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。

●ASUSノートPCのソフトウェアアップデートにマルウェア混入、「サプライチェーン攻撃」が原因

https://www.itmedia.co.jp/enterprise/articles/1903/26/news074.html
https://internet.watch.impress.co.jp/docs/news/1176553.html

このニュースをザックリ言うと・・・

- 3月25日（現地時間）、セキュリティベンダーのKaspersky社およびSymantec社より、ASUS社が同社ノートPC等にBIOS・ドライバ等のアップデートを提供する「ASUS Live Update」にマルウェアが混入されていたと発表されました。

- 2018年6月～11月にASUS社のアップデート配信サーバに正規の証明書が用いられた不正なアップデートファイルが置かれる攻撃が発生していたことをKaspersky社が今年1月に発見したもので、同社では今回発生した攻撃を「Operation ShadowHammer」と呼んでいます。

- Kaspersky社の発表では、同社セキュリティ製品の利用者だけでも57,000人以上が不正なASUS Live Updateをインストールしたことが確認された他、全世界で100万人以上が影響を受けた可能性があるとしており、国別ではロシア・ドイツ・フランスが大半を占める他、日本等でも少数の被害が出ているとしています。

- 3月26日にはASUS社より、Live Updateの最新バージョン3.6.8と、機器が影響を受けていないかチェックする診断ツールがリリースされています。

AUS便りからの所感等

- 今回のような、ソフトウェア開発者のアカウントを乗っ取る等の行為により、配布物にマルウェアを混入させることを「サプライチェーン攻撃」と呼び、2017年9月にはWindows用の人気ソフトウェア「CCleaner」において同様の攻撃の事例が報告されています（AUS便り 2017/09/25号参照）。

- マルウェアが混入したソフトウェアが開発者の正規の署名でリリースされることにより、アンチウイルスによる検出を回避しやすい状況を得るのがサプライチェーン攻撃を狙う理由とされます。

- ソフトウェア開発のみならず、Webサイトの運営・保守においても、同様の攻撃によりページやWebアプリケーションに内部からマルウェアを仕込まれる可能性があり、提供者サイドにおいては、末端の協力者等に至るまで十分なセキュリティ対策を行うよう徹底することが重要となるでしょう。


ITmedia エンタープライズ

ASUSの自動更新を悪用したサプライチェーン攻撃、ユーザーにマルウェア配信

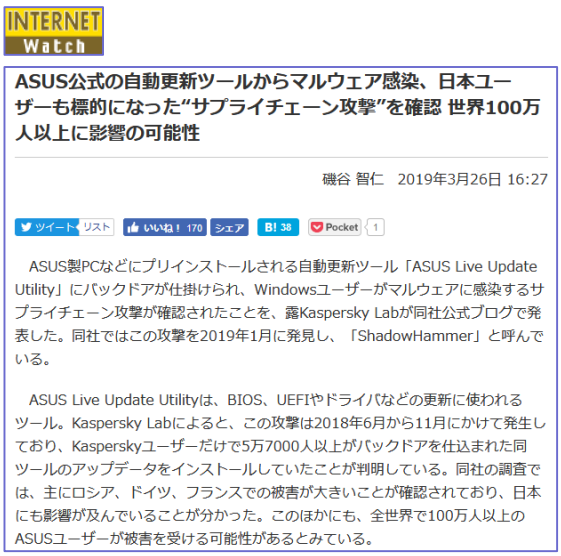
Kaspersky LabやSymantecによると、ASUSの自動更新システムが乗っ取られ、マルウェアの配信に利用されていたという。

2019年03月26日 09時06分 公開　[鈴木聖子，ITmedia]

印刷　115　161　B!　26

ロシアのセキュリティ企業Kaspersky Labは3月25日、台湾のASUSが配信したLive Updateソフトウェアにサプライチェーン攻撃が仕掛けられ、自動更新を通じてユーザーにマルウェアが配信されていたことが分かったと伝えた。この攻撃については米Symantecも26日のブログで報告している。

KASPERSKY
SECURELIST　THREATS　CATEGORIES　TAGS　STATISTICS　ENCYCLOPEDIA
APT REPORTS
Operation ShadowHammer
By GReAT on March 25, 2019. 1:01 pm
Earlier today, Motherboard published a story by Kim Zetter on Operation ShadowHammer, a newly discovered supply chain attack that leveraged ASUS Live Update software.


