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。

●富士フイルム、ランサムウェア攻撃でシステム一時停止…翌週中に復旧見込み

https://www.itmedia.co.jp/news/articles/2106/04/news066.html
https://www.jiji.com/jc/article?k=2021060401362&g=eco
https://www.fujifilm.com/jp/ja/news/list/6642

このニュースをザックリ言うと･･･

- 6月2日(日本時間)、富士フイルム社より、同1日深夜に攻撃を受けた可能性があるとして、一部サーバー・PCおよびネットワークの遮断を行ったと発表されました。

- 一時は電話・メールによる問合せにも対応できない状態にあった模様ですが、同4日の発表によれば、攻撃はランサムウェアによるもので、影響の範囲は国内の特定のネットワークに限定されるとしており、安全が確認されたサーバー・PCの稼働と遮断していたネットワークの通信を順次再開するとしています。

- 外部への情報流出は現時点で確認されておらず、また身代金の支払いには応じる予定もなく、7日の週内にはシステムの復旧を見込んでいるとのことです。

AUS便りからの所感等

- 2020年に発生したコロナ禍に合わせるようにランサムウェアによる攻撃が増加しているとされ、2020年6月には本田技研工業、同11月にはカプコンといった大手企業が被害を受けたことが報じられています。

- この他、アンチウイルスベンダー数社が、VPNサーバーの脆弱性を悪用して侵入する等の攻撃を行う新種のランサムウェア「Cring」について注意喚起を出しています(https://blog.trendmicro.co.jp/archives/27830 / https://www.kaspersky.co.jp/about/press-releases/2021_vir25052021 、なお今回のランサムウェアがCringか等は不明)。

- 富士フイルム社については二週間程度でのシステム復旧が見込まれる等、ランサムウェアへの対応が事前に行われていたとみられますが、これまでに発生した事例も参考にしつつ、ランサムウェアをはじめあらゆるマルウェアや攻撃を想定し、システム全体のOS・各種ソフトウェア・アンチウイルスのパターンファイル等を最新に保つこと、万が一の攻撃成立時にもマルウェアの外部への通信や情報の流出を遮断できるようUTM等を用いた適切なネットワーク構成をとること、データのバックアップと復旧が確実に実行できる体制を整えること等を各組織において少しでも進めていくことが肝要です。

ITmedia NEWS

富士フイルム、「ランサムウェア攻撃を受けた可能性」で一部システムを停止

2021年06月04日 09時25分 公開　[ITmedia]

印刷　91　Share　B!　16

富士フイルムは6月2日グローバルサイトで、1日深夜にランサムウェア攻撃の可能性に気付き、影響を受けるすべてのシステムを停止するための措置を講じたと発表した。

JIJI.COM

不正アクセスは身代金要求型　情報流出確認されず―富士フイルム

2021年06月04日22時29分

富士フイルムは４日、社内のサーバーが外部から受けた不正アクセスが、身代金要求型ウイルス「ランサムウエア」だったことが判明したと発表した。同社は「金銭の支払いには応じない」と説明。現時点で外部への情報流出は確認されていないという。安全が確認できたサーバーなどの稼働を同日から始め、来週中の復旧を見込んでいる。

FUJIFILM
Value from Innovation

重要なお知らせ　印刷

当社サーバーへの不正アクセスについて

2021年6月2日 12時
2021年6月2日 20時更新
2021年6月4日 18時更新

当社が利用しているサーバーに対する、外部からの不正なアクセスの疑いについて、外部専門家を含む特別対策チームを設置し、影響可能性のあるサーバーおよびパソコンの停止、ネットワークの遮断を行い、影響範囲等の特定を進めてまいりました。これまでに判明している事実および復旧状況を以下にてお知らせいたします。

- 2021年6月1日夜に認識した不正アクセスは、ランサムウエアであったことを確認しました。
- 影響の範囲が、国内の特定のネットワークに限定されていることを確認しました。
- 範囲が特定されたため、本日より、安全が確認されたサーバーとパソコンの稼働を進め、遮断していたネットワークも通信を順次開始しています。

本件に関しては、関係省庁等に報告するとともに、警察にも届けております。

引き続き、当社製品・サービスをお客様・お取引先様に安心してご利用いただけるよう、関係機関とも連携しながら対応を進めてまいります。
お客様・お取引先様に多大なるご迷惑およびご心配をおかけしますことを深くお詫び申し上げます。

富士フイルム株式会社

●意図しないサイトへのリダイレクト発生…古い翻訳サービスのスクリプト消し忘れが原因

https://scan.netsecurity.ne.jp/article/2021/06/08/45786.html
https://www.intra-mart.jp/topics/2021/006465.html
https://product.intra-mart.support/hc/ja/articles/900007230343

