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。

●国内のIPアドレスが対象、TCP 22・23・80番等へのポートスキャンをNICTが実施へ

https://internet.watch.impress.co.jp/docs/news/1152349.html
https://www.nict.go.jp/info/topics/2018/11/07-2.html

このニュースをザックリ言うと･･･

- 11月7日（日本時間）、国立研究開発法人情報通信研究機構（NICT）より、日本国内のIPアドレスを対象にしたポートスキャンを実施し、ポート開放状態のアドレス数の規模などの調査を行うことが発表されました。

- 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が5月16日に成立、11月1日に施行され、NICTの業務に「パスワード設定等に不備のあるIoT機器の調査」等が追加されたことを受けて実施されるものです。

- 11月14日から2019年1月末までをめどに、TCPポート22番(SSH)、23番(Telnet)および80番(HTTP)等を対象にスキャンを行うとともに、ポート開放状態のアドレスに対してバナー情報を取得し、サービス種類やバージョン情報、機器種別等の状況調査を行うとしています。

- また、パスワード設定に不備のある機器については、利用者を特定し、電気通信事業者（プロバイダ等）を通して設定変更の注意喚起も行うとのことです。

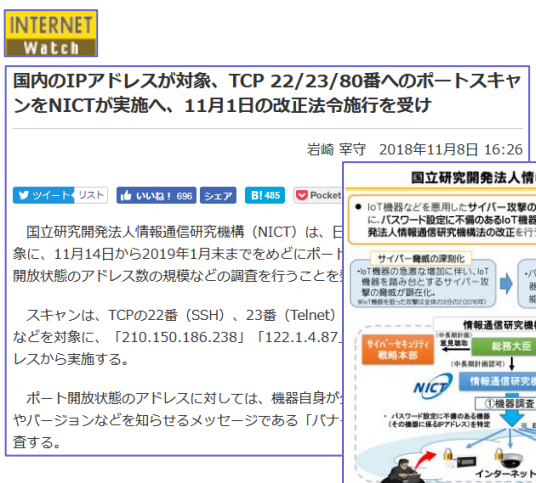
AUS便りからの所感等

- 改正法の概要では「2016年にはIoT機器を狙ったものがサイバー攻撃の3分の2を占め、パスワード設定などに不備のあるIoT機器の実態把握を行う調査能力の強化が急務」と記されています。

- 先日も、JPCERT/CCから定点観測の結果が報告されており、特にマルウェアが感染したIoT機器からとみられる、前述した3ポートや445番(Windows関連サービス)等へのアクセスが多く発生している模様です（AUS便り 2018/10/29号参照）。

- 各組織のネットワーク管理者におきましては、今回の調査実施を意識して何らかの対策を講じると考えるのではなく、普段から「意図して公開していないサービスへはアクセスさせない」ことを意識し、ファイアウォールやUTMによるアクセス制限を適切に設定し、IoT機器からルータ等（もちろんサーバについても）に至るまで様々な機器についてソフトウェアやファームウェアを最新に保つことを心掛けてください。