INTERNET Watch

ASUS公式の自動更新ツールからマルウェア感染、日本ユーザーも標的になった“サプライチェーン攻撃”を確認 世界100万人以上に影響の可能性

磯谷 智仁　2019年3月26日 16:27

ツイート　リスト　いいね！ 170　シェア　B! 38　Pocket 1

ASUS製PCなどにプリインストールされる自動更新ツール「ASUS Live Update Utility」にバックドアが仕掛けられ、Windowsユーザーがマルウェアに感染するサプライチェーン攻撃が確認されたことを、露Kaspersky Labが同社公式ブログで発表した。同社ではこの攻撃を2019年1月に発見し、「ShadowHammer」と呼んでいる。

ASUS Live Update Utilityは、BIOS、UEFIやドライバなどの更新に使われるツール。Kaspersky Labによると、この攻撃は2018年6月から11月にかけて発生しており、Kaspersky ユーザーだけで5万7000人以上がバックドアを仕込まれた同ツールのアップデータをインストールしていたことが判明している。同社の調査では、主にロシア、ドイツ、フランスでの被害が大きいことが確認されており、日本にも影響が及んでいることが分かった。このほかにも、全世界で100万人以上のASUSユーザーが被害を受ける可能性があるとみている。

●来年1月サポート終了のWindows 7、警告表示パッチがリリース

https://japan.cnet.com/article/35134561/

このニュースをザックリ言うと・・・

- 3月20日（現地時間）、米Mircosoft社より、Windows 7のサポート終了を知らせる通知を表示するパッチ「KB4493132」がリリースされています。

- Windows 7は2020年1月14日に全てのサポートが終了する予定となっており、このパッチの適用により、4月18日以降通知が表示されるとのことです。

- パッチはWindows Updateで配信されますが、自動ではインストールされず、またインストール後に通知を非表示にするチェックボックスも用意されるとのことです。

AUS便りからの所感等

- Windows 7（および8.1）は現在OSの既存の機能に対するセキュリティパッチのみが提供されており、Windows 10に追加されている新たなセキュリティ機能が7に提供される可能性は低く、Microsoftではそういった事情からも10へのアップグレードをユーザに求めています。

- サポート終了を通知するパッチはWindows XPのときも提供されていましたが、終了から6年が経とうとする現在もXPのシェアは依然少なからずあり、7についても同様の状況になる可能性は高いと言えます。
（https://news.mynavi.jp/article/20190104-750432/）

- ともあれ、その前例を繰り返さないよう、8.1以前が多く残っている組織では早々に10への移行に向け何らかの計画を行うべきでしょう。

●Facebookユーザ数億人分のパスワードを数年間可読状態で保存

https://www.itmedia.co.jp/news/articles/1903/22/news068.html

このニュースをザックリ言うと・・・

- 3月21日（現地時間）、米Facebook社より、Facebook・Instagram・Facebook Liteの数億人分のパスワードが社内で暗号化されていない平文の状態で保存されていたと発表されました。

- 問題を最初に報じた米セキュリティ情報サイトKrebs on Securityによれば、この形でのパスワードの保存は2012年以降から行われており、社内2万人以上の従業員が検索可能であった他、約2,000人がデータにアクセスしていたとのことです。

- Facebook社では1月にこの問題を修正しており、データには社外からはアクセスできず、また内部の人間が不正に利用した形跡もないとしていますが、念の為該当するユーザに対し通知する予定としています。

AUS便りからの所感等

- FacebookのようなWebサービスの運営においては、パスワードはハッシュ化を行い復号できない状態で保存するのが基本であり、「万が一パスワードを忘れたユーザに対し設定されていたパスワードをそのまま示せるよう平文で保存する」等というのはデメリットの方が大きく、そういうケースではパスワードの再設定を行わせる方が一般的です。

- Webサービスを提供する場合に限らず、社内システムにおけるアカウント管理においても、パスワードを含むアカウント情報を不特定多数がアクセス可能な場所に保存にしておくことは、内部ネットワークに攻撃者が侵入した場合を考慮すると危険なことは言うまでもありません。

- そういった機密情報データには必ず暗号化を行い、可能であれば管理者であってもログインしたそのままの状態ではアクセスできない形で隔離することが重要です。