このニュースをザックリ言うと・・・

- 6月3日(日本時間)、エヌ・ティ・ティ・データ・イントラマート社(以下・NTTDIM)より、同社の「ドキュメントアーカイブ」等のサイトで提供する製品ドキュメントの表示時に無関係の不審なサイトに誘導される状態になっていたと発表されました。

- ドキュメントの内容を別の言語に翻訳して表示する機能のために、外部サービスのスクリプトを読み込むよう設定されていましたが、スクリプトの読み込み先サイトのドメイン名が別企業に取得されたことが原因としています。

- NTTDIM社では5月18日に事象を確認し、同25日までに、同社サイト上のオンラインドキュメントについては当該スクリプトを除去する対応を行ったとしている一方、対応前に同社サイトからダウンロードされたドキュメントおよび製品同梱のDVDに収録されたドキュメントについては、スクリプト除去の対応ができないため、破棄するよう呼び掛けています。

AUS便りからの所感

- 発表によれば、翻訳機能については既に別のサービスへ切り替えており、Webサイト上のドキュメントにおいて以前のサービスのスクリプトが機能しないことも確認していたものの、スクリプトの読み込み自体を削除し忘れたとしています。

- 今回のケースのように明確にサービスの切り替えを行っていない限りは、自組織の管理するものではない外部サービスおよびスクリプトの読み込み先サイトが生きているかについて、なおさら確認が行き届かないことも多いと思われますので、Webサイト等で利用しているサービス・スクリプトが確実に存在していること等の運用管理を今後徹底して頂ければ幸いです。

- 著名な企業等のドメイン名が失効→第三者に入手され、別のサイトが表示されるという手口は以前から存在しており、著名なスクリプトの読み込み先等に利用者が多いCDNであっても同様の懸念は考えられますが、既に多くのWebブラウザーが対応している、外部から読み込むスクリプトが意図せず改変されていないかチェックする機能(サブリソース完全性, SRI)を利用できる場合があり、今回のようなケースでユーザーを保護することが期待できます(ただしスクリプトを提供する側もSRIに対応していること、例えば同一URL上でスクリプトが正規に更新されるケース等では使えないことに注意が必要です)。

ScanNetSecurity

NTTデータ・イントラマート、過去のスクリプトを削除せず意図しないサイトに遷移

株式会社エヌ・ティ・ティ・データ・イントラマートは6月3日、同社が提供したドキュメントに含まれる一部のファイルから、同社製品とは関係のないサイトへ誘導される事象が発生したと発表した。

株式会社エヌ・ティ・ティ・データ・イントラマートは6月3日、同社が提供したドキュメントに含まれる一部のファイルから、同社製品とは関係のないサイトへ誘導される事象が発生したと発表した。

これは同社が提供したドキュメントに含まれる一部のファイルについて、過去に利用していた外部サービスのスクリプトが残っていたことで、同社が意図しない外部サイトへ遷移することが判明したというもの。外部サービスのスクリプトは、同社サービスの提供にあたり、利用していた外部サービスのサイトへ遷移する処理であったが、現在は別企業が当該ドメインを取得している。

● 5月度フィッシング報告件数は35,016件、乱高下続くも高水準…対策協議会発表

https://www.antiphishing.jp/report/monthly/202105.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。

- 5月度の報告件数は35,016件で、4月度(https://www.antiphishing.jp/report/monthly/202104.html)の44,307件から9,291件の減少となるも、依然高い水準を維持しています。

- 報告全体に対するブランドの割合は、Amazonが46.6%(4月度 50.7%)、これに楽天・三井住友カード・イオンカード・JCBを合わせた5ブランドで約76.6%(4月度 81.2%)を占めている一方、悪用されたブランドの件数は今月度84件(4月度 66件)と急増し、過去最高となっています。

AUS便りからの所感

- 1・3・4月度の約44,000件からは急減したものの、歴代ではこれらに次ぐ4位の報告件数となっており、また2020年11月度以降は3万件以上を維持し続けています。

- フィッシングの全体的な傾向は先月度と概ね変わりなく、クレジットカード以外にも、仮想通貨(暗号資産)・ISP・ホスティング事業者や宅配業者の不在通知を騙るメール・SMSによるフィッシングあるいはユーザーのプライバシーを盗み見ていると偽って仮想通貨を要求する脅迫メール(セクストーション)が挙げられる一方、知り合いを騙るSMS(AUS便り 2021/05/25号参照)やワクチン接種予約を騙るもの等、新たな手口も確認されています。

- 引き続き、同協議会や各セキュリティ関連団体等の啓発、利用しているサービス等からの公式発表、Twitter等での報告に注意を払い、信頼できないメール・SMSのリンクはクリックせず、サービスの公式サイトにはブックマークからアクセスするよう努める等、フィッシングをはじめとする各種攻撃に対応できるよう慎重な行動をとるよう心掛けましょう。

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