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。

●2022年のランサムウェアによる身代金支払い、2021年の6割に減少…支払いに応じる割合も低下

https://pc.watch.impress.co.jp/docs/news/1472817.html
https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/
https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments
https://pc.watch.impress.co.jp/docs/news/1473841.html

このニュースをザックリ言うと･･･

- 1月19日(現地時間)、ブロックチェーン分析を行う米Chainalysis社より、2022年のランサムウェア攻撃に関する分析レポートが発表されました。
- ランサムウェア攻撃者に対して支払われた身代金(同社が確認している範囲)は2021年に約7億6560万ドルに上っていましたが、2022年には約6割の4億5,680万ドルにまで減少したとのことです。
- 同社ではこの結果について、攻撃の数が大きく減少したためではなく、被害者側が身代金の支払いに応じない傾向が強まっているためと分析しています。

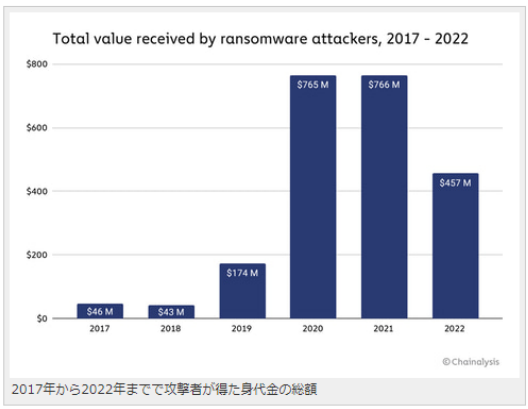
AUS便りからの所感等

- サイバーセキュリティ企業のCoveware社からも1月20日にランサムウェアに関する調査結果が出ており、身代金支払いに応じた割合は2019年には76%でしたが、2022年には41%に下がっています。
- また大型ランサムウェアの一つ「Hive」においては、2022年7月に暗号化されたデータを復号するキーをFBIが入手、被害者に提供されたことで身代金支払い阻止の一助となり、1月26日には、使用されていたサーバーが米国司法省等に差し押さえられる等の動きも出ています。
- ともあれ新たなランサムウェアの発生の可能性は決して皆無ではありませんので、アンチウイルスやUTM等も併せての感染の可能性の低減と、万が一の感染に対するデータの保護(バックアップ・バックアップデータの保護およびバックアップからの復元が確実に行える状態の保持)を適切に行っていくことを強く推奨致します。

Impress Watch

ランサムウェアの身代金支払い総額が減少。支払い拒否の傾向強まる

宇都宮 充　2023年1月24日 17:26



2017年から2022年までで攻撃者が得た身代金の総額

ブロックチェーン分析などを行なうChainalysisは19日(現地時間)、2022年のランサムウェア攻撃に関する分析結果を報告した。これによれば、2022年に攻撃者がランサムウェア攻撃によって得た身代金の総額は4億5,680万ドルで、2021年の7億6,560万ドルと比べて減少したという。

●ゲーム配信プラットフォーム、無断配布サイトを批判…不審なソフト抱き合わせ等の問題

https://automaton-media.com/articles/newsjp/20230121-234501/
https://twitter.com/itchio/status/1615507107545231360

このニュースをザックリ言うと・・・

- 1月18日(現地時間)、PC向けゲーム配信プラットフォームitch.ioより、同サイトのゲームソフトを無断で配布しているサイトを批判する声明が出されています。

- itch.ioのTwitterアカウントから、無断配布サイトとしてSoftonicを名指しし、開発者からコンテンツを盗み、無断配布しているページを広告で覆い尽くし、サーチエンジンで元の配布ページより上位に出るように工作するのをやめるよう呼び掛けています。

- ツイートでは、itch.ioのあるゲームが問題によって取り下げられた後もSoftonicで公開され続けていることも指摘し、開発者が自分のページを削除した後でも広告収入のためにホスティングを続けることをやめてほしいともしています。

