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。

●ソフトバンク・テクノロジーに不正アクセス、使われていないアカウントから侵入

http://itpro.nikkeibp.co.jp/atcl/news/17/072501974/
http://www.softbanktech.co.jp/corp/news/info/20170724/

このニュースをザックリ言うと・・・

- 7月24日（日本時間）、ソフトバンク・テクノロジー社より、同社が保有する保守契約管理システムの検証サーバが不正アクセスを受け侵入されたと発表されました。
- サーバには不正アクセスにより、仮想通貨採掘プログラムをインストールされた他、取引先の情報を格納したファイルが存在していたため、4071社の情報が外部に流出した恐れがあるとされています（その後、7月28日に流出の事実は確認されなかったとの続報がありました）。
- 当該サーバはインターネットに直接接続されており、不正アクセスの原因として、不要なアカウントが存在、かつパスワードが脆弱であり、外部アクセス対策が適切ではなかったことを挙げています。

AUS便りからの所感等

- 既に利用されていないアカウントの存在は、攻撃者にとって侵入の入り口となるのみならず、例えばメールサーバであれば外部へのメールの送信に悪用される等の可能性があります。
- 以前から問題となっている、いわゆる「リスト型攻撃」により、外部Webサービスとパスワードを共有していた等のアカウントが侵入されることも考えられます。
- 従業員の退職により利用者がいなくなった等、不要となったアカウントについては速やかに削除し、メールアドレス等であれば適宜他のユーザに転送する設定を行う、またサーバ・UTM等においてアクセスログを随時確認する、といった体制を整備しておくことが侵入の可能性を抑止するためには重要です。

ITpro

ソフトバンク・テクノロジーに不正アクセス、4071社の情報が流出の可能性

斉藤 壮司＝日経コンピュータ　2017/07/25　日経コンピュータ

目次一覧

ソフトバンク・テクノロジーは2017年7月24日、同社が保有する保守契約管理システムの検証サーバーに対する不正アクセスが確認されたと発表した。当該サーバーには取引先の情報を格納したファイルが存在し、4071社の情報が外部に流出した恐れがあるという。

2017/7/17	13:52	セキュリティ監視チームがマルウェアの実行および通信のブロックを検知。
2017/7/17	14:08	CISO、情報システム部門、CSIRTメンバーに情報展開。
2017/7/17	15:45	当該コンピュータのネットワーク隔離を開始。
2017/7/17	19:45	マルウェアの調査結果より、不正アクセスを受けた当該サーバーを特定。
2017/7/17	19:50	当該サーバーをネットワークから遮断。当該サーバーの調査開始。
2017/7/20	10:00	当該サーバーが不正アクセスを受けた形跡を確認。当該サーバーの取引先情報が格納されたファイルに、攻撃者がアクセス可能だったことが判明。第三者機関の手配開始。
2017/7/21	16:00	第三者機関による調査開始。
2017/7/22	13:50	第三者機関の一次調査完了。

SoftBank Technology

2017年7月24日

お客様各位

ソフトバンク・テクノロジー株式会社
代表取締役社長 CEO 阿多 親市

不正アクセスによる情報流出の可能性に関するお知らせとお詫び（第一報）

謹啓
貴社益々のご盛隆のこととお慶び申し上げます。平素は格別のお引きたてを賜り厚くお礼を申し上げます。

このたび、弊社の保持する検証サーバー（保守契約管理システムの検証サーバー、以下 当該サーバー）に対する不正アクセスが確認されました。当該サーバーには、保守契約管理システムの移行作業で利用する取引先
出した可
いたしま

現在、
および第
が、情報

2017年7月28日

お客様各位

ソフトバンク・テクノロジー株式会社
代表取締役社長 CEO 阿多 親市

不正アクセスによる情報流出の可能性に関する詳細調査のご報告（第二報）

謹啓
貴社益々のご盛隆のこととお慶び申し上げます。平素は格別のお引きたてを賜り厚くお礼を申し上げます。

2017年7月24日に発表した「不正アクセスによる情報流出の可能性に関するお知らせとお詫び（第一報）」のとおり、弊社の保持する検証サーバーへの不正アクセスを確認し、第三者（以下、攻撃者）に情報が流出した可能性があることが判明したため、第三者機関による詳細な調査を進めてまいりました。

第三者機関の詳細な調査の範囲において、**取引先情報が格納されたファイルが流出した事実は確認されませんでした。**従いまして、お客様に対する直接的な影響は想定しにくいと結論づけられますが、取引先の皆様におかれましては、流出の可能性が想定される事案がございましたら、誠に恐れ入りますが弊社にご連絡いただきますようお願い申し上げます。

今後は、再発防止策の推進フェーズに移り、二度とこのような事態が発生しないように努める所存です。調査報告も踏まえた詳細な報告を下記の通りご案内いたします。

取引先およびパートナーの皆様、そして株主や投資家をはじめとする多くの関係者に多大なるご心配とご迷惑をおかけしておりますことを心よりお詫び申し上げます。

●Adobe、「Flash」を2020年末に終了へ

http://www.itmedia.co.jp/news/articles/1707/26/news044.html

このニュースをザックリ言うと・・・

- 7月25日（現地時間）、Adobe社より、同社による「Flash」および「Flash Player」の開発・提供を2020年末に終了すると発表されました。

- 同社ではコンテンツ制作者に対し、それまでに既存のFlashコンテンツをHTML5等の新しいオープンフォーマットに移植するよう推奨していき、またMicrosoft・Google・Mozilla・Apple・Facebook等の技術パートナーと協力するとしており、Adobe社の発表と前後して各社からもブログ等でFlashの終了に関して発表が出されています。

