2023 年 9 月 25 日
デジタルアーツ株式会社

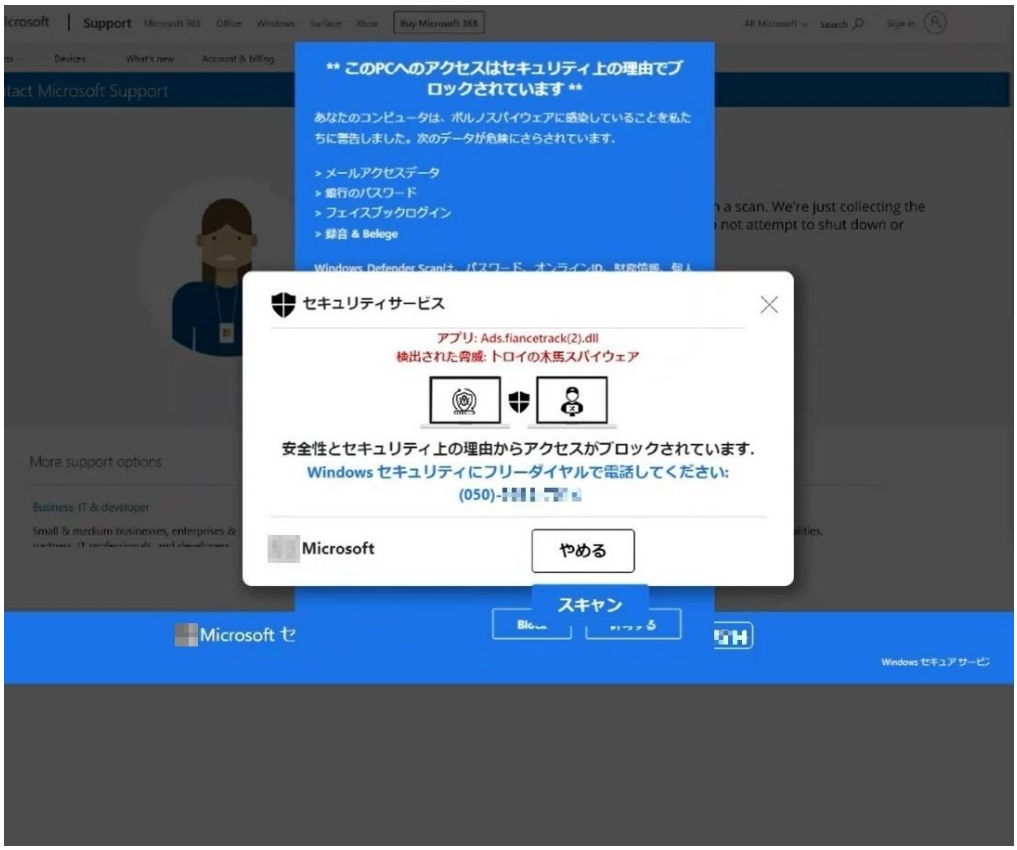
PRESS RELEASE

【セキュリティレポート】
広告クリックにおけるサポート詐欺の手口をデジタルアーツが分析
特定条件に合致する場合に限り、ランディングページからリダイレクトし、サポート詐欺サイトが表示

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、広告から遷移するサポート詐欺の手口を分析したレポートを公開しました。

■サポート詐欺の活発化

サポート詐欺とは、ウイルスに感染したかのような警告や警告音を出して不安を煽り、虚偽のサポート窓口に電話をかけさせて金銭を騙し取ろうとする詐欺行為です。IPA によると、「ウイルス検出の偽警告」に関する相談件数は年々増加傾向にあることから※1、昨今特にサポート詐欺が活発化していることがわかります。



今回デジタルアーツは Web サイト閲覧中にクリックした広告からサポート詐欺サイトに誘導された事例を分析しました。

※1　出典：情報セキュリティ安心相談窓口の相談状況［2023 年第 2 四半期（4 月～6 月）］| IPA 独立行政法人 情報処理推進機構

■サポート詐欺サイトは特定条件に合致したときに限り表示されることが判明

前提として一般的な広告は、閲覧者が広告をクリックした際に、広告主が指定した Web ページが表示される仕組みになっています。この指定されたページが、ランディングページと呼ばれるものであり、広告配信サービス側の審査を通過することで、広告が Web サイトに表示されるようになります。

今回表示された広告をクリックした際の通信を確認したところ、広告が直接サポート詐欺サイトに誘導しているのではなく、ランディングページを経由してサポート詐欺サイトが表示されていることがわかります。

Request...	Result	Protocol	Host	URL	Comments
POST	302	HTTPS	[redacted].net	/adk?sa=l&ai=ClNOsl2PQZIS7DY...	1.広告
GET	204	HTTPS	[redacted].com	/pagead/adk?sa=L&ai=C6ALll2P...	2.広告
GET	301	HTTPS	[redacted].info	/?gclid=EAIaIQobChMIxOKInczJ...	3.ランディングページ
GET	200	HTTPS	[redacted].page	/?phone=(050)-[redacted]&gclid...	4.サポート詐欺サイト

