリティレポート
ブラウザー拡張機能がマルウェア化
大手企業も被害に!?Webサイト改ざん被害とその対策とは

情報セキュリティメーカーのデジタルアーツでは、国内で検索可能なURL情報を収集・調査し、弊社製品ユーザー様を脅威から守るためデータベースを蓄積しております。このたび、海外で被害事例が多数報告され、国内でも被害増加が予測される、ブラウザー拡張機能によるWebサイト改ざん被害について検証しましたのでご紹介いたします。

有名企業も被害の可能性？本当は恐ろしいWebサイトの改ざん

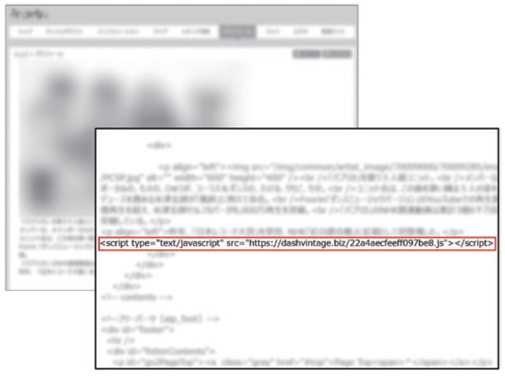
2020年4月、音楽系事業を運営するA社の公式Webサイト（以下、A社Webサイト）が、外部から改ざんされたことが発覚し約一週間公開停止となりました。A社は、公開停止の間不正な書き込みを削除し、その他不正な侵入の形跡が見つからなかったことが確認できたため、Webサイトの公開を再開、個人情報等の漏洩がおきた形跡はないと発表しました。

デジタルアーツでこのインシデントを独自に検証したところ、A社Webサイトの複数のページに不審なコードが記述されていた痕跡を発見しました。

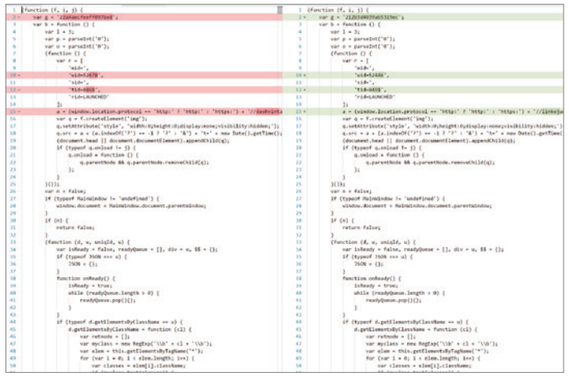
不正なブラウザー拡張機能がWebサイトを改ざん？
被害が増加する「LNKRキャンペーン（リンカーキャンペーン）」とは

A社の発表から約一か月前の3月、米国の著名なセキュリティ研究者が発表した調査結果が話題になりました※。米国の健康保険会社のWebサイトに不正なコードが埋め込まれており、その原因は「Webサイトを編集する従業員のブラウザーにインストールされた拡張機能によって挿入された」というのです。不正なコードが埋め込まれたWebサイトにアクセスすると、広告が表示させられていたとのこと。

そして、A社Webサイトで使われていたコードと、ほとんどが同じコードであったのです。但し、A社の発表内容からは、詳細内容まではわかっていません。



【図1】A社Webサイトの停止直前のページソースに記述されていた不審なコード



【図2】左がA社Webサイトで使われたJavaScriptファイル、右が既にLNKRで使われたと報告されたファイル

この不正なブラウザー拡張機能は、元は正常なアプリとしてダウンロードして利用されていたものが、他者に売却された結果マルウェアとなってしまったものであるといいます。このようにマルウェア化したブラウザー拡張機能をダウンロードしたユーザーが、自社のWebサイトを編集した際に不正なコードを書き込んでしまっているのです。この不正なブラウザー拡張機能を使ってWebサイトを改ざんし、不正に広告を表示させる攻撃が「LNKRキャンペーン」です。

攻撃者の狙いは？不正なブラウザー拡張機能がもたらす影響

ブラウザー拡張機能が悪用され、インストールした人の個人情報を窃取するといった被害は数年前から国内でも確認されていました。こうした不正なブラウザー拡張機能をWebサイト管理者がインストールしてしまい、企業や団体のWebサイト改ざんというインシデントに発展しているといえるでしょう。

