ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●小学館系ECサイト・三菱電機・日立システムズ…大手企業への不正アクセス相次ぐ

https://www.itmedia.co.jp/news/articles/2011/16/news121.html
https://www.itmedia.co.jp/news/articles/2011/20/news131.html
https://www3.nhk.or.jp/news/html/20201205/k10012747291000.html

このニュースをザックリ言うと･･･

- 11月16日(日本時間)、小学館パブリッシング・サービス社(以下、小学館PS)より、同社運営のECサイト「BOOK SHOP小学館」が不正アクセスを受け、2015年4月13日～2020年6月15日に決済に利用されたクレジットカード情報(カード名義人・番号・有効期限・セキュリティコード等)1036件が流出したと発表されました。

- また11月20日、三菱電機より、同社が利用するクラウドサービスが不正アクセスを受け、取引先の口座情報(銀行口座番号・名義・企業名・所在地・電話番号・代表者名等)8635件が流出したと発表されました。

- 次いで12月4日には、日立システムズ社(以下、日立SYS)より、同社が提供する企業システム運用監視サービス用のネットワークが不正アクセスを受けていたと発表されました。

AUS便りからの所感等

- 小学館PSの事案は6月12日に外部からの指摘を受けて発覚、同15日に決済を停止、既に不正利用も確認されているとのことですが、決済時のフォーム等の改ざんにより、入力内容が奪取されたという、頻出しているパターンと推測されます。

- 三菱電機の事案は11月16日に不正アクセスの検知で発覚、1月に発生していた同社ネットワークへの不正アクセスによる個人情報流出(AUS便り 2020/2/3号参照)とは、別の手口である可能性が高いとのことです。

- 日立SYSの事案は10月8日に発覚、サービスによって同社と常時接続している複数の企業も被害を受けた可能性があるとしています(あるいは顧客企業のネットワークから踏み台にされた可能性も考えられます)が、顧客情報の流出は確認されていないとのことです。

- 三菱電機はクラウドサービスが、日立SYSは独自のネットワークシステムが不正アクセスの被害を受けており、これだけでもどちらで構築したシステムがセキュリティ上より安全か、あるいは危険か、ということは一概には言えないことがわかります。

- また、大手企業がこのように相次いで攻撃を受ける一方、大きく報じられない中小企業の攻撃が今後も多数発生することは容易に想像されますので、今回のそれぞれの事案における詳細な攻撃経路が発表され、UTM等によるネットワークシステムの防御、Webサイトとその周辺での対策、クラウドにおける必要な防御策等、適切な対策をとるための参考となることが望まれます。

ITmedia NEWS

小学館子会社のネット書店に不正アクセス、1000件超のカード情報流出か

小学館パブリッシング・サービス（東京都千代田区）は11月16日、ECサイト「BOOK SHOP小学館」が不正アクセスを受け、1036件のクレジットカード情報が漏えいした疑いがあると発表した。一部は不正利用された可能性もあるという。何者かがサイトの脆弱（ぜいじゃく）性を突いた攻撃を行い、データベースに不正アクセスしたとしている。

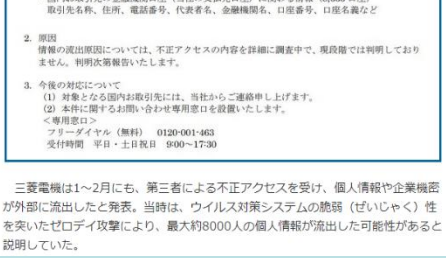
BOOK SHOP小学館では小学館の書籍やDVDなどを販売している。流出の疑いがあるのは、2015年4月13日～20年6月15日に同サイトでクレジットカード決済を行ったユーザーのカード名義人、カード番号、有効期限、セキュリティコードなど。

11月16日時点の「BOOK SHOP小学館」

ITmedia NEWS

三菱電機に不正アクセス、取引先の8635口座の情報が流出

同社は16日までにクラウドサービスへの不審なアクセスを発見。問題のアクセスを遮断し、流出の原因と被害状況の調査を始めた。20日までの調査で、国内の取引先企業の銀行口座番号や名義、企業名、所在地、電話番号、代表者名などが流出していることが分かった。



流出が判明した国内お取引先に関する情報と今後の対応について

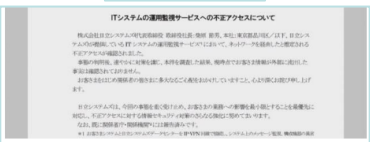
1. 流出が判明した国内お取引先に関する情報
11 月 20 日現在、判明している外部に流出した情報のうち、金融機関口座に関わる内容は次のとおりです。
・国内お取引先の金融機関口座（当社の支払先口座）に関わる情報（8,635 口座）
取引先名称、住所、電話番号、代表者名、金融機関名、口座番号、口座名義など

2. 原因
情報の流出原因については、不正アクセスの内容を詳細に調査中で、現段階では判明しておりません。判明次第報告いたします。

3. 今後の対応について
（1）対象となる国内お取引先には、当社から個別にご連絡申し上げます。
（2）本件に関するお問い合わせ専用窓口を設置いたします。
＜専用窓口＞
フリーダイヤル（無料） 0120-001-463
受付時間 平日・土日祝日 9:00～17:30

三菱電機は1～2月にも、第三者による不正アクセスを受け、個人情報や企業機密が外部に流出したと発表。当時は、ウイルス対策システムの脆弱（ぜいじゃく）性を突いたゼロデイ攻撃により、最大約8000人の個人情報が流出した可能性があると説明していた。

