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。

●2018年のサイバー攻撃関連通信は前年比で約1.4倍の増加…NICTが「NICTER観測レポート2018」を公開

https://news.mynavi.jp/article/20190212-770515/
https://enterprisezine.jp/article/detail/11688

このニュースをザックリ言うと・・・

- 2月6日（日本時間）、情報通信研究機構（NICT）サイバーセキュリティ研究所より、2018年のサイバー攻撃関連通信の観測分析結果が「NICTER観測レポート2018」として公開されました。

- 同研究所によって2018年に観測されたサイバー攻撃関連のパケットは約2,121億個と、前年（約1,504億個）の約1.4倍に増加しています。

- 宛先ポート別では、Telnetサービスで用いられるTCPポート23番宛の割合が21.7%（前年：38.5%）と減少、代わりにIoT機器の管理等で用いられる80・81・2323・8080・52869番宛の割合が増加しており、汎用的なサービスから特定機器のみで動作するサービスや脆弱性を狙った攻撃へのシフトがうかがえると分析しています。

- 一方でWannaCryによるとみられる445番ポート宛の攻撃パケットも依然多く確認されているとしています。

AUS便りからの所感等

- この他、国内で観測された特徴的なIoT機器の脆弱性を狙った事例として、ルータやネットワークビデオレコーダ、およびデバッグ機能が有効になっているAndroid機器に関するものが挙げられています。

- NICTでは昨年末より、IoT機器やルータに対する特定のポートのスキャン（AUS便り2018/11/12号参照）や、管理画面等に簡単にログイン可能でないか等を調査する取り組み（同2019/02/12号参照）を行っていますが、上記のような特殊なポートを網羅しているとは限らず、また他の脆弱性の有無を調査するまで踏み込むものではありません。

- まずは社内に設置されているネットワーク機器やIoT機器、特にインターネットに直接接続している機器の存在を全て把握し、外部から意図していないポートにアクセスされないかの確認と対策をとること、そしてベンダーから等の脆弱性情報に注視し、ファームウェア等のアップデートを確実に行う体制を整えることを推奨致します。


マイナビニュース

2019/02/12 13:29:34 印刷

スキャン対象ポートに変化傾向 - NICT、2018の年サイバー攻撃関連通信観測レポート

長岡弥太郎

関連キーワード：IoTセキュリティ， 脆弱性， サイバー攻撃

NICT(国立研究開発法人情報通信研究機構/National Institute of Information and Communications Technology)は、2018年のサーバー攻撃関連通信の観測分析「NICTER観測レポート2018」を2月6日に公開している。

レポートは、NICTサイバーセキュリティ研究所が2005年から行う大規模サイバー攻撃観測網(NICTERダークネット観測網)を用いて、サイバー攻撃関連のパケットを分析、年次で発表しているものだ。2018年1月1日から12月31日までの約2,121億パケットを観測している。2017年の約1504億パケットから大きく増加しているが、これは主に海外組織からの何らかの調査目的によるスキャンの増加が主な原因と仮定。攻撃傾向分析にはノイズになるこれらのスキャン活動を一定のルール(1つのIPアドレスからのスキャンパケットにおいて、宛先ポート番号のユニーク数が30以上、且つ総パケット数が30万パケット以上)で除外し、パケットを分析している。


EnterpriseZine
データテクノロジー／情報セキュリティ ITリーダー向け専門メディア

2018年のサイバー攻撃関連通信は前年比で約1.4倍の増加
——NICTが「NICTER観測レポート2018」を公開

サイバー攻撃 調査・レポート 情報通信研究機構

18 9 G+ B! 0 プッシュ通知

EnterpriseZine編集部[著] 2019/02/06 15:45

情報通信研究機構（NICT）のNICTサイバーセキュリティ研究所は、「NICTER観測レポート2018」を公開した。このレポートは、NICTERプロジェクトで実施しているダークネット観測および各種ハニーポットで捉えた2018年のサイバー攻撃の状況についてまとめたもの。

EnterpriseZine

NICTERプロジェクトの大規模サイバー攻撃観測網で2018年に観測されたサイバー攻撃関連通信は、2017年と比べて約1.4倍と昨年以上の増加傾向にある。内訳としては、海外組織からの調査目的と見られるスキャンの増加が著しく、総観測パケット数の35%を占めた。

