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。

●IoT機器セキュリティ調査「NOTICE」2019年度に2,249端末に注意喚起

https://cybersecurity-jp.com/news/36531
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00067.html

このニュースをザックリ言うと・・・

- 5月15日、総務省や情報通信研究機構(NICT)等によるプロジェクト「NOTICE」より、2019年度の「脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況」が発表されました。

- NOTICEでは、プロジェクトに参加したISP 50社が管理する約1.1億IPアドレスに対して調査を実施、うち管理画面等ID・パスワードが入力可能だったのは約100,000件で、さらに特定のID・パスワードでのログインが可能であった延べ2,249件に対し、ISPを通じて端末の所有者に注意喚起を実施したとしています。

- 注意喚起に対し利用者が対策を行っている一方で、新規に特定されるIoT機器も発生していることから、月あたりの注意喚起件数は300件程度で推移しているとのことです。

AUS便りからの所感等

- NOTICEが2019年初頭に開始された後、同年夏に調査プログラムの大幅な改良等により、月あたりの注意喚起件数が増加したとのことで、今後も同様の見直しや、さらなるISPの参加により、調査対象となる国内IPアドレスの網羅と、問題のある機器の検知が増えていくことが考えられます。

- 管理画面に外部からアクセス可能な状態であったり、パスワードを初期状態から変更していなかったりする機器は、遅かれ早かれ攻撃者に目をつけられ、侵入やマルウェア感染を引き起こされるものと心得た上で、NOTICEから注意喚起を受ける前に設定の点検を行い、最低でもパスワードは推測できないものに変更し、可能な限り社内の限定されたアクセス元からのみ管理画面にアクセス可能な設定とすることが重要です。

総務省 MIC Ministry of Internal Affairs and Communications

脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況（2019年度）

近年、IoT機器※1を悪用したサイバー攻撃が増加していることから、利用者自身が適切なセキュリティ対策を講じることが必要です。
総務省、国立研究開発法人情報通信研究機構（NICT）及び一般社団法人ICT-ISACは、インターネット・サービス・プロバイダ（ISP）と連携し、脆弱なID・パスワード設定等のためサイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」並びにNICTのNICTERプロジェクト※2によりマルウェアに感染していることが検知された機器の利用者への注意喚起を行う取組を実施しています。
今般、2019年度の実施状況を取りまとめましたので公表します。

1 経緯等

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や社会経済活動確保の観点から重要な課題となっています。
IoT機器が普及する一方で、IoT機器を狙ったサイバー攻撃は近年増加傾向にあります。センサーやウェブカメラなどのIoT機器は、機器の性能が限定されている、管理が行き届きにくい、ライフサイクルが長いなど、サイバー攻撃に狙われやすい特徴を持っています。セキュリティ対策に不備があるIoT機器は、マルウェアに感染しサイバー攻撃に悪用されるおそれがあります。諸外国においては、IoT機器を悪用した大規模なサイバー攻撃（DDoS攻撃）によりインターネットに障害が生じるなど、深刻な被害が発生していることから、我が国においても2020年東京オリンピック・パラリンピック競技大会などを控え、対策の必要性が高まっています。
このような状況を踏まえ、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等を追加（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2018年11月1日（木）に施行されました。

●フィッシングでメールアカウントを騙し取られ、さらなるフィッシングメール1,220件送信に悪用される

https://www.itmedia.co.jp/news/articles/2005/15/news103.html
https://www.mouse-jp.co.jp/news/news_2020_0513_01.html

このニュースをザックリ言うと･･･

- 5月15日(日本時間)、パソコン製造販売等を行うマウスコンピューター社より、同社社員のメールアカウントが外部への更なるフィッシングメールの送信に悪用されたと発表されました。

- 発表によれば、5月8日に同社宛に送られたフィッシングメールから、社員が偽サイトに誘導されてメールアカウントのID・パスワードを詐取され、のち同12日に当該アカウントからフィッシングメール1,220件が送信されていたことが受信者からの通報で発覚したとのことです。