攻撃者の狙いとしては、不正に表示させた広告をユーザーがクリックすることによって広告料を窃取するという、いわば金銭目的であることが予想されますが、目的ははっきりと分かってはいません。

金銭的な被害が直接出ないとはいえ、Webサイトが気付かないうちに改ざんされ犯罪に利用されてしまい、公開停止等に追い込まれユーザーに多大な影響を与えてしまう恐れがありますし、こうした機能を利用して改ざんサイトにアクセスしたユーザーの個人情報を窃取するという手法も技術的には可能となるので、看過することはできません。

国内でも被害が増加する可能性大
Webサイト管理者の端末もセキュリティ対策を

「LNKRキャンペーン」は、数百のサイトが被害に遭っていることが報告されており、日本のサイトも含まれていました。

Webサイト管理者の方はこうした被害に遭わないために、攻撃者によって改変されてマルウェア化したブラウザー拡張機能が市場に出ている恐れがあるということをご理解いただき、拡張機能の開発者が信頼できる企業であることを確認したうえで、インストールすべきかご判断いただくことをお勧めします。またWebサイトを管理する端末環境でもセキュリティ対策を必ず行ってください。

Webサイトを閲覧する側においては、今回の例のようにアクセスした正規のWebサイトが改ざんされてしまっている可能性があることを理解していても、人の目で見分けることは非常に困難です。Webフィルタリングを利用することで、不審なサイトへのアクセスをブロックすることができます。

新型コロナウイルス感染症拡大によりテレワークの導入が進んでいますが、様々な手口のサイバー攻撃が日々生み出されています。

いま一度、セキュリティ対策を見直してはいかがでしょうか。

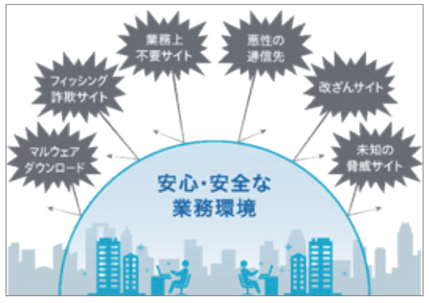
■詳細につきましては、以下デジタルアーツWebサイトにて公開しております

<ブラウザー拡張機能がWebサイトを改ざん？有名企業も被害の可能性>

https://www.daj.jp/security_reports/200716_1/

※ 2020年3月、セキュリティの専門家Brian Krebsがこのアドオンについて調査し、レポートを発表しました。https://krebsonsecurity.com/2020/03/the-case-for-limiting-your-browser-extensions/

Webセキュリティ「i-FILTER」で、改ざんサイトなど不審なサイトへのアクセスを防ぐ



強固なURLフィルタリング「ホワイトリスト運用」により、
ためらいなくWebアクセスできる安全な業務環境を構築

■強固なURLフィルタリング「ホワイトリスト運用」で未知の脅威サイトへのアクセスをブロック

国内で検索可能なURLを独自に収集し、安全を確認したURLのみアクセス可能とする「ホワイトリスト運用」により、安全なWeb環境を創出、攻撃者が用意した悪意あるWebサイトなど、未知の脅威サイトへのアクセスをブロックします。業務上必要なURL等を登録、組織の運用ルールに従ってアクセス許可／不許可等を設定することが可能です。

※今回のケースでは

A社Webサイトが改ざんされ、閲覧すると外部の不審なドメインのURLへと自動的にアクセスさせられていました。

しかしこの不審なドメイン（dashvintage[.]biz）のURLは、デジタルアーツで安全が確認できていないURLであったため「i-FILTER」Ver.10でブロックすることが可能でした。

詳細はこちらをご覧ください ▶ **https://www.daj.jp/bs/i-filter/**

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/

本ニュースレターに関するお問い合わせ

※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、
お問い合わせ先は下記とさせていただきます
デジタルアーツ株式会社　広報担当 山田
TEL : 090 1555 7254 / E mail : press@daj.co.jp

DigitalArts
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