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。

● 2021年に報告されたフィッシングサイトのドメイン名、「.jp」が3位に…JPCERT/CC発表

https://blogs.jpcert.or.jp/ja/2022/04/phishing2021.html

このニュースをザックリ言うと・・・

- 4月25日(日本時間)、JPCERT/CCの公式ブログにおいて、2021年に報告されたフィッシングサイトに関するインシデント23,104件についての傾向が発表されました。

- 月間での報告件数は1～7月まで2,000件未満でしたが、AmazonやETC利用照会を騙るサイトの報告が増加したことにより、8月に2,469件を記録して以降は2,000件を超える傾向が続いているとのことです。

- フィッシングサイトに使用されたドメイン名をgTLD(.com，.org，.net等サービスの分野毎)とccTLD(.jp，.uk，.cn等国毎)とでの内訳でみたところ、gTLDでは「.org」42%、「.com」26%(以下「.xyz」「.top」「.shop」)が上位に入り、ccTLDでは「.cn」69%、「.cc」7%に次いで、3位が「.jp」の4%(以下「.vu」「.ga」)となっています。

AUS便りからの所感等

- .jpドメインのフィッシングサイトの傾向として、フィッシングのためにドメイン名が取得されたケースの他に、正規のWebサイトが不正アクセスを受け改ざんされたケースも散見されたとしており、最も多く使われる.cnドメインに比べればまだ割合は低いものの、.jpドメインが使われる割合は今後より増えていき、ユーザーがフィッシングに引っかかる確率もその分増えていくことが予想されます。

- この他、フィッシングサイトにおいて使用されるドメイン名～サブドメイン名を含むFQDNの特徴や、実際に使われたドメイン名の一例なども挙げられており、日本国内をターゲットとしたフィッシングの傾向をつかむ参考にするには有用でしょう。

- ブラウザー・メーラーあるいはアンチウイルス・UTMのアンチフィッシング機能を確実に有効にした上で、フィッシングサイトやメールで表示されるドメイン名はすべからずすぐにフィッシングとわかるものであるといった確信のもとで行動するのではなく、そういったメールを受け取ったらネット上での報告がないか確認すること、あるいは実際に使用するサービスへは予めブックマーク等に登録してアクセスすることを心掛けるべきです。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

中井 尚子（Shoko Nakai） 2022/04/25

2021年に報告されたフィッシングサイトの傾向と利用されたドメインについて

JPCERT/CCでは、2021年に44,242件のインシデント報告が寄せられ、そのうちフィッシングサイトに関するインシデント件数は、23,104件でした。本ブログでは、JPCERT/CCに報告されたフィッシングサイトの情報をもとに、報告件数の推移やかたられたブランドの業種別割合、フィッシングサイトに利用されたドメインの傾向について解説します。

なお、この記事で示すフィッシングサイトは、実在するブランドをかたり、認証情報などの窃取を狙っている不正なWebサイトを指します。また、報告を受けたフィッシングサイトは、メール以外にもSMS経由で拡散されているものも含まれます。

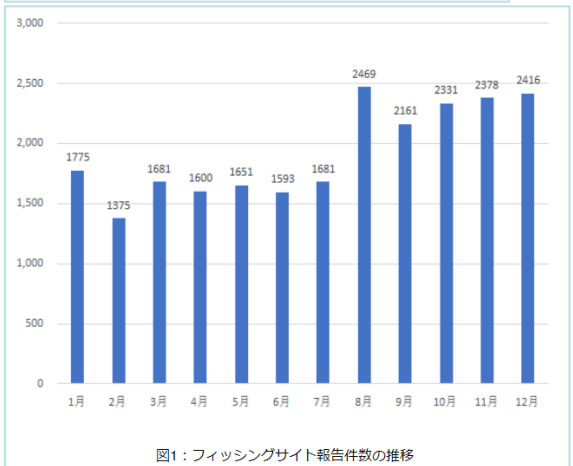

図1：フィッシングサイト報告件数の推移

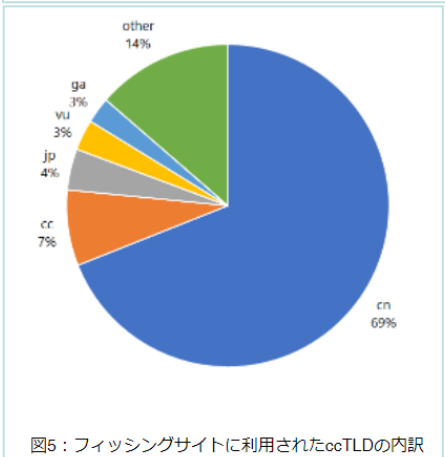

図5：フィッシングサイトに利用されたccTLDの内訳

●Javaのセキュリティアップデートがリリース…バージョン15以降にてECDSA証明書の処理に脆弱性

https://forest.watch.impress.co.jp/docs/news/1404535.html
https://www.jpcert.or.jp/at/2022/at220012.html

このニュースをザックリ言うと・・・

- 4月20日(日本時間)、米Oracle社より、Java SE(以下Java)のセキュリティアップデートであるバージョン18.0.1, 17.0.3, 11.0.15および8u331がリリースされました。