AUS便りからの所感

AUTOMATON
VERACITY IN GAMING

人気ゲーム配信プラットフォーム、ゲーム無断配布を巡ってSoftonicに名指しでキレる。かつて"邪魔なツールバー配布"で悪名馳せたサイト

By Seiji Narita - 2023-01-21 19:35

PC向けゲーム配信プラットフォームitch.ioは1月18日、公式Twitterアカウントを通じて、PC向けソフトの紹介・再配布サイトSoftonicに対する批判のコメントを公開した。itch.ioによれば、Softonicは権利者の意向に沿わず、無断でゲームファイルを配信するなどの行動が見られるという。

itch.io
@itchio · フォローする

.@softonic Who do we get in touch with to get you to stop stealing content from our developers, covering them with ads, *paying for search placement* above the actual creator, and continuing to host for ad revenue even after a developer takes their own page down? 😡

午前9:31 · 2023年1月18日

Twitterで会話をすべて読む

- Softonicにおいては、かつてはゲームも含めた各種ソフトウェアの配布と同時に、ブラウザーに表示されるツールバーをインストールさせるよう仕向ける等の問題が指摘され、現在もまだ発売されていないゲームのページ内で無関係のソフトをダウンロードさせる事例が確認されています。

- また、偽サイトがGoogle検索で公式サイトの上位に表示される事例として、2022年10月にGIMP公式サイトを騙る紛らわしいドメイン名の偽サイトが報告されています(AUS便り 2022/11/01号参照)。

- ソフトウェアの入手時には公式サイトや正式に認可されているミラーサイトから行うこと、一方で前述のような、リテラシーが十分になく検索でアクセスしてくるユーザーに独自のソフトウェアを抱き合わせでインストールさせようとするサイトが存在することを意識し、ブラウザーやアンチウイルス・UTMのアンチフィッシング機能等を有効にし、SNS等で不審なサイトの報告がないか等を参考にして、アクセスすべきサイトを慎重に判断することが重要です。

●元勤務先のサーバーに不正アクセス、データ消去容疑で逮捕

https://www.asahi.com/articles/ASR1S4HC4R1SUTIL008.html
https://www.kew-ltd.co.jp/news/detail/00224/

このニュースをザックリ言うと・・・

- 1月24日(日本時間)、警視庁より、不正アクセス禁止法違反と電子計算機損壊等業務妨害の疑いで会社員の男を逮捕したと発表されました。

- 容疑は、2022年3月～6月に、容疑者が勤務していた都内電気計器メーカーの社内ネットワークに不正アクセスし、データを消去したというものです。

- 容疑者は同社でシステム管理を担当、2021年12月に退職しており、同僚らのアカウント情報を持ち出して不正アクセスに利用したとされています。

AUS便りからの所感

朝日新聞 DIGITAL

元勤務先に不正アクセス、データ削除した疑い　退職していた男逮捕

大山稜　2023年1月24日 13時47分

警視庁本部

退職後に元勤務先のサーバーに侵入してデータを破壊したとして、警視庁は、埼玉県 上尾市 の会社員の男(33)を 不正アクセス禁止法 違反と電子計算機損壊等業務妨害の疑いで逮捕し、24日発表した。男は調べに対し、「自分はやっていない」と容疑を否認しているという。

サイバー犯罪 対策課によると、男は昨年6月4日、以前勤務していた「共立電気計器」(東京都 目黒区)の元同僚や元上司のIDやパスワードを勝手に使い、社内ネットワークや同社が契約しているクラウドに不正にログイン。サーバーに保管されていたデータを削除し、同社の業務を妨害した疑いがある。

- 容疑者は犯行を否認している一方、容疑者の私物PCから社内ネットワークにアクセスした履歴があったと一部で報じられています。

- 同社の発表では個人情報を含めたデータの外部流出は確認されておらず、消去されたデータもバックアップから復旧しているとのことですが、復旧には約660万円がかかったとのことです。

- 退職者が元勤務先のシステム上に残っているアカウント等で不正アクセスを行う事案はこれまでも問題視され、IPA「組織における内部不正防止ガイドライン」では2022年改訂版において、営業秘密の漏えいルートとして最も多いのが退職者による不正アクセスであるとする関連対策等がトピックとして追加されており(AUS便り 2022/04/12号参照)、くれぐれも退職者に外部から侵入されたり、メールの送受信を行われたりしないよう、アカウントの削除・無効化もしくはパスワードの変更を確実に行う体制を整えることが肝要です。