- 加えて、ポートスキャンやバージョン情報の収集以上のネットワークに対する詳細な調査について、是非とも第三者機関の診断を受けて頂ければ幸いです。


INTERNET Watch

国内のIPアドレスが対象、TCP 22/23/80番へのポートスキャンをNICTが実施へ、11月1日の改正法令施行を受け

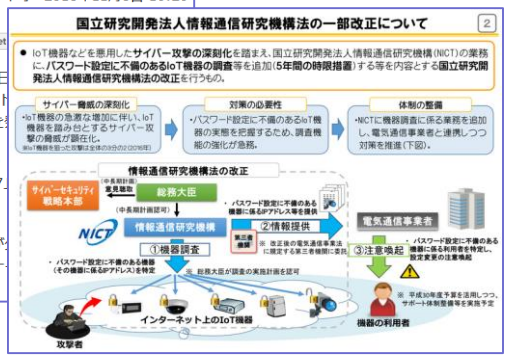
岩崎 宰守　2018年11月8日 16:26

ツイート リスト いいね！ 696 シェア B! 485 Pocket

国立研究開発法人情報通信研究機構（NICT）は、日
象に、11月14日から2019年1月末までをめどにポート
開放状態のアドレス数の規模などの調査を行うことを

スキャンは、TCPの22番（SSH）、23番（Telnet）
などを対象に、「210.150.186.238」「122.1.4.87
レスから実施する。

ポート開放状態のアドレスに対しては、機器自身が
やバージョンなどを知らせるメッセージである「バナ
査する。




NICT 国立研究開発法人 情報通信研究機構

日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

2018年11月7日
国立研究開発法人情報通信研究機構

ツイート いいね！ 144

国立研究開発法人情報通信研究機構（NICT）は、パスワード設定等に不備のあるIoT機器の調査等をNICTの業務に追加（5年間の時限措置）する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が今月1日に施行されたことを受け、同調査等の業務の実施（今年度内に開始予定）に向けた検討、準備を進めてまいります。

今後の具体的な検討にあたっては、日本国内でインターネットに接続されたIoT機器等につき、当該接続状況などの全体的な傾向、概数等を把握する必要があることから、ポート開放状況の把握など、現状に関して、事前の準備のための調査を実施することといたします。

○事前調査の概要
・日本国内のIPv4アドレスを対象に、22/TCP(SSH)、23/TCP(Telnet)、80/TCP(HTTP)などの宛先ポートに対してポートスキャンを実施し、ポート開放状態のアドレス数の規模などの調査を行います。
・ポート開放状態のアドレスに対してバナー情報※の取得を行い、サービス種類やバージョン情報、機器種別などの状況調査を行います。

○事前調査の実施時期
11月14日(水)に開始し、来年１月末までを目途に実施予定です。

●「世界盆栽大会」ドメインがアダルトサイトに…登録の削除呼び掛け

https://this.kiji.is/430363545500337249

このニュースをザックリ言うと・・・

- 10月31日（日本時間）、さいたま市より、2017年4月に開催された「第8回世界盆栽大会inさいたま」の公式ホームページのドメインが第三者に再利用されたとして、リンクを削除するよう呼び掛けています。

- 当該サイトはさいたま市などとは別の外部ドメイン上で運営されていましたが、同31日に市民からの通報を受けて市が確認したところ、アダルトサイトが表示されるようになっていたとのことです。

- さいたま市では同市公式ページからリンクを削除するとともに、関係団体等への周知を行っています。

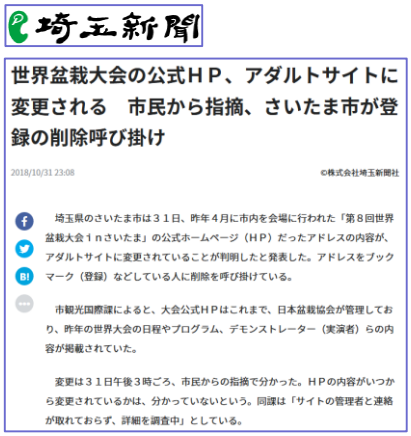
AUS便りからの所感等

- 当該サイトは、2015年に前述の第8回大会のために独自のドメインが取得され、立ち上げられたものでした。

- 今回のような経緯でイベント等のための独自ドメインが失効 → 第三者に取得されたケースとしては、2015年に内閣府が開催したシンポジウムのサイトについて等が挙げられます（AUS便り 2018/05/14号参照）。

- 独自ドメインが失効することへのこういったリスクは長年指摘されていることで、一時的なイベントや映画作品に関するドメインならなおさらですが、そうでないケースでも注意を怠るべきではありません。

- 既存のドメイン下のサブドメインで運用することをまずは検討し、それでも独自ドメインが必要であれば、取得・維持から使わなくなった際の後処理までを意識した運用を行うべきでしょう。


