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。

●総務省、脆弱なIoT機器のセキュリティ対策を促す「NOTICE」を開始

https://japan.zdnet.com/article/35132132/
https://news.mynavi.jp/article/20190201-765783/

このニュースをザックリ言うと・・・

- 2月1日（日本時間）、総務省と情報通信研究機構（NICT）より、インターネットに接続されている脆弱なIoT機器（ルータ、Webカメラ、センサー等）を調査し、ユーザにセキュリティ対策を促すためのプロジェクト「NOTICE(National Operation Towards IoT Clean Environment)」を2月20日に開始すると発表されました。

- NICTの業務としてパスワード設定等に不備のあるIoT機器の調査等を追加する法改正が昨年11月に施行され、同月から今年1月にかけてTelnet・SSHおよびHTTPポートが開いていないか等の調査が行われており（AUS便り 2018/11/12号参照）、NOTICEはこれに続いて行われるものとなります。

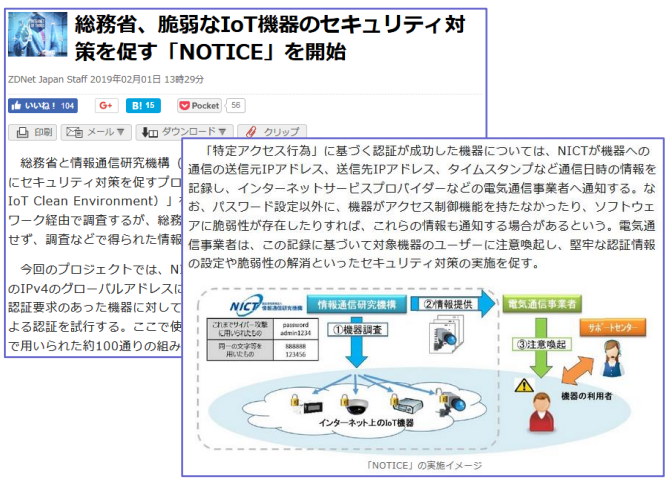
- NOTICEでは、国内のIPアドレス上のIoT機器に対し、攻撃者に容易に推測される可能性の高い100種類のパスワードを用いて管理画面等にログイン可能か（あるいはパスワードなしで入れるか）を調査し、問題のある機器の利用者に対してはそのIPアドレスを所有するプロバイダを介して注意喚起を行うとしています。

AUS便りからの所感等

- 1月下旬に当調査の実施についてメディアで報道されて以降、「政府が公然と不正アクセスを行う」「通信の秘密が侵害される」などといった批判がネット上では目立ちましたが、NOTICE専用WebサイトのFAQでは、当調査の実施業務は前述の法改正によって不正アクセス禁止法の対象から除外されているとしており、また機器と利用者との間の通信内容等を漏洩させる類のものではないこと等から、通信の秘密を侵害するものではないとしています。

- 「NOTICEによるアクセスに備えて」というのではなく、インターネットに接続されているあらゆる機器は常時どこからかの不正アクセスの脅威にさらされているものと認識し、「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」「第三者が不正に管理画面等に入れないよう強力なパスワードを設定する」といったセキュリティ設定の実施を行うことが肝要です。

ZDNet Japan



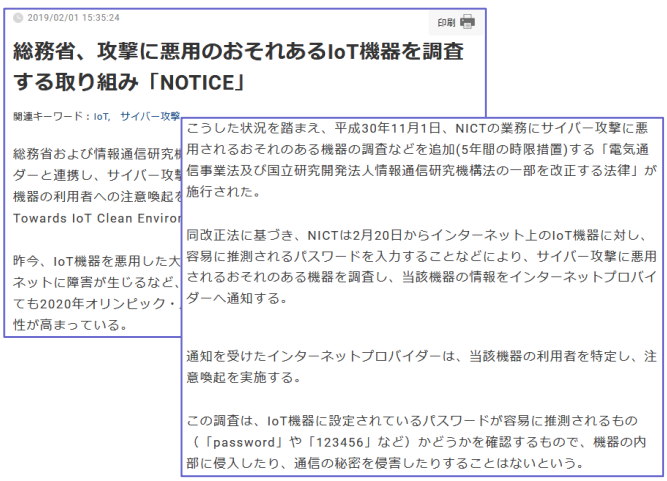
総務省、脆弱なIoT機器のセキュリティ対策を促す「NOTICE」を開始

ZDNet Japan Staff 2019年02月01日 13時29分

「特定アクセス行為」に基づく認証が成功した機器については、NICTが機器への通信の送信元IPアドレス、送信先IPアドレス、タイムスタンプなど通信日時の情報を記録し、インターネットサービスプロバイダーなどの電気通信事業者へ通知する。なお、パスワード設定以外に、機器がアクセス制御機能を持たなかったり、ソフトウェアに脆弱性が存在したりすれば、これらの情報も通知する場合があるという。電気通信事業者は、この記録に基づいて対象機器のユーザーに注意喚起し、堅牢な認証情報の設定や脆弱性の解消といったセキュリティ対策の実施を促す。

