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。

●国立感染症研究所のサーバーを踏み台にネット掲示板で不正な書き込み行われる

https://internet.watch.impress.co.jp/docs/news/1239062.html
https://xtech.nikkei.com/atcl/nxt/news/18/07230/
https://www.niid.go.jp/niid/ja/maintenance/9454-incidence200301.html

このニュースをザックリ言うと・・・

- 3月4日(日本時間)、国立感染症研究所より、同所のサーバーを踏み台にしてインターネット上の掲示板に不正な書き込みが行われたと発表されました。

- 発表によれば、書き込みは同2日0時39分頃に行われ、アクセス元として同所の旧ドメイン名(nih.go.jp)下のプロキシーサーバーが表示されていた模様です。

- 掲示板利用者からの連絡を受けて当該プロキシーサーバーを調査したところ、同研で使われていた古い公式Webサーバー(以下、旧Webサーバー)上に不審なプログラムが作成され、そこからプロキシーサーバーを経由しての掲示板へのアクセスが確認されたとしています。

AUS便りからの所感等

- 旧Webサーバーは公式Webサイトに利用されなくなった後も同所員が利用可能なファイルサーバーとして運用されていましたが、古いWebアプリケーションに脆弱性が存在し、これを悪用して不審なプログラムがアップロードされた可能性がある一方、幸いにも外部への掲示板への書き込み以外、内部サーバー等へのアクセスは確認されなかったとのことです。

- 従来の用途を終えた古いサーバーについては可能な限り撤去する、もしくは、不正アクセスの入口となり得る脆弱性を持ったプログラムを除去するとともに、さらなる踏み台にされないための出口対策として、各サーバー自身やルーターの設定、あるいはUTMの設置によるアウトバウンドアクセスの遮断・制限を行うことを強く推奨致します。

NIID 国立感染症研究所
NATIONAL INSTITUTE OF INFECTIOUS DISEASES

国立感染症研究所のドメインから一部の掲示板サイトへの不正な書き込みがあった事案について

印刷

PUBLISHED: 2020年3月04日

令和2年3月2日(月)に発生した、国立感染症研究所(以下感染研)のドメインから一部の掲示板に発出された不正な書き込みについて、報告いたします。

1．不正アクセスの概要

発生日時: 3月2日(月)0時39分頃

被害内容: 2012年まで利用されていた感染研の旧公式サーバ "www0.nih.go.jp" から、プロキシサーバ経由であるプライベートな掲示板に1件の書き込みがありました。

発見経緯: 書掲示板の利用者から感染研公式窓口(info@nih.go.jp)に連絡がありました。その後ただちに、プロキシサーバを調べ、当該掲示板に対するwww0からのアクセスを確認しました。

改竄されたサイト: 過去に設置したままであったアプリケーション直下のディレクトリに形跡を発見しました。プロキシサーバのログを解析し、当該掲示板へのアクセス履歴と、同時刻のwww0のwebサーバ利用履歴を照合した結果、上記のアプリケーションに通常存在しないプログラムが起動されている証跡を発見しました。

● JR東日本「えきねっと」で3,729人に不正ログイン、海外からアプリ経由で

https://xtech.nikkei.com/atcl/nxt/news/18/07231/

このニュースをザックリ言うと・・・

- 3月3日(日本時間)、JR東日本より、同社のネット予約サービス「えきねっと」において外部からの不正ログインが発生した可能性があると発表されました。

- 不正ログインは同2日午後5時30分～3日午後0時37分に発生し、3,729人分のユーザーアカウントがログインされ、うち13人分について、氏名・住所・電話番号・生年月日・メールアドレス・クレジットカード情報の一部(カード番号の下4桁・有効期限・ブランド名)および連携している交通系ICカードの番号を閲覧された可能性があるとしています。

- 同社では3,729人分のアカウントについてパスワードを強制的に変更して通知したとのことです。

AUS便りからの所感

- 不正ログインは海外の特定IPアドレスからスマホアプリ「えきねっとアプリ」で行われ、通常では考えられない多数のログイン試行があったとのことです。

- 当該サイトに不審なログイン試行を遮断する仕組みがあったのか、いわゆる「リスト型攻撃」だったのかは不明ですが、いずれにしろ当該サイトで不正ログインを受けた場合は攻撃者にパスワードを知られているものと考え、他のサイトも含めそのパスワードを使わないようにするのが、連鎖的な不正ログインを防ぐ為に不可欠です。

日経 XTECH

JR東日本「えきねっと」で3729人に不正ログイン、海外からアプリ経由で

清嶋 直樹　日経クロステック／日経コンピュータ

2020.03.05

PR

JR東日本は2020年3月3日、ネット予約サービス「えきねっと」が不正アクセスを受けたと発表した。不正にログインされた可能性がある3729人のアカウントについて同日夜にパスワードを強制リセットし、パスワードを変更しなければログインできないようにする措置を取った。

● TCPポート4567番に対する「Miraiボット」のアクセス増加、警察庁が注意喚起

https://internet.watch.impress.co.jp/docs/news/1237898.html
http://www.npa.go.jp/cyberpolice/important/2020/202002261.html

このニュースをザックリ言うと・・・

- 2月26日(日本時間)、警察庁より、IoTマルウェア「Mirai」の特徴を持つアクセスが増加したとして注意喚起が出されています。

- 同庁の定点観測によれば、昨年12月29日～2月2日において、TCPポート23番(Telnet)や80番・8080番(Web)へのパケットの他、4567番をターゲットとするパケットが15件/日・IPアドレスの頻度で観測されたとのことです。

- パケットの送信元を調査したところ、ネットワークカメラや海外製デジタルビデオレコーダーといったIoT機器のログイン画面が表示される状態となっており、またポート4567番への攻撃パケットは特定のビデオデジタルレコーダーの脆弱性を突いてID・パスワードを奪取する目的のものとされています。

AUS便りからの所感

- 発表された注意喚起では、他にもプリンターで使用される「PJL(Printer Job Language)」の探索を目的としたアクセスや、特定の入退室管理システムの脆弱性を狙ったアクセスについても言及されています。

- 管理画面等に不特定多数からアクセス可能な状態にあるIoT機器は「SHODAN」「Censys」といった専用のサーチエンジンに登録され、攻撃者に容易に存在を知られる可能性がありますので、第三者機関の診断や、時には前述のサーチエンジンを利用して機器の設定やポートフィルタリング状況をチェックし、UTMの設置等によるアクセス遮断を可能な限り行うこと、またファームウェアのアップデートを確実に行うことが重要です。

警察庁 National Police Agency @police

宛先ポート4567/TCP に対するMirai ボットの特徴を有するアクセスの増加等について

2020年2月26日
警察庁

- 宛先ポート4567/TCP に対するMirai ボットの特徴を有するアクセスの増加
- PJL(Printer Job Language)に対応した機器を標的としたアクセスの増加
- Linear eMerge E3-Series の脆弱性（CVE-2019-7256）を標的としたアクセスの増加