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。

●「note」投稿者のIPアドレスが外部から閲覧可能な状態に…対策済み

https://www.itmedia.co.jp/news/articles/2008/14/news088.html
https://note.jp/n/n3e6451c9b147
https://note.jp/n/naf3775e93a58

このニュースをザックリ言うと･･･

- 8月14日(日本時間)、note株式会社より、同社のコンテンツ配信サービス「note」において、記事投稿者のIPアドレス情報が閲覧可能な状態にあったと発表されました。
- noteの記事詳細ページのソースコードに、データベースに保持されていたIPアドレス情報が含まれる状態になっており、ソースコードを表示することにより、閲覧可能となっていたとのことです。
- 同社では同日6:14に問合せを受け問題を確認、サイト全体のアクセスを遮断し、データベースからIPアドレス情報を削除する等の修正を行い、11:56に対策を完了したとしています。

AUS便りからの所感等

- IPアドレス単体では必ずしも個人の識別に直結する情報とはなり得ませんが、その他の情報(記事が投稿された日時等)との照合により、それぞれの投稿者が同一である(あるいは同じ組織に属する)可能性は高いということを示すことになります。
- 近年はv6プラス等の登場により、無関係のユーザー同士で同一のIPv4アドレスを共有するケースもあるため、実際に同一人物かの確認には、さらなる情報との照合が必要な場合があります。
- いずれにせよ、Webサイトの提供・開発者側にとっては、IPアドレスをはじめとする個人情報に繋がり得るセンシティブな情報について、「不必要に取得しない」「場合によっては削除する」そして「(プログラムのデバッグ情報等から)不必要に出力されないようにする」ことに十分注意を払うべきでしょう(今回のように、通常ブラウザーに表示されないコメント・スクリプト部分は見過ごされがちです)。

ITmedia NEWS

noteユーザーのIPアドレスが漏えい、運営会社が謝罪　有名人のIPアドレスと一致する5ちゃんねる投稿が検索される事態に

2020年08月14日 13時58分 公開　[井上輝一，ITmedia]

印刷　見る　Share　B! 248

コンテンツ配信サービス「note」を運営するnote社は8月14日、記事投稿者のIPアドレスが第三者から確認できてしまう不具合があったとして謝罪した。漏えいした有名人のIPアドレスを、他サービスでの投稿に見られるIPアドレスと比較する者も現れている。

【お詫び】IPアドレスが他者からも確認できてしまう不具合について

♡ 14

note株式会社
2020/08/14 13:10

noteサービスにおいて、記事投稿者のIPアドレスが記事詳細ページのソースコードから確認できてしまう不具合が存在していました。

なお、一般的なIPアドレスから、個人情報を特定することはできません。

現在は、該当部分を修正し問題なくご利用いただける状態です。ご迷惑をおかけして、大変申し訳ありませんでした。

note社の発表文（一部）

●複数のISPを騙る当選詐欺に注意喚起

https://k-tai.watch.impress.co.jp/docs/news/1271174.html
https://support.mineo.jp/news/1013/
https://togetter.com/li/1578074

このニュースをザックリ言うと・・・

- 8月17日(日本時間)、光回線サービス「eo」やMVNOサービス「mineo」等を提供するオプテージ社より、同社を騙る当選詐欺の事例が確認されているとして注意喚起が出されています。

- 注意喚起によれば、ブラウザー上あるいはPC・スマートフォンの画面上に同社からの当選通知に見せかけた不審なポップアップが表示され、アンケートへの回答とともにクレジットカード情報を含む個人情報を入力させようとするWebサイトに誘導されるとのことで、同社とは一切無関係のメッセージであるとし、表示されたボタンをタップせず、個人情報欄には一切情報を入力しないよう呼び掛けています。

- Twitter上では他のISPを騙った同様の偽当選サイトも多数報告されています。

AUS便りからの所感

- 各ISPを騙る当選詐欺は、ポップアップが「○○○ユーザーの皆様、私たちは一周年記念日をお祝いしています」、またWebサイトは「○○○をご利用の皆様、おめでとうございます！」という見出しで始まり、「お客様がインターネットプロバイダーに○○○をお選びいただいたことに感謝の意を込めて」等と記載され、iPhoneやサムスン製スマートフォンを無料でプレゼントすると偽ってアンケートに回答させようとしている点で共通しています。

- 攻撃者が手口を変え、文言を変えていく可能性ももちろん十分に考えられますが、不審な文言についてサーチエンジンやSNSで検索し、同様の事案の報告がないか確認することは、フィッシング等の詐欺を回避するために有用です。

mineo 【A・D・S・AP・DP】弊社をかたる不審な当選サイトについて

●世界中のSSHサーバーをターゲットに感染するP2Pボットネット「FritzFrog」

https://www.ipa.go.jp/security/topics/alert20200803.html
https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/

このニュースをザックリ言うと・・・

- 8月19日(現地時間)、セキュリティ企業のGuardicore社より、SSH(セキュアシェル)サーバーをターゲットとした新種のボットネット「FritzFrog」について報告されています。

- FritzFrogは今年1月から確認されており、政府・教育・金融等の機関をターゲットとし、これまでに数千万のIPアドレスに攻撃を仕掛けており、欧米の有名大学や鉄道会社等の500台以上のサーバーに侵入成功している模様です。

- 感染したサーバー上でバックドアを設置する等の特徴を持っており、同社ではSSHサーバー上でFritzFrogに感染していないかを確認するためのスクリプトを提供しています。

AUS便りからの所感

- FritzFrogは、サーバー上にファイルを残さない、いわゆる「ファイルレス」のマルウェアである等の特徴を持ち、また明確な指令サーバーが存在せず、感染した各サーバーで管理を分散させるP2P型ボットネットを構成するとされており、その分完全にシャットダウンさせることが難しいとされています。

- SSHポート(TCPポート22番)が開いているサーバーにアクセスし、脆弱なパスワードを使用しているアカウントに不正ログインし、侵入するとみられますので、サーバーのユーザーアカウントに強固なパスワードを設定する、SSHからのログインを制限する(ログイン可能なユーザーの制限、パスワードでログインできないようにする等)、場合によってはサーバー自身あるいはUTMによるフィルタリングで不特定多数からSSHポートにアクセスできないようにする等も重要です。

GIGAZINE