- 最大7件の脆弱性が修正されていますが、うち18.0.1および17.0.3で修正された、ECDSA証明書の検証に関する脆弱性(CVE-2022-21449)が特に注意すべきものとされています。

- 悪用により、細工された偽のECDSA証明書が検証を通過する可能性があり、JPCERT/CC等から注意喚起が出されています。

AUS便りからの所感

- ECDSA証明書に関する脆弱性はJavaバージョン15以降に存在するもので、Javaプログラムが不正なサーバー証明書を持つ偽のWebサーバーへ誘導される、あるいはクライアント証明書によるアクセス制限等を行う場面で不正なクライアント証明書でのアクセス等を許可してしまう、といったシナリオが想定されます。

- 当該脆弱性の影響を受けるか否かに拘わらず、Javaバージョン9～10, 12～16は既にサポートが終了しており、他にも脆弱性は存在することから、もしもこれらのバージョンを使用している場合はLTS(長期サポートが提供)であるバージョン11や17への移行を行うようにしてください。

- JavaのセキュリティアップデートはOracle社各製品に対し3ヶ月に一度リリースされる「Critical Patch Update」の一環ですが、修正された脆弱性は複数のベンダーが提供する(OpenJDKベースの)Javaディストリビューションにも影響するので、それぞれでリリースされるアップデートを適用し、確実に最新バージョンに保つよう注意してください(本家Oracleからのリリースより数日かかる傾向があるため、最新バージョンがリリースされたかの確認は必須です)。

Impress Watch

「Java」に署名検証がフリーパスになってしまう危険な脆弱性 ～影響は計り知れず

2022年4月の「Critical Patch Update」で対策済み、最新版への更新を

樽井 秀人　2022年4月21日 12:35

先日の「Critical Patch Update」で修正された「Java」の脆弱性「CVE-2022-21449」は、悪用された場合の影響が大きいようだ。ECDSA（楕円曲線デジタル署名アルゴリズム）の実装に欠陥があり、不正なデジタル署名の検証が誤って成功してしまう。ForgeRock社のセキュリティ研究家は、SFテレビドラマ『ドクター・フー』（Doctor Who）に登場する架空の道具「サイキックペーパー」（望むままの内容を表示できる白紙。フリーパスの身分証明書として利用できる）になぞらえて、その危険性を指摘している。

●ゴールデンウィークにおける情報セキュリティの注意喚起、IPA・METI等より発表

https://www.ipa.go.jp/security/topics/alert20220420.html
https://www.meti.go.jp/press/2022/04/20220425003/20220425003.html

このニュースをザックリ言うと・・・

- 4月20日(日本時間)にIPAより、同25日には経済産業省(METI)・総務省・警察庁および内閣官房内閣サイバーセキュリティセンター(NISC)の連名で、ゴールデンウィークを迎えるにあたっての、情報セキュリティに関する注意喚起が出されています。

- 企業・組織によっては、この時期に多くの人が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

- IPAは毎年のこの時期および夏季・冬季休暇の時期に注意喚起を行っており(https://www.ipa.go.jp/security/measures/vacation.html)、今後JPCERT/CC等からも同様の注意喚起が出される場合があります。

AUS便りからの所感

- 注意喚起の内容は、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっています。

- IPAでは今回の注意喚起に加え、特に最近相談が多く寄せられている事例として「Emotet」および「偽のセキュリティ警告」についても注意を呼び掛けており、またMETIからも、「ブロードバンドルータ、無線LANルータ、監視カメラ用機器類、コピー機をはじめとするネットワークに接続された機器・装置類がマルウェアに感染したことに起因する攻撃通信が、増加傾向に」あるとの警告が出ています。

- 一方で、挙げられているセキュリティ対策の内容は毎回大きく異なるようなものではなく、この他にも長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/measures/everyday.html)」として別途まとまっており、GWまでに日にちがなく十分な対応が間に合わなかったとしても、GW明け以降に点検すべきことは多く存在しますし、以後も夏季休暇等に備えて、準備・点検を行うよう意識していくことが肝要です。

IPA

ゴールデンウィークにおける情報セキュリティに関する注意喚起

最終更新日：2022年4月26日
独立行政法人情報処理推進機構
セキュリティセンター

多くの人がゴールデンウィークの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

最近では外出自粛等の影響により、逆に家でパソコンなどを利用する時間が長くなり、ウイルス感染やネット詐欺被害のリスクが高まることも考えられます。

これらのような事態とならないよう、(1)企業や組織の管理者、(2)企業や組織の利用者、(3)個人の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

■長期休暇における情報セキュリティ対策

また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。

■日常における情報セキュリティ対策

被害に遭わないためにもこれらの対策の実施をお願いします。

政府からも大型連休に向けた注意喚起が行われていますので、あわせてご確認ください。

■春の大型連休に向けて実施いただきたいサイバーセキュリティ対策について注意喚起を行います

「Emotet」（エモテット）と呼ばれるウイルスへの感染を狙う攻撃メールが、国内の組織へ今後も着信する恐れがあります。長期休暇明けはメールが溜まっていることが想定されますので、不用意に不審なメールの添付ファイルを開かない、また不用意に本文中のURLにアクセスしないように注意してください。