Media Contacts

Mark Meissner	Melinda Reinicker
PCI Security Standards Council	RH-ISAC
+1-202-744-8557	202-507-5710
press@pcisecuritystandards.org	pr@rhisac.org
Twitter @PCISSC	Twitter @RH_ISAC

2019 年 8 月 1 日

ペイメントセキュリティにおけるオンラインスキミングの脅威

PCI セキュリティ・スタンダード・カウンシル(PCI SSC)と「リテール＆ホスピタリティ ISAC (https://rhisac.org/) 」は、緊急な対応を必要とする最新の脅威について共同で注意を呼びかけます

最新の脅威とは何か？

すべての加盟店とサービスプロバイダーはウェブベースまたはオンライン上でのスキミングの脅威が増大していることを認識すべきです。 これらの攻撃は、Sniffer *または JavaScript(JS)Sniffer* として知られ、悪意のあるコードで E コマースのウェブサイトに感染し、検知することは非常に困難です。ウェブサイトが感染すると、取引中に支払いカード情報がスキミングされ、加盟店や消費者は情報が侵害されたことを認識されません。

この脅威はメディアで時々「Magecart」と呼ばれています。「Magecart」は、さまざまなオンラインスキミング攻撃についてハッキンググループを調査しているセキュリティ研究者によって使用される包括的な用語です。この用語は犯罪者グループの攻撃の種類を識別するためにも使用されています。これらの攻撃は 2015 年から活発化しており、国際的な機関に対する相次ぐ高度な攻撃の背後でサイバー攻撃の脅威が進化し続けていることを表しています。

攻撃の手口とは?

これらの脅威アクターは、脆弱な「Plug-In」の悪用、「Brute Force」ログインの試み（資格情報の詰め込み)、フィッシングやその他のソーシャル エンジニアリング手法など、さまざまな方法を駆使してアクセスを試み、悪意のあるコードを注入しようとします。 これらの攻撃は E コマースの ウェブサイトに直接侵入するか、多くの場合、加盟店が委託するサービスプロバイダーのソフトウェアライブラリに侵入します。 これらのサービス プロバイダーは、セキュリティ

に重点を置いておらず、顧客を標的とする潜在的な脅威に焦点を当てていない場合、顧客のリスクを認識していない可能性があります。

サービスプロバイダーのアプリケーションやサービスに対するこれらの攻撃の例には、広告スクリプト、ライブチャット機能、顧客レーティング機能などがあります。侵害されると、これらのサービスプロバイダーのサービスは、攻撃者によって悪意のある JavaScript を標的のウェブサイトに注入するために使用されます。これらのサービスプロバイダーの機能は通常、複数の E コマースサイトで使用されるため、これらの機能のひとつが侵害されると、攻撃者は悪意のある JavaScript の大量配布を通じて多くの ウェブサイトを同時に侵害する可能性があります。

このコードは、多くの場合、被害者がチェックアウト時にペイメントデータを送信することが引き金となります。さまざまな脅威アクターは、請求先住所、氏名、電子メール、電話番号、クレジット カード情報、ユーザー名、パスワードなどを含むさまざまな情報を収集します。悪意のあるコードは、侵害された ウェブサイト上でローカルにペイメントデータをログに記録するか、又は脅威アクターによってコントロールされるコンピュータにリモートで記録します。

最も標的にされるのは誰か?

効果的なセキュリティ対策が実施されていない E コマースの実施・運用は、潜在的に脆弱です。攻撃は E コマースの ウェブサイト、サービス プロバイダー、および ウェブサイトで使用されるアプリケーションを提供する企業などを標的としています。「Magecart」ハッカーや同様の脅威アクターは、異なる標的に対して悪意のあるコードをカスタマイズしたり、パッチが適用されていない ウェブサイト のソフトウェアの脆弱性を悪用するなど、攻撃を進化させ続けています。

さらに、この脅威は持続性があります。 セキュリティ研究者 Willem de Groot (※1)の報告によると、「Magecart」に感染した5つウェブサイトの内 1 つは数日以内に再感染しています。そのため、影響を受けるシステムをクリーニングし、根本的な脆弱性を修正または軽減することも重要です。根本的な脆弱性が解決されない場合、または攻撃者のコードの一部がシステムに残っている場合は、再感染につながる可能性があります。

攻撃検知のためのベストプラクティスにはどのようなものがあるか？

損害をもたらす脅威を事前に検知することは極めて重要です。PCIDSS ではこの検知対応について以下の要件などを提示しています。

- 潜在的なコーディングの脆弱性を特定するためのコードレビュー(PCIDSS 要件 6)

- 脆弱性のセキュリティ評価ツールを使用して ウェブアプリケーションの脆弱性をテストする(PCIDSS 要件 6)
- 匿名もしくは疑わしい行為を特定するためにすべてのシステムコンポーネントにおいてログの監査、そしてログとセキュリティイベントのレビュー(PCIDSS 要件 10)
- ファイル整合性監視または変更検知ソフトウェアの使用(PCIDSS 要件 11)
- 内部および外部のネットワークの脆弱性スキャンの実行(PCIDSS 要件 11)
- セキュリティの弱点を特定するための定期侵入テストの実行(PCIDSS 要件 11)

プロキシログ内に、新たに観察されるドメインのアラートをポスティングすることによりサードパーティの JavaScript ライブラリ上の攻撃にむけた初期段階での偵察だけでなく、将来起こり得るフィッシング攻撃を検知する追加的な道筋をつくることができます。

攻撃防御のベストプラクティスにはどのようなものがあるか？

これらの攻撃への影響を緩和するための最善策はオペレーティングシステムとソフトウェアのセキュリティ対策を施すパッチを含む多層的な防御策の導入です。これに関し、PCIDSS では以下の要件を提示しています。

