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。

●4月度フィッシング報告件数は92,094件…過去最高をさらに更新

https://www.antiphishing.jp/report/monthly/202204.html

このニュースをザックリ言うと･･･

- 5月9日(日本時間)、フィッシング対策協議会より、4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。

- 4月度の報告件数は92,094件で、2月度(https://www.antiphishing.jp/report/monthly/202203.html)の82,380件から9,714件増加しており、フィッシングサイトのURL件数も10,928件(3月度 9,779件)と、それぞれ過去最高だった先月度をさらに更新しています。

- 悪用されたブランド件数も101件(3月度 105件)と依然高い水準で、報告全体に対するブランドの割合については、auおよびau PAYが先月度から約4.5倍増加して約22.4%と最も多くなり、これとメルカリ、Amazonの3ブランドがそれぞれ10,000件以上報告され、併せて約56.5%を占める結果となった模様です。

AUS便りからの所感等

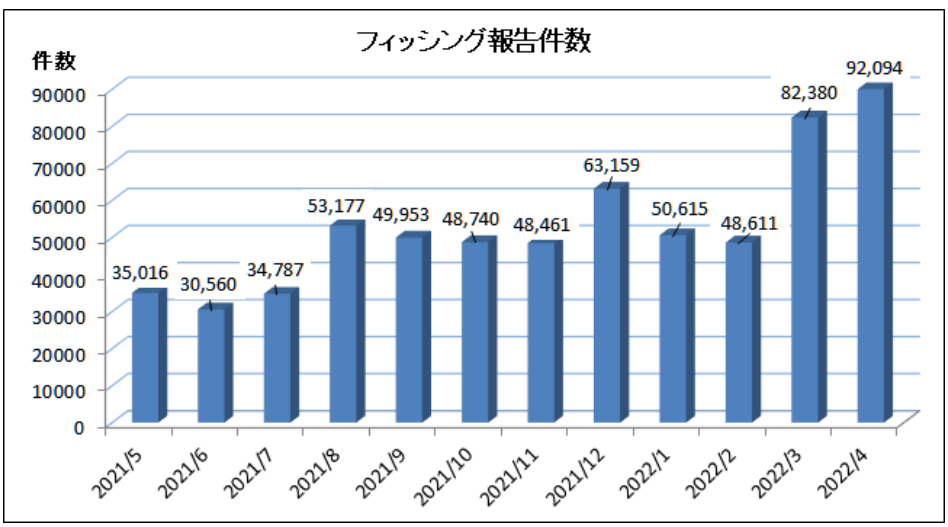
- 2021年8月以降半年近く5万件前後での推移(12月のみ6万件を突破)から一転して8万件台に急増した3月度の流れが続く形となっており、5月度の報告が10万件を突破する可能性は十分あると思われます。

- これまで最も悪用されるブランドだったAmazonが今回au等の後塵を拝することになった一方、メルカリについては4月18日から月末にかけてフィッシングメールが減少、3月度に報告全体の21.1%を占めたJRグループも4月度には11.1%になる等、どのブランドが主に悪用されるかについても流動的となっている模様です。

- 5月6日には、大胆にも同協議会を騙りながら、3Dセキュアのアップグレードの名目でクレジットカード情報の入力を求めるという荒唐無稽なフィッシングの事例が報告されました(https://www.antiphishing.jp/news/alert/apc_20220506.html)が、世に出回るフィッシングは、こういった明らかにおかしい文面のものから、本物のサービスから送られたメールの文面を借用するものまで様々であり、同協議会やサービス各社あるいはソーシャルネットワークでの報告がないか随時確認する癖をつけるとともに、利用するサービスへのアクセスは予め登録したブックマークから行う等の自衛策をとることが肝要です。

- この他、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おいて、差出人として正規のメールアドレス(ドメイン)を使用したなりすましメールの割合が増えているという報告もあり、なりすましメールでないことを証明するための機構であるSPF(およびDMARC・BIMI等)のメールサーバー側での導入がフィッシングメールの根絶には重要な対策となるでしょう。

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



●Emotetに拡張子「.lnk」のショートカット添付、クリックで感染の恐れ

https://www.itmedia.co.jp/news/articles/2204/26/news169.html
https://www.jpcert.or.jp/at/2022/at220006.html

このニュースをザックリ言うと・・・

- 4月26日(日本時間)、JPCERT/CCより、マルウェア「Emotet」が新たな攻撃の手口をとっていることが確認されたとして注意喚起が出されています。

- 同25日頃より、拡張子が「.lnk」のショートカットファイルあるいはそれを含むパスワード付きZIPファイルを添付したメールが新たに観測されており、ファイルを実行すると、PowerShellスクリプトファイルが生成、実行され、Emotetの感染に至るとしています。

- JPCERT/CCでは、WordやExcelのマクロやコンテンツ有効化を必要としない方法での感染を目的とした手法の変化である可能性があるとし、引き続き、不審なメールの添付ファイルやリンクを開かないよう呼び掛けています。

