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。

●太陽光発電施設の監視機器約800台が不正アクセス被害…不正送金の踏み台目的か

https://www.sankei.com/article/20240501-ZSOLVFVJZZL6BLQJR6S6SJ23GM/

このニュースをザックリ言うと･･･

- 5月1日(日本時間)、国内新聞各社より、国内各地の太陽光発電施設を遠隔監視する機器約800台が不正アクセスの被害を受けていたことが報じられました。
- 記事によれば、大阪市の電子機器メーカーが製造した監視機器に攻撃対策に対する欠陥があり、侵入によってバックドアを仕掛けられたとのことです。
- 不正アクセスには中国の攻撃者集団が関与の可能性があり、機器の一部がネットバンキングによる預金の不正送金に悪用されていたとしています。

AUS便りからの所感等

- 不正送金の際に身元を隠す目的、いわゆる「踏み台」のために乗っ取られたとされる他、発電施設に障害が起きる可能性もあったとされています。
- IoT機器への不正アクセス事案としては、2016年に発見された、機器に感染して大規模ボットネットを構築するマルウェア「Mirai」等も知られています。
- IoT機器が管理用途等で開いているポートに不特定多数からアクセス可能な状態となっていることはこのような攻撃者やマルウェアによる不正アクセスを招く恐れがあり、一方で管理者がいる組織内ネットワークを介して侵入される可能性も考慮、そして侵入の被害を受けた機器から外部への不正な通信を遮断するよう、UTM等を用いて機器を適切に隔離すること、また設置されている機器自体についてもファームウェアの更新など確実な管理を行うことが肝要です。

THE SANKEI NEWS

太陽光発電にサイバー攻撃　機器８００台を乗っ取り　身元隠し不正送金に悪用

2024/5/1 11:01

社会 | 事件・疑惑

太陽光パネル

各地の太陽光発電施設の遠隔監視機器、計約８００台がサイバー攻撃を受け、一部がインターネットバンキングによる預金の不正送金に悪用されていたことが１日、分かった。ハッカーはネット上の身元を隠すために機器を乗っ取ったとみられ、発電施設に障害が起きる恐れもあった。セキュリティー企業によると、中国のハッカー集団が関与した可能性がある。

●Mastercard・東京ガスを騙るフィッシングメール大量送信…対策協議会が注意喚起

https://www.antiphishing.jp/news/alert/mastercard_20240424.html
https://www.antiphishing.jp/news/alert/tokyogas_20240424.html
https://www.tokyo-gas.co.jp/news/notice/notice_01.html

このニュースをザックリ言うと･･･

- 4月24日(日本時間)、フィッシング対策協議会より、Mastercardおよび東京ガスを騙るフィッシングの報告を受けているとして注意喚起が出されています。

- Mastercardのフィッシングは、確認された件名として「【マスターカード 】カード年会費のお支払い方法に問題があります」「【緊急通知】マスターカードセキュリティ更新のお知らせ」「【ご注意】MasterCardカード不正使用疑惑のセキュリティチェック」「カードセキュリティの緊急アップデート：MasterCard カードの保護について」「MasterCardカード:不正使用疑惑のセキュリティチェック」が挙げられており、これ以外も使われている可能性があるとしています。

- 同じく東京ガスのフィッシングで確認された件名には「【東京ガス】ご請求料金確定のお知らせ」「【myTOKYOGAS】ご請求料金確定のお知らせ」が挙がっています。

- 同協議会では、これらのサイトで個人情報・電話番号・クレジットカード情報等を入力しないよう呼び掛けています。

AUS便りからの所感

- 上記のうち、特に件名「MasterCardカード:不正使用疑惑のセキュリティチェック」のフィッシングメールについて、筆者の手元では4月27日頃まで大量の受信を確認していました。