NHK



日立システムズに不正アクセス 顧客企業に被害のおそれも

2020年12月5日 10時17分　サイバー攻撃

シェアする

企業のサーバーやネットワークを監視するサービスを提供している日立システムズは、自社のシステムが不正アクセスを受けたことで、常時接続している複数の顧客の企業も不正アクセスを受けたおそれがあるとして、警察に相談して対応を進めています。

日立システムズによりますと、ことし10月8日に、顧客の企業などのサーバーやネットワークが順調に動いているかを監視するサービスのシステムが、不正アクセスを受けたことが確認されたということです。

● 11月のフィッシング報告件数、3万件突破…対策協議会発表

https://www.antiphishing.jp/report/monthly/202011.html

このニュースをザックリ言うと・・・

- 12月3日(日本時間)、フィッシング対策協議会より、11月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 11月度の報告件数は30,967件で、10月度(https://www.antiphishing.jp/report/monthly/202010.html)の28,727件より2,240件増加し、3万件の大台を突破しています。

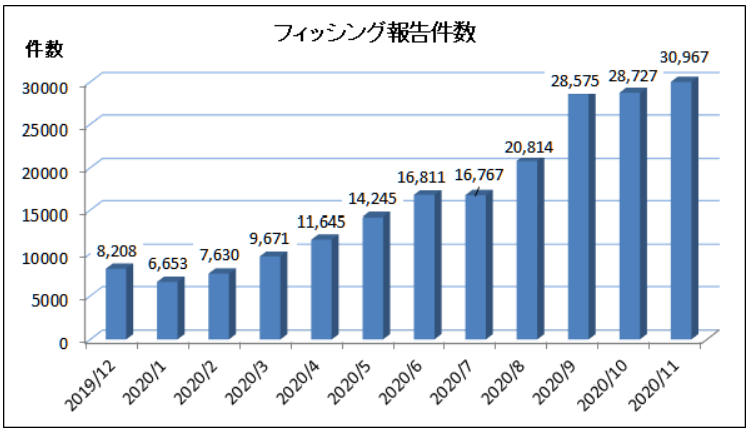
- Amazonを騙ったフィッシングの報告が全体の62.3%と最も多く、三井住友カード・楽天・MyJCB・アプラス(新生銀行カード)を加えたものが報告全体の約90.1%を占めていたとのことです。

AUS便りからの所感

- Amazonのフィッシングについては11月下旬にSMSによるいわゆる「スミッシング」への注意喚起が出されています(https://www.antiphishing.jp/news/alert/amazon_20201127.html)が、スミッシングはこれまでの宅配便の不在通知の他、楽天市場からの発送通知を騙るものも確認されているとのことです。

- 他にも国税庁を騙るフィッシングも同月下旬に報告されている(https://www.antiphishing.jp/news/alert/nta_20201120.html)等、多く報告されているブランド以外の企業や機関も当然ながら新たなフィッシングの対象となっているため、随時の情報収集はもちろん、公式サイトへはブックマークに登録したURLからアクセスする等の防御策を常にとっていくことが肝要です。

フィッシング対策協議会
Council of Anti-Phishing Japan



● 「Edge」の拡張機能ライブラリに広告を注入するものが混入…Microsoftが18種類を駆除

https://forest.watch.impress.co.jp/docs/news/1292580.html

このニュースをザックリ言うと・・・

- 11月25日(現地時間)、米Microsoftより、同社公式のEdgeブラウザー用拡張機能ライブラリから悪意のある拡張18種類を削除したと発表されました。

- 削除された拡張は、Greasemonkeyや各種VPN接続用等、Edge用には公式に提供されていない既存の拡張の偽物だったとされ、インストールにより、ブラウザーでの検索時に広告リンクが不正に挿入されるようになっていたとのことです。

- 掲示板サイトRedditで問題が報告され、Microsoftのスタッフも同じRedditのスレッド上で削除を報告した上で、該当する拡張をアンインストールするよう、またアンインストールや無効化しても広告が表示される場合は、現在インストールしている拡張機能のリストを添付してRedditに返信するよう呼び掛けています。

AUS便りからの所感

Impress Watch

- 問題となった偽拡張のうち、例えばGreasemonkeyはFirefoxでしか提供されておらず、同様の拡張であるTampermonkeyがChromeやEdge等で提供されています(それぞれの拡張の公式サイトで確認可能)。

- EdgeではGoogle公式の拡張ストアからのChrome用拡張機能のインストールにも対応していますが、こちらでも不正な行動をとる拡張機能がアップロードされ、削除される事態が時々発生しており、またそれまで問題のなかった拡張について、第三者に売却される等により、悪意のあるコードが挿入されるようになったケースもあります(AUS便り2020/11/02号参照)。

- Webブラウザーへの拡張機能のインストールは、時にはWebブラウザーのあらゆる機能を(一応は事前の警告、了承の上で)拡張機能に引き渡すことになるため、ネット上の評判や報告をもとに必要最低限の拡張をインストールし、問題となった拡張は即座にアンインストールするよう心がけましょう。


「Edge」の拡張機能ライブラリに広告を注入するものが混入
～Microsoftが18種類を駆除
「Greasemonkey」や「The Great Suspender」など有名なものも
- NordVPN
- Adguard VPN
- TunnelBear VPN
- The Great Suspender
- Floating Player - Picture-in-Picture Mode
- Ublock Adblock Plus
- Go Back With Backspace
- Wayback Machine
- friGate CDN - smooth access to websites
- Greasemonkey
- Full Page Screenshot
- One Click URL Shortener
- Guru Cleaner - cache and history cleaner
- Grammar and Spelling Checker
- Enable Right Click
- FNAF
- Night Shift Redux
- Old Layout for Facebook