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。

●2019年度セキュリティ動向予測、ウォッチガード社が発表

http://www.atmarkit.co.jp/ait/articles/1811/29/news061.html
https://www.watchguard.co.jp/press-release/2019_predictions.html

このニュースをザックリ言うと・・・

- 11月27日（日本時間）、大手セキュリティベンダーのウォッチガード社より、2019年における情報セキュリティ業界の動向予測が発表されました。

- 発表では以下の8つの動向予測が挙げられています：

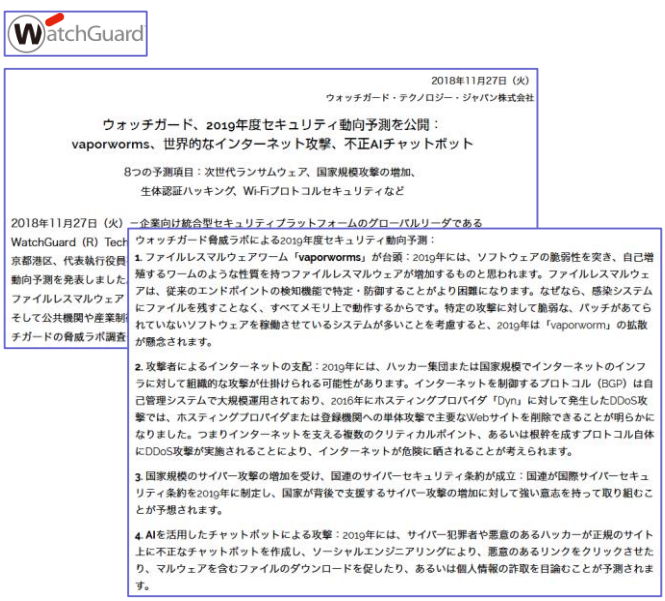
1：ファイルレス（ファイルを残さず全てメモリ上で活動する）ワーム「vaporworms」が台頭
2：攻撃者によるインターネットの支配（ハッカー集団あるいは国家規模での組織的攻撃）
3：国家規模のサイバー攻撃の増加を受け、国連のサイバーセキュリティ条約が成立
4：AIを活用したチャットボットによる攻撃（攻撃者が正規のサイトを改ざんして設置した偽のチャットボットにより、ユーザを誘導する）
5：生体認証の大規模ハッキングにより認証が多要素化
6：国家規模の「Fire Sale」攻撃（交通・金融・通信インフラへの同時多発サイバー攻撃）が現実化
7：公共機関や産業制御システムを標的としたランサムウェアにより都市機能が麻痺
8：WPA3 Wi-Fiネットワークのハッキング

AUS便りからの所感等

- 挙げられている脅威は、これまで存在していた脅威がさらに攻撃力を増していくものや、利便性と表裏一体で発生するもの等、様々です。

- またWPA3について「産業全体にわたりWi-Fiインフラでより包括的なセキュリティが適用されない限り、決して安全ではない」とされているように、WPA・WPA2のような古いプロトコルが使われ続けている限り、新しいプロトコルの持つセキュリティ機能が有効に働かないケースも存在し、その意味ではソフトウェアのみならずハードウェアについても、計画的な更新が重要と言えるでしょう。

- 話題となっているセキュリティの脅威について随時情報収集を行い、各人が慎重な行動をとり、またシステム管理者においては、万一攻撃が成功した場合の被害を最小限に抑えられるネットワークシステムの構築をUTM等を用いつつ行って頂ければ幸いです。



●監視カメラへの不正アクセス・乗っ取り50件以上…元自衛官を書類送検

https://www.asahi.com/articles/ASLCN4K50LCNPIHB01F.html

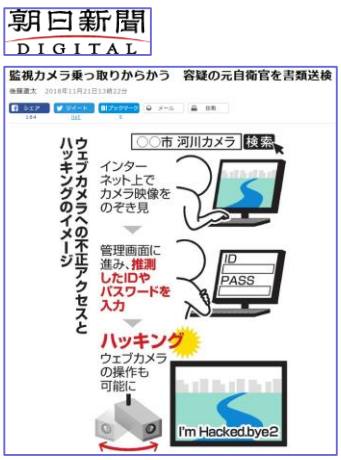
このニュースをザックリ言うと・・・

- 11月21日（日本時間）、兵庫県警より、インターネットに接続された監視カメラ等へ不正アクセスを行った電子計算機損壊等業務妨害容疑で、元自衛官の男を書類送検したと発表されました。

- 4月下旬に、神戸市東灘区の障害者施設の監視カメラ1台と千葉県八千代市の水位監視カメラ2台に不正アクセスし、画面に「I 'm Hacked. bye2」と書き込んだり、パスワードを変更したりしてそれぞれ業務を妨害した疑いが持たれています（AUS便り 2018/05/07号も参照）。

- 被害を受けた監視カメラは、パスワードが初期設定のまま変更されていなかったとのことです。

AUS便りからの所感等



- 同様の被害は今年60件以上発生しているとされ、また容疑者も50～100件以上同様の不正アクセスを行ったと供述しています。

- インターネット上から接続可能な状態になっている複合機やIoT機器等を検索できる「SHODAN」「Censys」といったサーチエンジンが存在し、今回の容疑者のみならず多くの攻撃者が日夜ターゲットとする機器を検索しているものと推測されます。

- 外部からアクセスされるべきでないサービスポートについては、UTMやファイアウォールによるフィルタリングを行い、画像をWebで公開しているカメラ等についても管理画面にはアクセスされないよう適切な設定を行うようにしましょう。

- 併せて、その状態で外部から不正アクセスを受ける可能性がないか、ネットワーク診断を受けることにより、安全性を確認することも一考に値するでしょう。

●Webサーバ「Nginx」の脆弱性を悪用する攻撃準備中か…最新版へのアップデートを

https://this.kiji.is/435938239837946977

このニュースをザックリ言うと・・・

- 11月15日（日本時間）、ビッグデータ分析等を行うシンガポールAntuit社より、Webサーバソフトウェア「Nginx」の脆弱性（CVE-2018-16843, CVE-2018-16844, CVE-2018-16845）を悪用する大規模な攻撃を攻撃者が計画しているとして注意喚起が出されています。

- 同社が11月8日頃からダークウェブフォーラムで傍受していた攻撃者の会話によれば、脆弱性の影響を受けやすいサーバを探し出すキャンペーンを計画しており、また脆弱性を突いてサーバの速度を低下あるいは完全に停止させられる攻撃ツールを設計しているとされています。

- また、この攻撃の標的となる可能性がある国は、米・英・日本および東南アジア諸国等とされています。

AUS便りからの所感等

- Nginxは、ApacheやIISと並んで高い人気を誇るWebサーバ（およびプロキシ）ソフトウェアで、ここ最近は脆弱性が報告されることが比較的少なかったのですが、11月7日、DoS攻撃等につながる脆弱性3件が一度に報告されています。

- 近年シェアを伸ばしていることもあり、攻撃者にとって今回の脆弱性が格好のターゲットであることは容易に想像できます。

- 脆弱性はNginxバージョン1.15.6以降または1.14.1以降で修正されていますので、利用している場合は速やかに最新バージョンへのアップデートを行うようにしてください。