AUS便りからの所感

- ショートカットファイルは、特にPC上に展開した際に、通常「.lnk」拡張子が表示されず、他の形式のファイルに偽装する形がよくとられることに注意が必要です。

- 上記の発表に先駆けて、JPCERT/CCが提供するEmotet感染チェックツール「Emocheck」がバージョン2.2に更新されていますが、過去のバージョンでチェックした際に感染が検知されなかったケースも有り得るため、更新されるたびにダウンロード・実行を行う習慣をつけることを推奨致します。

- 「不審なWord・Excelファイルを開いたり、マクロを有効化したりしない限り、マルウェアに感染することはない」といった先入観に囚われることなく、随時情報の追加が行われているJPCERT/CCのEmotet注意喚起ページをはじめ常に情報収集を行い、刻々と変化する攻撃手法について理解しつつ行動することが肝要です。


Emotetに新たな攻撃手段　添付されたショートカットファイルに注意

2022年04月26日 20時00分 公開　[ITmedia]

印刷　246　Share　B!　39

JPCERT/CCは4月26日、マルウェア「Emotet」に感染するメールの添付ファイルに、新たにショートカットファイルを使ったものが見つかったと発表した。ファイルを実行すると不正なスクリプトが実行され、Emotetに感染する。

更新: 2022年4月26日追記

2022年4月25日頃より、Emotetの感染に至るメールとして、ショートカットファイル（LNKファイル）あるいはそれを含むパスワード付きZipファイルを添付したメールが新たに観測されています。ファイルを実行すると、スクリプトファイルが生成、実行され、Emotetの感染に至ります。

WordやExcelのマクロやコンテンツ有効化を必要としない方法での感染を目的とした手法の変化である可能性があります。引き続き、不審なメールの添付ファイルやリンクは開かぬようご注意ください。

●改正個人情報保護法、4月より施行…漏えい被害者本人への通知義務も

https://www.ppc.go.jp/news/kaiseihogohou_checkpoint/

このニュースをザックリ言うと・・・

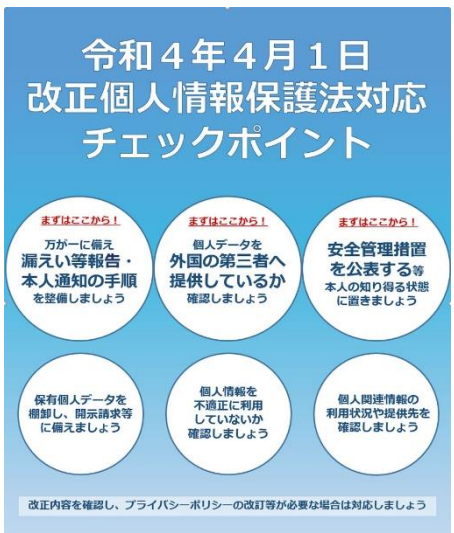
- 4月1日(日本時間)、改正個人情報保護法(2020年公布)が施行されました。

- 2003年施行の同法の改正は2015年以来となり、事業者に対し追加された責務として、個人情報漏洩時の個人情報保護委員会への報告および本人への通知が義務化された(通知が困難な場合は、特設の問い合わせ窓口などを設けた上で免除される)ことが大きな変更点の一つに挙げられます。

- また、本人に対する権利保護に関して、保有個人データの利用・第三者提供の停止および消去の請求できるケースの拡充、個人情報の第三者提供の記録に対する開示請求権(そのため提供側・受取側とも流通過程を明確に記録する必要あり)の追加等が行われた他、法令・措置命令等違反のペナルティも厳罰化されています。

- 施行に先立つ2月18日、個人情報保護委員会からは、改正法に関する6つのチェックポイントへの対応を呼び掛けるチラシが公開され、特に「まずはここから」対応してほしいとする3つのポイントとして「漏えい等報告・本人通知の手順の整備」「個人データを外国の第三者へ提供しているかの確認」「個人情報に対する安全管理措置を本人の知り得るよう公表する」を挙げています。

PPC 個人情報保護委員会



AUS便りからの所感

- 前述のような事業者側への責務・規制の強化等があった一方で、データ利活用の推進も図られ、例えば個人情報を個人が特定できないよう加工した情報について元の個人情報と同様の管理義務が課せられていたものが新たに「仮名加工情報」とされ、管理義務が緩和される等も行われています。

- 顧客情報をはじめ外部より提供を受けたものから、従業員のマイナンバー等に至るまで、会社で保管している多くの個人情報はサイバー犯罪の標的となり得るものであり、情報漏洩の多くは不正アクセスが原因で起こるものですが、その足掛かりとしてマルウェアに感染させられるケースも多いです。

- 守るべき情報を洗い出し、その情報がどこから漏れるのかを理解した上で、アンチウイルスやUTMにより、外部からの攻撃の遮断、あるいは内部に侵入した攻撃者やマルウェアが外部へ情報を送信したり、指令を受けるために外部サーバーへアクセスしたりするのを食い止めるよう対策を行うことが重要です。