- 既にiPhone・iPadやAndroidデバイスには事実上Flash Playerが提供されていない他、Firefox・Chrome・Edgeの各PCブラウザにおいても、Flashコンテンツをデフォルトでブロックする等の動きが進んでいます。

AUS便りからの所感等

- 2000年代頃までは、自身の機能が十分でなかったWebブラウザを補完する存在としてFlashは重宝されてきましたが、近年はHTML5・WebGL・SVG等の規格策定とブラウザへの実装に伴い、Flash Playerによる動画再生を行っていた動画サイト等でも急速にHTML5を用いたものへの置き換えが進んでいます。

- 企業のWebサイトで使われているようなFlashコンテンツの多くもHTML5等で置き換えられることが可能とみられ、少しでも早い段階から移行の準備を行うべきでしょう。

- 一方の利用者としては、古いバージョンのFlash Playerが搭載されたPCを主なターゲットとする、不正なFlashコンテンツを用いたマルウェアへの感染等を目論む攻撃の存在を引き続き念頭に置き、常にFlash Playerを最新の状態に保つことと、アンチウイルス・UTMあるいはブラウザの機能による不正なFlashコンテンツの遮断を確実に行っていくことも重要です。


ITmedia NEWS

Adobe、「Flash」を2020年末に終了へ

Adobe Systemsがついに「Flash」の開発および提供を2020年末に終了する。Apple、Google、Microsoft、Facebook、Mozillaなどが協力する。1996年に「Macromedia Flash」として誕生したコンテンツ技術が24年の生涯を閉じる。

[佐藤由紀子，ITmedia]

米Adobe Systemsは7月25日（現地時間）、「Flash」の開発および提供を2020年末に終了すると発表した。

「AdobeはFlashの終末（end-of-life）を計画している。具体的には、Flash Playerのアップデートと提供を2020年末に停止する。コンテンツ製作者に対し、それまでに既存のFlashコンテンツを新しいオープンフォーマット（HTML5やWebGLなど）に移植するよう推奨していく」としている。

Flash終了に当たっては、Apple、Facebook、Google、Microsoft、Mozilla（リンク先は各企業の公式ブログ）を含む技術パートナーと協力しているという。

●Google、Androidデバイスを守る「Google Play Protect」を提供開始

https://japan.cnet.com/article/35104578/

このニュースをザックリ言うと・・・

- 7月19日（米国時間）頃、Googleより、Androidデバイスを有害なアプリから保護するサービス「Google Play Protect」（日本語名「Google Play プロテクト」）がリリースされました。

- Play Protectは、Androidデバイスをスキャンして不正なAndroidアプリがインストールされていないか等をチェックし、既知の有害なアプリを削除し、その他有害な可能性のあるアプリについてもユーザに警告します。

- Play Protectは今後各Androidデバイスへ段階的に提供される予定であり、Google公式ストア「Google Play」で提供されるアプリのチェックにも用いられるとのことです。

AUS便りからの所感等

- Androidにおいては、非公式に配布されるアプリのみならず、Google Playで配布されるアプリにもマルウェアが同梱されるケースも珍しくなくなっており、先日も標的型スパイウェア「Lipizzan」を含むアプリが配信され、Play Protectによって検知、削除されるという出来事が早速発生しています（http://www.itmedia.co.jp/enterprise/articles/1707/27/news041.html）。

- iOSやWindows向けのアプリにも言えることですが、インストールの前にTwitterやブログ等複数の情報源をあたり、問題がないか判断することは大切です。

- AndroidにはWindowsと同様に、以前からアンチウイルスベンダー各社がアンチウイルスアプリを提供しており、Play Protectの導入後も併用して使っていくのが良いでしょう。


cnet Japan

「Android」をセキュリティスキャンする「Google Play Protect」提供へ

Jake Smith （Special to ZDNet.com） 翻訳校正： 湯本牧子 吉武稔夫 （ガリレオ） 2017年07月21日 15時30分

Googleは米国時間7月19日、「Google Play Protect」の提供を開始したと見られる。Google Play Protectは「Google Play」の新機能で、「Android」搭載デバイスに損害を与えるおそれのあるアプリを探すとともに、デバイスのセキュリティについてユーザーにより詳しい情報を提示する。

Play Protectはユーザーの Androidデバイスを自動的にスキャンして、デバイス、データ、アプリを安全な状態に保つ。Googleの「Verify Apps」機能に代わるもので、ユーザーが気づきやすくなったほか、セキュリティスキャンに関する詳細な情報を提供する。

機械学習を利用して毎日500億本のアプリをスキャンし、疑わしいマルウェアや悪意のあるマルウェアがないか確認する。マルウェアが「Google Play Store」に入り込まないようにするセーフチェックの仕組みもあるが、サードパーティーのマルウェア研究者から報告を受けるまで認識されないこともある。Play Protectは、Play Storeからダウンロードされたものでないアプリもスキャンする。

Googleはさらに、Play Protectに「Find My Device」機能を組み込んで、紛失した端末を探すこの機能に必要な改良を施した。そうした改良には、新たなアイコン、より使いやすくなったインターフェース、新しいバッテリおよびWi-Fiステータス表示、デバイスが最後に確認された場所に関する詳細情報などがある。

Play Protectは段階的にリリースされており、「Play Services 11」以降が必要なようだ。