IoT機器を狙った通信では、2017年に4割近くを占めていたTelnet（23/TCP）を狙う攻撃が減少する一方、IoT機器に固有の脆弱性を狙う攻撃が増加し、攻撃対象や攻撃手法が細分化している様子が観測されている。

●「【重要】三井住友カード緊急のご連絡」受信者の氏名入りフィッシングメールに注意

https://www.itmedia.co.jp/news/articles/1902/20/news077.html

このニュースをザックリ言うと･･･

- 2月18日（日本時間）、三井住友カードより、同社をかたるフィッシングメールが出回っているとして警告が出されています（同19日にはフィッシング対策協議会からも同様の警告が出ています）。

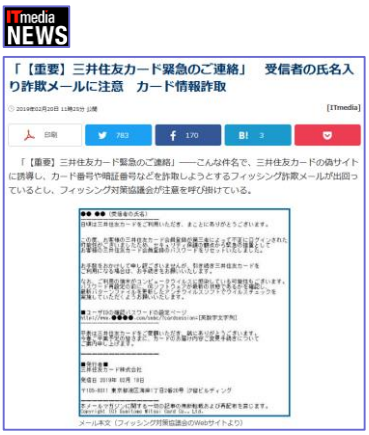
- フィッシングメールは、件名が「【重要】三井住友カード緊急のご連絡」、本文には受信者の氏名とともに「お客様の三井住友カード会員登録のパスワードをリセットいたしました。」等と記載、リンク先はカード番号・有効期限・セキュリティコード・暗証番号等の入力を促す偽のフォームが表示されるサイトとなっています。

- 同社等では、このようなフィッシングサイトにて、前述したクレジットカード情報等を絶対に入力しないよう警告しています。

AUS便りからの所感等

- 本物の三井住友カードのサイトは「https://」で始まり、EV-SSLによる証明書（「Sumitomo Mitsui Card Company, Limited」と表示）も使用されていることから、今回のケースについてその情報を把握していればフィッシングか否かの判断は可能です。

- ただし、EV-SSL証明書を用いているWebサイトであっても、そこに表示される組織名から名の知れたサービス名や運営元をイメージしづらいケースも起こり得るため、普段からのフィッシングサイトに対する防御として、メーラー・ブラウザ・セキュリティソフトおよびUTMのアンチスパム機能・アンチフィッシング機能を必ず有効にすることと、普段利用しているWebサイトは事前に登録したブラウザのブックマークからアクセスするよう心がけることを強く推奨致します。


ITmedia NEWS
「【重要】三井住友カード緊急のご連絡」　受信者の氏名入り詐欺メールに注意　カード情報詐取

●Google Playに不正な動画広告アプリ、月間10Gバイトのデータ消費も

https://www.itmedia.co.jp/news/articles/1902/22/news071.html

このニュースをザックリ言うと･･･

- 2月20日（現地時間）、米Oracle社より、Googleの公式アプリストア「Google Play」で提供されていた人気アプリに仕込まれた不正なコードによる詐欺の手口が見つかったと発表されました。

- 「DrainerBot」と名付けられたこの手口では、裏で動画広告をダウンロードさせ、アプリの画面に表示されず、ユーザの目には見えない形で動画を再生することにより、広告料金をだまし取っていたとされています。

- 一方で勝手に動画を再生させられたモバイル機器では、月間10Gバイトもの通信が発生し、通信量超過料金を支払わされていた可能性もあるとされています。

- DrainerBotのコードが見つかったアプリはゲームやメイクアップ関係等複数存在し、ダウンロードされた回数は合計で1,000万回を超えていたとされますが、殆どは既にGoogle Playから削除されているとのことです。

AUS便りからの所感等

- DrainerBotのコードが仕込まれたSDK（ソフトウェア開発キット）はオランダのソフトウェア企業が提供したものとされていますが、同企業では詐欺行為を行った疑惑を否定し、調査を行うとしており、SDKの開発の過程で攻撃者に侵入され、マルウェアが仕込まれた可能性が考えられます。

- とにかくあらゆるアプリについて、インストール時のみならず、以後もアップデートにより不正なコードが仕込まれる恐れもあることに注意し、SNSをはじめとするネット上の情報・評判を調査した上でインストール・アンインストールを行うことが重要です。


ITmedia NEWS
Google Playに不正な動画広告アプリ、月間10Gバイトのデータ消費も
Oracle Exposes "DrainerBot" Mobile Ad Fraud Operation