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。

●パスワードが総当たり攻撃で破られリモートデスクトップ侵入…勤怠・人事システムにランサムウェア攻撃

https://www.itmedia.co.jp/news/articles/2206/02/news106.html
https://www.viax.co.jp/pdf/20220601.pdf

このニュースをザックリ言うと･･･

- 6月1日(日本時間)、図書館受託運営・DM発送事業等を手掛けるヴィアックス社より、同社勤怠・人事給与管理システムがランサムウェアに感染、同社従業員や家族の個人情報等データが暗号化されたと発表されました。

- 被害を受けたのは、当該システムに登録されていた同社従業員1,872人分、退職者2,167人分、扶養者424人分および世帯主2,423人分の個人情報(氏名・生年月日・住所・電話番号・メールアドレス等)、勤怠システムデータ(ログインパスワード・出退勤打刻データ・各種申請履歴等)および支払い給与データ(銀行口座情報・給与額その他各種金額)とされています。

- ランサムウェア感染は外部からの不正アクセスによるもので、4月1日夜にデータの暗号化が行われ、翌2日朝に勤怠システムにアクセスできないとの連絡があったことから発覚したものとされています。

AUS便りからの所感等

- 発表によれば、攻撃者による身代金の要求もあった一方で、データの形式や運用上から、単体で直ちに内容を閲覧可能なものではなく、また取引先等に関するデータはサーバー上には含まれていなかったとのことです。

- データセンターのDMZ上にあった勤怠システムWebサーバーのメンテナンス上の都合により、外部からリモートデスクトップ接続が可能な設定になっていたところに、攻撃者が接続パスワードの総当たり攻撃による推測に成功したことにより、サーバーに侵入され、ランサムウェアを送り込まれたものとされています。

- 発表を率直に受け取る限り、今回の事例において、侵入～ランサムウェア感染等が発生した場合のデータ流出・破壊の恐れへの備えについては適宜に行われていたものと考えられ、逆に外部からサーバー管理のためにアクセスする手順が限定されていることを理由に先のような備えを疎かにしていたり、外部からの侵入への対策のみに重点を置いた防御策をとっていたりした場合、「蟻の一穴」の破れが致命的な損害をもたらすことに注意し、システム・データを適切に保護できる体制となっているかの確認・見直しを確実に行うことが肝要です。

ITmedia NEWS

リモートデスクトップ経由で侵入か　人事システムにランサムウェア攻撃　社員の給与情報など暗号化

2022年06月02日 12時33分 公開　　[岡田有花，ITmedia]

図書館の受託運営やDM発送事業などを手掛けるヴィアックス（東京都中野区）は6月1日、同社の勤怠・人事給与管理システムがランサムウェア攻撃を受け、従業員1871人分、退職者2167人分などの情報が暗号化されたと発表した。攻撃者に身代金を要求されたという。

データセンター内のDMZ（DeMilitarized Zone）にあるシステムのWebサーバメンテナンス時、外部からWebサーバへのリモートデスクトップ接続が可能になっていた。このパスワードが総当たり攻撃により推測されて不正侵入を受け、ランサムウェアを実行された可能性があるという。

●5月度のフィッシング報告件数は88,132件…サイト件数過去最高更新

https://www.antiphishing.jp/report/monthly/202205.html

このニュースをザックリ言うと・・・

- 6月3日(日本時間)、フィッシング対策協議会より、5月に寄せられたフィッシング報告状況が発表されました。

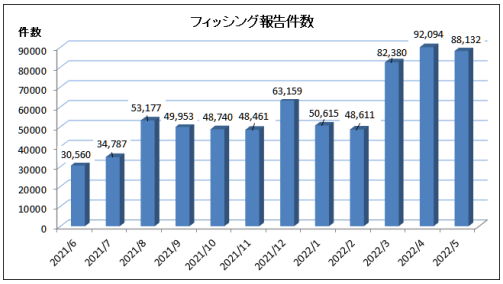
- 5月度の報告件数は88,132件で、4月度(https://www.antiphishing.jp/report/monthly/202204.html)に過去最高の記録となった92,094件からは3,962件減少するも、歴代2位の件数となっています。

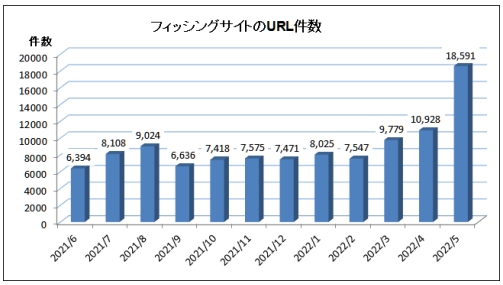
- フィッシングサイトのURL件数は18,591件で、4月度の10,928件から7,663件の急増となり、過去最高を引き続き更新しています(ただしIPアドレスが同一のものが多いとされています)。

