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。

●神奈川県庁の行政文書大量流出…転売されたHDDから復元される

https://www.asahi.com/articles/ASMD57WSXMD5UTIL065.html
https://www.itmedia.co.jp/news/articles/1912/06/news099.html
https://www.nikkei.com/article/DGXMZO53095920X01C19A2CZ8000/
https://www.pref.kanagawa.jp/docs/fz7/prs/r0273317.html

このニュースをザックリ言うと･･･

- 12月6日(日本時間)、納税等に関する大量の個人情報や秘密情報を含む神奈川県庁の行政文書を記録していたハードディスク(HDD)がインターネットオークション上で転売されていたと朝日新聞等で報じられました。

- HDDは県庁内のファイルサーバーで使われていたもので、当該サーバーを貸し出していたリース業者が、HDDを破壊あるいはデータを復元できない状態にして処分するよう別業者に委託していましたが、その委託先業者の従業員(のち窃盗罪で逮捕)により一部が持ち出され、出品された模様です。

- オークションへの出品が確認されたHDDは計18台で総容量にして54TBに上り、従業員によって簡単なフォーマットが行われたのみの状態であったとされ、うち9台(27TB分)の落札者により、削除されたデータが復元可能な状態にあったことが確認されています。

- その後、この従業員により、USBフラッシュメモリ等も含めた3,904個の記憶媒体(スマートフォン・タブレット等を合わせた情報機器全体では7,844個とされます)がオークションやフリマアプリで出品・転売されていたことが明らかになっています。

AUS便りからの所感等

- 社員の内部犯行による機密情報の大量流出としては、2014年のベネッセの事件をはじめとして、2018年に日経新聞社社員がPCを分解しHDDを抜き取って持ち出したケース(AUS便り 2018/7/9号参照)等も挙げられます。

- 以後の報道において、前述したHDDの破壊あるいはデータ完全消去や、その過程の公開または第三者による結果の証明、および未処理のHDDを内部の人間が持ち出すような行為の防止等が適切に行われていなかった可能性等が指摘されており、例えば業者への委託ではなくユーザー企業側でHDDを廃棄することが推奨される流れとなることも考えられます。

- データ流出対策としてよく挙げられる「HDDのデータ領域ないし全体の暗号化」は、ダウンロードしたデータが狙われる可能性を考慮するとクライアントPC側で是非とも導入されるべきである一方、今回のようなケースを回避する目的で、また通常は個々のPCに追加でソフトウェアを導入する必要がないことからも、ファイルサーバー側からの導入の検討も有用であるものと思われます(いずれにせよ運用上見過ごせないデメリットがないか次第となるでしょう)。

朝日新聞 DIGITAL

【独自】行政文書が大量流出　納税記録などのHDD転売

≡ 神奈川HDD流出

茂木克信　2019年12月6日 05時00分

シェア　ツイート　ブックマーク　メール　印刷

list　0

神奈川県庁＝横浜市中区

納税などに関する大量の個人情報や秘密情報を含む神奈川県庁の行政文書が蓄積されたハードディスク（HDD）が、ネットオークションを通じて転売され、流出していたことが朝日新聞の取材で分かった。県のサーバーから取り外されたHDDのデータ消去が不十分なまま、中古品として出回っていた。県によると、データの消去から廃棄までを請け負った業者の社員が、転売に関与したことを認めているという。

●Windows 7をターゲットとするマルウェア、2018年より71%増加

https://news.mynavi.jp/article/20191205-933493/
https://www.webroot.com/jp/ja/about/press-room/releases/windows-771

このニュースをザックリ言うと・・・

- 12月5日(日本時間)、セキュリティベンダーのウェブルート社より、セキュリティ業界の最新状況をまとめた「ウェブルート脅威レポート2019 中間アップデート」が発表されました。

- 同社では、一般にWindows 7を使用しているマシンは、Windows 10を使用するマシンの倍感染する可能性が高いとしており、7マシンをターゲットとするマルウェアも2018年に比べ71%増加したとしています。