- 不必要なポート、サービス、機能などの利用を不可能化する。また、業界に適合するシステム強化基準に沿って安全にシステムコンポーネントを設定する(PCIDSS 要件2)
- マルウェア保護を実装し、最新の状態に保つ(PCIDSS 要件5)
- すべてのソフトウェアにセキュリティパッチを適用する(PCIDSS 要件6)
- 安全なコーディングの実装とコードレビューの実施(PCIDSS 要件6)
- 絶対に必要なものだけにアクセスを制限し、デフォルトで他のすべてのアクセスを拒否する(PCIDSS 要件7)
- システムコンポーネントへのすべてのアクセスに強力な認証を使用する(PCIDSS 要件8)
- 侵入を検知し防止するための侵入検知かつ／または侵入防止措置の実施(PCIDSS 要件 11)
- サードパーティサービスプロバイダーを採用する前に適正はデューデリジェンスの実施とサービスプロバイダーの PCIDSS 準拠状況の監視(PCIDSS 要件 12)
- ホスティングサービスプロバイダーによる顧客のホスティング環境とデータ保護のための追加策(PCIDSS Appendix A1)

サードパーティによるサービスとプロダクツはその組織内の PCIDSS スコープ上での影響を特定するためにレビューされるべきです。カード会員データ環境のスコープをホスティングする外部アセットに拡大させるので、組織はカード会員データを受け入れるウエブページ上では外部のアセットを禁止することが推奨されます。 顧客と接するポータルベンダーは組織のスコープの一部としてレビューされるべきサードパーティサービスプロバイダーの一例です。不必要な「Plug-In」とサービスを取り除く、または利用不可化するこことが推奨されます。（PCIDSS 要件2） ウェブサイト上のその他のページで表示されるサードパーティスクリプトがペイメントのページやその他の機微なエリアに確実にアクセスできないようにしておくことが重要です。（PCIDSS 要件2・6）

サードパーティのインフラが安全であること、アクセスが制限されていること、サードパーティスクリプトが信頼できる情報源のみに許可されていることは必須要件です。加盟店はサービスプロバイダにより対応される PCIDSS 要件を明確に特定しサービスプロバイダの委託元が実施すべき責任の範囲が明確に区別されているべきです。組織は E コマース上で悪意のあるコードの注入をブロックできていることを積極的に監視すべきです。外部でホスティングされる JavaScript や CSS(Cascading Style Sheets) でのペイメント受付ページ上で許可されるべきではありません。可能であれば、サードパーティスクリプトからサードパーティスクリプトを内部ホストされたコピーの使用に移行することで悪意のある変更リスクを大きく軽減することができます。サードパーティスクリプトは変更検知のために監視されるべきであり、その変更措置は実行前に潜在的に悪意のあるコードを特定するためにレビューされるべきです。ホワイトリストに明示的に存在しないソースからの JavaScript の実行から準拠ブラウザを制限するために Content Security Policies (CSP) の活用は取り込むべき追加的な保護策でもあります。

組織はサードパーティサービスプロバイダーに対するデューデリジェンスを実施し、そして信頼できるソフトウェアのみを使用すべきです。 ソフトウェアに適正なセキュリティを構築しそのライフサイクルを通じてセキュリティのアップデートのためのサポートを提供するソフトウェアベンダーを選択してください。 サービスプロバイダーは顧客の E コマース環境にリスクを及ぼさない安全なサービスを提供することをコミットされています。

組織はシステムサポートや運用機能だけでなく E コマースシステムへの全てのアクセスに Multi-Factor Authentication (MFA) を導入すべきです。（PCIDSS 要件 8.3）そうすることによって組織は悪意のある脅威アクターからリポジトリへのアクセスの可能性を防止し、インフラをより安全にすることができます。いくつかの単純な緩和策の中には、有効なアンチウィルスでウェブパス内の全てのホストを保護すること、ウェブパス内ですべてのシステムからの外向けのトラフィックを制限すること、そして開発者がサードパーティのコードリポジトリを使わないことを確実にすることなどがあります。

###

PCI セキュリティ・スタンダード・カウンシルについて

PCI セキュリティ・スタンダード・カウンシル(PCI SSC)は業界主導型で柔軟かつ効果的なデータセキュリティ基準を提供することにより、支払いセキュリティを強化するためのグローバルな業界横断的な取り組みをリードしています。企業がサイバー攻撃や侵害を検出、軽減、防止するのに役立つプログラムです。LinkedIn の PCI SSC に接続します。Twitter の@PCISSC で会話に参加してください。PCI パースペクティブ ブログを購読します。

「リテール＆ホスピタリティ ISAC」について

「リテール＆ホスピタリティ ISAC」(RH-ISAC)は、セクター固有のサイバーセキュリティ情報とインテリジェンスを共有するための信頼できるコミュニティとして運営されています。RH-ISAC は、戦略的、運用的、戦術的なレベルで情報セキュリティチームを結び付け、問題や課題に取り組み、プラクティスと洞察を共有し、お互いにベンチマークを行い、より良いセキュリティを構築することを目標としています。コラボレーションを通じて、小売業とホスピタリティ業界を取り入れていきます。RH-ISAC は現在、小売、ホテル、レストラン、ゲーム、その他の消費者向け事業体にサービスを提供しています。詳細については、www.rhisac.org にアクセスし、Twitter でフォローしてください: @RH_ISAC と LinkedIn

---

[1](※1)カタリン・シンパヌ,「Magecart」感染された 5 サイトの内 1 サイトは数日以内に再感染します, 11 月 15, 2018 - 06:30 GMT, https://www.zdnet.com/article/one-in-five-magecart-infected-stores-get-reinfected-within-days/