広告からサポート詐欺サイトが表示されるまでの通信

本事例では、「広告が指定したランディングページを通常どおり表示する場合」と、「広告が指定したランディングページからリダイレクトしてサポート詐欺サイトを表示する場合」の 2 パターンの挙動が確認されました。後者のリダイレクトしてサポート詐欺サイトを表示する場合は、「User-Agent に『Windows』や『mobi』などの特定の文字列が含まれている」かつ、「閲覧者が特定の IP アドレスでない」といった特定条件に合致したときのみ、生じることがわかりました。

アクセス条件によって異なる挙動

ランディングページをそのまま表示

```
[redacted] --Header "User-Agent: hoge" https://[redacted].info/
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 07 Aug 2023 08:14:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/8.0.29
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Link: <https://[redacted].info/index.php?rest_route=/>; rel="https://api.w
X-Powered-By: PleskLin
```

サポート詐欺サイトへとリダイレクト

```
[redacted] --Header "User-Agent: Windows" https://[redacted].info/
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 07 Aug 2023 08:13:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/8.0.29
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Link: <https://[redacted].info/index.php?rest_route=/>; rel="https://api.w
location: https://[redacted].page/
X-Powered-By: PleskLin
```

一方で、『curl』や『wget』といった文字列は例外であることや、プロキシサービスの IP アドレス・VPN サービスの IP アドレスでアクセスした場合は、リダイレクトされないことも確認されました。また、アクセスしたタイミングによってはリダイレクトしない場合もあるため、時間帯によって挙動しない設定がなされていることも考えられます。

このように攻撃者は、IP アドレス、Web ブラウザー情報といった様々な情報を元に、サポート詐欺サイトの表示条件を設定していると考えられます。そのため、広告配信サービスの審査時やアンチウイルス製品とわかる IP アドレスなどは避け、ターゲットに対してピンポイントでサポート詐欺サイトを表示させようと巧みな攻撃を行っていることがわかります。

■もっともらしいランディングページで大手広告配信サービスの審査をすり抜け表示

本事例で閲覧していた Web サイトは、旅行や乗り物関連の国内サイトでした。そのためサポート詐欺サイトに遭遇するのは、外国語などの見慣れない Web サイトに限らないと言えます。また、表示された広告は大手の広告配信サービスを利用していたことから、審査を上手くすり抜けるようなランディングページが作成されていることも分かります。

加えて、サポート詐欺サイトやその URL は次々と自動生成され、短期間で使い捨てることで、ブラックリストによる捕捉を行えないようにするなどの特徴も見られました。

本事例のランディングページへのアクセスログ（i-FILTER/i-FILTER@Cloud のクラウドルックアップされたログ）の集計では、およそ 1 か月半で 4000 アクセス、組織数でみると 800 組織がアクセスを行っていました。ひとつのランディングページでこれだけ広範囲に攻撃が届いています。

ランディングページは他にも多数存在し、さらにそこからリダイレクトするサポート詐欺サイトを考えると膨大な数になるため、遭遇しないような対策は必要ではあるものの、動的に生成されたり使い捨てにされたりという場合は未然に防ぎきれないことが多くあります。

そのため、遭遇した際の対処方法やこのような詐欺手口を知っておくことも重要だと考えられます。

◆参考情報

下記のリンクではサポート詐欺の注意喚起および、表示されてしまった際の対処方法などについて掲載されています。併せてご覧ください。

IPA 独立行政法人 情報処理推進機構　偽のセキュリティ警告に表示された番号に電話をかけないで

マイクロソフト　マイクロソフトのサポートを装った詐欺にご注意ください

◆デジタルアーツ製品「i-FILTER」で出来ること

デジタルアーツでは日々様々な情報をもとにデータの収集を行っており、本事例のような攻撃に用いられる URL は「i-FILTER」のフィルターデータベースへと迅速に配信され、[フィッシング詐欺]や[違法ソフト・反社会行為]カテゴリにてブロックすることが可能です。さらに、フィルターデータベースに反映されていない URL であっても「ホワイト運用」を行うことで、デジタルアーツが安全を確認した URL にのみアクセスを許可し未知の悪性 URL をブロックすることができます。

本事例での調査時において、ランディングページは、フィルターデータベースに反映済みのため[違法ソフト・反社会行為]カテゴリでブロックが可能であり、万が一フィルターデータベースの反映前であっても「ホワイト運用」でブロックすることが可能です。実際に、サポート詐欺サイトは、短時間で使い捨てにされるため[カテゴリ外]ではあるものの、「ホワイト運用」でブロックすることができます。広告についても、[広告・バナー]カテゴリを設定でブロックすることで、広告そのものを表示させないことが可能です。

https://www.daj.jp/bs/i-filter/

●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。

https://www.daj.jp/security_reports/34/

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　　TEL　: 080-8163-0311/ E-mail : press@daj.co.jp