「NOTICE」の実施イメージ

マイナビニュース



2019/02/01 15:35:24

総務省、攻撃に悪用のおそれあるIoT機器を調査する取り組み「NOTICE」

関連キーワード：IoT、サイバー攻撃

総務省および情報通信研究機構（NICT）は2月1日、NICTの業務にサイバー攻撃に悪用されるおそれのある機器の調査などを追加(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」が施行された。

同改正法に基づき、NICTは2月20日からインターネット上のIoT機器に対し、容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報をインターネットプロバイダーへ通知する。

通知を受けたインターネットプロバイダーは、当該機器の利用者を特定し、注意喚起を実施する。

この調査は、IoT機器に設定されているパスワードが容易に推測されるもの（「password」や「123456」など）かどうかを確認するもので、機器の内部に侵入したり、通信の秘密を侵害したりすることはないという。

●偽セキュリティ警告画面を表示…メディア再生ソフト「GOMPlayer」で不審な広告の報告相次ぐ

https://togetter.com/li/1315178

このニュースをザックリ言うと･･･

- 1月31日（日本時間）頃、メディア再生ソフト「GOMPlayer」のユーザにより、ソフトのアップデート後に不審な広告が表示されるようになったとの報告がTwitter上等で相次いでいます。

- 報告によれば、ソフト終了時に大音量のビープ音とともに「Windowsセキュリティシステムが破損してます」等というポップアップが表示され、「更新」ボタンをクリックすると不正なファイルがダウンロードされるというものです。

- 通称「Win Erx03」等と呼ばれるこの偽警告画面は、実際には役に立たない偽セキュリティソフトウェア等をインストールするよう誘導する、いわゆる「スケアウェア」の一種です。

AUS便りからの所感等

- スケアウェアによってダウンロードされるソフトを一旦インストールしてしまうと、ブラウザ上で表示される広告が書き換えられる等のさらなる被害が発生する恐れがあります。

- ソフト終了時にブラウザが広告ページを開く形をとっており、ブラウザや拡張、アンチウイルスやUTMによる広告ブロック機能により遮断できる場面もある他、ポップアップ上の「更新」や「閉じる」ボタンをクリックせずにブラウザを強制終了させる等の回避策も有効とされます。

- 偽警告画面を表示するスケアウェアの手口は決して新しいものではありませんが、それでも今までにない種類のものが発生する可能性は常に考えられるため、ネット上での注意喚起情報の収集により、いざこういったものに直面しても慌てずに行動できるよう備えておくことが大切でしょう。

●福岡県警でランサムウェア感染か…CD-Rから侵入の可能性

https://tech.nikkeibp.co.jp/atcl/nxt/news/18/04092/

このニュースをザックリ言うと･･･

- 2月7日（日本時間）、福岡県警察本部より、ランサムウェアとみられるマルウェアの感染が発生し、一部業務に支障が出ていたことが発表されました。

- 発表によれば、2月5日に県警本部職員がCD-R上のファイルをノートPCにコピーしたところ、そのファイルにマルウェアが紛れていたとされており、PCをイントラネットに接続したところ、県警のサーバ上のファイルが暗号化されたとのことです。

- 現在、捜査情報や個人情報の流出は確認されていないとのことです。

AUS便りからの所感等

- 県警担当者によれば「ウイルスのチェックシステムがあるが、すり抜けてしまった」とのことですが、特にランサムウェアはアンチウイルスで検知されにくいケースが一時は多く確認されていました。

- WindowsにはCD-ROM等の指定されたファイルを自動的に実行する機能があり、これを悪用して不正なプログラムが実行された可能性も考えられますので、このような機能は可能な限り無効に設定するのが良いでしょう。
（ただしUSBメモリ等がマルウェアに感染していた場合にはこれを回避できないことも考えられ、別途注意が必要です。）