- 同社ではメールアカウントのパスワード変更を行い、フィッシングメールの送信先となった同社の取引先法人に対し、メールの削除および偽サイトにアクセスしないよう呼びかけたとしています。

AUS便りからの所感

- メールアカウントの奪取は、内外への不正なメール送信だけでなく、メールボックスに保存されているメールの読み取りにも繋がり得ることに注意が必要です(今回についても発表では明言されていないものの、フィッシングメールが同社の取引先に対して送信されたことから、既存のメールあるいはアドレス帳のメールアドレスが読み取られた可能性があります)。

- Webサービス等において、フィッシングによるアカウント奪取への対策として二段階認証(ないし多要素認証)が有効となるケースもありますが、古くから使われているPOPやIMAPのアカウントに対してそういった認証を設定することは容易ではなく、それに対応する「G Suite」等への移行は、移行コストや移行で得られるその他の利点なども鑑みつつ慎重に検討すべきでしょう。

ITmedia NEWS

マウスコンピューター、不正アクセス被害でフィッシングメール1220件送信　偽サイトでメール情報盗まれ

2020年05月15日 15時45分 公開　[谷井将人，ITmedia]

印刷　見る　Share　B!　7

マウスコンピューターは5月15日、同社社員のメールアドレスから1220件のフィッシングメールが取引先の企業に向けて送信されたとして謝罪した。社員が閲覧した偽サイトでメールのIDとパスワードを盗まれ、メールアカウントに不正アクセスされたことが原因としている。

●DNSサーバー「BIND」にDoS攻撃の脆弱性2件、うち1件は他のサーバーソフトにも影響

https://news.mynavi.jp/article/20200522-1040159/
https://www.jpcert.or.jp/at/2020/at200023.html

このニュースをザックリ言うと･･･

- 5月20日(現地時間)、DNSサーバー「BIND」の開発元の米ISCより、BINDに2件の脆弱性が発見されたとして、修正バージョン(9.16.3/9.14.12/9.11.19)がリリースされました。

- 脆弱性は、キャッシュ用DNSサーバーをDoS攻撃の踏み台にする等が可能となるもの(CVE-2020-8616)と、BINDを不正にダウンさせられるもの(CVE-2020-8617)が報告されており、JPCERT/CC等からも脆弱性についての注意喚起が出され、速やかなアップデートが推奨されています。

- 前者の脆弱性については、他のDNSサーバーソフトにも同様の問題が存在し、相次いでアップデートがリリースされています(https://jprs.jp/tech/)。

AUS便りからの所感

- BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあり、ISCやLinuxディストリビューションからのアップデートがリリースされ次第、即座に適用できる体制を整えておくべきです。

- BINDの代替となる、よりセキュアと評価されるソフトウェア(Unbound等)も多く開発されており、管理コスト削減等のためそれらを利用するケースもよく見られますが、前述のとおりそれらについても同様の脆弱性が報告されており、どのソフトウェアを選ぶにしてもセキュリティアップデートの適用は不可欠です。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

ISC BIND 9 の脆弱性 (CVE-2020-8616, CVE-2020-8617) に関する注意喚起

最終更新: 2020-05-21

ツイート　メール

JPCERT-AT-2020-0023
JPCERT/CC
2020-05-21

I. 概要

ISC BIND 9 には、複数の脆弱性 (CVE-2020-8616, CVE-2020-8617) があります。脆弱性 CVE-2020-8616 は、DNSの名前解決の動作に起因しており、リモートからの攻撃によって、フルリゾルバを DNS リフレクション攻撃に利用されたり、フルリゾルバのパフォーマンスを低下させられる恐れがあります。脆弱性 CVE-2020-8617 は、TSIG リソースレコードを含むメッセージの有効性のチェックの不具合に起因しており、特別に細工されたメッセージを受け取った場合に named の異常終了や、異常な動作が発生する可能性があります。 BIND 9では TSIG のローカルセッション鍵がデフォルトで設定されるため、TSIG を利用する設定をしていない場合も、対象となります。