-悪用されたブランド件数も同じく過去最高の110件(4月度 101件)で、報告全体に対するブランドの割合については、先月度と同様auおよびau PAYが約21.7%と最も多く、これとAmazon、えきねっと(JR東日本)の3ブランドで併せて約49.5%を占める結果となった模様です。

AUS便りからの所感

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





- 月々のフィッシング報告件数は、2019年1月～2020年10月はほぼ右肩上がりの状態、2020年11月に3万件を突破してからは2021年7月まで4万件台とのジグザク状態、2021年8月に5万件台突破後は今年2月まで48,000件台以上を維持、そして同3月以降は8万件台を維持と、その水準が1年以内のスパンで上昇し続けています。

- 同協議会の調査用メールアドレス宛に届いたフィッシングメールについては、メール差出人として正規のメールアドレスを不正に使用する「なりすまし」メールが約69.5%となっている一方、受信検知・防止機構のうちSPF(送信ドメイン認証)において「hardfail(認証失敗により廃棄)」と検出できたメールは約7.1%(4月度 約37.1%)と激減、「softfail(認証は失敗したがメールは受信する)」と検出したメールが約49.7%(4月度 約31.7%)と増加傾向にあり、設定が弱いドメイン名(ブランド)を狙った可能性を示唆するとともに、既にSPFのみを導入している組織においては今後DMARCの追加導入を検討する段階になりつつあるようにも見受けられます。

- 自組織が差出人となっているメールの受信者を保護するためにもSPF・DMARCといった機構の導入は重要となりますが、PCのマルウェア感染等によるフィッシングメールの不正配信を防ぐという観点から、PC・UTMあるいはメールサーバー側におけるメールのウイルススキャンやその他のソリューションの導入も忘れてはいけないでしょう。

● Webブラウザのトラフィック乗っ取るマルウェア「ChromeLoader」の活動が活発化

https://news.mynavi.jp/techplus/article/20220529-2352899/
https://redcanary.com/blog/chromeloader/

このニュースをザックリ言うと・・・

- 5月25日(現地時間)、セキュリティベンダーの米Red Canary社より、「ChromeLoader」と呼ばれるマルウェアに関する注意喚起が出されています。

- ChromeLoaderは海賊版のゲームアプリや映画・テレビ番組を装った実行ファイルを介してWebブラウザーの拡張機能としてインストールされ、ブラウザーの設定を変更し、検索クエリを乗っ取ったり、トラフィックを不正に広告サイトにリダイレクトしたりといった活動をとるとされています。

- 同社では、このような形をとるマルウェアは通常直接的な被害は比較的小さいとしている一方、不正なPowerShellスクリプトを実行することにより、他の不正な拡張機能をインストールする挙動をもとっており、より大きな脅威の足掛かりとして使われる可能性があるとして注意を促しています。

AUS便りからの所感

TECHI Powered by マイナビニュース


Webブラウザのトラフィック乗っ取るマルウェア
「ChromeLoader」の活動が活発化
2022/05/29 12:06
米Red Canaryのセキュリティチームが5月25日（現地時間）、公式ブログ「ChromeLoader: a pushy malvertiser」において、「ChromeLoader」と呼ばれるマルウェアの活動が活発化している兆しがあると警告している。ChromeLoaderは被害者のWebブラウザ設定を変更してトラフィックを不正に広告サイトにリダイレクトするタイプのマルウェアで、2022年の初め頃に確認された。

- ChromeLoaderは今年初めに存在が確認され、(名前の通り)元々はChromeブラウザーを標的としていましたが、4月下旬頃からはSafariブラウザーも標的に加えたmacOSバージョンの存在も確認されているとのことです。

- 同社の記事では、BitTorrent等からダウンロードされる不審なゲームアプリのISOファイルにChromeLoaderのインストーラーが含まれている様子が挙げられており、有償ソフトウェア等を無償で不正に入手しようとするユーザーをこのようなファイルによってマルウェア感染の格好のターゲットとしていることにくれぐれも留意すべきでしょう。

- この他、Webブラウザーにインストールされた拡張機能が不正にブラウザーの権限を要求した場合、これを許可してしまうことにより、理論上Webブラウザーのあらゆる機能を拡張機能に引き渡すことになりますので、必要最低限の拡張機能のみインストール・有効化すること、権限を要求するダイアログの表示に注意し、身に覚えのない拡張機能が入っていれば速やかにアンインストールすることを心掛けてください。