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。

●三井住友銀行等システム関連のソースコード、GitHubにアップロードされる

https://www.itmedia.co.jp/news/articles/2101/29/news107.html

このニュースをザックリ言うと･･･

- 1月28日(日本時間)頃、Twitter上で、委託業務で開発したソースコードをコード共有サービス「GitHub」にアップロードしたとする投稿があり、そのソースコードに三井住友銀行(以下SMBC)等大手企業のシステムに関連するものが含まれている可能性が指摘される等の事態となりました。

- 同29日、SMBCより、当該ソースコードは同行内システムで使用されていたものと一致したものの、顧客情報やセキュリティに影響を与える情報は含まれていないと発表されました。

- その後、アップロードされていたソースコードには、SMBC以外にもNECやNTTデータ子会社等、複数社からの業務委託によるコードが含まれていたと報じられています。

AUS便りからの所感等

- GitHubにアップロードされたソースコードの多くはシステムの核心に関わるようなものではない雑多なコードの断片だったとみられ、その内容よりも、業務で作成したコードを外部に持ち出す行為についてが議論点となっているようです。

- GitHubをはじめ、企業・組織等での利用も想定した機能も提供されているネットサービスもあるにも拘らず、今回の事件によって、業務での利用が十把一からげに禁止されたり、サービスへのアクセスの遮断が行われる傾向が進むことは大いに懸念されるところであり、一般社団法人コンピュータソフトウェア協会(CSAJ)からは「外部のクラウドサービス利用の萎縮につながらないよう、各社の節度ある情報セキュリティ設計を要請する」という声明や、今回のような事案への具体的な対策等が発表されています(https://internet.watch.impress.co.jp/docs/yajiuma/1304122.html)。

- 安易な「GitHubを使わない」というルール付けやアクセス遮断に依存するのではなく、場合によっては企業で正式に有償サービス等の契約を選択し、管理側・利用側ともに安全で適切にサービスを利用するよう教育が行われることが望ましいでしょう。

ITmedia NEWS

三井住友銀行などのソースコードが流出 “年収診断”したさにGitHubに公開か【追記あり】

2021年01月29日 14時29分 公開　[樋口隆充，ITmedia]

印刷　見る　Share　B! 76

三井住友銀行（SMBC）は1月29日、同行のシステムに関連するソースコードが外部のWebサイト上に無断で公開されていたと明らかにした。委託先の企業に勤務するSE（システムエンジニア）から流出したとみられるものの、顧客情報の流出はなく、セキュリティに影響はないとしている。

ソースコードが流出したSMBC（出典：公式Facebook）

委託先のSEとみられる人物が、自身の書いたソースコードから年収を診断できるWebサービスを利用するため、SMBCなどから委託を受けて開発したコードをソースコード共有サービス「GitHub」に公開したのが原因。

●1月のフィッシング報告件数、先月より急増で4万件突破…対策協議会発表

https://www.antiphishing.jp/report/monthly/202101.html

このニュースをザックリ言うと・・・

- 2月3日(日本時間)、フィッシング対策協議会より、1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。

- 1月度の報告件数は43,972件で、2020年12月度(https://www.antiphishing.jp/report/monthly/202012.html)の32,171件から11,801件の増加となり、一気に4万件を突破しています。

- フィッシングメールに悪用されたブランドとしてはAmazonが全体の61.4%と最も多く、これに三井住友カード・楽天・MyJCB・三菱UFJニコスを合わせた5ブランドが報告全体の約88.6%を占めていたとのことです(また、フィッシングに悪用されたブランド件数67件のうち、クレジット・信販系が20、金融機関系が8となっています)。

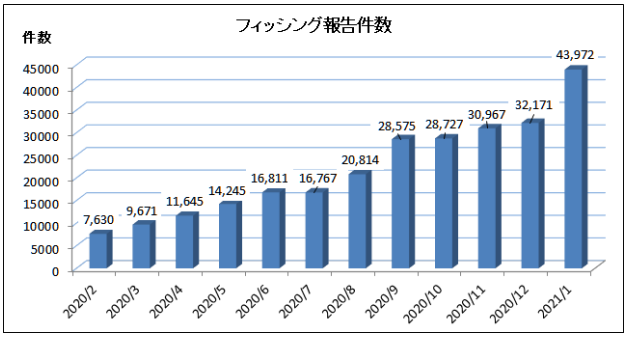
AUS便りからの所感

- 2020年4月度に1万件を突破(11,645件)後、4か月後の8月度に2万件越え(20,814件)、3か月後の11月度に3万件越え(30,967件)、そして2か月後の今回と、大台を突破する間隔が徐々に短くなっている他、今回は8月度→9月度(28,575件)において前月度から7,761件増加となったのをさらに凌ぐ急増を見せており、これが一時的な増加か、同様の増加が以後も続くかは2月度以降の動向次第とは思われるものの、決して警戒を怠るべきではないでしょう。

- 12月度と同様、これまで悪用されていなかったブランドがターゲットとなる傾向が続いているとみられ、例えば同協議会からはジャックス・エムアイカード等を騙るフィッシングへの注意喚起が出されています。

- フィッシングの手口に関して大きな変動があったわけではないものの、今後も不審なメールやショートメッセージの受信時に慎重に行動できるよう、サービスや企業・組織の公式サイトあるいはSNS等から随時情報を収集する、利用しているサービスの公式サイトへブックマークからアクセスする、等の防御策をとることを強く推奨致します。

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



● 「タブと空白だけで記述された」マルウェアが発見される

https://news.mynavi.jp/article/20210207-1691845/

このニュースをザックリ言うと・・・

- 2月2日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、PHPスクリプト内に人間には見えないようタブと空白だけで記述されたマルウェアを発見したと発表されました。

- マルウェアはlisence.phpというテキストファイルに偽装し、PHPコメントでライセンスの条文が書かれていましたが、途中でコメントを区切る形でPHPのコードが挿入され、末尾にタブと空白でマルウェアのコードが仕込まれていたとのことです。

- Sucuri社では以前にも、CSSファイルにタブ・空白・改行で構成された見えないコードが仕込まれていることを発見したとのことです。

AUS便りからの所感

TECH+ Powered by マイナビニュース

- 限られた文字だけを用いて記述するアプローチをとるプログラミング言語として、8通りの記号だけで記述するBrainf**kや、やはりタブ・空白・改行だけで記述するWhitespaceといったものが知られています。

- 攻撃者がマルウェアを作成する際、人間や解析プログラムによる解析を困難にするためコードの隠ぺいや難読化を行うことがよくあり、今回はWhitespaceを用いたものと考えられます。

- このように隠された不審なコードを人間の目で見つけ出すことは不可能に近く、そういった手口へ対応している、あるいは生成・実行されたマルウェアがとる不審な挙動をもとに検知する「振る舞い検知」を行うようなアンチウイルスやUTMによる防御は今後さらに必要不可欠となるでしょう。