- 東京ガスからは、この他にも4月以降「料金の未払い案内の偽SMSや給湯器点検を装う訪問が急増」しているとの注意喚起が出されています。

- フィッシングメール・サイトからの自衛策として、これまでも度々言われていることですが、不審なメールが届いた場合には、同協議会等が発表する情報あるいはソーシャルネットワークでの報告がないか確認すること、利用しているサービスのサイトへは事前に登録したブラウザーのブックマーク等からアクセスするよう心掛けること等、慎重な行動をとることが推奨されます。

フィッシング対策協議会
Council of Anti-Phishing Japan


Mastercard をかたるフィッシング (2024/04/24)

ポスト
2024年04月24日

概要
Mastercard をかたるフィッシングの報告を受けています。

メールの件名
【マスターカード 】カード年会費のお支払い方法に問題があります
【緊急通知】マスターカードセキュリティ更新のお知らせ
【ご注意】MasterCardカード不正使用疑惑のセキュリティチェック
カードセキュリティの緊急アップデート：MasterCard カードの保護について
MasterCardカード:不正使用疑惑のセキュリティチェック

※上記以外の件名も使われている可能性があります。

メール・SMSの文面例

●4月はWordPressのプラグインに43件の脆弱性報告…Sucuri社発表

- https://blog.sucuri.net/2024/04/wordpress-vulnerability-patch-roundup-april-2024.html

このニュースをザックリ言うと･･･

- 4月29日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、WordPressプラグインにおいて4月に報告された43件の脆弱性のまとめ記事が発表されました。

- 最も危険度が高い「High」にあたるのは「Email Subscribes by Icegram Express」のSQLインジェクションおよび「User Registration」の権限昇格の2件となります。

- 危険度「Medium」「Low」についてはクロスサイトスクリプティング(XSS)が39件、他にもファイルの不正なアップロードとディレクトリトラバーサルが1件ずつ報告されています。

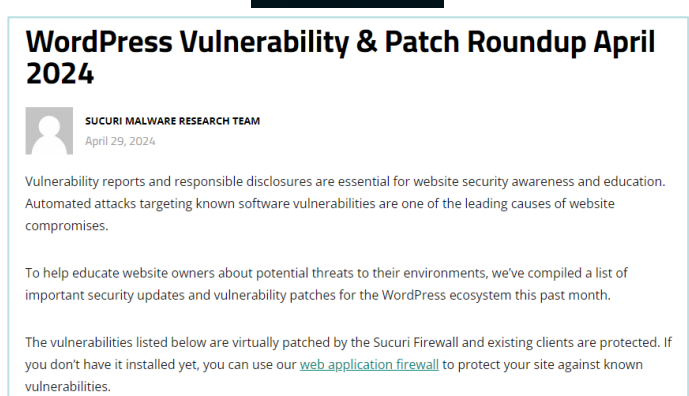
AUS便りからの所感

- Sucuri社が毎月行っているまとめでは、1～3月分でそれぞれ28件・29件・30件の報告でしたが、約1.5倍に増加しています。

- ディレクトリトラバーサルは一般に危険度が高い脆弱性ですが、攻撃を行うための条件が限定的なため、危険度「Low」と評価されたと思われます。

- WordPress本体においても4月にセキュリティアップデート6.5.2等がリリースされるなど、不定期に更新されることがあり、本体・プラグインともインストールした状態のままで放置するようなことは決してせず最新に保つよう努めること、加えてセキュリティを強化するプラグインを必ずインストールすること、併せて(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入も検討に値します。

SUCURI


WordPress Vulnerability & Patch Roundup April 2024

SUCURI MALWARE RESEARCH TEAM
April 29, 2024

Vulnerability reports and responsible disclosures are essential for website security awareness and education. Automated attacks targeting known software vulnerabilities are one of the leading causes of website compromises.

To help educate website owners about potential threats to their environments, we've compiled a list of important security updates and vulnerability patches for the WordPress ecosystem this past month.

The vulnerabilities listed below are virtually patched by the Sucuri Firewall and existing clients are protected. If you don't have it installed yet, you can use our web application firewall to protect your site against known vulnerabilities.