埼玉新聞

世界盆栽大会の公式ＨＰ、アダルトサイトに変更される　市民から指摘、さいたま市が登録の削除呼び掛け

2018/10/31 23:08　©株式会社埼玉新聞社

埼玉県のさいたま市は３１日、昨年４月に市内を会場に行われた「第８回世界盆栽大会１ｎさいたま」の公式ホームページ（ＨＰ）だったアドレスの内容が、アダルトサイトに変更されていることが判明したと発表した。アドレスをブックマーク（登録）などしている人に削除を呼び掛けている。

市観光国際課によると、大会公式ＨＰはこれまで、日本盆栽協会が管理しており、昨年の世界大会の日程やプログラム、デモンストレーター（実演者）らの内容が掲載されていた。

変更は３１日午後３時ごろ、市民からの指摘で分かった。ＨＰの内容がいつから変更されているかは、分かっていないという。同課は「サイトの管理者と連絡が取れておらず、詳細を調査中」としている。

●Facebookアカウント81,000件以上の情報盗難、販売か…個人的メッセージなど

https://japan.cnet.com/article/35128078/

このニュースをザックリ言うと・・・

- 11月2日（現地時間）、英BBCより、Facebookアカウントから少なくとも81,000件の個人的なメッセージがハッカーによって売りに出されていると報じられました。

- 被害を受けたアカウントは多くがウクライナとロシア、その他に米･英･ブラジルのものも含まれるとされています。

- ハッカーは1億2,000万件分のアカウントから情報を取得し、1アカウントにつき10セントで情報を売るとしていますが、3月に発覚した約5,000万人分の流出（AUS便り 2018/04/02号参照）や、9月に発表された約3,000万人分の流出（同 2018/10/22号参照）とは関連がないと述べたとのことです。

AUS便りからの所感等

- Facebookでは、悪質なブラウザの拡張機能によってアカウント情報が収集された疑いがあるとし、ブラウザ開発元に情報の共有を依頼するとともに、完全に信頼できる拡張以外は全て削除するようユーザに呼び掛けています。

- Facebookからの情報流出については、この他に10月にも、25万人以上のユーザの携帯電話番号やメッセージのやりとりがネット上で発見されています。(※)

- こと今年に入り度重なって発覚する情報流出に対し、他のSNSへの移行やそれを奨める記事も散見され、SNSとの付き合い方について各ユーザが改めて慎重になることが求められるでしょう。


cnet Japan

Facebookアカウント8.1万件の情報盗難、販売か--個人的メッセージなど

SEAN KEANE（CNET News）　翻訳校正：編集部　2018年11月05日 08時27分

Facebookアカウントから、少なくとも8万1000件の個人的なメッセージが、ハッカーによって売りに出されていると報じられている。

BBCは英国時間11月2日、被害に遭ったアカウントの多くがウクライナとロシアのFacebookユーザーのものだが、米国、英国、ブラジルなどの国のユーザーのものも一部含まれていると報じた。

ハッカーは、1億2000万件のアカウントからの情報を取得したと主張しており、1アカウントにつき10セントで売るとしているという。

Facebookがこれほど大規模な情報流出を認識していなかったとは考えにくいとBBCは指摘している。しかしBBCは、8万1000件を超えるアカウントが個人的メッセージを含むサンプルとして公開されており、ロシア人ユーザー5人が、その中に自分のメッセージがあったと証言したことを確認している。データが公開されたサイトの1つは、サンクトペテルブルクで設定されたようだとBBCは述べている。

アカウントを売りに出したハッカーはBBCに対し、今回のハッキングデータは、Cambridge Analytica関連のスキャンダルや、Facebookが9月に報告した情報流出とは関連がないと述べたという。

(※) http://www.tokyo-np.co.jp/article/economics/list/201810/CK2018100702000120.html