- この他、マルウェア感染等の恐れのある「悪意あるURL」について、1/4近くのホストが信頼性の高いドメインだったこと、50件に1件のURLが悪意あるものであったことを挙げており、オフィスワーカーの1/3近くが1日に仕事関連のリンクを25回以上クリックしていることを考えると、高い割合であるとしています。

AUS便りからの所感

- 来月に迫っているWindows 7の無償サポート終了後、Professional等一部エディションについて有償サポートが提供されることはすでに発表されています(AUS便り 2019/10/7号参照)が、企業等のユーザーに実際にどれだけ利用されるかは未知数で、実際には未対策のまま7が使われ続けるケースも多く発生するものと思われます。

- Windows 10では、7になかった新機能に脆弱性が見つかるケースも皆無ではないとはいえ、大抵は新たなセキュリティ機構により、マルウェアへの感染が抑制されているケースの方が上回っているものと推測されます。

- いずれにしろ、無償サポート終了を機にマルウェアの活動はさらに活発化することは容易に予想されますので、根本的対策としての10への移行を行い、やむを得ない事情で7を使用し続けるマシンは可能な限りアンチウイルス・UTM等を用い、外部・内部のネットワークとの隔離を行うことが肝要です。

マイナビニュース

Windows 7をターゲットとするマルウェアが71%増加

関連キーワード：マルウェア， エンドポイントセキュリティ， 調査データ　2019/12/05 11:46

ウェブルートは12月4日、セキュリティ業界の最新状況をまとめた「ウェブルート脅威レポート2019　中間アップデート」を発表した。同レポートは、機械学習ベースの脅威分析アーキテクチャ「Webrootプラットフォーム」で使用しているデータと、同社脅威調査チームからの傾向、洞察および予測をまとめたもの。

● JPCERT/CCより年末年始における情報セキュリティに関する注意喚起…リモートアクセスサービスへの侵入等に注意

https://www.jpcert.or.jp/newsflash/20191205O1.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となる年末年始を迎えるにあたり、12月12日(日本時間)にJPCERT/CCより、情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になることにより、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う可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- 注意喚起の一例として、テレワークや遠隔保守のために外部からの接続を許可しているケースで、今年5月に発表されたリモートデスクトップサービスの脆弱性を突いて攻撃者がサーバーPC等に侵入し、そこを踏み台に内部ネットワークに侵入する等の攻撃を行う可能性を挙げており、対策として「ソフトウエアやハードウエアを最新の状態に保つ」「アクセスに用いるIPアドレスやポートを制限する」「リモートからアクセス可能なサービスを把握する」「インシデントを適切に検知するために、ログの記録、分析方法を確認する」を挙げています。

AUS便りからの所感等

- 同様の注意喚起はIPAも毎回同時期に行っており(https://www.ipa.go.jp/security/measures/vacation.html)、こちらも近日中に更新されるとみられますが、こういったセキュリティ機関の呼びかけでは、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントが挙げられており、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有が、そういった攻撃による被害を最小限に抑えられるために大切なことと言えます。

- もしこのAUS便りを年明けにご覧になったとしても、その時点で点検すべきことは多く存在します。以後も、ゴールデンウィークや夏季といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。

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

長期休暇に備えて 2019/12　最終更新: 2019-12-12

ツイート　メール

CyberNewsFlash一覧

冬の長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、要点をまとめました。 今年は

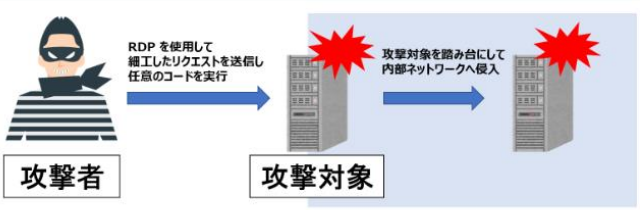

図1:「リモートデスクトップサービスを狙った攻撃」のイメージ